## CC600/CC6000 Customer Concierge





## Handbuch zur Integration für Android<sup>™</sup> 8.1.0 Oreo

## Copyright

ZEBRA und der stilisierte Zebrakopf sind in vielen Ländern eingetragene Marken von Zebra Technologies Corporation. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

©2019-2021 Zebra Technologies Corporation und/oder Tochterunternehmen. Alle Rechte vorbehalten. Google™, Android, Google Play™ und andere Marken sind Marken von Google LLC; Oreo ist eine Marke von Mondelez International, Inc. Alle anderen Marken sind das Eigentum ihrer jeweiligen Inhaber.

URHEBERRECHTE UND MARKEN: Ausführliche Informationen zu Urheberrecht und Marken finden Sie unter www.zebra.com/copyright.

GARANTIE: Vollständige Informationen zur Garantie finden Sie unter www.zebra.com/warranty.

LIZENZVEREINBARUNG FÜR DEN ENDBENUTZER: Ausführliche EULA-Informationen finden Sie unter www.zebra.com/eula.

### Nutzungsbedingungen

Urheberrechtshinweis

Diese Bedienungsanleitung enthält eigentumsrechtlich geschützte Informationen von Zebra Technologies Corporation und deren Tochterunternehmen ("Zebra Technologies"). Sie dient ausschließlich zur Information und zur Verwendung durch Parteien, die die hier beschriebene Ausrüstung verwenden und warten. Derartige urheberrechtlich geschützte Informationen dürfen ohne ausdrückliche schriftliche Genehmigung von Zebra Technologies weder verwendet, reproduziert noch an Dritte weitergegeben werden.

Produktverbesserungen

Die kontinuierliche Verbesserung von Produkten gehört zur Firmenpolitik von Zebra Technologies. Alle Spezifikationen und Designs können ohne vorherige Ankündigung geändert werden.

Haftungsausschluss

Zebra Technologies ergreift Maßnahmen, um sicherzustellen, dass die veröffentlichten technischen Vorgaben und Handbücher korrekt sind. Es können jedoch Fehler auftreten. Zebra Technologies behält sich das Recht zur Korrektur solcher Fehler vor und schließt jegliche Haftung für daraus entstandene Schäden aus.

Haftungsbeschränkung

In keinem Fall haftet Zebra Technologies oder eine Person, die an der Entwicklung, Produktion oder Lieferung des beiliegenden Produkts (einschließlich Hardware und Software) beteiligt war, für Schäden jeglicher Art (unter anderem für Folgeschäden wie entgangenem Gewinn, Geschäftsunterbrechung oder Verlust von Geschäftsinformationen), die aus der Verwendung, dem Ergebnis der Verwendung oder der Nichtverwendbarkeit des Produkts entstehen, selbst wenn Zebra Technologies von der Möglichkeit solcher Schäden unterrichtet wurde. Einige Rechtsgebiete lassen den Ausschluss oder die Beschränkung von Neben- oder Folgeschäden nicht zu, sodass die oben aufgeführten Ausschlüsse und Beschränkungen möglicherweise nicht für Sie gelten.

### Revisionsverlauf

Änderung	Datum	Beschreibung
-01 Rev. A	4/2019	Erste Veröffentlichung
-02 Rev. A	8/2020	Doppelte Bildschirmaufnahmen entfernt. Imager als Kamera entfernt. Näherungssensor in Abbildung 1 beschriftet. Abschnitte "Dokumentationssatz", "Unterstützte Decoder" und "Übertragen von Dateien mit einem Host-Computer über USB" aktualisiert.

Änderungen am ursprünglichen Handbuch sind unten aufgeführt:

## Inhaltsverzeichnis

Copyright	. 2
Nutzungsbedingungen	. 2
Revisionsverlauf	. 2

Informationen zu diesem Leitfaden	10
Einführung	10
Dokumentationssatz	10
Konfigurationen	11
Zubehör	12
Softwareversionen	12
Kapitelbeschreibungen	13
Schreibkonventionen	14
Kundendienstinformationen	14
Feedback zur Dokumentation	14

Erste Schritte	15
Einführung	15
Auspacken	15
Merkmale	16
Einrichtung	20
Installieren der microSD-Karte (optional)	21
Montieren des Geräts	21
Einrichten eines Google-Kontos	28
Zebra Visibility Services	28
Zurücksetzen des Geräts	28

Einstellungen	30
Einführung	30
WLAN-Konfiguration	30

Konfigurieren eines sicheren WLAN-Netzwerks	30
Manuelles Hinzufügen eines WLAN-Netzwerks	32
Konfigurieren für einen Proxyserver	33
Konfigurieren des Geräts für die Verwendung einer statischen IP-Adresse	34
WLAN-Einstellungen	35
Erweiterte WLAN-Einstellungen	36
Wi-Fi Direct	38
Einstellen der Bildschirmsperre	38
Einstellen der Bildschirmsperre mit PIN	39
Einrichten der Bildschirm-Entsperrfunktion mit Kennwort	40
Einrichten der Bildschirm-Entsperrfunktion mit Muster	41
Anzeigen von Kennwörtern	41
Konten	42
Sprachverwendung	42
Ändern der Spracheinstellung	42
Hinzufügen von Wörtern zum Wörterbuch	42
Tastatureinstellungen	42
Konfigurieren von PTT Express	43
RxLogger	43
Konfigurieren von RxLogger	43
RxLogger-Einstellungen	44
ANR-Modul	44
Kernel-Modul	44
Logcat-Modul	45
LTS-Modul	47
Ramoops-Modul	47
Ressourcenmodul	48
Snapshot-Wodul	48 40
Tombstone-Modul	49 49
Konfigurationsdatei	49
Aktivieren der Protokollierung	49
Deaktivieren der Protokollierung	49
Extrahieren von Protokolldateien	50
RxLogger-Dienstprogramm	50
App-Ansicht	50
Anzeigen von Protokollen	50
Backup	52
Archivieren von Daten	52
Overlay-Ansicht	52
Starten des Haupt-Chat-Heads	53
Entfernen des Haupt-Chat-Heads	53
Anzeigen von Protokollen	53

Entfernen eines Symbols für einen untergeordneten Chat-Head	54
Backup in der Overlay-Ansicht durchführen	54
Telefoninfo	. 54

USB/Ethernet-Kommunikation	56
Einführung	56
Übertragen von Dateien mit einem Host-Computer über USB	56
Übertragen von Dateien	56
Übertragen von Fotos	57
Trennen vom Host-Computer	57
USB/Ethernet-Kommunikation	58
Ethernet-Einstellungen	58
Konfigurieren der Ethernet-Proxyeinstellungen	58
Konfigurieren von statischen IP-Adressen für Ethernet	59
Herstellen der Ethernet-Verbindung	60

Codabar	. 74
UPC/EAN-Parameter	. 80
Lesegerät-Parameter	. 82
Scan-Parameter	. 86
UDI-Parameter	. 8/
Aktivierung bei Unterprechung beibenalten	. 8/ 97
	. 01
	. 89
Intent-Ausgabe	. 90
Uberblick über Intents	. 91
IP-Ausgabe	. 92
Verwendung	. 93
Verwenden der IP-Ausgabe mit IP/vedge	. 94
Verwenden der IP-Ausgabe ohne IPWedge	. 95
Erstellen von Regeln für die erweiterte Datenformatierungsregel	96
Konfigurieren des ADF-Plug-ins	. 96
Erstellen einer Regel	. 97
Definieren einer Regel	. 98
Definieren von Kriterien	. 98
	100
Loschen einer Regel	100
Softiefen der Regelliste	100
	102
DataWedge-Finstellungen	102
Importieren einer Konfigurationsdatei	106
Exportieren einer Konfigurationsdatei	106
Importieren einer Profildatei	107
Exportieren eines Profils	107
Wiederberstellen von DataWedge	107
Kenfigurations, und Profildateiverweltung	107
	100
	108
	108
Hinweise zur Programmierung	108
Erfassen von Daten und Aufnehmen von Fotos in derselben Anwendung	109
Deaktivieren von DataWedge auf dem Gerät und Verwenden der	
Massenbereitstellung	109
DataWedge-APIs	109
Berichterstellung	109
Soft-Scanauslöser	110
Funktionsprototyp	110
Scanner-Eingabe-Plug-in	110
Funktionsprototyp	110
Parameter	110

Rückgabewerte	. 110
Beispiel	. 111
Kommentare	. 111
Scanner auflisten	
Funktionsprototyp	. 112
Parameter	. 112
Rückgabewerte	. 112
Beispiel	. 113
Kommentare	. 113
Standardprofil festlegen	. 114
Standardprofile: Wiederholung	. 114
Nutzungsszenario	. 114
Funktionsprototyp	. 114
Parameter	. 114
Rückgabewerte	. 114
Beispiel	. 115
Kommentare	. 115
Standardprofil zurücksetzen	. 115
Funktionsprototyp	. 116
Parameter	. 116
Rückgabewerte	. 116
Beispiel	. 116
Kommentare	. 116
Zu Profil wechseln	. 117
Wiederholuna: Profile	. 117
Nutzungsszenario	. 117
Funktionsprototyp	. 117
Parameter	. 118
Rückgabewerte	. 118
Beispiel	. 118
Kommentare	. 119
Hinweise	. 119
	-

Anwendungsinstallation	120
Einführung	120
Sicherheit	120
Sichere Zertifikate	120
Installieren eines sicheren Zertifikats	120
Konfigurieren der Speichereinstellungen für Anmeldedaten	121
Entwicklungstools	122
Android	122
EMDK für Android	123
StageNow	123
ADB-Setup über USB	123

### Inhaltsverzeichnis

Aktivieren von USB-Debugging	124
Anwendungsinstallation	124
Installieren von Anwendungen über die USB-Verbindung	125
Installieren von Anwendungen mithilfe von Android Debug Bridge	126
Installieren von Anwendungen über eine microSD-Karte	127
Deinstallieren einer Anwendung	128
Durchführen einer Systemaktualisierung	129
Herunterladen des Systemaktualisierungspakets	129
Verwenden der microSD-Karte	129
Verwenden von ADB	130
Überprüfen der Systemaktualisierungsinstallation	131
Durchführen eines Enterprise-Reset	131
Herunterladen des Enterprise-Reset-Pakets	131
Verwenden der microSD-Karte	132
Verwenden von ADB	132
Zurücksetzen auf die Werkseinstellungen (Factory-Reset)	133
Herunterladen des Factory-Reset-Pakets	133
Verwenden der microSD-Karte	133
Verwenden von ADB	134
Speicher	135
Speicher mit direktem Zugriff (Random Access Memory, RAM)	135
Interner Speicher	135
Externer Speicher	137
Formatieren der microSD-Karte	138
Formatieren als internen Speicher	139
Enterprise-Ordner	140
Anwendungsverwaltung	140
Anzeigen von App-Details	141
Verwalten von Downloads	142

143
143
143
143
144
144
144
144
145
145
145
<b>1</b> 11 11 11 11 11

#### Inhaltsverzeichnis

Gehäuse	145
Display	145
Kamera und Scanfenster	145
Fehlerbehebung	146

Гесhnische Daten 1	148
Einführung1	148
Technische Daten	148
CC6000 1	148
CC600 1	150
Decodierabstände 1	152
CC6000 – SE4710 Scan-Engine 1	152
CC600 – SE2100 Scan-Engine 1	153

# Informationen zu diesem Leitfaden

## Einführung

Dieses Handbuch enthält Informationen zur Verwendung und zum Zubehör des CC600 und CC6000 Customer Concierge.



**HINWEIS:** Die in diesem Handbuch abgebildeten Bildschirme und Fenster sind Beispiele und können von den tatsächlichen Bildschirmen Ihres Geräts abweichen.

### Dokumentationssatz

Der Dokumentationssatz stellt entsprechend den jeweiligen spezifischen Benutzeranforderungen Informationen bereit und umfasst:

- CC600/CC6000 Customer Concierge Kurzanleitung für Android Version 8.1, p/n MN-003315-xx: Beschreibt, wie Sie das Gerät für den Betrieb einrichten.
- CC600/CC6000 Customer Concierge Benutzerhandbuch f
  ür Android Version 8.1, p/n MN-003313-xx: Beschreibt die Verwendung des Ger
  äts.
- CC600/CC6000 Customer Concierge Handbuch zur Integration für Android Version 8.1, p/n Mn-003411-xx: Beschreibt die Einrichtung des Geräts und des Zubehörs.

Die aktuelle Version dieses Handbuchs (und aller anderen Handbücher) erhalten Sie unter: www.zebra.com/support

## Konfigurationen

Dieses Handbuch bezieht sich auf die in Tabelle 1 und Tabelle 2 aufgeführten Konfigurationen.

 Tabelle 1
 CC600-Gerätekonfigurationen

Konfiguration	Beschreibung	Kamera an der Vorderseite	Scan- Engine
CC600-5-3200LNWW	5 Zoll, BS: Android <sup>™</sup> 8.1.0 Oreo, 32 GB Ethernet/WLAN, Imager, weltweite Konfiguration	Nein	SE2100
CC600-5-3200LNNA	5 Zoll, BS: Android <sup>™</sup> 8.1.0 Oreo, 32 GB Ethernet/WLAN, Imager, Konfiguration für Nordamerika	Nein	SE2100
CC600-5-3200LNEU	5 Zoll, BS: Android™ 8.1.0 Oreo, 32 GB Ethernet/WLAN, Imager, Konfiguration für Europa	Nein	SE2100
CC600-5-3200LNIN	5 Zoll, BS: Android <sup>™</sup> 8.1.0 Oreo, 32 GB Ethernet/WLAN, Imager, Konfiguration für Indien	Nein	SE2100

 Tabelle 2
 CC6000-Gerätekonfigurationen

Konfiguration	Beschreibung	Kamera an der Vorderseite	Scan- Engine
CC6000-10-3200LCWW	10 Zoll, BS: Android ™ 8.1.0 Oreo, 32 GB, Querformat, Imager, weltweite Konfiguration	Nein	SE4710
CC6000-10-3200PCWW	10 Zoll, BS: Android ™ 8.1.0 Oreo, 32 GB, Hochformat, Imager, weltweite Konfiguration	Ja	SE4710
CC6000-10-3200LCNA	10 Zoll, BS: Android ™ 8.1.0 Oreo, 32 GB, Hochformat, Imager, Konfiguration für Nordamerika	Ja	SE4710
CC6000-10-3200PCNA	10 Zoll, BS: Android ™ 8.1.0 Oreo, 32 GB, Hochformat, Imager, Konfiguration für Nordamerika	Ja	SE4710
CC6000-10-3200LNNA	10 Zoll, BS: Android ™ 8.1.0 Oreo, 32 GB, Querformat, Imager, Konfiguration für Nordamerika	Nein	SE4710

## Zubehör

#### Tabelle 3Zubehör

Zubehör	Teilenummer	Beschreibung
Montageplatten	'	
CC600-Wandmontage	21-118517-01R	CC600-Wandmontagesatz
CC600-Mastmontage	21-118517-02R	CC600-Mastmontagesatz
CC6000-Wandmontagesatz	KT-152097-03	CC6000-Wandmontagesatz mit Aufbewahrung für Netzteil
CC6000-Wandmontagesatz	KT-152097-01	100 mm VESA
CC6000-Wandmontagesatz	KT-152098-03	Schlankere Halterung, spezifisch für CC6000
CC6000-Mastmontagesatz	KT-152096-03	100 mm VESA
		Enthält zusätzliches Lagerregal zur Aufbewahrung des Netzteils
		Gegenüber KT0152096-02 geändert, um Netzteile der Stufe VI besser aufzubewahren.
CC6000-Mastmontagesatz	KT-152096-01	100 mm VESA
Kommunikationskabel		
USB-C-Kabel	CBL-TC2X-USBC-01	Dient zur Kommunikation mit CC6000 über den USB-OTG-Anschluss.
USB-C-Kabel	CBL-TC5X-USBC2A-01	Dient zur Kommunikation mit CC6000 über den USB-OTG-Anschluss.
Netzteile	•	
Gleichstromkabel	CBL-DC-383A1-01	Mit Stromversorgung (PWR-BUA5V16W0WW)
		Kabellänge 1,8 m
Netzteil	PWR-BUA5V16W0WW	100–240 V AC, 5,4 V, 3 A, 16 W
		Erfüllt den Effizienzstandard der Stufe VI des US-amerikanischen Energieministeriums
		Ersetzt PVVKS-14000-249K
Wechselstrom-Netzkabel	50-16000-182R	Verwendet mit 50-14000-147R/50-14000-249R?PWRS- 14000-249R/PWR-BUA5V16W0WW

#### Softwareversionen

So bestimmen Sie die aktuelle Softwareversion:

- 1. Wischen Sie vom oberen Rand nach unten, um die Schnelleinstellungen zu öffnen.
- 2. Berühren Sie 🏟 > System.
- 3. Berühren Sie About phone (Telefoninfo).

- 4. Die folgenden Informationen werden angezeigt:
  - Status
  - SW-Komponenten
  - Rechtliche Informationen
  - Modell
  - Android-Version
  - Android Security Patch-Niveau
  - Kernel-Version
  - Build-Fingerabdruck
  - Build-Nummer

Um die Geräteseriennummer zu bestimmen, berühren Sie **About phone** (Telefoninfo) > **Status**. **Serial number** (Seriennummer) wird angezeigt.

#### Kapitelbeschreibungen

In diesem Handbuch werden folgende Themen behandelt:

- Erste Schritte stellt Informationen zur Erstinbetriebnahme des Geräts bereit.
- Einstellungen enthält die Einstellungen für die Konfiguration des Geräts.
- USB/Ethernet-Kommunikation beschreibt die Verbindung des Geräts mit einem Host-Computer über USB und Ethernet.
- DataWedge beschreibt, wie die Anwendung DataWedge verwendet und konfiguriert wird.
- Anwendungsinstallation enthält Informationen zur Entwicklung und Verwaltung von Anwendungen.
- Wartung und Fehlerbehebung enthält Anleitungen zur Reinigung und Aufbewahrung des Geräts sowie Lösungen zur Fehlerbehebung bei potenziellen Problemen während der Verwendung des Geräts.
- Technische Daten stellt Informationen zu den technischen Daten des Geräts bereit.

#### Schreibkonventionen

Die folgenden Konventionen werden in diesem Dokument verwendet:

- "Gerät" bezieht sich auf alle Konfigurationen der Geräte CC600 Customer Concierge und CC6000 Customer Concierge.
- In Fettschrift wird Folgendes hervorgehoben:
  - Dialogfelder, Fenster und Namen von Bildschirmen
  - Drop-down-Listen und Namen von Listenfeldern
  - Kontrollkästchen und Namen von Optionsschaltflächen
  - Symbole auf einem Bildschirm
  - · Namen von Tasten auf einer Tastatur
  - · Namen von Schaltflächen auf einem Bildschirm
- Aufzählungszeichen (•) geben Folgendes an:
  - Ma
    ßnahmen
  - Listen alternativer Optionen
  - · Listen erforderlicher Schritte (nicht unbedingt in der angegebenen Reihenfolge auszuführen)
- Listen, in denen die Reihenfolge beachtet werden muss (z. B. bei schrittweisen Verfahrensweisen), werden als nummerierte Liste angegeben.

### Kundendienstinformationen

Sollten Probleme mit Ihrem Gerät auftreten, wenden Sie sich an den für Ihr Gebiet zuständigen Kundendienst. Die Kontaktinformationen finden Sie unter: <u>zebra.com/support</u>.

Halten Sie bitte die folgenden Informationen bereit, wenn Sie sich an den Kundendienst wenden:

- Seriennummer des Geräts (auf dem Herstellungsetikett angegeben)
- Modellnummer oder Produktname (auf dem Herstellungsetikett angegeben)
- Softwaretyp und Versionsnummer
- IMEI-Nummer

Der Kundendienst beantwortet Anfragen per E-Mail oder Telefon innerhalb der jeweils in den Supportverträgen vereinbarten Fristen.

Sollte das Problem nicht vom Kundendienst behoben werden können, muss der Benutzer das Gerät u. U. zur Wartung an uns zurücksenden. Anweisungen hierzu erhalten Sie vom Kundendienst. Wir übernehmen keine Verantwortung für Beschädigungen, die während des Transports auftreten, wenn der Versand nicht in der genehmigten Versandverpackung erfolgte. Durch einen unsachgemäßen Versand wird die Garantieleistung u. U. außer Kraft gesetzt. Entfernen Sie die SIM-Karte und/oder microSD-Karte, bevor Sie das Gerät zur Wartung einsenden.

Wenn Sie Ihr Gerät von einem Geschäftspartner erworben haben, wenden Sie sich bitte an diesen.

#### Feedback zur Dokumentation

Wenn Sie Kommentare, Fragen oder Vorschläge zu dieser Anleitung haben, senden Sie eine E-Mail an <u>EVM-Techdocs@zebra.com</u>.

## **Erste Schritte**

## Einführung

In diesem Kapitel finden Sie Informationen zur erstmaligen Verwendung des Geräts.

#### Auspacken

- 1. Entfernen Sie vorsichtig das Schutzmaterial vom Gerät, und heben Sie die Versandverpackung für spätere Lager- oder Versandzwecke auf.
- 2. Überprüfen Sie, ob Folgendes enthalten ist:
  - CC600 oder CC6000 interaktives Kiosk-System.
  - Leitfaden zu Rechtsvorschriften.
  - Nur für CC600: Ferritperle für EMI. Anschluss an das DC-Leistungsmodul.
- 3. Vergewissern Sie sich, dass der Packungsinhalt unbeschädigt ist. Falls der Packungsinhalt nicht vollständig oder beschädigt ist, wenden Sie sich unverzüglich an den globalen Kundendienst.
- 4. Entfernen Sie vor dem ersten Gebrauch des Geräts die Schutzfolie, die während des Versands das Display bedeckt.

## Merkmale



**HINWEIS:** Die Seitenausrichtungen der CC6000 Hochformat- und Querformat-Geräte weichen zwar voneinander ab, die Funktionen unterscheiden sich jedoch nicht.













Abbildung 4 CC6000 – Rückansicht mit Halterung









Abbildung 7 CC600 – Strom- und Kabelanschlüsse







Element	Funktion	
Touchscreen und Display	Zeigt alle für die Bedienung des Geräts benötigten Informationen an.	
Scanfenster (Scanner)	Erfasst Daten mit dem Imager und liest Barcodes.	
	<b>Hinweis</b> : Zum Lesen eines Barcodes muss eine zum Scannen geeignete App auf dem Gerät installiert sein.	
Lautsprecher	Bietet Audio für die Video- und Musikwiedergabe. Bietet Audio im Freisprechtelefonmodus.	
NFC-Antenne	Liest NFC-Tags. (nur CC6000)	
Näherungssensor	Erkennt die Nähe eines Benutzers zum Einschalten des Displays.	
Mikrofon	Für die Kommunikation im Freisprechmodus.	
Nach vorne gerichtete	Nimmt Fotos und Videos auf.	
Kamera	Hinweis: Nur bestimmte CC6000-Geräte.	
Schnittstellenanschlüsse	Siehe Abbildung 3 und Abbildung 7.	
Lautstärketaste	Erhöhen und Verringern der Lautstärke (programmierbar).	
Externes Display	Zur Verwendung des USB-C-Anschlusses.	

## Einrichtung

Führen Sie dieses Verfahren aus, wenn Sie das Gerät zum ersten Mal verwenden.

- Installieren Sie eine Micro Secure Digital (SD)-Karte (optional).
- Schließen Sie das Netzteil an, um das Gerät einzuschalten.
- Konfigurieren Sie das Gerät.
- Montieren Sie das Gerät mit der Montagehalterung.
- Richten Sie ein Google-Konto ein.

## Installieren der microSD-Karte (optional)

Der microSD-Kartensteckplatz stellt einen sekundären, nicht flüchtigen Speicher bereit. Der Steckplatz befindet sich auf der Rückseite des Geräts rechts neben der Audio-Buchse. Weitere Informationen entnehmen Sie bitte der mit der Karte gelieferten Dokumentation. Beachten Sie die Verwendungsempfehlungen des Herstellers.



**VORSICHT:** Beachten Sie die Vorkehrungen gegen elektrostatische Entladungen (Electrostatic Discharge, ESD), um eine Beschädigung der microSD-Karte zu vermeiden. Zu diesen ESD-Vorkehrungen gehören u. a. die Verwendung einer Antistatikunterlage und die ordnungsgemäße Erdung des Benutzers.

So setzen Sie die microSD-Karte ein:

- 1. Falls das Gerät in der Montagehalterung installiert ist, nehmen Sie es heraus.
- 2. Schieben Sie die Anschlüsse der microSD-Karte nach unten in das Gerät, wie in Abbildung 9 gezeigt.

#### Abbildung 9 Einsetzen der microSD-Karte



#### Montieren des Geräts

Für jede Konfiguration des Geräts ist eine entsprechende Montagehalterung erforderlich, um das Gerät an einer Wand oder einer anderen flachen Oberfläche zu befestigen. Der Durchmesser der Löcher für die Schrauben an der Wand beträgt 5,8 mm (0,228 Zoll).



HINWEIS: Gerätemessungen in Abbildung 10, Abbildung 11 und Abbildung 12 sind in Millimetern angegeben.







Abbildung 11 CC6000 – Abmessungen im Hochformat

















#### Erste Schritte





#### Abbildung 15 CC6000 Montagehalterung (KT-152098-03) – Querformat



So montieren Sie das Gerät:

- 1. Legen Sie fest, wo Sie das CC600 oder CC6000 montieren möchten.
- 2. Befestigen Sie die Montageplatte mit den mitgelieferten Schrauben an der Wand (drei Schrauben für das CC600, vier Schrauben für das CC6000).

Abbildung 16 Anbringen der CC600-Halterung an der Wand



Abbildung 17 Anbringen der CC6000-Halterung an der Wand



3. Setzen Sie die vier Schulterschrauben (ebenfalls im Lieferumfang enthalten) in die Montagelöcher an der Rückseite des Geräts ein.

#### Erste Schritte

#### Abbildung 18 Einsetzen der Schulterschrauben





- 4. Verbinden Sie das Netzteil mit dem Netzanschluss. Verbinden Sie alle zusätzlichen Kabel mit den entsprechenden Anschlüssen, wie in Abbildung 3 und Abbildung 7 dargestellt.
- 5. Montieren Sie das Gerät, indem Sie die Schulterschrauben durch die vier Löcher auf der Montageplatte stecken, und schieben Sie das Gerät nach unten, um es zu befestigen.





6. Setzen Sie die Verriegelungsschraube durch das Loch in der Halterung oben an der Montageplatte ein. Ziehen Sie die Schraube mit der Hand fest, um das Gerät zu befestigen.

#### **Einrichten eines Google-Kontos**



**HINWEIS:** Zum Einrichten eines Google-Kontos (optional) muss das Gerät mit dem Internet verbunden werden. Ein Google-Konto ist nur bei Geräten mit GMS-Software erforderlich.

Beim ersten Start des Geräts wird der Einrichtungsassistent angezeigt. Befolgen Sie die Anweisungen auf dem Bildschirm zum Einrichten eines Google-Kontos, zum Konfigurieren von Google Wallet zum Kauf von Artikeln im Play Store, zur Eingabe Ihrer persönlichen Informationen und zur Aktivierung der Backup-/ Wiederherstellungsfunktionen (optional).

#### **Zebra Visibility Services**

Das Gerät erfasst Geräteanalysedaten und bietet eine Geräteanalyse für Systemadministratoren. Beim ersten Hochfahren des Geräts (oder nach einer Wiederherstellung der Werkseinstellungen) wird der Vereinbarungsbildschirm **Zebra Services** angezeigt.

Zebra Data Services
Device Data Help Zebra improve its products and services by sending machine data related to device usage. Required for Zebra Mobility DNA and Visibility Services. About machine data.
ОК

Abbildung 20 Zebra Services

Berühren Sie den Schalter **Device Data** (Gerätedaten), um das Senden von Analysedaten durch das Gerät zu deaktivieren.

### Zurücksetzen des Geräts

Das Gerät verfügt über eine eingelassene Rücksetztaste (die Position der Taste finden Sie unter Merkmale auf Seite 16).

Um die Rücksetztaste zu aktivieren, setzen Sie die Spitze einer kleinen Büroklammer (1 mm Durchmesser) in die Aussparung ein, und halten Sie sie 3 Sekunden lang gedrückt.

Das Gerät verfügt über eine Wiederherstellungskonsole, auf die beim Einschalten des Geräts durch Drücken der Taste Nr. 1 auf der Rückseite oder über ADB-Verbindung und Befehl zugegriffen werden kann.

Folgende Rücksetzfunktionen werden unterstützt:

- · Ein Soft-Reset wird per ADB-Befehl ausgeführt.
- Enterprise-Reset (weitere Informationen finden Sie unter StageNow auf Seite 123)
- Zurücksetzen auf Werkseinstellungen (weitere Informationen finden Sie unter StageNow auf Seite 123)

#### Erste Schritte

Der Modus zur Gerätewiederherstellung unterstützt die folgenden Funktionen:

- Flash-Bild aus einer ZIP-Datei auf einer SD-Karte oder von einem internen Flash.
- Systemaktualisierung einer SD-Karte oder eines internen Flashs.

## Einstellungen

## Einführung

In diesem Kapitel werden die für die Konfiguration des Geräts verfügbaren Einstellungen beschrieben.

## **WLAN-Konfiguration**

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der WLAN-Einstellungen.

#### Konfigurieren eines sicheren WLAN-Netzwerks

So richten Sie ein WLAN-Netzwerk ein:

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Network & Internet (Netzwerk und Internet) > Wi-Fi (WLAN).
- 3. Schieben Sie den Schalter in die Position ON (EIN).
- 4. Das Gerät sucht nach WLANs in der Umgebung und führt sie auf dem Bildschirm auf.
- 5. Scrollen Sie durch die Liste, und wählen Sie das gewünschte WLAN-Netzwerk aus.

 Berühren Sie das gewünschte Netzwerk. Wenn die Netzwerksicherheit auf Open (Offen) eingestellt ist, stellt das Gerät automatisch eine Verbindung mit dem Netzwerk her. Für alle anderen Netzwerksicherheitseinstellungen wird ein Dialogfeld angezeigt.

Abbildung 21	Dialogfeld zur WLAN WEP-Netzwerksicherheit
--------------	--

WLAN	
Password	
Show password	
Advanced options	$\sim$
CANCEL	CONNECT

Abbildung 22 Dialogfeld zur WLAN 802.11 EAP-Netzwerksicherheit

WLAN		
EAP method <b>PEAP</b>		•
Phase 2 authentica MSCHAPV2	ation	•
CA certificate (unspecified)		•
Identity		
Anonymous identit	у	
Password		
Show passwore	d	
Advanced options		$\checkmark$
	CANCEL	CONNECT

7. Wenn die Netzwerksicherheit auf **WEP** oder **WPA/WPS2 PSK** eingestellt ist, geben Sie das erforderliche Kennwort ein, und berühren Sie dann **Connect** (Verbinden).

- 8. Wenn die Netzwerksicherheit "802.1x EAP" lautet:
  - Berühren Sie die Drop-down-Liste EAP method (EAP-Methode), und wählen Sie PEAP, TLS, TTLS, oder LEAP aus.
  - Berühren Sie die Drop-down-Liste Phase 2 authentication (Phase 2-Authentifizierung), und wählen Sie eine Authentifizierungsmethode.
  - Berühren Sie, falls erforderlich, CA certificate (CA-Zertifikat), und wählen Sie ein Zertifikat einer Zertifizierungsstelle (CA). Hinweis: Zertifikate werden mit den Einstellungen für Security (Sicherheit) installiert.
  - Berühren Sie, falls erforderlich, User certificate (Benutzerzertifikat), und wählen Sie ein Benutzerzertifikat. Hinweis: Benutzerzertifikate werden mit den Einstellungen für "Location & security" (Standort und Sicherheit) installiert.
  - Geben Sie, falls erforderlich, im Textfeld Identity (Identität), die Anmeldeinformationen f
    ür den Benutzernamen ein.
  - Geben Sie, sofern gewünscht, einen anonymen Benutzernamen in das Textfeld Anonymous identity (Anonyme Identität) ein.
  - Geben Sie, falls erforderlich, im Textfeld Password (Kennwort) das Kennwort für diese Identität ein.



**HINWEIS:** Standardmäßig ist der Netzwerk-Proxy auf **None** (Kein) und die IP-Einstellungen auf **DHCP** eingestellt. Siehe Konfigurieren für einen Proxyserver auf Seite 33, um Informationen zum Einstellen der Verbindung zu einem Proxyserver, und Konfigurieren des Geräts für die Verwendung einer statischen IP-Adresse auf Seite 34, um Informationen zum Einstellen des Geräts für die Verwendung einer statischen IP-Adresse zu erhalten.

- 9. Berühren Sie Connect (Verbinden).
- 10.Berühren Sie 🔘.

#### Manuelles Hinzufügen eines WLAN-Netzwerks

Fügen Sie manuell ein WLAN-Netzwerk hinzu, wenn das Netzwerk seinen Namen (SSID) nicht überträgt oder Sie sich außerhalb der Reichweite befinden.

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🏟.
- 2. Berühren Sie Network & Internet (Netzwerk und Internet) > Wi-Fi (WLAN).
- 3. Schieben Sie den WLAN-Schalter in die Position ON (EIN).
- 4. Scrollen Sie in der Liste nach unten, und wählen Sie Add network (Netzwerk hinzufügen) aus.
- 5. Geben Sie im Textfeld Network name (Netzwerkname) die Adresse des WLAN-Netzwerks ein.
- 6. Wählen Sie in der Drop-down-Liste Security (Sicherheit) den Sicherheitstyp aus:
  - None
  - WEP
  - WPA/WPA2 PSK
  - 802.1x EAP.
- 7. Wenn die Netzwerksicherheit auf None (Keine) eingestellt ist, berühren Sie Save (Speichern).
- 8. Wenn die Netzwerksicherheit auf **WEP** oder **WPA/WPA2 PSK** eingestellt ist, geben Sie das erforderliche Kennwort ein, und berühren Sie dann **Save** (Speichern).

- 9. Wenn die Netzwerksicherheit 802.1x EAP lautet:
  - Berühren Sie die Drop-down-Liste **EAP method** (EAP-Methode), und wählen Sie **PEAP**, **TLS**, **TTLS**, **PWD** oder **LEAP** aus.
  - Berühren Sie die Drop-down-Liste **Phase 2 authentication** (Phase 2-Authentifizierung), und wählen Sie eine Authentifizierungsmethode.
  - Berühren Sie, falls erforderlich, CA certificate (CA-Zertifikat), und wählen Sie ein Zertifikat einer Zertifizierungsstelle (CA). Hinweis: Zertifikate werden mit den Einstellungen für Security (Sicherheit) installiert.
  - Berühren Sie, falls erforderlich, User certificate (Benutzerzertifikat), und wählen Sie ein Benutzerzertifikat. Hinweis: Benutzerzertifikate werden mit den Einstellungen für Security (Sicherheit) installiert.
  - Geben Sie, falls erforderlich, im Textfeld Identity (Identität), die Anmeldeinformationen für den Benutzernamen ein.
  - Geben Sie, sofern gewünscht, einen anonymen Benutzernamen in das Textfeld **Anonymous identity** (Anonyme Identität) ein.
  - Geben Sie, falls erforderlich, im Textfeld **Password** (Kennwort) das Kennwort für die entsprechende Identität ein.



**HINWEIS:** Standardmäßig ist der Netzwerk-Proxy auf **None** (Kein) und die IP-Einstellungen auf **DHCP** eingestellt. Siehe Konfigurieren für einen Proxyserver auf Seite 33, um Informationen zum Einstellen der Verbindung zu einem Proxyserver, und Konfigurieren des Geräts für die Verwendung einer statischen IP-Adresse auf Seite 34, um Informationen zum Einstellen des Geräts für die Verwendung einer statischen IP-Adresse zu erhalten.

- 10. Berühren Sie **Save** (Speichern). Um eine Verbindung zu einem gespeicherten Netzwerk herzustellen, berühren und halten Sie das gespeicherte Netzwerk, und wählen Sie **Connect to network** (Mit Netzwerk verbinden).
- 11.Berühren Sie O.

#### Konfigurieren für einen Proxyserver

Ein Proxyserver ist ein Server, der als Vermittler für Anforderungen von Clients agiert, die Ressourcen von anderen Servern anfordern. Ein Client stellt eine Verbindung zum Proxyserver her und fordert einen Service an, wie z. B. eine Datei, eine Verbindung, eine Webseite oder eine andere Ressource, die auf einem anderen Server zur Verfügung steht. Der Proxyserver wertet die Anforderung gemäß seinen Filterregeln aus. Zum Beispiel kann er den Datenverkehr nach der IP-Adresse oder dem Protokoll filtern. Wenn die Anforderung durch den Filter bestätigt wird, stellt der Proxy die Ressource zur Verfügung, indem er eine Verbindung zum jeweiligen Server herstellt und den Service im Namen des Clients anfordert.

Es ist wichtig für Unternehmen, sichere IT-Umgebungen innerhalb des Unternehmens einrichten zu können, und die Proxykonfiguration spielt hierbei eine wichtige Rolle. Die Proxykonfiguration fungiert als Sicherheitsbarriere und stellt sicher, dass der Proxyserver sämtlichen Datenverkehr zwischen dem Internet und dem Intranet überwacht. Dies ist normalerweise ein integraler Bestandteil der Sicherheitsdurchsetzung in Unternehmens-Firewalls innerhalb von Intranets.

So konfigurieren Sie das Gerät für einen Proxy-Server:

- 1. Berühren Sie ein Netzwerk im Dialogfeld "Network" (Netzwerk).
- 2. Berühren Sie Advanced options (Erweiterte Optionen).

3. Berühren Sie Proxy, und wählen Sie Manual (Manuell).

<b></b>
<b></b>

WLAN Proxy Manual •		
other apps.		
Proxy hostname		
proxy.example.com		
Proxy port		
8080		
Bypass proxy for		
example.com,mycomp.test.com,l		
IP settings		
DHCP		
CANCEL CONNECT		

- 4. Geben Sie im Textfeld Proxy hostname (Proxy-Hostname) die Adresse des Proxyservers ein.
- 5. Geben Sie im Textfeld Proxy port (Proxy-Port) die Portnummer des Proxyservers ein.
- Geben Sie im Textfeld Bypass proxy for (Proxy umgehen f
  ür) Adressen f
  ür Websites ein, die nicht 
  über den Proxyserver verlaufen m
  üssen. Verwenden Sie ein Komma (,) zwischen den Adressen. Verwenden Sie keine Leerzeichen oder Zeilenumbr
  üche zwischen Adressen.
- 7. Berühren Sie Connect (Verbinden).
- 8. Berühren Sie 🔘.

#### Konfigurieren des Geräts für die Verwendung einer statischen IP-Adresse

Standardmäßig ist das Gerät für die Verwendung von DHCP (Dynamic Host Configuration Protocol) zum Zuweisen einer IP-Adresse (Internet Protocol) bei der Verbindung mit einem drahtlosen Netzwerk konfiguriert.

So konfigurieren Sie das Gerät für die Verbindung mit einem Netzwerk unter Verwendung einer statischen IP-Adresse:

- 1. Berühren Sie ein Netzwerk im Dialogfeld "Network" (Netzwerk).
- 2. Berühren Sie Advanced options (Erweiterte Optionen).

3. Berühren Sie IP settings (IP-Einstellungen), und wählen Sie Static (Statisch).

Abbildung 24	Statische IP-Einstellungen
--------------	----------------------------

WLAN IP settings Static	Ŧ
IP address	
192.168.1.128	
Gateway	
192.168.1.1	
Network prefix length	
24	
DNS 1	
8.8.8.8	
DNS 2	
8.8.4.4	
CANCEL	CONNECT

- 4. Geben Sie im Textfeld IP address (IP-Adresse) eine IP-Adresse für das Gerät ein.
- 5. Geben Sie gegebenenfalls im Textfeld Gateway eine Gateway-Adresse für das Gerät ein.
- 6. Geben Sie gegebenenfalls im Textfeld Network prefix length (Netzwerk-Präfixlänge) die Präfixlänge ein.
- 7. Geben Sie gegebenenfalls im Textfeld DNS 1 eine Domain Name System (DNS)-Adresse für das Gerät ein.
- 8. Geben Sie gegebenenfalls im Textfeld **DNS 2** eine DNS-Adresse ein.
- 9. Berühren Sie **Connect** (Verbinden).
- 10. Berühren Sie 🔘.

#### WLAN-Einstellungen

Verwenden Sie die Einstellungen unter **Wi-Fi preferences** (WLAN-Einstellungen) zum Konfigurieren erweiterter WLAN-Einstellungen. Scrollen Sie vom WLAN-Bildschirm nach unten zum unteren Bildschirmrand, und berühren Sie **Wi-Fi preferences** (WLAN-Einstellungen).

- **Open network notification** (Benachrichtigung bei offenem Netzwerk): Wenn diese Option aktiviert ist, wird der Benutzer benachrichtigt, wenn ein offenes Netzwerk verfügbar ist.
- Advanced (Erweitert): Zum Erweitern der Optionen berühren.
  - Additional settings (Zusätzliche Einstellungen): Siehe "Zusätzliche Einstellungen".
  - Install Certificates (Zertifikate installieren): Zum Installieren von Zertifikaten berühren.
  - Network rating provider (Netzwerkbewertungsanbieter): Deaktiviert (AOSP-Geräte). Um festzustellen, was ein gutes WLAN-Netzwerk ausmacht, unterstützt Android externe Netzwerkbewertungsanbieter, die Informationen über die Qualität offener WLAN-Netzwerke bereitstellen. Wählen Sie einen der aufgeführten Anbieter aus, oder wählen Sie None (Keine) aus. Wenn keine Anbieter verfügbar oder ausgewählt sind, ist die Funktion für Verbindungen zu offenen Netzwerken deaktiviert.
  - Wi-Fi Direct: Zeigt eine Liste der Geräte an, die für eine direkte WLAN-Verbindung verfügbar sind.
  - MAC address (MAC-Adresse): Zeigt die MAC (Media Access Control)-Adresse des Geräts an, wenn eine Verbindung zu WLAN-Netzwerken hergestellt wird.
  - **IP address** (IP-Adresse): Zeigt die IP-Adresse des Geräts an, wenn eine Verbindung zu WLAN-Netzwerken hergestellt wird.

#### Erweiterte WLAN-Einstellungen



HINWEIS: Erweiterte WLAN-Einstellungen gelten für das Gerät und nicht für ein bestimmtes drahtloses Netzwerk.

Verwenden Sie die Einstellungen unter **Advanced** (Erweitert) zum Konfigurieren zusätzlicher WLAN-Einstellungen. Um die zusätzlichen WLAN-Einstellungen anzuzeigen, scollen Sie zum unteren Rand des Bildschirms **Wi-Fi** (WLAN), und berühren Sie **Wi-Fi Preferences** (WLAN-Einstellungen) **> Advanced** (Erweitert) **> Additional settings** (Zusätzliche Einstellungen).

- Richtlinienkonformität
  - **Country selection** (Auswahl des Landes): Zeigt den erhaltenen Ländercode an, wenn 802.11d aktiviert ist; sonst zeigt es den aktuell ausgewählten Ländercode an.
  - Region code (Regionalcode): Zeigt den Code der aktuellen Region an.
- Band- und Kanalwahl
  - Wi-Fi frequency band (WLAN-Frequenzband): Einstellen des Frequenzbands: Auto (Standard), 5 GHz only (Nur 5 GHz) oder 2.4 GHz only (Nur 2,4 GHz).
  - Available channels (2,4 GHz) (Verfügbare Kanäle (2,4 Ghz)): Zum Anzeigen des Menüs Available channels (Verfügbare Kanäle) berühren. Wählen Sie die entsprechenden Kanäle aus, und berühren Sie OK.
  - Available channels (5 GHz) (Verfügbare Kanäle (5 Ghz)): Zum Anzeigen des Menüs Available channels (Verfügbare Kanäle) berühren. Wählen Sie die entsprechenden Kanäle aus, und berühren Sie OK.
- Protokollierung
  - Advanced Logging (Erweiterte Protokollierung): Berühren Sie diese Option, um die erweiterte Protokollierung zu aktivieren oder das Protokollverzeichnis zu ändern.
  - Wireless logs (WLAN-Protokolle): Zum Aufzeichnen von WLAN-Protokolldateien.
    - Fusion Logger: Zum Öffnen der Fusion Logger-Anwendung berühren. Diese Anwendung speichert eine Reihe von WLAN-Ereignissen auf hoher Ebene, die Ihnen helfen können, den Status der Verbindung genauer zu verstehen.
    - Fusion Status (Fusion-Status): Zur Anzeige des Live-Status des WLAN-Status berühren. Bietet auch Informationen zum Gerät und zum verbundenen Profil.
- Info
  - Version: Zeigt die aktuellen Informationen zu Fusion an.


			▼⊿1 11:57
FusionLogger			
T1:22:4500nnection Completed with: 84:24:80:ae:0a:42			
11:22:45 Channel 149			
11:22:45 Wi-Fi Frequency Band : Auto			
11:22:45 Connected to "WLAN"			
11:22:45 Disconnected			
11:22:45 Disconnected			
11:22:46 Disconnected			
11:22:46 Disconnected			
11:23:09 Disconnected			
11:23:09 Scanning			
11:23:09 Scanning:			
11:23:10 Scanning			
11:22:10 Connecting to WLAN"			
11:22:10 Connecting to "W/LAN!"			
11:23:10 Authenticating with "MLAN"			
11:23:10 Four-way Handebake			
11:23:10 Group Handshake			
11:23:11 Authenticating with "W/LAN"			
11:23:11 Connecting to "WLAN"			
11:23:11 Obtaining IP address from "WI AN"			
11:23:11 Connection Completed with 84:24:8d:af:06:52			
11:23:11 "ZGuest" lpAddress:10.10.203.13			
11:23:11Connection Completed with: 84:24:8d:af:06:52			
11:23:11 Channel 11			
11:23:11 Wi-Fi Frequency Band : Auto			
11:23:11 Connected to "WLAN"			
11:23:11 "ZGuest" lpAddress:10.10.203.13			
11:23:11Connection Completed with: 84:24:8d:af:06:52			
11:23:11 Channel 11			
11:23:11 Wi-Fi Frequency Band : Auto			
11:23:11 Connected to "WLAN"			
11:29:29 ASSOCIATED			
11:29:29 "ZGuest" IpAddress:10.10.203.13			
11:29:29Connection Completed with: 84:24:8d:ae:6a:42			
11:29:29 Channel 149			
11:29:29 WI-FI Frequency Band : Auto			
11:29:29 Connected to "WLAN"			
11:29:29 Connection Completed with 84:24:80:ae:0a:42			
SAVE	CLE	AR	Scroll
UNITE			
	0		



				՝ 🛪 🖌 📲 11:58
Fusion Sta	tus			
SSID	: WLAN			
Status	: Connected			
MAC Address	: 40:83:de:b8:56:79			
AP MAC Address	: 84:24:8d:ae:6a:42			
Signal Strength	: Good			
Channel	: 149			
RSSI	: -59dBm			
Link Speed	: 173Mbps			
IP Address	: 10.10.203.13			
Gateway	: 10.10.200.1			
Netmask	: 255.255.252.0			
DNS1	: 8.8.8.8			
DNS2	: 4.2.2.2			
		$\triangleleft$	0	

# Wi-Fi Direct

Wi-Fi Direct-Geräte können miteinander verbunden werden, ohne dass ein zentraler Zugangspunkt verwendet werden muss. Wi-Fi Direct-Geräte richten bei Bedarf ein eigenes Ad-hoc-Netzwerk ein, sodass Sie sehen können, welche Geräte verfügbar sind, und auswählen können, mit welchem Gerät Sie eine Verbindung herstellen möchten.

- 1. Streichen Sie von der Statusleiste aus nach unten, und berühren Sie dann 🏟.
- Berühren Sie Wi-Fi (WLAN) > Wi-Fi preferences (WLAN-Einstellungen) > Advanced (Erweitert) > Wi-Fi Direct. Das Gerät beginnt mit der Suche nach einem anderen Wi-Fi Direct-Gerät.

←	Wi-F SEARCHING RENAME DEVICE	Ξ
	Android_4f0d	
	Peer devices	
	Android_baaf Available	

Abbildung 27 Bildschirm "Wi-Fi Direct"

- 3. Berühren Sie unter Peer devices (Peer-Geräte) den anderen Gerätenamen.
- 4. Wählen Sie auf dem anderen Gerät Accept (Annehmen) aus.
- 5. Auf dem Gerät wird **Connected** (Verbunden) angezeigt. Auf beiden Geräten wird in den entsprechenden Wi-Fi Direct-Bildschirmen der Name des anderen Geräts in der Liste angezeigt.

# Einstellen der Bildschirmsperre

Verwenden Sie die Einstellungen unter **Device security** (Gerätesicherheit), um die Einstellungen zum Sperren des Bildschirms festzulegen.

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🏟.
- 2. Berühren Sie Security & location (Sicherheit und Standort).



HINWEIS: Die Optionen variieren je nach den Richtlinien einiger Apps, z. B. E-Mail.

- **Screen lock** (Bildschirmsperre): Berühren Sie diese Option, um das Gerät so zu konfigurieren, dass zum Entsperren des Bildschirms eine Wischgeste, ein Muster, eine PIN oder ein Kennwort erforderlich ist.
  - None (Keine): Die Sicherheitsfunktion zum Entsperren des Bildschirms wird deaktiviert.
  - Swipe (Wischen): Verschieben Sie das Sperrsymbol, um den Bildschirm zu entsperren.
  - **Pattern** (Muster): Zeichnen Sie ein Muster, um den Bildschirm zu entsperren. Weitere Informationen sind unter Einrichten der Bildschirm-Entsperrfunktion mit Muster auf Seite 41 zu finden.
  - **PIN**: Geben Sie eine numerische PIN zum Entsperren des Bildschirms ein. Weitere Informationen sind unter Einstellen der Bildschirmsperre mit PIN auf Seite 39 zu finden.
  - **Password** (Kennwort): Geben Sie ein Kennwort ein, um den Bildschirm zu entsperren. Weitere Informationen sind unter Einrichten der Bildschirm-Entsperrfunktion mit Kennwort auf Seite 40 zu finden.

Sperren Sie den Bildschirm, um die Daten auf dem Gerät vor Zugriff zu schützen. Einige E-Mail-Konten erfordern ein Sperren des Bildschirms. Die Sperrfunktion funktioniert im Ein- und Mehrbenutzermodus unterschiedlich.

Wischen Sie auf dem Bildschirm nach oben, um ihn zu entsperren. Wenn die Entsperrfunktion durch Eingabe eines Musters aktiviert wird, wird der Bildschirm zur Mustereingabe anstelle des Sperrbildschirms angezeigt.

Wenn die Entsperrfunktion durch Eingabe einer PIN oder eines Kennworts aktiviert ist, geben Sie nach dem Entsperren des Bildschirms die entsprechende PIN oder das Kennwort ein.

## Einstellen der Bildschirmsperre mit PIN

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🏟.
- 2. Berühren Sie Security & location (Sicherheit und Standort).
- 3. Berühren Sie Screen lock (Bildschirmsperre).
- 4. Berühren Sie PIN.
- 5. Um beim Starten des Geräts eine PIN anzufordern, wählen Sie **Yes** (Ja), oder wählen Sie **No** (Nein), um keine PIN anzufordern.



Ê		
Set a scree	n lock	
For security, set a	a PIN	
PIN must be at leas	st 4 digits	
CANCEL		NEXT
1	2  ABC	3 DEF
<b>4</b> GHI	5 JKL	6 MNO
7 PQRS	<b>8</b> TUV	9 wxyz
$\langle \times \rangle$	0	$\rightarrow$

- 6. Berühren Sie das Textfeld.
- 7. Geben Sie eine PIN (4 Ziffern) ein, und berühren Sie Next (Weiter).
- 8. Geben Sie die PIN erneut ein, und berühren Sie dann Next (Weiter).
- 9. Wählen Sie die Art der Benachrichtigungen aus, die angezeigt werden sollen, wenn der Bildschirm gesperrt ist, und berühren Sie dann **Done** (Fertig).
- 10.Berühren Sie O. Wenn das Gerät das nächste Mal in den Ruhemodus wechselt, ist bei der Reaktivierung eine PIN erforderlich.

# Einrichten der Bildschirm-Entsperrfunktion mit Kennwort

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🎝.
- 2. Berühren Sie Security & location (Sicherheit und Standort).
- 3. Berühren Sie Screen lock (Bildschirmsperre).
- 4. Berühren Sie Password (Kennwort).
- 5. Um beim Starten des Geräts ein Kennwort anzufordern, wählen Sie **Yes** (Ja), oder wählen Sie **No** (Nein), um kein Kennwort anzufordern.
- 6. Berühren Sie das Textfeld.

Abbildung 29 Bildschirm zur Kennworteingabe

Se Fol	et a	SCI urity,	<b>'eer</b> set a	n Io pass	ck sword				
Mu CA	st be a	at lea:	st 4 ch	naract	ers		N	EXT	
1	2	3	4	5	6	7	8	9	0
q	w	е	r	t	у	u	i	0	р
а	s	d	f	g	h	j	k	.	I
仑	z	х	с	v	b	n	m	יו	$\times$
?123	,						] .		€

- 7. Geben Sie ein Kennwort ein (zwischen 4 und 16 Zeichen), und berühren Sie dann Next (Weiter).
- 8. Geben Sie das Kennwort erneut ein, und berühren Sie dann Next (Weiter).
- 9. Wählen Sie die Art der Benachrichtigungen aus, die angezeigt werden sollen, wenn der Bildschirm gesperrt ist, und berühren Sie dann **Done** (Fertig).
- 10.Berühren Sie O. Wenn das Gerät das nächste Mal in den Ruhemodus wechselt, ist bei der Reaktivierung ein Kennwort erforderlich.

## Einrichten der Bildschirm-Entsperrfunktion mit Muster

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Security & location (Sicherheit und Standort).
- 3. Berühren Sie Screen lock (Bildschirmsperre).
- 4. Berühren Sie Pattern (Muster).
- 5. Um beim Starten des Geräts ein Muster anzufordern, wählen Sie **Yes** (Ja), oder wählen Sie **No** (Nein), um kein Muster anzufordern.

Abbildung 30 Bildschirm zur Auswahl des Musters



- 6. Zeichnen Sie ein Muster, das mindestens vier Punkte verbindet.
- 7. Berühren Sie Continue (Fortfahren).
- 8. Zeichnen Sie das Muster erneut.
- 9. Berühren Sie Confirm (Bestätigen).
- 10. Wählen Sie die Art der Benachrichtigungen aus, die angezeigt werden sollen, wenn der Bildschirm gesperrt ist, und berühren Sie dann **Done** (Fertig).
- 11.Berühren Sie O. Wenn das Gerät das nächste Mal in den Ruhemodus wechselt, ist bei der Reaktivierung ein Muster erforderlich.

# Anzeigen von Kennwörtern

So stellen Sie das Gerät so ein, dass während der Eingabe die Kennwortzeichen kurz angezeigt werden:

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend \$\$.
- 2. Berühren Sie Security & location (Sicherheit und Standort).
- Schieben Sie den Schalter Show passwords (Kennwörter anzeigen) in die Position ON (EIN).

# Konten

Verwenden Sie die **Kontoeinstellungen**, um Konten hinzuzufügen, zu entfernen und zu verwalten. Mit diesen Einstellungen können Sie steuern, wie Anwendungen Daten senden, empfangen und synchronisieren und ob Anwendungen Benutzerdaten automatisch synchronisieren können.

Anwendungen können auch ihre eigenen Einstellungen aufweisen, um zu steuern, wie sie Daten synchronisieren. Weitere Informationen finden Sie in der Dokumentation zu diesen Anwendungen.

# Sprachverwendung

Verwenden Sie die Einstellungen für Language & input (Sprache und Eingabe), um die Sprache des Geräts zu ändern, einschließlich der Wörter, die dem Wörterbuch hinzugefügt wurden.

# Ändern der Spracheinstellung

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie System > Languages & input (Sprachen und Eingabe).
- 3. Berühren Sie Languages (Sprachen). Eine Liste der verfügbaren Sprachen wird angezeigt.
- 4. Wenn die gewünschte Sprache nicht aufgeführt ist, berühren Sie **Add a language** (Sprache hinzufügen), und wählen Sie eine Sprache aus der Liste aus.
- 5. Berühren und halten Sie = rechts von der gewünschten Sprache, und ziehen Sie sie dann an den Anfang der Liste.
- 6. Der Betriebssystemtext wird in die ausgewählte Sprache geändert.

# Hinzufügen von Wörtern zum Wörterbuch

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- Berühren Sie System > Languages & input (Sprachen und Eingaben) > Advanced (Erweitert) > Personal dictionary (Persönliches Wörterbuch).
- 3. Wenn Sie dazu aufgefordert werden, wählen Sie die Sprache aus, in der dieses Wort oder dieser Ausdruck gespeichert werden soll.
- 4. Berühren Sie +, um dem Wörterbuch ein neues Wort oder einen neuen Ausdruck hinzuzufügen.
- 5. Geben Sie das Wort oder den Ausdruck ein.
- 6. Geben Sie in das Textfeld Shortcut (Kurzform) eine Kurzform für das Wort oder den Ausdruck ein.
- 7. Berühren Sie O.

# Tastatureinstellungen

Mithilfe der Einstellungen unter **Languages & input** (Sprachen und Eingabe) können Sie die Bildschirmtastaturen konfigurieren. Das Gerät umfasst die folgenden Tastatureinstellungen:

- Android-Tastatur: nur AOSP-Geräte
- Enterprise-Tastatur
- Gboard: nur GMS-Geräte

# Konfigurieren von PTT Express

Weitere Informationen zur Konfiguration der PTT Express-Client-Anwendung finden Sie im PTT Express-Benutzerhandbuch unter <u>www.zebra.com/support</u>.

# RxLogger

RxLogger ist ein umfassendes Diagnosetool, das Anwendungs- und Systemmetriken bereitstellt, die Erstellung benutzerdefinierter Plug-ins ermöglicht und Geräte- und Anwendungsprobleme diagnostiziert. RxLogger protokolliert die folgenden Informationen: CPU-Belastung, Speicherauslastung, Speicherschnappschüsse, Betriebszustände, WLAN-Protokollierung, Mobilfunk-Protokollierung, TCP-Dumps, Bluetooth-Protokollierung, GPS-Protokollierung, Logcat, FTP-Push/Pull, ANR-Dumps usw. Alle Protokolle und generierten Dateien werden im Flash-Speicher auf dem Gerät (intern oder extern) gespeichert.





# Konfigurieren von RxLogger

RxLogger ist mit einer erweiterbaren Plug-in-Architektur ausgestattet und wird mit einer Reihe von bereits integrierten Plug-ins geliefert. Die im Lieferumfang enthaltenen Plug-ins werden im Folgenden beschrieben.

Um den Konfigurationsbildschirm zu öffnen, berühren Sie auf dem Startbildschirm von RxLogger **Settings** (Einstellungen).

Abbildung 32	Bildschirm zu	r Konfiguration von	RxLogger
--------------	---------------	---------------------	----------

SAVE	CANCEL
RxLogger Settings	
ANRModule	
KernelModule	
LogcatModule	
LTSModule	
RamoopsModule	
ResourceModule	
SnapshotModule	
TCPDumpModule	
TombstoneModule	

# **RxLogger-Einstellungen**

Das Einstellungsmodul für RxLogger bietet zusätzliche Einstellungen für RxLogger.

- Enable notifications (Benachrichtigungen aktivieren): Wählen Sie diese Option aus, um RxLogger-Benachrichtigungen in der Statusleiste und im Benachrichtigungsfenster zuzulassen.
- Enable debug logs (Debug-Protokolle aktivieren): Wählen Sie diese Option aus, um Debug-Protokolle zu aktivieren.

#### ANR-Modul

ANR (Application Not Responsive, Anwendung reagiert nicht) zeigt an, dass der UI-Thread einer laufenden Anwendung für einen bestimmten Zeitraum nicht reagiert. RxLogger kann diesen Zustand erkennen und eine Kopie des Aufruflisten-Verlaufs der nicht reagierenden Anwendung im Protokollverzeichnis auslösen. Das Ereignis wird auch im allgemeinen CSV-Protokoll angezeigt.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log path (Protokollpfad): Gibt den Standardprotokollpfad zum Speichern der ANR-Protokolldateien an.
- Collect Historic ANRs (ANR-Verlaufsdaten erfassen): Sammelt ANR-Verlaufsdateien aus dem System.

#### **Kernel-Modul**

Das Kernel-Modul erfasst systemseitige Kernel-Meldungen.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Kernel-Modul.
- Log path (Protokollpfad): Legt den allgemeinen Protokollpfad für die Speicherung aller Kernel-Protokolle fest. Diese Einstellung gilt global für alle Kernel-Puffer.
- Kernal Log filename (Name der Kernelprotokolldatei): Legt den Basisdateinamen des Protokolls f
  ür diesen Kernel-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angeh
  ängt.

- Max Kernal log file size (Max. Größe der Kernel-Protokolldatei): Gibt die maximale Größe einer einzelnen Protokolldatei in Megabyte an.
- Kernal Log interval (Intervall des Kernel-Protokolls): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
- Kernal Log file count (Anzahl der Kernprotokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
- Enable System Timestamp in Kernal Log (Systemzeitstempel im Kernel-Protokoll aktivieren): Aktiviert Systemzeitstempel in den Kernel-Protokollen.
- System Timestamp Interval (Systemzeitstempelintervall): Legt das Intervall zwischen Systemzeitstempeln in Sekunden fest.
- Enable Logcat Integration override (Überschreiben der Logcat-Integration aktivieren): Aktiviert das Überschreiben der Logcat-Integration.

## Logcat-Modul

Logcat ist ein wichtiges Debugging-Tool auf Android-Geräten. RxLogger ermöglicht die Aufzeichnung von Daten aus allen vier verfügbaren Logcat-Puffern. Das Logcat-Plug-in kann Daten aus mehreren vom System bereitgestellten Logcat-Puffern sammeln. Dabei handelt es sich um Haupt-, Ereignis-, Funk- und Systempuffer. Sofern nicht anders angegeben, stehen die einzelnen Einstellungen für den jeweiligen Puffer unabhängig zur Verfügung.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log path (Protokollpfad): Legt den allgemeinen Protokollpfad für die Speicherung aller Logcat-Protokolle fest. Diese Einstellung gilt global für alle Logcat-Puffer.
- Enable main logcat (Logcat für Hauptpuffer aktivieren): Aktiviert die Protokollierung für diesen Logcat-Puffer.
  - **Main Log interval (sec)** (Intervall für Hauptpuffer-Protokoll in Sekunden): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
  - **Main Log filename** (Name der Hauptpuffer-Protokolldatei): Legt den Basisdateinamen des Protokolls für diesen Logcat-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
  - Main Log file count (Anzahl der Hauptpuffer-Protokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
  - Main log file size (MB) (Größe der Hauptpuffer-Protokolldatei in MB): Gibt die maximale Größe einer einzelnen Protokolldatei in Megabyte an.
  - **Main log filter** (Filter für Hauptpufferprotokoll): Benutzerdefinierter Logcat-Filter zur Ausführung auf dem Hauptpuffer.
- **Enable main logcat** (Logcat für Ereignispuffer aktivieren): Aktiviert die Protokollierung für diesen Logcat-Puffer.
  - Event log interval (sec) (Intervall für Ereignispuffer in Sekunden): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
  - Event log filename (Name der Ereignispuffer-Protokolldatei): Legt den Basisdateinamen des Protokolls für diesen Logcat-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
  - Event log file count (Anzahl der Ereignispuffer-Protokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
  - Event log file size (MB) (Größe der Ereignispuffer-Protokolldatei in MB): Gibt die maximale Größe einer einzelnen Protokolldatei in Megabyte an.
  - Event log filter (Filter für Ereignispufferprotokoll): Benutzerdefinierter Logcat-Filter zur Ausführung auf dem Ereignispuffer.

- **Enable radio logcat** (Logcat für Funkpuffer aktivieren): Aktiviert die Protokollierung für diesen Logcat-Puffer.
  - Radio Log interval (sec) (Intervall für Funkpuffer-Protokoll in Sekunden): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei gelöscht werden soll.
  - Radio Log filename (Name der Funkpuffer-Protokolldatei): Legt den Basisdateinamen des Protokolls für diesen Logcat-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
  - Radio Log file count (Anzahl der Funkpuffer-Protokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
  - Radio log file size (MB) (Größe der Funkpuffer-Protokolldatei in MB): Gibt die maximale Größe einer einzelnen Protokolldatei in Kilobyte an.
  - Radio log filter (Filter für Funkpufferprotokoll): Benutzerdefinierter Logcat-Filter zur Ausführung auf dem Funkpuffer.
- **Enable radio logcat** (Logcat für Systempuffer aktivieren): Aktiviert die Protokollierung für diesen Logcat-Puffer.
  - System Log interval (sec) (Intervall für Systempuffer-Protokoll in Sekunden): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
  - **System Log filename** (Name der Systempuffer-Protokolldatei): Legt den Basisdateinamen des Protokolls für diesen Logcat-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
  - System Log file count (Anzahl der Systempuffer-Protokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
  - System log file size (MB) (Größe der Systempuffer-Protokolldatei in MB): Gibt die maximale Größe einer einzelnen Protokolldatei in Kilobyte an.
  - System log filter (Systemprotokollfilter): Benutzerdefinierter Logcat-Filter, der im Systempuffer ausgeführt wird.
- Enable crash logcat (Logcat f
  ür Absturz aktivieren): Aktiviert die Protokollierung f
  ür diesen Logcat-Absturzpuffer.
  - Crash log interval (sec) (Intervall für Absturzprotokoll in Sekunden): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
  - Crash log filename (Name der Absturzprotokolldatei): Legt den Basisdateinamen des Protokolls für diesen Logcat-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
  - Crash log file count (Anzahl der Absturzprotokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
  - Crash log file size (MB) (Größe der Hauptpuffer-Protokolldatei in MB): Gibt die maximale Größe einer einzelnen Protokolldatei in Megabyte an.
  - Crash log filter (Filter für Absturzprotokoll): Benutzerdefinierter Logcat-Filter zur Ausführung auf dem Absturzpuffer.

- **Enable combined logcat** (Kombinierte Logcat-Datei aktivieren): Aktiviert die Protokollierung für diesen Logcat-Puffer.
  - Enable main buffer (Hauptpuffer aktivieren): Aktiviert oder deaktiviert das Hinzufügen des Hauptpuffers zur kombinierten Logcat-Datei.
  - Enable event buffer (Ereignispuffer aktivieren): Aktiviert oder deaktiviert das Hinzufügen des Ereignispuffers zur kombinierten Logcat-Datei.
  - Enable radio buffer (Funkpuffer aktivieren): Aktiviert oder deaktiviert das Hinzufügen des Funkpuffers zur kombinierten Logcat-Datei.
  - Enable system buffer (Systempuffer aktivieren): Aktiviert oder deaktiviert das Hinzufügen des Systempuffers zur kombinierten Logcat-Datei.
  - Enable crash buffer (Absturzpuffer aktivieren): Aktiviert oder deaktiviert das Hinzufügen des Absturzpuffers zur kombinierten Logcat-Datei.
  - **Combine log interval (sec)** (Intervall für kombinierte Protokolldatei in Sekunden): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
  - **Combined log filename** (Name der kombinierten Protokolldatei): Legt den Basisdateinamen des Protokolls für diesen Logcat-Puffer fest. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
  - **Combined log file count** (Anzahl der kombinierten Protokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
  - **Combined log file size (MB)** (Größe der kombinierten Protokolldatei in MB): Gibt die maximale Größe einer einzelnen Protokolldatei in Megabyte an.
  - **Combined log filter** (Filter für kombiniertes Protokoll): Benutzerdefinierter Logcat-Filter zur Ausführung auf dem kombinierten Puffer.

## LTS-Modul

Das LTS-Modul (Long Term Storage) erfasst Daten über einen längeren Zeitraum, ohne dass dabei Daten verloren gehen. Wenn eine Datei geschrieben wurde, wird sie über LTS als GZ-Datei in einem verwalteten Pfad zur späteren Verwendung gespeichert.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- **Storage Directory** (Speicherverzeichnis): Legt den allgemeinen Protokollpfad für die Speicherung aller Logcat-Protokolle fest. Diese Einstellung gilt global für alle Logcat-Puffer.

#### **Ramoops-Modul**

Das Ramoops-Modul erfasst die letzte Kernel-Meldung des Geräts.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log path (Protokollpfad): Legt den allgemeinen Protokollpfad für die Speicherung aller ramoops-Protokolle fest. Diese Einstellung gilt global für alle Ramoops-Puffer.
- **Base filename** (Basisdateiname): Gibt den Basisprotokolldateinamen für diesen Kernel-Puffer an. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
- Ramoops log file count (Anzahl der Ramoops-Dateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte Protokollgröße.

## Ressourcenmodul

Das Ressourcenmodul erfasst Geräteinformationen und Systemstatistiken in festgelegten Intervallen. Die Daten werden verwendet, um den Zustand des Geräts über einen bestimmten Zeitraum hinweg zu erfassen.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log Path (Protokollpfad): Legt den allgemeinen Protokollpfad für die Speicherung aller Ressourcenprotokolle fest. Diese Einstellung gilt global für alle Ressourcenpuffer.
- **Resource Log interval** (Intervall des Ressourcenprotokolls): Legt das Intervall in Sekunden fest, in dem der Protokollpuffer in die Datei geleert werden soll.
- **Resource Log file size** (Größe der Ressourcen-Protokolldatei): Gibt die maximale Größe einer einzelnen Protokolldatei in Megabyte an.
- Resource Log file count (Anzahl der Ressourcenprotokolldateien): Gibt die Anzahl der Protokolldateien an, die beibehalten und durchlaufen werden sollen. Für jede Protokolldatei gilt die in der entsprechenden Option festgelegte maximale Protokollgröße.
- **System Resource** (Systemressource): Aktiviert oder deaktiviert die Erfassung von Systemressourceninformationen.
- Network (Netzwerk): Aktiviert oder deaktiviert die Erfassung des Netzwerkstatus.
- Bluetooth: Aktiviert oder deaktiviert die Erfassung von Bluetooth-Informationen.
- Light (Light): Aktiviert oder deaktiviert die Erfassung der Umgebungshelligkeit.
- Heater (Heizung): nicht unterstützt.

## **Snapshot-Modul**

Das Snapshot-Modul erfasst in regelmäßigen Abständen detaillierte Gerätestatistiken, über die Sie genaue Informationen zu Geräten erhalten.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log Path (Protokollpfad): Gibt den Basispfad zum Speichern der Snapshot-Dateien an.
- Log filename (Protokolldateiname): Gibt den Basisdateinamen für alle Snapshot-Dateien an. Die aktuelle Dateianzahl wird an diesen Namen angehängt.
- Log Interval (sec) (Protokollintervall in Sekunden): Gibt das Intervall in Sekunden an, zu dem ein detaillierter Snapshot aufgerufen werden soll.
- Snapshot file count (Anzahl der Snapshot-Dateien): Die maximale Anzahl an Snapshot-Dateien, die gleichzeitig beibehalten werden können.
- Top (Oben): Aktiviert oder deaktiviert die Ausführung des Befehls top für die Datenerfassung.
- CPU Info (CPU-Info): Aktiviert die detaillierte prozessbezogene CPU-Protokollierung im Snapshot.
- **Memory Info** (Speicherinformationen): Aktiviert die Protokollierung der detaillierten prozessbezogenen Speichernutzung im Snapshot.
- Wake Locks: Aktiviert oder deaktiviert die Sammlung von sys/fs wake\_lock-Informationen.
- Time in State (Zeit im Zustand): Aktiviert oder deaktiviert die Sammlung von sys/fs cpufreq für jeden Kern.
- **Processes** (Prozesse): Ermöglicht das Erstellen eines Speicherauszugs der vollständigen Prozessliste im Snapshot.
- Threads: Ermöglicht das Erstellen eines Speicherauszugs für alle Prozesse und deren Threads im Snapshot.
- **Properties** (Eigenschaften): Ermöglicht das Erstellen eines Speicherauszugs aller Systemeigenschaften auf dem Gerät. Dazu gehören Build-/Versionsinformationen sowie Statusinformationen.
- Interfaces (Schnittstellen): Aktiviert oder deaktiviert die Ausführung des Befehls netcfg für die Datenerfassung.
- IP Routing Table (IP-Routing-Tabelle): Aktiviert oder deaktiviert die Erfassung der Netzroute für die Datenerfassung.
- **Connectivity** (Konnektivität): Aktiviert oder deaktiviert die Ausführung des Befehls dumpsys connectivity für die Datenerfassung.

- Wifi: Aktiviert oder deaktiviert die Ausführung des Befehls dumpsys wifi für die Datenerfassung.
- File systems (Dateisysteme): Ermöglicht das Erstellen eines Speicherauszugs der verfügbaren Volumes im Dateisystem und des freien Speicherplatzes für jedes Volume.
- Usage stats (Nutzungsstatistiken): Ermöglicht das Erstellen eines Speicherauszugs detaillierter Nutzungsinformationen für jedes Paket auf dem Gerät. Dazu gehören die Anzahl der Starts und die Dauer jedes Durchlaufs.

## **TCPDump-Modul**

Das TCPDump-Modul erfasst TCP-Daten, die über die Netzwerke des Geräts übertragen werden.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log path (Protokollpfad): Gibt den Speicherort zum Speichern der TCPDump-Ausgabeprotokolldateien an.
- Base filename (Basisdateiname): Gibt den Basisdateinamen an, der zum Speichern der TCPDump-Dateien verwendet werden soll. Die Indexnummer der aktuellen Protokolldatei wird an den Dateinamen angehängt.
- **Tcpdump file size (MB)** (Größe der Tcpdump-Datei): Gibt die maximale Dateigröße in Megabyte für jede erstellte Protokolldatei an.
- Tcpdump file count (Anzahl der Tcpdump-Dateien): Gibt die Anzahl der Protokolldateien an, die beim Speichern der Netzwerkverfolgungen durchlaufen werden sollen.

#### **Tombstone-Modul**

Das Tombstone-Modul sammelt Tombstone-Protokolle (Linux Native Crashes) von einem Gerät.

- Enable Module (Modul aktivieren): Aktiviert die Protokollierung für dieses Modul.
- Log path (Protokollpfad): Gibt den Speicherort zum Speichern der Tombstone-Ausgabeprotokolldateien an.
- **Collect Historic tombstones** (Tombstone-Verlaufsdaten erfassen): Sammelt neue und vorhandene Tombstone-Dateien.

## Konfigurationsdatei

Die Konfiguration von RxLogger kann mithilfe einer XML-Datei festgelegt werden. Die Konfigurationsdatei config.xml befindet sich auf der microSD-Karte im Ordner RxLogger\config. Kopieren Sie die Datei vom Gerät über eine USB-Verbindung auf einen Host-Computer. Bearbeiten Sie die Konfigurationsdatei, und ersetzen Sie dann die XML-Datei auf dem Gerät. Der RxLogger Service muss nicht angehalten und neu gestartet werden, da die Dateiänderung automatisch erkannt wird.

# Aktivieren der Protokollierung

So aktivieren Sie die Protokollierung:

- 1. Wischen Sie auf dem Bildschirm nach oben, und wählen Sie 🚱 aus.
- 2. Berühren Sie Start (Starten).
- 3. Berühren Sie O.

## Deaktivieren der Protokollierung

So deaktivieren Sie die Protokollierung:

- 1. Wischen Sie auf dem Bildschirm nach oben, und wählen Sie 🚯 aus.
- 2. Berühren Sie Stop (Stoppen).
- Berühren Sie O.

# Extrahieren von Protokolldateien

- 1. Schließen Sie das Gerät über eine USB-Verbindung an einen Host-Computer an.
- 2. Navigieren Sie mithilfe des Datei-Explorers zum Ordner RxLogger.
- 3. Kopieren Sie die Datei vom Gerät auf den Host-Computer.
- 4. Trennen Sie das Gerät vom Host-Computer.

## **RxLogger-Dienstprogramm**

Das RxLogger-Dienstprogramm ist eine Überwachungsanwendung zum Anzeigen von Protokollen auf dem Gerät, während RxLogger ausgeführt wird. Der Zugriff auf die Protokolle und RxLogger-Dienstprogrammfunktionen ist in der App-Ansicht oder Overlay-Ansicht möglich.

# **App-Ansicht**

In der App-Ansicht können Protokolle im RxLogger-Dienstprogramm angezeigt werden.



#### Abbildung 33 App-Ansicht

## Anzeigen von Protokollen

So zeigen Sie Protokolle an:

1. Berühren Sie das Symbol für den Haupt-Chat-Head. Der Bildschirm mit der Overlay-Ansicht wird angezeigt.

gerUtility	
Logcat	~
Snapshots	~
Kernel Log	*
Resource	*

Abbildung 34 Bildschirm mit Overlay-Ansicht

- 2. Berühren Sie ein Protokoll, um es zu öffnen. Es können mehrere Protokolle geöffnet werden, für die jeweils ein neuer untergeordneter Chat-Head angezeigt wird.
- 3. Scrollen Sie bei Bedarf nach links oder rechts, um weitere Symbole für untergeordnete Chat-Heads anzuzeigen.
- 4. Berühren Sie einen untergeordneten Chat-Head, um die Protokollinhalte anzuzeigen.

#### Abbildung 35 Protokolldatei

<3> [ 218.085848] send_adm_cal_block: DSP returned error[ADSP_EUNSUPPORTED]
<6> [ 222.850030] ddd: timestamp 2018-10-02 17:29:58:948
<3> [ 223.619498] adm_callback: cmd = 0x10328 returned error = 0x3
<3> [ 223.624220] send_adm_cal_block: DSP returned error[ADSP_EUNSUPPORTED]
<6> [ 232.848958] ddd: timestamp 2018-10-02 17:30:08:947
<3> [ 242.412613] adm_callback: cmd = 0x10328 returned error = 0x3
<3> [ 242.417309] send_adm_cal_block: DSP returned error[ADSP_EUNSUPPORTED]
<6> [ 242.848787] ddd: timestamp 2018-10-02 17:30:18:947
<6> [ 252.849570] ddd: timestamp 2018-10-02 17:30:28:948
<3> [ 256.906434] adm_callback: cmd = 0x10328 returned error = 0x3
<3> [ 256.911172] send_adm_cal_block: DSP returned error[ADSP_EUNSUPPORTED]

### Backup

Mit dem Dienstprogramm RxLogger kann eine ZIP-Datei des Ordners RxLogger im Gerät erstellt werden, die standardmäßig alle im Gerät gespeicherten RxLogger-Protokolle enthält.

Um die Backupdaten zu speichern, berühren Sie BACKUP > Yes (Ja).

#### Abbildung 36 Backup-Meldung

Backup Now	
You are going to take backup of to push RxLogger directory. Do want to continue?	of logs o you
CANCEL	YES

#### Archivieren von Daten

Sie können alle RxLogger-Protokolle anzeigen, die im Standardverzeichnis von **RxLogger** gespeichert sind. Im Archivfenster angezeigte Protokolle sind nicht live.

Abbildung 3	37 Archiv
-------------	-----------

Archive	
Crash0.txt	
Event0.txt	
KLog0.txt	
Main0.txt	
Radio0.txt	
Resource0.csv	
System0.txt	
snapshot0.txt	

Um die Protokolldateien anzuzeigen, berühren Sie **ARCHIVE DATA** (Daten archivieren) und dann eine Protokolldatei.

# **Overlay-Ansicht**

Verwenden Sie die Overlay-Ansicht, um Informationen zu RxLogger anzuzeigen, während Sie andere Apps oder den Startbildschirm verwenden. Der Zugriff auf die Overlay-Ansicht erfolgt über den Haupt-Chat-Head.

## **Starten des Haupt-Chat-Heads**

So starten Sie den Haupt-Chat-Head:

- 1. Öffnen Sie **RxLogger**.
- 2. Berühren Sie **> Toggle Chat Head** (Chat-Head ein/aus). Das Symbol für den Haupt-Chat-Head wird auf dem Bildschirm angezeigt.
- 3. Berühren Sie das Symbol, und ziehen Sie es, um es auf dem Bildschirm zu verschieben.

#### **Entfernen des Haupt-Chat-Heads**

So entfernen Sie das Symbol für den Haupt-Chat-Head:

- 1. Berühren und ziehen Sie das Symbol. Ein Kreis mit einem X wird angezeigt.
- 2. Bewegen Sie das Symbol über den Kreis, und lassen Sie es anschließend los.

#### Anzeigen von Protokollen

So zeigen Sie Protokolle an:

1. Berühren Sie das Symbol für den Haupt-Chat-Head. Der Bildschirm mit der Overlay-Ansicht wird angezeigt.

Abbildung 38	Bildschirm mit Overla	y-Ansicht
--------------	-----------------------	-----------

B B gerUtility	
Logcat	~
Snapshots	~
Kernel Log	٠
Resource	\$

- 2. Berühren Sie ein Protokoll, um es zu öffnen. Es können mehrere Protokolle geöffnet werden, für die jeweils ein neuer untergeordneter Chat-Head angezeigt wird.
- Scrollen Sie bei Bedarf nach links oder rechts, um weitere Symbole f
  ür untergeordnete Chat-Heads anzuzeigen.

4. Berühren Sie einen untergeordneten Chat-Head, um die Protokollinhalte anzuzeigen.

Abbildung 39 P	Protokolldatei
Radio Kernel Log 1 Resource J1	
<3> [ 218.085848] send_adr returned error[ADSP_EUNSUF	n_cal_block: DSP PPORTED]
<6> [ 222.850030] ddd: time 17:29:58:948	estamp 2018-10-02
<3> [ 223.619498] adm_call returned error = 0x3	back: cmd = 0x10328
<3> [ 223.624220] send_adr returned error[ADSP_EUNSUF	n_cal_block: DSP PPORTED]
<6> [ 232.848958] ddd: time 17:30:08:947	estamp 2018-10-02
<3> [ 242.412613] adm_call returned error = 0x3	back: cmd = 0x10328
<3> [ 242.417309] send_adr returned error[ADSP_EUNSUF	n_cal_block: DSP PPORTED]
<6> [ 242.848787] ddd: time 17:30:18:947	estamp 2018-10-02
<6> [ 252.849570] ddd: time 17:30:28:948	estamp 2018-10-02
<3> [ 256.906434] adm_call returned error = 0x3	back: cmd = 0x10328
<3> [ 256.911172] send_adr returned error[ADSP_EUNSUF	n_cal_block: DSP PPORTED]

#### Entfernen eines Symbols für einen untergeordneten Chat-Head

Um ein Symbol für einen untergeordneten Chat-Head zu entfernen, halten Sie das Symbol gedrückt, bis es nicht mehr angezeigt wird.

#### Backup in der Overlay-Ansicht durchführen

Mit dem Dienstprogramm RxLogger kann eine ZIP-Datei des Ordners RxLogger im Gerät erstellt werden, die standardmäßig alle im Gerät gespeicherten RxLogger-Protokolle enthält.

Das Backup-Symbol ist in der Overlay-Ansicht immer verfügbar.

- 1. Berühren Sie 💾. Das Dialogfeld "Backup" wird angezeigt.
- 2. Berühren Sie Yes (Ja), um das Backup zu erstellen.

# Telefoninfo

Verwenden Sie Einstellungen unter About phone (Telefoninfo), um Informationen über das Gerät anzuzeigen. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend **‡** > **System** > **About phone** (Telefoninfo).

- Status: Berühren Sie diese Option, um Folgendes anzuzeigen:
  - **IP Address** (IP-Adresse): Die aktuelle IP-Adresse des Geräts.
  - Wi-Fi MAC address (WLAN-MAC-Adresse): Zeigt die MAC-Adresse des WLAN-Funkgeräts an.
  - WLAN-MAC-Adresse (Ethernet-MAC-Adresse): Zeigt die MAC-Adresse des Ethernet-Treibers an.
  - Bluetooth address (Bluetooth-Adresse): Zeigt die Bluetooth-Adresse des Bluetooth-Funkgeräts an.
  - Serial number (Seriennummer): Zeigt die Seriennummer des Geräts an.
  - **MSM serial number** (MSM-Seriennummer): Zeigt die Seriennummer des MSM an.
  - Up time (Betriebszeit): Zeigt die Betriebszeit des Geräts seit dem Einschalten an.
- **SW components** (SW-Komponenten): Führt Dateinamen und Versionen der auf dem Gerät installierten Software auf.
  - Audio
  - Akustik
  - MX
  - Hardware-ID
  - NFC
  - Scanner
  - Touch
  - Build-Datum
  - Geräteaktualisierungsversion
  - Baseline
  - Sicherer Startzustand
  - ABL ARB-Version
  - Verbleibende Neustarts bis zum Sperren
- Legal information (Rechtliche Hinweise): Öffnet einen Bildschirm, in dem rechtliche Informationen zur auf dem Gerät enthaltenen Software angezeigt werden.
  - Drittanbieterlizenzen
  - Google Legal
  - System WebView-Lizenzen
  - Wallpaper
  - Zebra EULA
- Model (Modell): Zeigt die Modellnummer des Geräts an.
- Android Version (Android-Version): Zeigt die Version des Betriebssystems an.
- Android security patch level (Android-Sicherheitspatchebene): Zeigt das Datum der Sicherheitspatchebene an.
- **Baseband version** (Basisband-Version): Zeigt die Firmware-Version der WAN-Funkverbindung an (nur WWAN).
- Kernel Version (Kernel-Version): Zeigt die Kernel-Versionsnummer an.
- **Build Fingerprint** (Build-Fingerabdruck): Definiert Gerätehersteller, Modell, Android-Version und Build-Version an einem Ort.
- Build number (Buildnummer): Zeigt die Software Build-Nummer an.

# USB/Ethernet-Kommunikation

# Einführung

In diesem Kapitel werden die Verwendung und Konfiguration der USB-Anschlüsse und der Ethernet-Verbindung beschrieben.

Das CC6000 verfügt über zwei USB-2-Anschlüsse für externe Peripheriegeräte und einen USB-C-Anschluss, der für OTG oder einen externen Monitor verwendet werden kann.

Das CC600 enthält einen USB-C-Anschluss, der als OTG-Anschluss verwendet werden oder an einen externen Monitor oder USB-Peripheriegeräte angeschlossen werden kann (für den gleichzeitigen Anschluss ist ein Splitter erforderlich).

# Übertragen von Dateien mit einem Host-Computer über USB

Schließen Sie das Gerät über ein USB-Kabel an einen Host-Computer an, um Dateien zwischen dem Gerät und dem Host-Computer zu übertragen.

Beim Anschließen des Geräts an einen Host-Computer sind die für den Host-Computer geltenden Anweisungen zum Anschließen und Trennen von USB-Geräten zu befolgen, um die Beschädigung oder Zerstörung von Dateien zu vermeiden.

# Übertragen von Dateien



**HINWEIS:** Verwenden Sie zum Kopieren von Dateien zwischen dem Gerät (interner Speicher oder microSD-Karte) und dem Host-Computer die Option "Transfer files" (Dateien übertragen).

1. Schließen Sie ein USB-Kabel an das Gerät an.

2. Ziehen Sie das Benachrichtigungsfeld nach unten, und berühren Sie "**USB connect this device**" (Dieses Gerät über USB verbinden).

Standardmäßig ist "Connect this device" (Dieses Gerät verbinden) ausgewählt.

Abbildung 40 Dialogfeld "Use USB to" (USB für folgenden Zweck verwenden)

Use USB to	
Onnect this device	
○ Transfer files	
○ Transfer photos (PTP)	
◯ Use device as MIDI	
	CANCEL

- 3. Berühren Sie Transfer files (Dateien übertragen).
- 4. Öffnen Sie auf dem Host-Computer eine Anwendung zur Dateisuche.
- 5. Suchen Sie das Gerät als mobiles Gerät.
- 6. Öffnen Sie den Ordner SD card (SD-Karte) oder Internal storage (Interner Speicher).
- 7. Kopieren Sie Dateien zum und vom Gerät, oder löschen Sie Dateien nach Bedarf.

# Übertragen von Fotos

So übertragen Sie mit dem Photo Transfer Protocol Fotos:



**HINWEIS:** Verwenden Sie das Photo Transfer Protocol (PTP) zum Kopieren von Fotos von der MicroSD-Karte oder vom internen Speicher zum Host-Computer.

- 1. Schließen Sie das USB-Kabel an das Gerät an. (Informationen zu den Kommunikationsports finden Sie unter Merkmale auf Seite 16.)
- 2. Ziehen Sie das Benachrichtigungsfeld nach unten, und berühren Sie "**USB connect this device**" (Dieses Gerät über USB verbinden).
- 3. Berühren Sie Transfer photos (PTP) (Fotos übertragen (PTP)).
- 4. Öffnen Sie auf dem Host-Computer eine Anwendung zur Dateisuche.
- 5. Öffnen Sie den Ordner SD card (SD-Karte) oder Internal storage (Interner Speicher).
- 6. Kopieren oder löschen Sie Fotos nach Bedarf.

# **Trennen vom Host-Computer**

So trennen Sie das Gerät vom Host Computer:



**VORSICHT:** Befolgen Sie die für den Host-Computer geltenden Anweisungen zum Deaktivieren der microSD-Karte, und trennen Sie die USB-Geräte ordnungsgemäß, um Informationsverluste zu vermeiden.

- 1. Deaktivieren Sie das Gerät auf dem Host-Computer.
- 2. Entfernen Sie das USB-Kabel vom Gerät.

# **USB/Ethernet-Kommunikation**

Schließen Sie für die PoE-Kommunikation (Ethernet) ein Ethernet-Kabel an den Anschluss 👫 an.

Schließen Sie für die USB-Kommunikation ein USB-Kabel an den Anschluss eqrapsilon an.

## **Ethernet-Einstellungen**

Die folgenden Einstellungen können bei Verwendung der Ethernet-Kommunikation konfiguriert werden:

- Proxy-Einstellungen
- Statische IP-Adresse.

## Konfigurieren der Ethernet-Proxyeinstellungen



HINWEIS: Ethernet ist für das Gerät standardmäßig aktiviert.

So konfigurieren Sie die Ethernet-Verbindung:

- 1. Schließen Sie das eine Ende des Ethernet-Kabels an den PoE-Anschluss des Geräts an.
- 2. Schließen Sie das andere Ende an eine aktive Ethernet-Buchse oder einen aktiven Ethernet-Hub an.
- 3. Wischen Sie mit zwei Fingern von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 4. Berühren Sie Network & Internet (Netzwerk und Internet).
- 5. Berühren Sie Ethernet.
- 6. Schieben Sie den Schalter in die Position ON (EIN).
- 7. Berühren und halten Sie Eth0, bis das Menü angezeigt wird.
- 8. Berühren Sie Modify Proxy (Proxy ändern).
- 9. Berühren Sie die Drop-down-Liste Proxy, und wählen Sie Manual (Manuell).

#### Abbildung 41 Ethernet-Proxyeinstellungen

$\langle \! \cdots \!  angle$ eth0		
Proxy Manual		-
Proxy hostname		
proxy.example.cc	m	
Proxy port		
8080		
Bypass proxy for		
example.com,my	comp.tes	st.com,l
	CANCEL	MODIFY

- 10. Geben Sie im Feld Proxy hostname (Proxy-Hostname) die Adresse des Proxyservers ein.
- 11. Geben Sie im Feld Proxy port (Proxy-Portnummer) die Portnummer des Proxyservers ein.



**HINWEIS:** Bei der Eingabe von Proxyadressen in das Feld "Bypass proxy for" (Proxy umgehen für) dürfen Sie keine Leerzeichen oder Zeilenumbrüche zwischen

Adressen eingeben.

- 12. Geben Sie im Textfeld **Bypass proxy for** (Proxy umgehen für) Adressen für Websites ein, die nicht über den Proxyserver verlaufen müssen. Verwenden Sie das Trennzeichen "I" zwischen den Adressen.
- 13. Berühren Sie MODIFY (Ändern).
- 14.Berühren Sie 🔘.

## Konfigurieren von statischen IP-Adressen für Ethernet

So konfigurieren Sie eine statische IP-Adresse für Ethernet:

- 1. Wischen Sie mit zwei Fingern von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Network & Internet (Netzwerk und Internet).
- 3. Berühren Sie Ethernet.
- 4. Schieben Sie den Schalter in die Position ON (EIN).
- 5. Berühren Sie Eth0.
- 6. Berühren Sie die Drop-down-Liste IP settings (IP-Einstellungen), und wählen Sie Static (Statisch) aus.

Abbildung 42 Statische IP-Einstellungen

<⊷> eth0	
Proxy None	*
IP settings Static	•
IP address	
192.168.1.128	
Gateway	
192.168.1.1	
Netmask	
255.255.255.0	
DNS 1	
8.8.8.8	
DNS 2	
4.4.4.4	

CANCEL CONNECT

- 7. Geben Sie im Feld IP address (IP-Adresse) die Adresse des Proxyservers ein.
- 8. Geben Sie gegebenenfalls im Feld Gateway eine Gateway-Adresse für das Gerät ein.
- 9. Geben Sie gegebenenfalls im Feld Netmask (Netzmaske) die Adresse der Netzwerkmaske ein.
- 10. Geben Sie gegebenenfalls in den DNS-Adressfeldern die Domain Name System (DNS)-Adressen ein.
- 11.Berühren Sie **CONNECT** (Verbinden).
- 12.Berühren Sie 🔘.

## Herstellen der Ethernet-Verbindung

- 1. Wischen Sie mit zwei Fingern von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Network & Internet (Netzwerk und Internet).
- 3. Berühren Sie Ethernet.
- 4. Setzen Sie das Gerät in einen Steckplatz ein.
- 6. Tippen Sie auf Eth0, um Details zur Ethernet-Verbindung anzuzeigen.

# DataWedge

# Einführung

Dieses Kapitel bezieht sich auf DataWedge auf Android-Geräten. DataWedge ist eine Anwendung, die Daten liest, verarbeitet und an eine Anwendung sendet.

# **Grundlegendes Scannen**

Der Scanvorgang kann über den Portierdienst des CC600 und CC6000 oder einen Imager wie den DS22X8 oder den DS81X8 durchgeführt werden.

# Erfassen von Barcodes per Imager

So erfassen Sie Barcode-Daten über den Portierdienst des CC600/CC6000.

- 1. Stellen Sie sicher, dass auf dem Gerät eine Anwendung geöffnet ist und sich ein Textfeld im Fokus befindet (Textcursor in Textfeld).
- 2. Platzieren Sie den Barcode so, dass das Scanfenster des Geräts diesen erfassen kann. Achten Sie darauf, dass sich der Barcode innerhalb des Lasermusters des Scanners befindet.
- 3. Die LEDs leuchten grün, und ein Signalton ertönt standardmäßig, wenn der Barcode erfolgreich decodiert wurde. Wenn sich das Gerät im Entnahmelistenmodus befindet, decodiert das Gerät den Barcode solange nicht, bis die Mitte der leuchtenden Zeile oder des Punktes den Barcode berührt.

So erfassen Sie Barcode-Daten über den Imager DS22X8 oder DS81X8:

- 1. Stellen Sie sicher, dass auf dem Gerät eine Anwendung geöffnet ist und sich ein Textfeld im Fokus befindet (Textcursor in Textfeld).
- 2. Halten Sie die Auslösetaste gedrückt, bis eine der folgenden Möglichkeiten zutrifft:
  - a. Der Bildscanner liest den Barcode. Der Scanner gibt einen Piepton aus, die LED blinkt, und die Scanzeile wird ausgeschaltet.

oder

b. Der Bildscanner liest den Barcode nicht, und die Scanzeile wird ausgeschaltet.

Wenn sich das Gerät im Entnahmelistenmodus befindet, decodiert das Gerät den Barcode solange nicht, bis die Mitte der leuchtenden Zeile oder des Punktes den Barcode berührt.

## DataWedge

#### Abbildung 43 Zielmuster auf Barcode – DS22X8 und DS81X8



- 3. Lassen Sie den Auslöser los.
- 4. Der Inhalt des Barcodes wird im Textfeld angezeigt.

# Profile

DataWedge basiert auf Profilen und Plug-ins. Ein Profil enthält Informationen darüber, wie sich DataWedge in Bezug auf verschiedene Anwendungen verhalten soll.

Die Profilinformationen umfassen:

- Zugeordnete Anwendungen
- Data Capture Plus-Konfigurationen
- · Konfigurationen des Eingabe-Plug-ins
- Konfigurationen des Ausgabe-Plug-ins
- Konfigurationen des Verarbeitungs-Plug-ins

Mithilfe von Profilen kann für jede Anwendung eine spezifische DataWedge-Konfiguration definiert werden. Beispielsweise kann jede Benutzeranwendung ein Profil aufweisen, das gescannte Daten im erforderlichen Format ausgibt, wenn diese Anwendung im Vordergrund ausgeführt wird. DataWedge kann so konfiguriert werden, dass derselbe Satz erfasster Daten je nach Anforderungen der jeweiligen Anwendung unterschiedlich verarbeitet wird.

DataWedge enthält die folgenden vorkonfigurierten Profile zur Unterstützung integrierter Anwendungen:

- Sichtbare Profile:
  - Profile0 (Profil0): Wird beim ersten Ausführen von DataWedge automatisch erstellt. Es handelt sich um ein generisches Profil, das verwendet wird, wenn keine vom Benutzer erstellten Profile mit einer Anwendung verknüpft sind.
  - Launcher (Startprogramm): Ermöglicht das Scannen, wenn das Startprogramm im Vordergrund ausgeführt wird.
  - **DWDemo**: Bietet Unterstützung für die DWDemo-Anwendung.

Einige Zebra-Anwendungen können Daten durch Scannen erfassen. Zu diesem Zweck bietet DataWedge vorinstallierte private und verborgene Profile. Es gibt keine Möglichkeit, diese privaten Profile zu ändern.

## Profil0

**Profil0** kann bearbeitet, aber nicht mit einer Anwendung verknüpft werden. Das heißt **DataWedge** ermöglicht die Bearbeitung von Plug-in-Einstellungen für **Profil0**, erlaubt jedoch keine Zuweisung einer im Vordergrund ausgeführten Anwendung. Mit dieser Konfiguration kann **DataWedge** Ausgabedaten an alle Vordergrundanwendungen senden, die nicht mit benutzerdefinierten Profilen verknüpft sind, wenn **Profil0** aktiviert ist.

**Profil0** kann deaktiviert werden, damit **DataWedge** nur Ausgabedaten an Anwendungen senden kann, die mit benutzerdefinierten Profilen verknüpft sind. Sie können beispielsweise ein Profil erstellen, das einer bestimmten Anwendung zugeordnet ist, **Profil0** deaktivieren und dann den Scan durchführen. **DataWedge** sendet nur Daten an die Anwendung, die in dem vom Benutzer erstellten Profil angegeben ist. Dies erhöht die Sicherheit von **DataWedge** und ermöglicht, dass Daten nur an bestimmte Anwendungen gesendet werden.

# **Plug-ins**

Ein Plug-in ist ein Softwaremodul, das verwendet wird, um die DataWedge-Funktionalität auf Technologien wie das Scannen von Barcodes zu erweitern. Die Plug-ins können basierend auf den von ihnen ausgeführten Funktionen in drei Typen eingeteilt werden:

- Eingabe-Plug-ins
- Ausgabe-Plug-ins
- Verarbeitungs-Plug-ins

# **Eingabe-Plug-ins**

Ein Eingabe-Plug-in unterstützt ein Eingabegerät, z. B. einen Barcodescanner, der in einem Gerät enthalten bzw. an ein Gerät angeschlossen ist. **DataWedge** enthält Basis-Plug-ins für diese Eingabegeräte.



**WICHTIG:** Eingabe-Plug-in für Barcodescanner: Das Eingabe-Plug-in für Barcodescanner ist für das Lesen von Daten aus dem integrierten Barcodescanner zuständig und unterstützt verschiedene Arten von Barcodelesegeräten wie Laser, Imager und interne Kameras. Vom Barcodescanner gelesene Rohdaten können nach Bedarf mithilfe der entsprechenden Verarbeitungs-Plug-ins verarbeitet oder formatiert werden. DataWedge verfügt über eine integrierte Feedback-Funktion, mit der der Barcodescanner Benutzerwarnungen ausgeben kann. Die Feedbackeinstellungen können entsprechend den Benutzeranforderungen konfiguriert werden.

# Verarbeitungs-Plug-ins

Verarbeitungs-Plug-ins werden in **DataWedge** verwendet, um die empfangenen Daten gemäß den Anforderungen zu bearbeiten, bevor sie über das Ausgabe-Plug-in an die Vordergrundanwendung gesendet werden.

- Plug-in für die erweiterte Datenformatierung: Mit dem Plug-in für die erweiterte Datenformatierung kann DataWedge Regeln (Aktionen, die auf Grundlage definierter Kriterien durchgeführt werden sollen) auf die über ein Eingabe-Plug-in empfangenen Daten anwenden, bevor sie an ein Ausgabe-Plug-in übergeben werden.

# Ausgabe-Plug-ins

Ausgabe-Plug-ins sind dafür zuständig, die Daten der Eingabe-Plug-ins an eine Vordergrundanwendung auf dem Gerät zu senden.

- Plug-in f
  ür die Tastenanschlag-Ausgabe: Das Plug-in f
  ür die Tastenanschlag-Ausgabe sammelt und sendet Daten, die vom Eingabe-Plug-in durch Emulation von Tastatureingaben empfangen wurden, an die Vordergrundanwendungen.
- Intent-Ausgabe-Plug-in: Das Intent-Ausgabe-Plug-in sammelt und sendet Daten, die von den Eingabe-Plug-ins empfangen wurden, mithilfe des Android Intent-Mechanismus an Vordergrundanwendungen.
- IP-Ausgabe-Plug-in: Das IP-Ausgabe-Plug-in sammelt und sendet Daten, die von den Input Plug-ins empfangen wurden, über eine Netzwerkverbindung an einen Host-Computer. Erfasste Daten können über ein IP-Netzwerk an eine angegebene IP-Adresse und einen festgelegten Port gesendet werden, wobei entweder TCP- oder UDP-Transportprotokolle verwendet werden.

# **Profil-Bildschirm**

Um DataWedge zu starten, wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **▶**. Standardmäßig werden drei Profile angezeigt:

- Profile0
- Launcher (Startprogramm)
- DWDemo

"Profile0" (Profil0) ist das Standardprofil und wird verwendet, wenn kein anderes Profil angewendet werden kann.

Abbildung 44 Bildschirm "DataWedge Profiles" (DataWedge-Profile)



Profilnamen sind farbcodiert. Aktivierte Profile werden weiß und deaktivierte Profile grau dargestellt.

Tippen Sie zum Konfigurieren eines Profils auf den zugehörigen Namen.

## Profil-Kontextmenü

Berühren und halten Sie ein Profil, um ein Kontextmenü zu öffnen, in dem zusätzliche Aktionen für das ausgewählte Profil ausgeführt werden können.

#### Abbildung 45 Profil-Kontextmenü

Profile1	
Edit profile	
Rename profile	
Delete profile	
Clone profile	

Im Profil-Kontextmenü kann das Profil bearbeitet, umbenannt oder gelöscht werden. (Es kann auch durch Tippen auf das Profil geöffnet werden.)

# Optionsmenü

Berühren Sie 🚦, um das Optionsmenü zu öffnen.

Abbildung 46 DataWedge-Optionsmenü

New profile	
Settings	
About	

Das Menü bietet Optionen zum Erstellen eines neuen Profils, für den Zugriff auf allgemeine DataWedge-Einstellungen und DataWedge-Versionsinformationen.

# Deaktivieren von DataWedge

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie k.
- 2. Berühren Sie
- 3. Berühren Sie Settings (Einstellungen).
- 4. Berühren Sie DataWedge enabled (DataWedge aktiviert).

Das blaue Häkchen verschwindet aus dem Kontrollkästchen. Dies zeigt an, dass DataWedge deaktiviert ist.

# **Erstellen eines neuen Profils**

So erstellen Sie ein neues Profil:

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie k.
- 2. Berühren Sie
- 3. Berühren Sie New Profile (Neues Profil).
- 4. Geben Sie im Dialogfeld **New Profile** (Neues Profil) einen Namen für das neue Profil ein. Profilnamen sollten eindeutig sein und nur aus alphanumerischen Zeichen (A–Z, a–z, 0–9) bestehen.

#### Abbildung 47 Dialogfeld "Neuer Profilname"

New profile		
Enter profile name		
	CANCEL	ОК

5. Berühren Sie OK.

Der neue Profilname wird im Bildschirm DataWedge profile (DataWedge-Profil) angezeigt.

# Profilkonfiguration

Um Profil0 oder ein vom Benutzer erstelltes Profil zu konfigurieren, berühren Sie den Profilnamen.

nirm

Profile: Profile1	
Profile enabled Enable/disable this profile	
Applications	
Associated apps Associate apps and activities to this profile	
Data Capture Plus	
Enabled Enable or disable Data Capture Plus	
Barcode input	
Enabled Enable/disable scanner input	
Scanner selection Auto (2D Barcode Imager)	

Der Konfigurationsbildschirm enthält die folgenden Abschnitte:

- "Profile enabled" (Profil aktiviert)
- "Applications" (Anwendungen)
- Data Capture Plus (DCP)
- "Barcode Input" (Barcode-Eingabe)
- "Keystroke Output" (Tastenanschlag-Ausgabe)
- "Intent Output" (Intent-Ausgabe)
- "Voice Output" (Sprachausgabe)
- "IP Output" (IP-Ausgabe)

# Zuordnen von Anwendungen

Über die Option "Applications" (Anwendungen) können diesem Profil Anwendungen zugeordnet werden. Vom Benutzer erstellte Profile sollten einer oder mehreren Anwendungen und deren Aktivitäten zugeordnet werden.

1. Berühren Sie **Associated apps** (Zugeordnete Apps). Es wird eine Liste der dem Profil zugeordneten Anwendungen/Aktivitäten angezeigt. Zunächst enthält die Liste keine Anwendungen/Aktivitäten.

Abbildung 49 Bildschirm "Associated Apps" (Zugeordnete Apps)



- 2. Berühren Sie 🚦.
- 3. Berühren Sie New app/activity (Neue Anwendung/Aktivität).

Abbildung 50 Menü "Select Application" (Anwendung auswählen)



- 4. Wählen Sie im Bildschirm **Select application** (Anwendung auswählen) die gewünschte Anwendung aus der Liste aus.
- 5. Wenn Sie im Menü Select activity (Aktivität auswählen) die Aktivität auswählen, wird diese Kombination aus Anwendung und Aktivität der zugehörigen Anwendungsliste für dieses Profil hinzugefügt. Wenn Sie \* als Aktivität auswählen, werden dem Profil alle Aktivitäten innerhalb dieser Anwendung zugeordnet. Während des Betriebs versucht DataWedge, die spezifischen Kombinationen aus Anwendung/Aktivität mit

## DataWedge

der Vordergrundanwendung/-aktivität abzugleichen, bevor versucht wird, die allgemeinen Kombinationen aus Anwendung/\* zu vergleichen.

6. Berühren Sie **⊲**.

Abbildung 51 Ausgewählte Anwendung/Aktivität



# **Data Capture Plus**

Data Capture Plus (DCP) ist eine DataWedge-Funktion, mit der der Benutzer die Datenerfassung durch Berühren eines bestimmten Teils des Bildschirms starten kann. Dieses variable Bildschirm-Overlay verhält sich wie eine Scanschaltfläche.

← New note	Î	
		DCP-Taste
The	I Hi 🌵	
$Q^{1}W^{2}E^{3}R^{4}T$	$^{5}$ Y $^{6}$ U $^{7}$ I $^{8}$ O $^{9}$ P $^{0}$	
ASDF	GHJKL	
🛧 Z X C	V B N M 💌	
?1☺ ,	. 🕹	

Abbildung 52 Minimiertes Datenerfassungsfenster

## DataWedge

Im Profilkonfigurationsbildschirm von DataWedge kann der Benutzer konfigurieren, wie DCP auf dem Bildschirm angezeigt wird, sobald das jeweilige Profil aktiviert ist. Standardmäßig ist DCP deaktiviert. Wenn Sie die DCP-Option aktivieren, werden sieben zusätzliche Konfigurationsparameter angezeigt.

Abbildung 53	Einstellungen für da	s Datenerfassungsfeld

Profile: Profile0 (default)	
Data Capture Plus	
Enabled Enable or disable Data Capture Plus	
Dock button on Left or right	
<b>Start in</b> Button mode	
Button highest position 0% of screen height	
Button lowest position 100% of screen height	
Drag detect time 100 ms prior to scanner activation	

- "Enable" (Aktivieren): Wählen Sie diese Option aus, um Data Capture Plus zu aktivieren (Standardeinstellung: deaktiviert).
- Dock button on (Taste andocken an): Ermöglicht die Auswahl der Tastenposition.
  - Left or right (Links oder rechts): Ermöglicht es dem Benutzer, die Schaltfläche entweder auf dem rechten oder linken Bildschirmrand zu platzieren.
  - Left only (Nur links): Platziert die Schaltfläche am linken Rand des Bildschirms.
  - Right only (Nur rechts): Platziert die Schaltfläche am rechten Rand des Bildschirms.
- Start in (Starten in): Ermöglicht die Auswahl des ursprünglichen DCP-Status.
  - Fullscreen mode (Vollbildmodus): DCP deckt den gesamten Bildschirm ab.
  - Button mode (Schaltflächenmodus): DCP wird als kreisförmige Schaltfläche auf dem Bildschirm angezeigt und kann in den Vollbildmodus umgeschaltet werden.
  - **Button only mode** (Nur Schaltflächenmodus): DCP wird als kreisförmige Schaltfläche auf dem Bildschirm angezeigt und kann nicht in den Vollbildmodus umgeschaltet werden.
- Button highest position (Höchste Position der Schaltfläche): Wählen Sie den obersten Bereich aus, in dem der Benutzer DCP verschieben darf, angegeben als Prozentsatz der Bildschirmhöhe. (Standardeinstellung: 0)
- Button lowest position (Niedrigste Position der Schaltfläche): Wählen Sie den niedrigsten Bereich aus, in dem der Benutzer DCP verschieben darf, angegeben als Prozentsatz der Bildschirmhöhe. (Standardeinstellung: 100)
- Drag detect time (Zeit bis zur Erkennung des Ziehvorgangs): Wählen Sie die Zeit in Millisekunden bis zur Aktivierung des Scanners aus. Auf diese Weise kann der Benutzer die Schaltfläche ziehen, ohne den Scanner zu starten (Standardeinstellung: 100 ms, maximal 1000 ms).



**HINWEIS:** DCP wird nicht angezeigt, wenn der Scanner im Profil deaktiviert ist, obwohl die Option **Enabled** (Aktiviert) ausgewählt ist.

Im Schaltflächenmodus kann der Benutzer DCP in den Vollbildmodus versetzen, indem er die Schaltfläche über den **Vollbildmodus** zieht. Das Overlay deckt den gesamten Bildschirm ab.

Abbildung 54	DCP maximiert
--------------	---------------

← New note	Î
The I Hi	Ŷ
$Q^{1} W^{2} E^{3} R^{4} T^{5} Y^{6} U^{7} I^{8} C$	° P°
A S D F G H J K	L
🛧 Z X C V B N M	×
?1© , .	æ

Wischen Sie nach unten, um zum Schaltflächenmodus zurückzukehren.

# **Barcode Input**

Verwenden Sie die Optionen für **Barcode Input** (Barcode-Eingabe), um das Eingabe-Plug-in für den Barcodescanner für das Profil zu konfigurieren.

#### Aktiviert

Aktiviert oder deaktiviert dieses Plug-in. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist.

#### Scannerauswahl

Konfiguriert, welches Scangerät für die Erfassung von Barcodedaten verwendet werden soll, wenn das Profil aktiv ist.

- Auto: Die Software ermittelt automatisch das beste Scangerät.
- Camera Scanner (Kamerascanner): Das Scannen erfolgt mit der nach hinten gerichteten Kamera.
- 2D Barcode Imager: Das Scannen erfolgt mit dem 2D-Imager.
- Bluetooth Scanner (Bluetooth-Scanner): Das Scannen wird mit dem optionalen Bluetooth-Scanner durchgeführt.
- RS6000 Bluetooth Scanner: Das Scannen erfolgt über den RS6000 Bluetooth-Scanner.
- DS3678 Bluetooth Scanner: Das Scannen erfolgt mit dem Bluetooth-Scanner DS3678.
- LI3678 Bluetooth Scanner: Das Scannen erfolgt mit dem Bluetooth-Scanner DS3678.

#### Bei Ereignis automatisches Umschalten auf Standardeinstellung

Mit dieser Funktion wird DataWedge so konfiguriert, dass sofort nach dem Anschließen ein externer Scanner als Standard-Scanner ausgewählt und bei getrenntem externen Scanner wieder ein integrierter Scanner

## DataWedge

verwendet wird. Zu den externen Scannern gehören Geräte, die über Bluetooth, ein serielles Kabel oder ein anklemmbares Modul angeschlossen werden. Standardmäßig deaktiviert. Diese Option ist nur verfügbar, wenn **Scanner Selection** (Scannerauswahl) auf **Auto** (Automatisch) eingestellt ist.

So können Unterbrechungen des Scan-Workflows reduziert werden, wenn ein neuer Bluetooth-Scanner eingesetzt und/oder die Verbindung getrennt wird, weil die Stromversorgung unterbrochen wird oder sich der Scanner außerhalb der Reichweite befindet.

Bei Bluetooth-Scannern wird vor der automatischen Verbindung ein Kopplungs-Barcode angezeigt, wenn das Gerät zuvor noch nicht gekoppelt war.

- **Disabled** (Deaktiviert): Wenn ein externer Scanner angeschlossen oder getrennt wird, erfolgt keine Scannerumschaltung (Standardeinstellung).
- **On connect** (Beim Verbinden): Der externe Scanner wird sofort nach dem Anschließen als Standardscanner ausgewählt.
- On disconnect (Beim Trennen): Wechsel zu einem integrierten Scanner basierend auf der Position in einer intern verwalteten Scannerliste (die je nach Hostgerät variiert). Dies ist in der Regel der Scanner, der vor der externen Verbindung zuletzt verwendet wurde (siehe Hinweise unten).
- On connect/disconnect (Beim Verbinden/Trennen): Der externe Scanner wird sofort nach dem Anschließen als Standardscanner ausgewählt. Nach dem Trennen der Verbindung wird wieder der Scanner als Standardscanner verwendet, der vor der externen Verbindung festgelegt war.



**HINWEIS:** Das System wählt den Standardscanner basierend auf dem Verbindungsstatus und der Position des Scanners in einer intern verwalteten Scannerliste aus. Wenn sich der neu angeschlossene Scanner in der Scannerliste an einer Position unter dem aktuell ausgewählten Standardscanner befindet, wird der neu angeschlossene Scanner zum Standardscanner.

Bei Geräten mit nur einem integrierten Scanner oder Imager wird bei Auswahl der Option **On disconnect** (Beim Trennen) wieder die Verbindung zu diesem integrierten Scanner oder Imager hergestellt.

### Konfigurieren der Scannereinstellungen

Wählen Sie "Configure Scanner Settings" (Scannereinstellungen konfigurieren), um Folgendes festzulegen:

- Scanner zum Einstellen der Parameter auswählen
- Decoder
- Decoder-Parameter
- UPC/EAN-Parameter
- · Lesegerät-Parameter
- Scan-Parameter
- · UDI-Parameter
- Grundlegende Multibarcode-Parameter
- · Aktivierung bei Unterbrechung beibehalten

#### Decoder

Konfiguriert, welche Barcode-Decoder aktiviert oder deaktiviert sind. Deaktivieren Sie für eine optimale Leistung alle nicht benötigten Decoder.

Berühren Sie **Decoders** (Decoder). Der Bildschirm **Barcode input** (Barcode-Eingabe) wird angezeigt. Ein Häkchen im Kontrollkästchen zeigt an, dass der Decoder aktiviert ist. Standardmäßig sind die am häufigsten verwendeten Decoder aktiviert (unten mit einem X dargestellt). Folgende Decoder werden unterstützt:



HINWEIS: DataWedge unterstützt die unten aufgeführten Decoder, wobei jedoch nicht alle mit diesem Gerät kompatibel sind.

 Tabelle 5
 Unterstützte Decoder

Decoder	Interner Imager SE2100	Interner Imager SE4710	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
Australian Postal	0	0	0	0	0	0	
Aztec	Х	Х	Х	Х	Х	Х	
Canadian Postal	0	0		0			
Chinese 2 of 5	0	0	0	0	0	0	0
Codabar	Х	Х	Х	Х	Х	Х	Х
Code 11	0	0	0	0	0	0	0
Code 128	Х	Х	Х	Х	Х	Х	Х
Code 39	Х	Х	Х	Х	Х	Х	Х
Code 93	0	0	0	0	0	0	0
Composite AB	0	0	0	0	0	0	
Composite C	0	0	0	0	0	0	
Discrete 2 of 5	0	0	0	0	0	0	0
Datamatrix	Х	Х	Х	Х	Х	Х	
Dutch Postal	0	0	0	0	0	0	
EAN13	Х	Х	Х	Х	Х	Х	Х
EAN8	Х	Х	Х	Х	Х	Х	Х
GS1 DataBar	Х	Х	Х	Х	Х	Х	Х
GS1 DataBar Expanded	Х	Х	Х	Х	Х	Х	Х
GS1 DataBar Limited	0	0	0	0	0	0	0
GS1 Datamatrix	0	0		0	0	0	
GS1 QRCode	0	0		0	0	0	
HAN XIN	0	0		0	0	0	
<u>Taste</u> X = Aktiviert O = Deaktiviert							

-- = Nicht unterstützt
Tabelle 5	Unterstützte Decoder	(Fortsetzung)
-----------	----------------------	---------------

Decoder	Interner Imager SE2100	Interner Imager SE4710	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
Interleaved 2 of 5	0	0	0	0	0	0	0
Japanese Postal	0	0	0	0	0	0	
Korean 3 of 5	0	0	0	0	0	0	0
MAIL MARK	Х	Х		Х	Х	Х	
Matrix 2 of 5	0	0	0	0	0	0	0
Maxicode	Х	Х	Х	Х	Х	Х	
MicroPDF	0	0	0	0	0	0	
MicroQR	0	0	0	0	0	0	
MSI	0	0	0	0	0	0	0
PDF417	Х	Х	Х	Х	Х	Х	
QR-Code	Х	Х	Х	Х	Х	Х	
Decoder Signature	0	0	0	0	0		
TLC 39	0	0	0	0	0	0	0
Trioptic 39	0	0	0	0	0	0	0
UK Postal	0	0	0	0	0	0	
UPCA	Х	Х	Х	Х	Х	Х	Х
UPCE0	Х	Х	Х	Х	Х	Х	Х
UPCE1	0	0	0	0	0	0	0
US4state	0	0	0	0	0	0	
US4state FICS	0	0	0	0	0	0	
US Planet	0	0	0	0	0	0	
US Postnet	0	0	0	0	0	0	
Taste X = Aktiviert O = Deaktiviert = Nicht unterstützt							

Berühren Sie **〈**, um zum vorangehenden Bildschirm zurückzukehren.

## **Decoder-Parameter**

Verwenden Sie **Decode Params** (Dekodierungsparameter), um einzelne Decoder-Parameter zu konfigurieren.



**HINWEIS:** Nicht alle Parameteroptionen sind für alle Scanner verfügbar. Die verfügbaren Scanner- und Parameteroptionen finden Sie in der DataWedge-App auf dem jeweiligen Gerät.

## Codabar

- CLSI Editing (CLSI-Bearbeitung): Bei Aktivierung dieses Parameters werden die Start- und Stoppzeichen entfernt und es wird eine Lücke nach dem ersten, fünften und zehnten Zeichen eines Codabar-Symbols mit 14 Zeichen eingefügt. Aktivieren Sie diese Funktion, wenn das Host-System dieses Datenformat benötigt (Standardeinstellung: deaktiviert).
- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 6). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 55). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- NOTIS Editing (NOTIS-Bearbeitung): Bei Aktivierung dieses Parameters werden die Start- und Stoppzeichen von einem decodierten Codabar-Symbol entfernt. Aktivieren Sie diese Funktion, wenn das Host-System dieses Datenformat benötigt (Standardeinstellung: deaktiviert).
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: aktiviert).

### Code 11

- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 4). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 55). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: aktiviert).
- Report Check Digit (Prüfziffer übertragen): Sendet Code 11-Daten mit oder ohne Prüfziffer. Ein Häkchen im Kontrollkästchen bedeutet, dass Code 11-Daten mit Prüfziffer gesendet werden sollen (Standard: deaktiviert).
- Verify Check Digit (Prüfziffer überprüfen): Bei Aktivierung dieser Funktion prüft der Scanner die Integrität aller Code 11-Symbole, um die Übereinstimmung der Daten mit dem festgelegten Prüfziffern-Algorithmus zu kontrollieren. Hierdurch wird der Prüfziffern-Mechanismus für den decodierten Code 11-Barcode ausgewählt.
  - No Check Digit (Keine Prüfziffer): Die Prüfziffer wird nicht verifiziert.
  - 1 Check Digit (1 Prüfziffer): Barcode enthält eine Prüfziffer (Standard).
  - 2 Check Digits (2 Prüfziffern): Barcode enthält zwei Prüfziffern.

### Code128

- **Code128 Reduced Quiet Zone** (Code128 mit reduzierter Ruhezone): Ermöglicht die Decodierung von Code 128-Barcodes ohne Rand (Standardeinstellung: deaktiviert).
- Ignore Code128 FNC4 (Code128 FNC4 ignorieren): Wenn diese Option aktiviert ist und ein Code128-Barcode ein eingebettetes FNC4-Zeichen enthält, wird er aus den Daten entfernt, und die folgenden Zeichen werden nicht geändert. Wenn die Funktion deaktiviert ist, wird das FNC4-Zeichen nicht übertragen, dem folgenden Zeichen wird jedoch 128 hinzugefügt (Standardeinstellung: deaktiviert).
- Check ISBT Table (ISBT-Tabelle prüfen): Die ISBT-Spezifikation enthält eine Tabelle, in der verschiedene Arten von ISBT-Barcodes aufgeführt sind, die häufig paarweise verwendet werden. Wenn der ISBT128-Verkettungsmodus eingerichtet ist, aktivieren Sie "Check ISBT Table" (ISBT-Tabelle prüfen), um nur die in dieser Tabelle gefundenen Paare zu verketten. Andere Arten von ISBT-Codes werden nicht verkettet. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: deaktiviert).

- Enable GS1-128 (GS1-128 aktivieren): Legen Sie den GS1-128-Untertyp fest. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).
- Enable ISBT128 (ISBT128 aktivieren): Legen Sie den ISBT128-Untertyp fest. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).
- Enable Plain Code128 (Code128 Klartext aktivieren): Legen Sie den Untertyp Code128 Klartext fest. Aktiviert andere Untertypen von Code 128 (nicht EAN oder ISBT). Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).
- **ISBT128 Concatenation Mode** (ISBT128-Verkettungsmodus): Wählen Sie eine Option zum Verketten von ISBT-Codetypen aus:
  - **Concat Mode Never** (Verkettungsmodus nie verwenden): Es erfolgt keine Verkettung von ISBT-Codepaaren (Standard).
  - **Concat Mode Always** (Verkettungsmodus immer verwenden): Zur Decodierung und Verkettung müssen zwei ISBT-Codes vorhanden sein. Einzelne ISBT-Symbole werden nicht decodiert.
  - Concat Mode Auto (Verkettungsmodus automatisch verwenden): ISBT-Codepaare werden sofort decodiert und verkettet. Wenn nur ein einzelnes ISBT-Symbol vorhanden ist, muss das Gerät das Symbol so oft decodieren, wie in der DataWedge-Konfiguration 4 – 11 Redundanz – Code128 festgelegt wurde, bevor es seine Daten überträgt, um zu bestätigen, dass kein zusätzliches ISBT-Symbol vorhanden ist.
- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 0). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 55). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: deaktiviert).
- Security Level (Sicherheitsstufe): Der Scanner bietet vier Decodierungsstufen für Code 128-Barcodes. Wählen Sie für Barcodes geringerer Qualität eine höhere Sicherheitsstufe aus. Zwischen Sicherheit und "Aggressivität" des Scanners besteht ein umgekehrtes Verhältnis; achten Sie daher darauf, für jede gegebene Anwendung nur die hierfür erforderliche Sicherheitsstufe zu wählen.
  - Security Level 0 (Sicherheitsstufe 0): Mit dieser Einstellung kann der Scanner in seinem "aggressivsten" Zustand betrieben werden, und dies bietet gleichzeitig eine ausreichende Sicherheit beim Decodieren der meisten Barcodes innerhalb der Spezifikation.
  - **Security Level 1** (Sicherheitsstufe 1): Mit dieser Einstellung werden die meisten Decodierfehler verhindert (Standardeinstellung).
  - Security Level 2 (Sicherheitsstufe 2): Wählen Sie diese Option aus, wenn Sicherheitsstufe 1 die Decodierfehler nicht verhindert.
  - Security Level 3 (Sicherheitsstufe 3): Wenn Sicherheitsstufe 2 ausgewählt ist und immer noch eine falsche Decodierung auftritt, wählen Sie diese Sicherheitsstufe aus. Es wird darauf hingewiesen, dass die Auswahl dieser Option eine extreme Maßnahme gegen die fehlerhafte Decodierung von besonders stark abweichenden Barcodes darstellt. Die Auswahl dieser Sicherheitsstufe kann die Decodierfähigkeit des Scanners bedeutend beeinträchtigen. Versuchen Sie, die Qualität der Barcodes zu verbessern, wenn diese Sicherheitsstufe erforderlich ist.

### Code39

- **Code39 Reduced Quiet Zone** (Code39 mit reduzierter Ruhezone): Ermöglicht die Decodierung von Code 39-Barcodes ohne Rand (Standardeinstellung: deaktiviert).
- Convert Code39 To Code32 (Code39 in Code32 konvertieren): Code 32 ist eine Variante von Code 39, die von der italienischen Pharmaindustrie verwendet wird. Scannen Sie zum Aktivieren oder Deaktivieren der Konvertierung von Code 39 in Code 32 den entsprechenden nachstehend abgebildeten Barcode (Standardeinstellung: deaktiviert).
- Full ASCII (Vollständiger ASCII-Zeichensatz): Code 39 Full ASCII ist eine Variante von Code 39, in der Zeichen zugewiesen werden, um den vollständigen ASCII-Zeichensatz zu codieren.
- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 0). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.

- Length2 (Länge2): Zum Einstellen der Decodierungslängen (Standardeinstellung: 55). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: deaktiviert).
- Report Check Digit (Pr
  üfziffer 
  übertragen): Sendet Code 39-Daten mit oder ohne Pr
  üfziffer. Ein H
  äkchen im Kontrollk
  ästchen bedeutet, dass Code 39-Daten mit Pr
  üfziffer gesendet werden sollen (Standard: deaktiviert).
- Report Code32 Prefix (Code32-Präfix übertragen): Scannen Sie den entsprechenden Barcode, um das Hinzufügen des Präfixzeichens "A" zu allen Code 32-Barcodes zu aktivieren oder zu deaktivieren (Standardeinstellung: deaktiviert).
- Security Level (Sicherheitsstufe): Optionen: Security level 0 (Sicherheitsstufe 0), Security Level 1 (Sicherheitsstufe 1), Security Level 2 (Sicherheitsstufe 2) und Security Level 3 (Sicherheitsstufe 3) (Standardeinstellung: Sicherheitsstufe 1).
  - Security Level 0 (Sicherheitsstufe 0): Mit dieser Einstellung kann der Scanner in seinem "aggressivsten" Zustand betrieben werden, und dies bietet gleichzeitig eine ausreichende Sicherheit beim Decodieren der meisten Barcodes innerhalb der Spezifikation.
  - **Security Level 1** (Sicherheitsstufe 1): Mit dieser Einstellung werden die meisten Decodierfehler verhindert (Standardeinstellung).
  - Security Level 2 (Sicherheitsstufe 2): Wählen Sie diese Option aus, wenn Sicherheitsstufe 1 die Decodierfehler nicht verhindert.
  - Security Level 3 (Sicherheitsstufe 3): Wenn Sicherheitsstufe 2 ausgewählt ist und immer noch eine falsche Decodierung auftritt, wählen Sie diese Sicherheitsstufe aus. Es wird darauf hingewiesen, dass die Auswahl dieser Option eine extreme Maßnahme gegen die fehlerhafte Decodierung von besonders stark abweichenden Barcodes darstellt. Die Auswahl dieser Sicherheitsstufe kann die Decodierfähigkeit des Scanners bedeutend beeinträchtigen. Versuchen Sie, die Qualität der Barcodes zu verbessern, wenn diese Sicherheitsstufe erforderlich ist.
- Verify Check Digit (Prüfziffer überprüfen): Bei Aktivierung dieser Funktion prüft der Scanner die Integrität aller Code 39-Symbole, um die Übereinstimmung der Daten mit dem festgelegten Prüfziffern-Algorithmus zu kontrollieren. Der digitale Scanner decodiert nur die Code 39-Symbole, die eine Modulo 43-Prüfziffer enthalten. Aktivieren Sie diese Funktion nur, wenn die Code 39-Symbole eine Modulo 43-Prüfziffer enthalten (Standardeinstellung: deaktiviert).

### Code93

- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 0). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 55). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: deaktiviert).

### **Composite AB**

- UCC-Verknüpfungsmodus
  - Link Flag ignored (Verknüpfungsmarkierung wird ignoriert): Es wird eine 1D-Komponente übertragen, unabhängig davon, ob eine 2D-Komponente erkannt wird.
  - Always Linked (Immer verknüpft): 1D- und die 2D-Komponenten werden übertragen. Wenn 2D nicht vorhanden ist, wird die 1D-Komponente nicht übertragen.
  - Auto Discriminate (Automatische Unterscheidung): Der digitale Scanner ermittelt, ob ein 2D-Teil vorhanden ist, und überträgt dann die 1D-Komponente sowie den 2D-Teil, falls vorhanden. (Standard).

### Discrete 2 of 5

- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 0). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 14). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: aktiviert).

### GS1 DataBar Limited

- Sicherheitsstufen für GS1 Limited
  - **GS1 Security Level 1** (GS1 Sicherheitsstufe 1): Mit dieser Einstellung kann der Scanner in seinem "aggressivsten" Zustand betrieben werden, und dies bietet gleichzeitig eine ausreichende Sicherheit beim Decodieren der meisten Barcodes innerhalb der Spezifikation.
  - **GS1 Security Level 2** (GS1 Sicherheitsstufe 2): Mit dieser Einstellung werden die meisten Decodierfehler vermieden (Standardeinstellung).
  - **GS1 Security Level 3** (GS1 Sicherheitsstufe 3): Wählen Sie diese Option aus, wenn Sicherheitsstufe 2 nicht ausreicht, um Decodierfehler zu vermeiden.
  - **GS1 Security Level 4** (GS1 Sicherheitsstufe 4): Wenn Sicherheitsstufe 3 ausgewählt ist und immer noch falsche Decodierungen auftreten, wählen Sie diese Sicherheitsstufe aus. Es wird darauf hingewiesen, dass die Auswahl dieser Option eine extreme Maßnahme gegen die fehlerhafte Decodierung von besonders stark abweichenden Barcodes darstellt. Die Auswahl dieser Sicherheitsstufe kann die Decodierfähigkeit des Scanners bedeutend beeinträchtigen. Versuchen Sie, die Qualität der Barcodes zu verbessern, wenn diese Sicherheitsstufe erforderlich ist.

### HAN XIN

- HAN XIN Inverse
  - **Disable** (Deaktivieren): Deaktiviert die Decodierung von HAN XIN Inverse-Barcodes (Standardeinstellung).
  - Enable (Aktivieren): Aktiviert die Decodierung von HAN XIN Inverse-Barcodes.
  - Auto: Decodiert sowohl reguläre als auch HAN XIN Inverse-Barcodes.

### Interleaved 2 of 5

- Prüfziffer
  - **No Check Digit** (Keine Prüfziffer): Es wird keine Prüfziffer verwendet. (Standard)
  - **USS Check Digit** (USS-Prüfziffer): Bei Aktivierung dieser Option prüft der Scanner die Integrität aller Symbole des Interleaved 2 of 5-Barcodes, um die Übereinstimmung der Daten mit dem Prüfziffer-Algorithmus "Uniform Symbology Specification" (USS) zu kontrollieren.
  - OPCC Check Digit (OPCC-Pr
    üfziffer): Bei Aktivierung dieser Option pr
    üft der Scanner die Integrit
    ät aller Symbole des Interleaved 2 of 5-Barcodes, um die 
    Übereinstimmung der Daten mit dem Pr
    üfziffer-Algorithmus Optical Product Code Council (OPCC) zu kontrollieren.
- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 14). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 10). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- **Redundancy** (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: aktiviert).

- **Report Check Digit** (Prüfziffer übertragen): Sendet Interleaved 2 of 5-Daten mit oder ohne Prüfziffer. Ein Häkchen im Kontrollkästchen bedeutet, dass Interleaved 2 of 5-Daten mit Prüfziffer gesendet werden sollen (Standardeinstellung: deaktiviert).
- I 2 of 5 Security Level (I 2 of 5 Sicherheitsstufe): Optionen: I 2 of 5 Security level 0 (I 2 of 5 mit Sicherheitsstufe 0), I 2 of 5 Security Level 1 (I 2 of 5 mit Sicherheitsstufe 1), I 2 of 5 Security Level 2 (I 2 of 5 mit Sicherheitsstufe 2) und I 2 of 5 Security Level 3 (I 2 of 5 mit Sicherheitsstufe 3) (Standardeinstellung: Sicherheitsstufe 1).
- Convert ITF-14 To EAN13 (ITF-14 in EAN13 konvertieren): 14-stellige Interleaved 2 of 5-Barcodes werden in EAN-13 konvertiert und als EAN-13 übertragen. Der Barcode "Interleaved 2 of 5" muss aktiviert sein und eine führende Null sowie eine gültige EAN-13-Prüfziffer aufweisen. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: deaktiviert).
- **I 2 of 5 Reduced Quiet Zone** (I 2 of 5 mit reduzierter Ruhezone): Ermöglicht die Decodierung von I 2 of 5-Barcodes ohne Rand (Standardeinstellung: deaktiviert).

### Matrix 2 of 5

- Length1 (Länge1): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 10). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length2 (Länge2): Ermöglicht das Einstellen der Decodierungslängen (Standardeinstellung: 0). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: deaktiviert).
- Report Check Digit (Pr
  üfziffer 
  übertragen): Sendet Matrix 2 of 5-Daten mit oder ohne Pr
  üfziffer. Ein H
  äkchen im Kontrollk
  ästchen bedeutet, dass Matrix 2 of 5-Daten mit Pr
  üfziffer gesendet werden sollen (Standardeinstellung: aktiviert).
- Verify Check Digit (Prüfziffer überprüfen): Bei Aktivierung dieser Funktion prüft der Scanner die Integrität aller Symbole des Matrix 2 of 5-Barcodes, um die Übereinstimmung der Daten mit dem festgelegten Prüfziffern-Algorithmus zu kontrollieren (Standardeinstellung: aktiviert).

### MSI

- **Check Digit** (Prüfziffer): Bei MSI-Symbolen ist eine Prüfziffer obligatorisch, und dies wird stets durch das Lesegerät überprüft. Die zweite Prüfziffer ist optional.
  - **One Check Digit** (Eine Prüfziffer): Es wird überprüft, ob der Barcode eine Prüfziffer enthält (Standardeinstellung).
  - Two Check Digits (Zwei Prüfziffern): Es wird überprüft, ob der Barcode zwei Prüfziffern enthält.
- Check Digit Scheme (Schema der Prüfziffer): Für die Überprüfung der zweiten MSI-Prüfziffer sind zwei Algorithmen möglich. Wählen Sie den Algorithmus aus, mit dem die Prüfziffer codiert wird.
  - **Mod-11-10**: Die erste Prüfziffer wird gemäß Modulo 11 und die zweite Prüfziffer gemäß Modulo 10 berechnet (Standardeinstellung).
  - **Mod-10-10**: Beide Prüfziffern werden gemäß Modulo 10 berechnet.
- Length 1 (Länge 1): Zum Einstellen der Decodierungslängen (Standardeinstellung: 4). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- Length 2 (Länge 2): Zum Einstellen der Decodierungslängen (Standardeinstellung: 55). Weitere Informationen sind unter Decodierungslängen auf Seite 80 zu finden.
- **Redundancy** (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: aktiviert).
- **Report Check Digit** (Prüfziffer übertragen): Sendet MSI-Daten mit oder ohne Prüfziffer. Ein Häkchen im Kontrollkästchen zeigt an, dass MSI mit Prüfziffer gesendet werden sollen (Standardeinstellung: deaktiviert).

### Trioptic 39

 Redundancy (Redundanz): Legt fest, dass der Barcode zweimal vom Lesegerät gelesen wird, bevor Daten akzeptiert werden. Ein Häkchen im Kontrollkästchen zeigt an, dass Redundanz aktiviert ist (Standardeinstellung: deaktiviert).

### UK Postal

Report Check Digit (Pr
üfziffer 
übertragen): Sendet UK Postal-Daten mit oder ohne Pr
üfziffer. Ein H
äkchen
im Kontrollk
ästchen zeigt an, dass UK Postal-Daten mit Pr
üfziffer gesendet werden sollen
(Standardeinstellung: deaktiviert).

### UPCA

• **Preamble** (Präambel): Die Präambel-Zeichen sind Teil des UPC-Symbols und bestehen aus Ländercode und Systemzeichen. Wählen Sie die passende Option in Übereinstimmung mit dem Host-System.

Es gibt drei Optionen für die Übertragung einer UPCA-Präambel:

- Preamble None (Keine Präambel): Die Übertragung erfolgt ohne Präambel.
- **Preamble Sys Char** (Nur Systemzeichen als Präambel): Es werden nur Systemzeichen als Präambel übertragen (Standardeinstellung).
- Preamble Country and Sys Char (Ländercode und Systemzeichen als Präambel): Es werden nur Systemzeichen und Ländercode übertragen ("0" für USA). Wählen Sie die passende Option in Übereinstimmung mit dem Host-System.
- Report Check Digit (Pr
  üfziffer 
  übertragen): Die Pr
  üfziffer ist das letzte Zeichen des verwendeten Symbols
  und dient zur Integrit
  ätspr
  üfung der Daten. Aktiviert oder deaktiviert diese Option. Ein H
  äkchen im
  Kontrollk
  ästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).

### UPCE0

- Convert UPCE0 To UPCA (UPCE0 in UPCA konvertieren): Ermöglicht die Konvertierung von decodierten UPCE0-Daten (ohne Unterdrückung) vor der Übertragung in das UPC-A-Format. Nach der Konvertierung folgen die Daten dem UPC-A-Format und werden durch die Optionen der UPC-A-Programmierung beeinflusst. Deaktivieren Sie diese Option, um decodierte UPCE0-Daten ohne Konvertierung als UPCE0-Daten zu übertragen (Standardeinstellung: deaktiviert).
- **Preamble** (Präambel): Die Präambel-Zeichen sind Teil des UPC-Symbols und bestehen aus Ländercode und Systemzeichen. Wählen Sie die passende Option in Übereinstimmung mit dem Host-System.

Es gibt drei Optionen für die Übertragung einer UPCE0-Präambel:

- Preamble None (Keine Präambel): Die Übertragung erfolgt ohne Präambel (Standardeinstellung).
- **Preamble Sys Char** (Nur Systemzeichen als Präambel): Es werden nur Systemzeichen als Präambel übertragen.
- **Preamble Country and Sys Char** (Ländercode und Systemzeichen als Präambel): Es werden nur Systemzeichen und Ländercode übertragen ("0" für USA).
- Report Check Digit (Pr
  üfziffer 
  übertragen): Die Pr
  üfziffer ist das letzte Zeichen des verwendeten Symbols
  und dient zur Integrit
  ätspr
  üfung der Daten. Aktiviert oder deaktiviert diese Option. Ein H
  äkchen im
  Kontrollk
  ästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: deaktiviert).

### UPCE1

 Convert UPCE1 To UPCA (UPCE1 in UPCA konvertieren): Aktivieren Sie diese Option, um decodierte UPCE1-Daten vor der Übertragung in das UPC-A-Format zu konvertieren. Nach der Konvertierung folgen die Daten dem UPC-A-Format und werden durch die Optionen der UPC-A-Programmierung beeinflusst. Deaktivieren Sie diese Option, um decodierte UPCE1-Daten ohne Konvertierung als UPCE1-Daten zu übertragen (Standardeinstellung: deaktiviert). • **Preamble** (Präambel): Die Präambel-Zeichen sind Teil des UPC-Symbols und bestehen aus Ländercode und Systemzeichen. Wählen Sie die passende Option in Übereinstimmung mit dem Host-System.

Es gibt drei Optionen für die Übertragung einer UPCE1-Präambel:

- Preamble None (Keine Präambel): Die Übertragung erfolgt ohne Präambel (Standardeinstellung).
- **Preamble Sys Char** (Nur Systemzeichen als Präambel): Es werden nur Systemzeichen als Präambel übertragen.
- **Preamble Country and Sys Char** (Ländercode und Systemzeichen als Präambel): Es werden nur Systemzeichen und Ländercode übertragen ("0" für USA).
- Report Check Digit (Pr
  üfziffer 
  übertragen): Die Pr
  üfziffer ist das letzte Zeichen des verwendeten Symbols
  und dient zur Integrit
  ätspr
  üfung der Daten. Aktiviert oder deaktiviert diese Option. Ein H
  äkchen im
  Kontrollk
  ästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: deaktiviert).

### US Planet

Report Check Digit (Pr
üfziffer 
übertragen): Die Pr
üfziffer ist das letzte Zeichen des verwendeten Symbols
und dient zur Integrit
ätspr
üfung der Daten. Aktiviert oder deaktiviert diese Option. Ein H
äkchen im
Kontrollk
ästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: deaktiviert).

### Decodierungslängen

Die zulässigen Decodierungslängen werden durch die Optionen **Length1** (Länge 1) und **Length2** (Länge 2) wie folgt angegeben:

- Variable Länge: Ermöglicht die Decodierung von Symbolen, die eine beliebige Anzahl von Zeichen enthalten.
  - Legen Sie für Length1 (Länge 1) sowie für Length2 (Länge 2) 0 fest.
- Bereich: Ermöglicht die Decodierung eines Symbols mit einem bestimmten Längenbereich (von *a* bis *b*, einschließlich *a* und *b*).
  - Legen Sie für Length1 (Länge 1) a und für Length2 (Länge 2) b fest.
- Zwei unterschiedliche Längen: Es werden nur Symbole decodiert, die eine von zwei ausgewählten Längen aufweisen.
  - Legen Sie f
    ür Length1 (L
    änge 1) oder Length2 (L
    änge 2) eine bestimmte L
    änge fest. Length1 (L
    änge 1)
    muss gr
    ößer als Length2 (L
    änge 2) sein.
- Eine bestimmte Länge: Es werden nur Symbole decodiert, die eine bestimmte Länge aufweisen.
  - Legen Sie für Length1 (Länge 1) und Length2 (Länge 2) diese bestimmte Länge fest.

### **UPC/EAN-Parameter**

Ermöglicht die Konfiguration der Parameter, die für mehr als einen UPC- oder EAN-Decoder gelten.



**HINWEIS:** Nicht alle Parameteroptionen sind für alle Scanner verfügbar. Die verfügbaren Scanner- und Parameteroptionen finden Sie in der DataWedge-App auf dem jeweiligen Gerät.

- **Convert DataBar To UPC EAN** (DataBar in UPC/EAN konvertieren): Wenn diese Option festgelegt ist, werden DataBar-Barcodes in das UPC/EAN-Format konvertiert. Damit diese Einstellung funktioniert, müssen UPC/EAN-Symbologien aktiviert sein. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist. (Standardeinstellung: deaktiviert).
- UPC Reduced Quiet Zone (UPC mit reduzierter Ruhezone): Ermöglicht die Decodierung randloser UPC-Barcodes. (Standardeinstellung: deaktiviert)
- **Bookland**: Ermöglicht die Decodierung von Bookland-Barcodes. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist. (Standardeinstellung: deaktiviert).
- **Bookland Format** (Bookland-Format): Wenn Bookland-EAN aktiviert ist, wählen Sie eines der folgenden Formate für Bookland-Daten aus:
  - Format ISBN-10 (ISBN-10-Format): Der Decoder meldet Bookland-Daten ab 978 im traditionellen 10-stelligen Format mit der speziellen Bookland-Prüfziffer für Abwärtskompatibilität. Daten, die mit 979 beginnen, werden in diesem Modus nicht als Bookland-Daten berücksichtigt. (Standard)
  - Format ISBN-13 (ISBN-13-Format): Der Decoder meldet Bookland-Daten (ab 978 oder 979) als EAN-13 im 13-stelligen Format in Übereinstimmung mit dem 2007 ISBN-13-Protokoll.

- **Coupon**: Aktiviert die Decodierung von Coupon-Codes. Beachten Sie, dass für die erforderliche Decodierung von Coupon-Codes alle richtigen Decoder aktiviert sein müssen. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist. (Standardeinstellung: deaktiviert).
- Coupon Report Mode (Coupon-Lesemodus): Herkömmliche Coupon-Symbole bestehen aus zwei Barcodes: UPC/EAN und Code 128. Neue Coupon-Symbole bestehen aus einem einzelnen Data Expanded-Barcode. Das neue Format bietet mehr Optionen für Einkaufswerte (bis zu 999.999 US-Dollar) und unterstützt zudem komplexe Rabattangebote. Es gibt auch ein Coupon-Symbol für den Übergang, das beide Arten von Barcodes umfasst: UPC/EAN und DataBar Expanded. Dieses Format eignet sich sowohl für Einzelhändler, die die im neuen Coupon-Symbol enthaltenen zusätzlichen Informationen nicht einlesen oder verwenden, als auch für Händler, die neue Coupon-Symbole verarbeiten können.
  - Old Coupon Report Mode (Lesemodus f
    ür alte Coupons): Beim Scannen eines alten Coupon-Symbols werden sowohl UPC als auch Code 128 gelesen. Beim Scannen eines Interim-Coupon-Symbols wird UPC gemeldet, und beim Scannen eines neuen Coupon-Symbols erfolgt keine Aktion (keine Decodierung).
  - New Coupon Report Mode (Lesemodus f
    ür neue Coupons): Beim Scannen eines alten Coupon-Symbols wird entweder UPC oder Code 128 gelesen. Beim Scannen eines Interim-Coupon-Symbols oder eines neuen Coupon-Symbols wird Databar Expanded gemeldet.
  - Both Coupon Report Modes (Lesemodus f
    ür beide Coupons): Beim Scannen eines alten Coupon-Symbols werden sowohl UPC als auch Code 128 gelesen. Beim Scannen eines Interim-Coupon-Symbols oder eines neuen Coupon-Symbols wird Databar Expanded gemeldet. (Standard)
- Ean Zero Extend (EAN mit Nullen): Bei Aktivierung dieses Parameters werden fünf Nullen vor gelesenen EAN-8-Symbolen eingefügt, um diese mit den Symbolen im EAN-13-Format kompatibel zu machen. Deaktivieren Sie diese Option, um EAN-8-Symbole unverändert zu übertragen. (Standardeinstellung: deaktiviert).
- Retry Count (Anzahl Wiederholungen): Anzahl der Wiederholungen für die automatische Unterscheidung von Zusätzen. Mögliche Werte sind 2 bis einschließlich 20. Beachten Sie, dass diese Markierung nur berücksichtigt wird, wenn "Supplemental Mode UPC EAN" (Zusatzmodus UPC/EAN) auf einen der folgenden Werte gesetzt ist: Supplementals Auto (Automatischer Zusatzmodus), Supplementals Smart (Intelligenter Zusatzmodus), Supplementals 378-379 (Zusätze 378-379), Supplementals 978-979), Supplementals 977 (Zusätze 977) oder Supplementals 414-419-434-439 (Zusätze 414-419-434-439) (2 bis 20, Standardeinstellung 10).
- Security Level (Sicherheitsstufe): Der Scanner bietet vier Decodierungsstufen für UPC/EAN-Barcodes. Wählen Sie höhere Sicherheitsstufen für Barcodes geringerer Qualität aus. Sicherheit und Decodiergeschwindigkeit des Scanners stehen in umgekehrtem Verhältnis zueinander; achten Sie daher darauf, für jede Anwendung nur die hierfür erforderliche Sicherheitsstufe zu wählen.
  - Level 0 (Stufe 0): Diese Standardeinstellung ermöglicht den schnellsten Betrieb des Scanners und bietet gleichzeitig eine ausreichende Sicherheit beim Decodieren von UPC/EAN-Barcodes.
  - Level 1 (Stufe 1): Mit abnehmender Qualität der Barcodes sind bestimmte Zeichen anfälliger für Decodierungsfehler als andere (z. B. 1, 2, 7, 8). Wenn der Scanner schlecht gedruckte Barcodes falsch decodiert und die Decodierfehler auf diese Zeichen beschränkt sind, wählen Sie diese Sicherheitsstufe aus. (Standard).
  - Level 2 (Stufe 2): Wenn der Scanner schlecht gedruckte Barcodes falsch decodiert und die Decodierfehler nicht auf die Zeichen 1, 2, 7 und 8 beschränkt sind, wählen Sie diese Sicherheitsstufe aus.
  - Level 3 (Stufe 3): Wenn der Scanner noch immer falsch decodiert, wählen Sie diese Sicherheitsstufe aus. Es wird darauf hingewiesen, dass die Auswahl dieser Option eine extreme Maßnahme gegen die fehlerhafte Decodierung von besonders stark abweichenden Barcodes darstellt. Die Auswahl dieser Sicherheitsstufe kann die Decodierfähigkeit des Scanners bedeutend beeinträchtigen. Versuchen Sie die Qualität der Barcodes zu verbessern, wenn diese Sicherheitsstufe erforderlich ist.
- Supplemental2 (Zusatz 2): Aktiviert oder deaktiviert diese Option. Ein H\u00e4kchen im Kontrollk\u00e4stchen zeigt an, dass die Option aktiviert ist.
- **Supplemental5** (Zusatz 5): Aktiviert oder deaktiviert diese Option. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist.

### Modus mit Zusatzsymbolen

- **No Supplementals** (Keine Zusatzsymbole): Der Scanner liest UPC/EAN und das zusätzliche Symbol, decodiert UPC/EAN und ignoriert die zusätzlichen Zeichen (Standard).
- **Supplemental Always** (Immer Zusatzsymbole): Der Scanner decodiert nur UPC/EAN-Symbole mit zusätzlichen Zeichen und ignoriert Symbole ohne Zusatzsymbole.
- Supplements Auto (Zusatzsymbole automatisch): Der Scanner decodiert sofort UPC/EAN-Symbole mit zusätzlichen Zeichen. Wenn das Symbol keine zusätzlichen Zeichen enthält, muss der Scanner, bevor er seine Daten überträgt, den Barcode entsprechend der Anzahl der Wiederholungen lesen, die für die UPC/EAN-Zusatzzeichenredundanz festgelegt wurde, um zu bestätigen, dass keine zusätzlichen Daten vorhanden sind.
- Supplemental Smart (Intelligenter Modus für Zusatzzeichen): Aktiviert den intelligenten Modus für Zusatzzeichen. In diesem Modus gibt der Decoder den decodierten Wert des Hauptblocks sofort zurück, wenn er nicht zu einem der folgenden zusätzlichen Typen gehört: 378, 379, 977, 978, 979, 414, 419, 434 oder 439. Wenn der Barcode mit einem der Präfixe beginnt, wird das Symbol "aggressiver" nach zusätzlichen Zeichen durchsucht. Es wird versucht, möglicherweise vorhandene Zusatzzeichen zu scannen. Wenn das Scannen zusätzlicher Zeichen fehlgeschlagen ist, wird der Hauptbarcode zurückgegeben.
- Supplemental 378-379 (Zusatzzeichen 378-979): Aktiviert (automatische Unterscheidung) Zusatzzeichen für UPC/EAN-Codes ab 378 oder 379. Deaktiviert das Lesen zusätzlicher Zeichen für alle anderen UPC/EAN-Barcodes, die nicht mit 378 oder 379 beginnen. Es wird versucht, möglicherweise vorhandene Zusatzzeichen zu scannen. Wenn das Scannen zusätzlicher Zeichen fehlgeschlagen ist, wird der Hauptbarcode zurückgegeben.
- Supplemental 978-979 (Zusatzzeichen 978-979): Aktiviert (automatische Unterscheidung) Zusatzzeichen f
  ür UPC/EAN-Codes ab 378 oder 979. Deaktiviert das Lesen zus
  ätzlicher Zeichen f
  ür alle anderen UPC/EAN-Barcodes, die nicht mit 978 oder 979 beginnen. Es wird versucht, möglicherweise vorhandene Zusatzzeichen zu scannen. Wenn das Scannen zus
  ätzlicher Zeichen fehlgeschlagen ist, wird der Hauptbarcode zur
  ückgegeben.
- **Supplemental 414-419-434-439** (Zusatzzeichen 414-419-434-439): Aktiviert (automatische Unterscheidung) Zusatzzeichen für UPC/EAN-Codes ab 414, 419, 434 oder 439. Deaktiviert das Lesen zusätzlicher Zeichen für andere UPC/EAN-Barcodes, 4 16, die nicht mit 414, 419, 434 oder 439 beginnen. Es wird versucht, möglicherweise vorhandene Zusatzzeichen zu scannen. Wenn das Scannen zusätzlicher Zeichen fehlgeschlagen ist, wird der Hauptbarcode zurückgegeben.
- **Supplemental 977** (Zusatzzeichen 977): Aktiviert (automatische Unterscheidung) Zusatzzeichen für UPC/EAN-Codes ab 977. Deaktiviert das Lesen zusätzlicher Zeichen für alle anderen UPC/EAN-Barcodes, die nicht mit 977 beginnen. Es wird versucht, möglicherweise vorhandene Zusatzzeichen zu scannen. Wenn das Scannen zusätzlicher Zeichen fehlgeschlagen ist, wird der Hauptbarcode zurückgegeben.

### Lesegerät-Parameter

Ermöglicht die Konfiguration von Parametern, die für das ausgewählte Barcode-Lesegerät spezifisch sind.



**HINWEIS:** Nicht alle Parameteroptionen sind für alle Scanner verfügbar. Die verfügbaren Scanner- und Parameteroptionen finden Sie in der DataWedge-App auf dem jeweiligen Gerät.

- **Character Set Configuration** (Zeichensatzkonfiguration): Zur Unterstützung der chinesischen Zeichencodierung GB2312.
  - Character Set Selection (Zeichensatzauswahl): Ermöglicht es dem Benutzer, die Barcode-Daten zu konvertieren, wenn sie sich vom Standardcodierungstyp unterscheiden.
    - Auto Character Set Selection (Best Effort) (Automatische Zeichensatzauswahl bestmögliche Umsetzung): Option zur automatischen Zeichenkonvertierung. Es wird versucht, die Daten aus der bevorzugten Auswahl zu decodieren. Der erste korrekt decodierbare Zeichensatz wird zum Konvertieren der Daten verwendet und gesendet.
    - **ISO-8859-1**: Teil der ISO/IEC 8859-Serie ASCII-basierter Standardzeichencodierungen. Diese sind in der Regel für westeuropäische Sprachen vorgesehen.

- Shift\_JIS: Shift Japanese Industrial Standards (JIS) ist eine Zeichencodierung f
  ür die japanische Sprache.
- **GB18030**: Chinesischer codierter Zeichensatz, der die erforderliche Sprachen- und Zeichenunterstützung für Software in China definiert.
- **UTF-8**: Eine Zeichencodierung, mit der alle möglichen Zeichen oder Codepunkte, die durch Unicode definiert sind, codiert werden können (Standardeinstellung).
- Auto Character Set Preferred Order (Bevorzugte Reihenfolge des automatischen Zeichensatzes): Im Modus Auto Character Set Selection (Automatische Zeichensatzauswahl) versucht das System, die Daten in einer bevorzugten Reihenfolge von Zeichensätzen zu decodieren. Mit dem verwendeten Algorithmus wird die bestmögliche Umsetzung angestrebt. Das heißt, dass es auch Fälle geben kann, in denen die Daten aus mehr als einem Zeichensatz decodiert werden können. Der erste Zeichensatz aus der bevorzugten Liste, der die Daten erfolgreich entschlüsseln kann, wird ausgewählt, um die Daten zu decodieren und an den Benutzer zu senden. Alle anderen Zeichensätze, die in der Liste enthalten sind, aber in der bevorzugten Reihenfolge weiter unten stehen, werden nicht berücksichtigt, selbst wenn die Daten mit einem solchen Zeichensatz erfolgreich decodiert werden könnten.

Der bevorzugte Zeichensatz und seine bevorzugte Reihenfolge können vom Benutzer über das Menü **Auto Character Set Preferred Order** (Bevorzugte Reihenfolge für automatische Zeichensätze) konfiguriert werden. Benutzer können die Reihenfolge durch Ziehen des entsprechenden Menüelementsymbols ändern. Um ein Element zu löschen, halten Sie das Element gedrückt, bis die Option **Delete** (Löschen) angezeigt wird. Um ein neues Element hinzuzufügen, tippen Sie auf das Menüsymbol in der oberen rechten Ecke. Daraufhin werden Optionen zum Hinzufügen von UTF-8 und GB2312 angezeigt.

- **UTF-8:** Eine Zeichencodierung, mit der alle möglichen Zeichen oder Codepunkte, die durch Unicode definiert sind, codiert werden können (Standardeinstellung).
- **GB2312:** Ein Zeichensatz für vereinfachte chinesische Schriftzeichen.
- Auto Character Set Failure Option (Option bei Fehlschlagen der automatischen Zeichensatzauswahl): Wenn das System keinen Zeichensatz aus der bevorzugten Liste finden kann, der zur erfolgreichen Decodierung der Daten verwendet werden kann, wird der in der Option Auto Character Set Failure Option (Option bei Fehlschlagen der automatischen Zeichensatzauswahl) ausgewählte Zeichensatz verwendet, um die Daten zu decodieren und an den Benutzer zu senden. Wenn NONE (Keine) verwendet wird, werden Nulldaten als Zeichenfolgendaten zurückgegeben.
  - NONE (Keine)
  - **UTF-8:** Eine Zeichencodierung, mit der alle möglichen Zeichen oder Codepunkte, die durch Unicode definiert sind, codiert werden können (Standardeinstellung).
  - **ISO-8859-1:** Teil der ISO/IEC 8859-Serie ASCII-basierter Standardzeichencodierungen. Diese sind in der Regel für westeuropäische Sprachen vorgesehen.
  - Shift\_JIS: Für westeuropäische Sprachen vorgesehen.
  - Shift\_JIS: Shift Japanese Industrial Standards (JIS) ist eine Zeichencodierung für die japanische Sprache.
  - **GB18030:** Chinesischer codierter Zeichensatz, der die erforderliche Sprachen- und Zeichenunterstützung für Software in China definiert.
- **Presentation Parameters** (Darstellungsparameter): Wählen Sie die Barcode-Eingabe für die Motiverkennungsbedingungen aus.
  - **Proximity Sensor Input** (Näherungssensoreingang): Aktiviert den Darstellungsmodus nur nach einem Näherungsereignis.
  - None (Keine): Aktiviert den Standarddarstellungsmodus.
- 1D Quiet Zone Level (Stufe für 1D-Ruhezone): Legt die "Aggressivität" bei der Decodierung von Barcodes mit einer reduzierten Ruhezone (Bereich vor und am Ende eines Barcodes) fest und gilt für Symbologien, die durch den Parameter "Reduced Quiet Zone" (Reduzierte Ruhezone) aktiviert werden. Da höhere Stufen die Decodierungszeit und das Risiko einer Fehldecodierung erhöhen, empfiehlt Zebra dringend, nur die

Symbologien zu aktivieren, die eine höhere Ruhezonenstufe erfordern, und die Option "Reduced Quiet Zone" (Reduzierte Ruhezone) für alle anderen Symbologien deaktiviert zu lassen.

Folgende Optionen stehen zur Verfügung:

- **0**: Der Scanner arbeitet normal in Bezug auf die Ruhezone.
- 1: Der Scanner arbeitet "aggressiver" in Bezug auf die Ruhezone (Standardeinstellung).
- 2: Der Scanner benötigt nur eine Seite des Barcode-Endes für die Decodierung.
- 3: Der Scanner decodiert alles in Bezug auf die Ruhezone oder das Ende des Barcodes.
- Adaptive Scanning (Adaptives Scannen): Nicht zutreffend.
  - **Disable** (Deaktivieren)
  - Enable (Aktivieren) (Standardeinstellung).
- Beam Width (Strahlbreite): Die Strahlbreite ist nur bei linearen Scannern anwendbar.
  - Narrow (Schmal)
  - Normal (Standard)
  - Wide (Breit)
- Aim mode (Zielmodus): Schaltet die Scannerbeleuchtung ein oder aus.
- On (Ein): Die Beleuchtung ist eingeschaltet (Standard).
- Off (Aus): Die Beleuchtung ist ausgeschaltet.
- Aim Timer (Ziel-Timer): Legt die maximale Zeitdauer f
  ür die Ausrichtung des Scanners auf ein Ziel fest (0– 60.000 ms in Schritten von 100 ms). Bei einem Wert von 0 bleibt der Ziel-Timer auf unbestimmte Zeit eingeschaltet (Standardeinstellung: 500).
- Aim Typ (Art der Zielausrichtung): Legt die Verwendung der Zielausrichtung fest: Auslöser, Präsentation oder kontinuierliches Lesen.
  - Trigger (Auslöser): Ein Auslöserereignis aktiviert die Decodierungsverarbeitung, die so lange fortgesetzt wird, bis das Auslöserereignis beendet wird oder eine gültige Decodierung stattfindet (Standardeinstellung).
  - **Presentation** (Präsentation): Aktiviert das Scannen im Präsentationsmodus.
  - Continuous Read (Kontinuierliches Lesen): Wählen Sie den Soft-Auslöser aus, um ein kontinuierliches Lesen desselben Barcodes zu starten. Wenn der Imager ein Objekt im Sichtfeld erkennt, wird er ausgelöst und versucht, zu decodieren.
- Beam Timer (Strahl-Timer): Legt die maximale Zeitdauer für die Ausrichtung des Lesegeräts auf ein Ziel fest (0–60.000 ms in Schritten von 100 ms). Bei einem Wert von 0 bleibt das Lesegerät auf unbestimmte Zeit eingeschaltet (Standardeinstellung: 5.000).
- Time Delay to Low Power (Zeitverzögerung bis Energiesparmodus): Legt die Zeit fest, die der Decoder nach der Decodierung aktiv bleibt. Nach einer Scansitzung wechselt der Decoder nach diesem Zeitraum in den Energiesparmodus. Optionen: 1 Second (1 Sekunde) (Standardeinstellung), 30 Seconds (30 Sekunden), 1 Minute (1 Minute) oder 5 Minutes (5 Minuten).
- **Different Symbol Timeout** (Timeout zwischen unterschiedlichen Symbolen): Steuert die Zeit, die der Scanner zwischen dem Decodieren verschiedener Symbole inaktiv ist. Programmierbar in Schritten von 500 ms von 0 bis 5 Sekunden. Die Standardeinstellung ist 500 ms.
- **Digimarc Decoding** (Digimarc-Decodierung): Aktiviert/deaktiviert die Unterstützung für Digimarc, die herkömmliche Barcode-Daten codiert und unsichtbar in die Produktverpackung integriert. Wird nur bei Verwendung eines internen Imagers unterstützt. (Standardeinstellung: aktiviert).
- Illumination Brightness (Beleuchtungshelligkeit): Einstellung der Helligkeit der Beleuchtung durch Änderung der LED-Leistung. Die Standardeinstellung ist 10, das heißt maximale LED-Helligkeit. Bei Werten von 1 bis 10 variiert die LED-Helligkeit von der niedrigsten bis zur höchsten Helligkeitsstufe.

- Illumination mode (Beleuchtungsmodus): Schaltet die Imager-Beleuchtung ein und aus. Diese Option ist nur verfügbar, wenn Bluetooth Scanner (Bluetooth-Scanner) unter Barcode input (Barcode-Eingabe), Scanner selection (Scannerauswahl) ausgewählt wurde.
  - Off (Aus): Die Beleuchtung ist ausgeschaltet.
  - **On** (Ein): Die Beleuchtung ist eingeschaltet (Standardeinstellung).
- Inverse 1D Mode (1D-Inversmodus): Mit diesem Parameter kann der Benutzer die Decodierung inverser 1D-Barcodes auswählen.
  - Disable (Deaktivieren): Deaktiviert die Decodierung inverser 1D-Barcodes (Standardeinstellung).
  - Enable (Aktivieren): Aktiviert nur die Decodierung inverser 1D-Barcodes.
  - Auto: Ermöglicht die Decodierung von positiven und inversen 1D-Barcodes.
- Keep Pairing Info After Reboot (Kopplungsinformationen nach Neustart beibehalten)
  - **Disable** (Deaktivieren): Kopplungsinformationen werden nach einem Neustart nicht beibehalten.
  - **Enable** (Aktivieren): Ermöglicht die Beibehaltung von Kopplungsinformationen nach einem Neustart. (Standard).
- LCD Mode (LCD-Modus): Aktiviert oder deaktiviert den LCD-Modus. Der LCD-Modus verbessert die Fähigkeit des Imagers, Barcodes von LCD-Displays wie Mobiltelefonen zu lesen.
  - **Disable** (Deaktivieren): Deaktiviert den LCD-Modus (Standardeinstellung).
  - Enable (Aktivieren): Aktiviert den LCD-Modus.
- Linear Security Level (Lineare Sicherheitsstufe): Legt fest, wie oft ein Barcode gelesen wird, um eine genaue Decodierung zu bestätigen.
  - Security Short or Codabar (Sicherheit bei kurzem Barcode oder Codabar): Zweifache Leseredundanz bei kurzem Barcode oder Codabar (Standard).
  - Security All Two (Sicherheit immer zweifach): Zweifache Leseredundanz für alle Barcodes.
  - Security Long and Short (Sicherheit bei kurzen und langen Barcodes): Zweifache Leseredundanz bei langen Barcodes, dreifache bei kurzen Barcodes.
  - Security All Thrice (Sicherheit immer dreifach): Dreifache Leseredundanz für alle Barcodes.
- HW Engine Low Power Timeout (Timeout bis HW-Engine-Energiesparmodus): Zeit der Inaktivität (0– 1.000 ms in Schritten von 50 ms), bevor der Scanner in den Energiesparmodus wechselt (Standardeinstellung: 250).
- Pickliste (Auswahlliste): Ermöglicht es dem Imager, nur den Barcode zu decodieren, der sich direkt innerhalb des beleuchteten Scanpunkts befindet. Diese Funktion ist bei Anwendungen nützlich, in denen mehrere Barcodes während einer Decodierungssitzung im Sichtfeld angezeigt werden können und nur einer davon für die Decodierung vorgesehen ist.
  - **Disabled** (Deaktiviert): Deaktiviert den Auswahllistenmodus. Jeder Barcode im Sichtfeld kann decodiert werden (Standardeinstellung).
  - **Enabled** (Aktiviert): Aktiviert den Auswahllistenmodus, sodass nur der Barcode unter dem projizierten Fadenkreuz decodiert werden kann.
- **Poor Quality Decode Effort** (Decodierung bei schlechter Qualität): Aktivieren Sie diese Funktion zur Verbesserung der Decodierung schlecht lesbarer Barcodes.
- Same Symbol Timeout (Timeout zwischen gleichen Symbolen): Steuert die Zeit, die der Scanner zwischen dem Decodieren gleicher Symbole inaktiv ist. Programmierbar in Schritten von 500 ms von 0 bis 5 Sekunden. Die Standardeinstellung ist 500 ms.
- Scanning Modes (Scanmodi): Auf dem Gerät verfügbare Scanoptionen.
  - Single (Einfach): Zum Scannen allgemeiner Barcodes (Standardeinstellung).
  - UDI: Zum Scannen von Barcodes für das Gesundheitswesen.

## Scan-Parameter

Ermöglicht die Konfiguration von Code-ID- und Decodierungs-Feedback-Optionen.



**HINWEIS:** Nicht alle Parameteroptionen sind für alle Scanner verfügbar. Die verfügbaren Scanner- und Parameteroptionen finden Sie in der DataWedge-App auf dem jeweiligen Gerät.

- **Code ID Type** (Code-ID-Typ): Ein Code-ID-Zeichen kennzeichnet den Codetypen eines gescannten Barcodes. Dies kann hilfreich sein, wenn der Scanner mehr als einen Codetypen decodiert. Wählen Sie ein Code-ID-Zeichen aus, das zwischen dem Präfix und dem decodierten Symbol eingefügt werden soll.
  - Code ID Type None (Kein Code-ID-Typ): Kein Präfix (Standardeinstellung)
  - Code ID Type AIM (AIM-Code-ID-Typ): Einfügen eines AIM-Zeichenpräfixes.
  - Code ID Type Symbol (Symbol-Code-ID-Typ): Einfügen eines Symbolzeichenpräfixes.
- Engine Decode LED (Engine für Decodierungs-LED): Zum Einschalten der roten LED des Scanners, wenn der Scanstrahl entweder über den Scannerauslöser oder über die Softscan-Taste ausgelöst wird.
- **BT Disconnect On Exit** (BT-Verbindung beim Beenden trennen): Die Bluetooth-Verbindung wird getrennt, wenn die Datenerfassungsanwendung geschlossen wird.
- **Connection Idle Time** (Zeitbegrenzung für Verbindung): Legen Sie die Zeitbegrenzung für die Verbindung fest. Die Bluetooth-Verbindung wird getrennt, nachdem sie für eine bestimmte Zeit inaktiv war.
- Display BT Address Barcode (BT-Adressbarcode anzeigen): Aktivieren oder deaktivieren Sie die Anzeige des Bluetooth-Adressbarcodes, wenn die Anwendung versucht, den Bluetooth-Scanner zu aktivieren und keine Bluetooth-Scanner-Kopplung vorhanden ist.
- Establish Connection Time (Zeit bis zum Herstellen der Verbindung): Das Zeitlimit, nach dem das Gerät versucht, den Bluetooth-Scanner zu aktivieren oder erneut zu verbinden, wenn sich der Bluetooth-Scanner nicht in der Nähe befindet oder nicht gekoppelt ist.
- Audio Feedback Mode (Akustische Rückmeldung): Wählen Sie ein Tonsignal für die erfolgreiche Decodierung aus.
  - Local Audio Feedback (Akustische lokale Rückmeldung): Tonsignal für die erfolgreiche Decodierung nur auf dem Gerät.
  - **Remote Audio Feedback** (Akustische Remote-Rückmeldung): Tonsignal für die erfolgreiche Decodierung.
  - Both (Beide): Tonsignal für die erfolgreiche Decodierung auf Gerät und Scanner (Standard).
  - **Disable** (Deaktivieren): Kein Tonsignal für die erfolgreiche Decodierung auf dem Gerät oder Scanner.
- LED Feedback Mode (LED-Feedback-Modus): Wählen Sie ein LED-Signal für die erfolgreiche Decodierung aus.
  - Local LED Feedback (Lokales LED-Feedback): LED-Signal für die erfolgreiche Decodierung nur auf dem Gerät.
  - Remote LED Feedback (Remote-LED-Feedback): LED-Signal für die erfolgreiche Decodierung auf dem Scanner.
  - Both (Beide): LED-Signal für die erfolgreiche Decodierung auf Gerät und Scanner (Standard).
  - **Disable** (Deaktivieren): Kein LED-Signal für die erfolgreiche Decodierung auf dem Gerät oder Scanner.
- **Decode Audio Feedback** (Akustische Rückmeldung bei Decodierung): Wählen Sie einen Signalton aus, der bei einer erfolgreichen Decodierung ertönen soll (standardmäßig optimierter Signalton).
- Decoding LED Notification (LED-Benachrichtigung bei Decodierung): Die rote Datenerfassungs-LED auf dem Gerät wird eingeschaltet, wenn die Datenerfassung läuft. (Standardeinstellung: deaktiviert).
- Decode Feedback LED Timer (LED-Timer f
  ür Decodierungs-Feedback): Legen Sie fest, wie lange (in Millisekunden) die gr
  üne Datenerfassungs-LED nach einer erfolgreichen Decodierung leuchten soll. (Standardeinstellung: 75 ms)
- Beep Volume Control (Lautstärkeregelung für Signalton): Stellen Sie den Signalton für die erfolgreiche Decodierung auf einen Systemton oder einen anderen Ton ein. Dies ermöglicht eine unabhängige Steuerung der Lautstärkeregelung des Signaltons bei erfolgreicher Decodierung.



**HINWEIS:** Nicht alle Klingeltöne werden als Decodierungstöne vollständig unterstützt, und längere Klingeltöne können gekürzt werden, wenn sie als Decodierungston verwendet werden. Es wird empfohlen, den ausgewählten Ton vor der Bereitstellung an einem Kundenstandort zu testen.

- Ringer (Klingelton): Stellen Sie den Signalton für die erfolgreiche Decodierung für den Klingelton ein.
- **Music and Media** (Musik und Medien): Stellen Sie den Signalton für die erfolgreiche Decodierung für den Medienton ein.
- Alarms (Alarme): Stellen Sie den Signalton für die erfolgreiche Decodierung für den Alarmton ein.
- **Notifications** (Benachrichtigung): Stellen Sie den Signalton für die erfolgreiche Decodierung für den Benachrichtigungston ein (Standardeinstellung).

### **UDI-Parameter**

Ermöglicht die Konfiguration von Parametern, die für im Gesundheitswesen verwendete Barcodes spezifisch sind.

- Enable UDI-GSI (UDI-GSI aktivieren): UDI mit GS1-Standards aktivieren (Standardeinstellung: aktiviert).
- Enable UDI-HIBCC (UDI-HIBCC aktivieren): UDI mit HIBCC-Standards aktivieren (Standardeinstellung: aktiviert).
- Enable UDI-ICCBBA (UDI-ICCBBA aktivieren): UDI mit HIBCC-Standards aktivieren (Standardeinstellung: aktiviert).

## Aktivierung bei Unterbrechung beibehalten

Die Aktivierung des Bluetooth-Scanners wird nach einer Unterbrechung beibehalten (standardmäßig deaktiviert).

# Spracheingabe

DataWedge unterstützt die Ausgabe von Tastenanschlägen, d. h. die verarbeiteten Daten werden erfasst und als Tastenfolge an die Vordergrundanwendung gesendet, sodass die Datenerfassung in Anwendungen möglich ist, ohne Code schreiben zu müssen. DataWedge sendet erfasste Daten über Intents, die für Benutzeranwendungen genutzt werden können, ohne sich Gedanken über das Schreiben von komplexem Code zur Datenerfassung machen zu müssen. DataWedge erfasst derzeit keine Daten für die Spracheingabe. Zebra GMS-Geräte verfügen über eine integrierte Google-Spracherkennungs-Engine. Durch die Nutzung der Spracherkennungsfunktionen wurde die automatisierte Datenerfassung für Benutzeranwendungen über Sprache in DataWedge erweitert.

Die Erfassung von Sprachdaten beginnt, nachdem Sie den vordefinierten Startsatz gesprochen haben, und endet, wenn Sie die Daten oder den Endsatz sprechen, sofern ein solcher definiert wurde.

### WICHTIG:

- Die gleichzeitige Verwendung der Spracheingabe in DataWedge und Google Voice wird nicht unterstützt.
- Die Spracheingabe wird nicht unterstützt, wenn sich der Enterprise Home Screen (EHS) im eingeschränkten Modus befindet. Die Spracheingabe kann jedoch durch die Aktivierung aller Berechtigungseinstellungen in EHS wieder aktiviert werden.
- Die Spracheingabe wird nicht unterstützt, wenn die Gerätesprache in eine andere Sprache geändert wird, z. B. Chinesisch.

Über die Option Voice Input (Spracheingabe) kann das Spracheingabe-Plug-in konfiguriert werden.

- Enabled (Aktiviert): Aktiviert oder deaktiviert dieses Plug-in. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist.
- **Data capture start phrase** (Startsatz für die Datenerfassung): Startet die Datenerfassung mit dem in dieses Feld eingegebenen Satz. Dieses Feld ist obligatorisch. (Standardeinstellung: **start**).

Die Angabe von Zahlen und anderen Sonderzeichen als Startsatz für die Datenerfassung wird nicht unterstützt.

- Data capture end phrase (Endsatz für die Datenerfassung): Beendet die Datenerfassung mit dem in dieses Feld eingegebenen Ausdruck, falls erforderlich. Die Eingabe in diesem Feld ist nicht obligatorisch. (Standardeinstellung: leer).
- **Tab command** (Tabulatorbefehl): Aktiviert den Tabulatorbefehl. Dadurch wird eine Tabulatortaste übertragen, wenn der Benutzer den Befehl **Tabulator senden** sagt. Die Befehle werden nur unterstützt, wenn sich das Gerät im Zustand **Warten auf Startsatz** befindet.
- ENTER command (Eingabetastenbefehl): Aktiviert den Eingabetastenbefehl. Dadurch wird eine Eingabetaste übertragen, wenn der Benutzer den Befehl Tabulatortaste senden sagt. Die Befehle werden nur unterstützt, wenn sich das Gerät im Zustand Warten auf Startsatz befindet.
- **Data type** (Datentyp): Ermöglicht dem Benutzer, den Datentyp zu konfigurieren. Legen Sie den Datentyp fest, um die Datenerfassung gemäß den festgelegten Einstellungen zu begrenzen. Verfügbare Optionen:
  - Any (Beliebig): Beim Scannen eines Barcodes von ABC123 wird ABC123 zurückgegeben.
  - Alpha (Alphabetische Zeichen): Beim Scannen eines Barcodes von ABC123 wird ABC zurückgegeben.
  - Numeric (Numerische Zeichen): Beim Scannen eines Barcodes von ABC wird nur 123 zurückgegeben.
- Start phrase waiting tone (Warteton für Startsatz): Aktiviert oder deaktiviert diese Option. Aktiviert die akustische Rückmeldung für Warten auf Start. Diese Option benachrichtigt den Benutzer, dass das Gerät auf den Start des Sprachmoduls wartet, wenn Sie die Ankündigungsmeldung verpassen und sich der Status Warten auf Start ändert.
- Data capture waiting tone (Warteton für Datenerfassung): Aktiviert oder deaktiviert diese Option. Aktiviert die akustische Rückmeldung für Warten auf Daten. Diese Option benachrichtigt den Benutzer, dass das Gerät darauf wartet, Daten zu erfassen, wenn Sie die Ankündigungsmeldung verpassen.
- Validation window (Validierungsfenster): Aktiviert oder deaktiviert das Fenster Validate captured data (Erfasste Daten validieren). Aktivieren Sie diese Option, um das Ergebnis Ihrer Spracheingabe zu bestätigen. Im Fenster werden die gesprochenen Daten angezeigt, und die Daten können auf demselben Bildschirm bearbeitet werden, falls Änderungen erforderlich sind. Dies ist sehr nützlich, wenn Sie im Offline-Modus arbeiten.

Die Bearbeitung im Validierungsfenster wird nicht unterstützt, wenn die Tastenanschlag-Eingabe in dem Profil aktiviert ist, in dem die Spracheingabe aktiviert ist.

• Offline speech recognition (Offline-Spracherkennung): Aktiviert oder deaktiviert die Spracherkennung. Aktivieren Sie diese Option, um die Spracheingabe zu verwenden, wenn Sie keinen Zugriff auf das Internet haben. Bei dieser Option wird ein Sprachmodul für die Offline-Spracherkennung verwendet, um die von Ihnen gesprochenen Daten zu erkennen.

# Tastenanschlag-Ausgabe

Verwenden Sie diese Option, um das Plug-in für die Tastenanschlag-Ausgabe für das Profil zu konfigurieren.

- Enabled (Aktiviert): Aktiviert oder deaktiviert dieses Plug-in. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: aktiviert).
- Action key character (Schlüsselzeichen für Aktion): Ermöglicht die Decodierung eines in Barcode-Daten eingebetteten Sonderzeichens für die Verwendung in nativen Android-Anwendungen. Diese Funktion ist hilfreich, wenn Sie ein Formular ausfüllen oder verarbeiten.
  - None (Keine): Die Funktion für Aktionsschlüsselzeichen ist deaktiviert (Standardeinstellung).
  - **Tab** (Tabulator): Der Tabulatorzeichencode in einem Barcode wird verarbeitet. Wenn DataWedge diesen Zeichencode in einem Barcode erkennt, wird der Fokus auf das nächste Feld verschoben.
  - Line feed (Zeilenvorschub): Zeilenvorschub-Zeichencode in einem Barcode wird verarbeitet. Wenn DataWedge diesen Zeichencode in einem Barcode erkennt, wird der Fokus auf das nächste Feld verschoben.
  - **Carriage return** (Wagenrücklauf): Wagenrücklaufzeichen in einem Barcode werden verarbeitet. Wenn DataWedge diesen Zeichencode in einem Barcode erkennt, wird der Fokus auf das nächste Feld verschoben.
- Inter character delay (Verzögerung zwischen Zeichen): Legen Sie die Verzögerung zwischen Tastenanschlägen fest (in Millisekunden).
- Delay Multibyte characters only (Verzögerungen nur bei Multibyte-Zeichen): Wenn die Verzögerung zwischen Zeichen eingestellt ist, aktivieren Sie diese Option, um nur Multibyte-Zeichen zu verzögern.
- Key event delay (Verzögerung für Schlüsselereignis): Legen Sie die Wartezeit (in Millisekunden) für Steuerzeichen fest. (Standard: 0)
- Data formatting and ordering (Datenformatierung und -reihenfolge): Ermöglicht die Formatierung und Sortierung von UDI-Daten.
  - **UDI specific** (UDI-spezifisch): Ermöglicht die Anpassung der Ausgabereihenfolge der erfassten UDI-Daten und das optionale Einfügen von Tabulator-, Zeilenvorschub- oder Wagenrücklaufzeichen zwischen den Token.
    - Send tokens (Token senden): Mit dieser Option wählen Sie das Ausgabeformat für UDI-Daten aus. (Standardeinstellung: deaktiviert)
    - **Token separator** (Tokentrennzeichen): Mit dieser Option wählen Sie ein Trennzeichen aus. Wenn kein Trennzeichen ausgewählt ist und für "Send tokens" (Token senden) Barcodes und Token festgelegt sind, werden zwei Instanzen derselben Daten gesendet. (Standardeinstellung: keine)
    - **Token order** (Tokenreihenfolge): Mit dieser Option legen Sie fest, ob Token in die Ausgabe einbezogen oder davon ausgeschlossen werden sollen, und passen die Ausgabereihenfolge an.
    - **Barcode separator** (Barcode-Trennzeichen): Wählen Sie ein Trennzeichen aus. Wenn kein Trennzeichen ausgewählt ist, wird der Datensatz als einzelne Zeichenfolge gesendet.
- Advanced data formatting (Erweiterte Datenformatierung): Bietet die Möglichkeit, Daten vor der Übertragung anzupassen. Mithilfe der erweiterten Datenformatierung (Advanced Data Formatting, ADF) können Sie Scandaten Ihren Anforderungen entsprechend anpassen.
  - **Enable** (Aktivieren): Aktiviert oder deaktiviert ADF. Ein Häkchen im Kontrollkästchen zeigt an, dass ADF aktiviert ist (Standardeinstellung: deaktiviert).
  - Rules (Regeln): ADF verwendet Regeln zum Anpassen von Daten. Diese Regeln führen detaillierte Aktionen aus, wenn die Daten bestimmte Kriterien erfüllen. Eine Regel muss aus einem Kriterium oder mehreren Kriterien bestehen, die für eine oder mehrere Aktionen gelten. Weitere Informationen sind unter Erstellen von Regeln für die erweiterte Datenformatierungsregel auf Seite 96 zu finden.

- **Basic data formatting** (Grundlegende Datenformatierung): Ermöglicht die Konfiguration aller Datenformatierungen für das zugehörige Ausgabe-Plug-in. Wenn das Plug-in deaktiviert ist, werden alle Daten ohne Änderung übergeben.
  - **Enabled** (Aktiviert): Aktiviert oder deaktiviert die grundlegende Datenformatierung. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).
  - **Prefix to data** (Als Daten-Präfix): Fügen Sie dem Anfang der Daten Zeichen hinzu, wenn diese gesendet werden.
  - Suffix to data (Als Daten-Suffix): Fügen Sie dem Ende der Daten Zeichen hinzu, wenn diese gesendet werden.
  - Send data (Daten senden): Mit dieser Option legen Sie fest, dass die erfassten Daten an die Vordergrundanwendung übertragen werden. Wenn Sie diese Option deaktivieren, werden die eigentlichen Daten nicht übertragen. Die Präfix- und Suffixzeichenfolgen, sofern vorhanden, werden jedoch auch dann übertragen, wenn diese Option deaktiviert ist (Standardeinstellung: aktiviert).
  - Send as hex (Als Hexadezimalwert senden): Mit dieser Option legen Sie fest, dass die Daten im Hexadezimalformat gesendet werden sollen. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).
  - Send TAB key (TAB-Taste senden): Legt fest, dass ein Tabulatorzeichen an das Ende der verarbeiteten Daten angehängt wird. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).
  - Send ENTER key (ENTER-Taste senden): Legt fest, dass ein ENTER-Zeichen an das Ende der verarbeiteten Daten angehängt wird. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).

# Intent-Ausgabe

Ermöglicht die Konfiguration des Intent-Ausgabe-Plug-ins für das Profil. Mit dem Intent-Ausgabe-Plug-in können die erfassten Daten in Form eines impliziten Intents an eine Anwendung gesendet werden. Weitere Informationen finden Sie auf der Android Developer-Website unter <u>http://developer.android.com</u>.

- Enabled (Aktiviert): Aktiviert oder deaktiviert dieses Plug-in. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: aktiviert).
- Intent action (Intent-Aktion): Geben Sie den Namen der Intent-Aktion ein (erforderlich).
- Intent category (Intent-Kategorie): Geben Sie den Namen der Intent-Kategorie ein (erforderlich).
- Intent delivery (Intent-Zustellung): Wählen Sie die Methode zur Übertragung des Intents aus:
  - Senden über StartActivity
  - Senden über startService (Standard)
  - Intent senden
- **Receiver foreground flag** (Markierung für Empfänger im Vordergrund): Legen Sie die Markierung zum Senden des Intents bei der Intent-Übertragung fest. (DS3678).
- Advanced data formatting (Erweiterte Datenformatierung): Bietet die Möglichkeit, Daten vor der Übertragung anzupassen. Mithilfe der erweiterten Datenformatierung (Advanced Data Formatting, ADF) können Sie Scandaten Ihren Anforderungen entsprechend anpassen.
  - Enable (Aktivieren): Aktiviert oder deaktiviert ADF. Ein Häkchen im Kontrollkästchen zeigt an, dass ADF aktiviert ist (Standardeinstellung: deaktiviert).
  - Rules (Regeln): ADF verwendet Regeln zum Anpassen von Daten. Diese Regeln führen detaillierte Aktionen aus, wenn die Daten bestimmte Kriterien erfüllen. Eine Regel muss aus einem Kriterium oder mehreren Kriterien bestehen, die für eine oder mehrere Aktionen gelten. Weitere Informationen sind unter Erstellen von Regeln für die erweiterte Datenformatierungsregel auf Seite 96 zu finden.

- **Basic data formatting** (Grundlegende Datenformatierung): Ermöglicht die Konfiguration aller Datenformatierungen für das zugehörige Ausgabe-Plug-in. Wenn das Plug-in deaktiviert ist, werden alle Daten ohne Änderung übergeben.
  - **Enabled** (Aktiviert): Aktiviert oder deaktiviert die grundlegende Datenformatierung. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).
  - **Prefix to data** (Als Daten-Präfix): Fügen Sie dem Anfang der Daten Zeichen hinzu, wenn diese gesendet werden.
  - Suffix to data (Als Daten-Suffix): Fügen Sie dem Ende der Daten Zeichen hinzu, wenn diese gesendet werden.
  - Send data (Daten senden): Mit dieser Option legen Sie fest, dass die erfassten Daten an die Vordergrundanwendung übertragen werden. Wenn Sie diese Option deaktivieren, werden die eigentlichen Daten nicht übertragen. Die Präfix- und Suffixzeichenfolgen, sofern vorhanden, werden jedoch auch dann übertragen, wenn diese Option deaktiviert ist (Standardeinstellung: aktiviert).
  - Send as hex (Als Hexadezimalwert senden): Mit dieser Option legen Sie fest, dass die Daten im Hexadezimalformat gesendet werden sollen. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).
  - Send TAB key (TAB-Taste senden): Legt fest, dass ein Tabulatorzeichen an das Ende der verarbeiteten Daten angehängt wird. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).
  - Send ENTER key (ENTER-Taste senden): Legt fest, dass ein ENTER-Zeichen an das Ende der verarbeiteten Daten angehängt wird. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).

### Überblick über Intents

Die Kernkomponenten einer Android-Anwendung (Aktivitäten, Dienste und Sendeempfänger) werden durch Intents aktiviert. Ein Intent ist ein Informationspaket (ein Intent-Objekt), das eine gewünschte Aktion beschreibt, einschließlich der zu bearbeitenden Daten, der Kategorie der Komponente, die die Aktion ausführen soll, und anderer relevanter Anweisungen. Android sucht nach einer geeigneten Komponente, um auf das Intent zu reagieren, startet bei Bedarf eine neue Instanz der Komponente und übergibt sie an das Intent-Objekt.

Komponenten geben ihre Fähigkeiten und die Art der Intents, auf die sie reagieren können, mithilfe von Intent-Filtern an. Da das System lernen muss, welche Intents eine Komponente verarbeiten kann, bevor es die Komponente startet, werden Intent-Filter im Manifest als <intent-filter>Elemente festgelegt. Eine Komponente kann über eine beliebige Anzahl von Filtern verfügen, von denen jeder eine andere Funktion beschreibt. Wenn das Manifest beispielsweise Folgendes enthält:

```
<intent-filter . . . >
<action android:name="android.intent.action.DEFAULT" />
<category android:name="android.intent.category.MAIN" />
</intent-filter>
```

In der Konfigurationen des Intent-Ausgabe-Plug-ins würde die Intent-Aktion folgendermaßen aussehen: android.intent.category.DEFAULT

und die Intent-Kategorie wäre:

android.intent.category.MAIN.

Mit der Option **Intent delivery** (Intent-Zustellung) kann die Methode zur Übertragung des Intents angegeben werden. Die Zustellungsmechanismen sind **Send via startActivity** (Senden über startActivity), **Send via StartService** (Senden über startService) oder **Broadcast intent** (Intent senden).

Die decodierungsbezogenen Daten, die dem Intent-Paket hinzugefügt wurden, können mithilfe der Aufrufe **Intent.getStringExtra()** und **Intent.getSerializableExtra()** abgerufen werden, wobei die folgenden String-Tags verwendet werden:

- String LABEL\_TYPE\_TAG = "com.symbol.emdk.datawedge.label\_type";
  - Der String enthält den Etikettentyp des Barcodes.
- String DATA\_STRING\_TAG = "com.symbol.emdk.datawedge.data\_string";
  - Der String enthält die Ausgabedaten als String. Bei verketteten Barcodes werden die Decodierungsdaten verkettet und als eine Zeichenfolge gesendet.
- String DECODE\_DATA\_TAG = "com.symbol.emdk.datawedge.decode\_data";
  - Decodierungsdaten werden als Liste von Byte-Arrays zurückgegeben. In den meisten Fällen handelt es sich um ein Byte-Array pro Decodierung. Bei Barcode-Symbologien, die Verkettungen unterstützen, z. B. Codabar, Code128, MicroPDF usw., werden die decodierten Daten in Multibyte-Arrays gespeichert (ein Byte-Array pro Barcode). Clients können durch Übergabe eines Index Daten in jedem Byte-Array abrufen.

In den meisten Scananwendungen sollen Benutzer Daten decodieren und diese Decodierungsdaten an die \*current\* (aktuelle) Aktivität senden, ohne dass diese unbedingt angezeigt werden soll. In diesem Fall muss die Aktivität in der zugehörigen AndroidManifest.xml-Datei als "singleTop" markiert werden. Wenn Ihre Aktivität nicht als "singleTop" definiert ist, erstellt das System bei jeder Decodierung eine weitere Kopie Ihrer Aktivität und sendet die Decodierungsdaten an diese zweite Kopie.

Schließlich gibt es für jedes Verarbeitungs-Plug-in eine Konfigurationsoption, sodass das Verarbeitungs-Plug-in speziell für die Intent-Ausgabe konfiguriert werden kann, was in diesem Fall das Verarbeitungs-Plug-in für die grundlegende Datenformatierung ist.

# **IP-Ausgabe**



**HINWEIS:** Die Anwendung IPWedge ist auf einem Host-Computer erforderlich. Laden Sie die IPWedge-Anwendung über die Support-Website von Zebra herunter: <u>www.zebra.com/support</u>.

Über die IP-Ausgabe kann DataWedge erfasste Daten per Netzwerkverbindung an einen Host-Computer senden. Erfasste Daten können über ein IP-Netzwerk an eine angegebene IP-Adresse und einen festgelegten Port gesendet werden, wobei entweder TCP- oder UDP-Transportprotokolle verwendet werden.

- Enabled (Aktiviert): Aktiviert oder deaktiviert dieses Plug-in. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: aktiviert).
- **Remote Wedge**: Aktivieren oder deaktivieren Sie die Option "Remote Wedge" (Standardeinstellung: aktiviert). Remote Wedge wird mit der Anwendung IPWedge verwendet.
- Protocol (Protokoll): W\u00e4hlen Sie das Protokoll aus, das von der Remote-Anwendung verwendet wird. Optionen: TCP (Standard) oder UDP.
- IP address (IP-Adresse): Geben Sie die von der Remote-Anwendung verwendete IP-Adresse ein (Standardeinstellung: 0.0.0.0).
- Port: Geben Sie die von der Remote-Anwendung verwendete Portnummer ein (Standardeinstellung: 58627).
- Data formatting and ordering (Datenformatierung und -reihenfolge): Ermöglicht die Formatierung und Sortierung von UDI-Daten.
  - **UDI specific** (UDI-spezifisch): Ermöglicht die Anpassung der Ausgabereihenfolge der erfassten UDI-Daten und das optionale Einfügen von Tabulator-, Zeilenvorschub- oder Wagenrücklaufzeichen zwischen den Token.
    - Send tokens (Token senden): Mit dieser Option wählen Sie das Ausgabeformat für UDI-Daten aus. (Standardeinstellung: deaktiviert)
    - **Token separator** (Tokentrennzeichen): Mit dieser Option wählen Sie ein Trennzeichen aus. Wenn kein Trennzeichen ausgewählt ist und für "Send tokens" (Token senden) Barcodes und Token festgelegt sind, werden zwei Instanzen derselben Daten gesendet. (Standardeinstellung: keine)
    - **Token order** (Tokenreihenfolge): Mit dieser Option legen Sie fest, ob Token in die Ausgabe einbezogen oder davon ausgeschlossen werden sollen, und passen die Ausgabereihenfolge an.

- Advanced data formatting (Erweiterte Datenformatierung): Bietet die Möglichkeit, Daten vor der Übertragung anzupassen. Mithilfe der erweiterten Datenformatierung (Advanced Data Formatting, ADF) können Sie Scandaten Ihren Anforderungen entsprechend anpassen.
  - Enable (Aktivieren): Aktiviert oder deaktiviert ADF. Ein Häkchen im Kontrollkästchen zeigt an, dass ADF aktiviert ist (Standardeinstellung: deaktiviert).
  - Rules (Regeln): ADF verwendet Regeln zum Anpassen von Daten. Diese Regeln führen detaillierte Aktionen aus, wenn die Daten bestimmte Kriterien erfüllen. Eine Regel muss aus einem Kriterium oder mehreren Kriterien bestehen, die für eine oder mehrere Aktionen gelten. Weitere Informationen sind unter Erstellen von Regeln für die erweiterte Datenformatierungsregel auf Seite 96 zu finden.
- Basic data formatting (Grundlegende Datenformatierung): Ermöglicht die Konfiguration aller Datenformatierungen f
  ür das zugeh
  örige Ausgabe-Plug-in. Wenn das Plug-in deaktiviert ist, werden alle Daten ohne Änderung 
  übergeben.
  - Enabled (Aktiviert): Aktiviert oder deaktiviert die grundlegende Datenformatierung. Ein Häkchen im Kontrollkästchen zeigt an, dass die Option aktiviert ist (Standardeinstellung: aktiviert).
  - Prefix to data (Als Daten-Präfix): Fügen Sie dem Anfang der Daten Zeichen hinzu, wenn diese gesendet werden.
  - Suffix to data (Als Daten-Suffix): Fügen Sie dem Ende der Daten Zeichen hinzu, wenn diese gesendet werden.
  - Send data (Daten senden): Mit dieser Option legen Sie fest, dass die erfassten Daten an die Vordergrundanwendung übertragen werden. Wenn Sie diese Option deaktivieren, werden die eigentlichen Daten nicht übertragen. Die Präfix- und Suffixzeichenfolgen, sofern vorhanden, werden jedoch auch dann übertragen, wenn diese Option deaktiviert ist (Standardeinstellung: aktiviert).
  - Send as hex (Als Hexadezimalwert senden): Mit dieser Option legen Sie fest, dass die Daten im Hexadezimalformat gesendet werden sollen. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).
  - Send TAB key (TAB-Taste senden): Legt fest, dass ein Tabulatorzeichen an das Ende der verarbeiteten Daten angehängt wird. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).
  - Send ENTER key (ENTER-Taste senden): Legt fest, dass ein ENTER-Zeichen an das Ende der verarbeiteten Daten angehängt wird. Ein Häkchen im Kontrollkästchen zeigt an, dass das Plug-in aktiviert ist (Standardeinstellung: deaktiviert).

### Verwendung

Dieser Abschnitt enthält Informationen zur Konfiguration der IP-Ausgabe über die Benutzeroberfläche der DataWedge-Konfiguration. So verwenden Sie die IP-Ausgabe in einem bestimmten DataWedge-Profil (z. B. **Profile0** (Profil 0). Scrollen Sie nach unten zu **IP Output** (IP-Ausgabe).

Profile: Test	
IP output	
Enabled Enable/disable output via IP	
Remote Wedge Enable/disable Remote Wedge option	
Protocol TCP	
IP address 0.0.0.0	
<b>Port</b> 58627	
Data formatting and ordering UDI/Multibarcode data formatting and ordering IP output	for

Abbildung 55 Bildschirm "IP-Ausgabe"

# Verwenden der IP-Ausgabe mit IPWedge

IPWedge ist eine Computeranwendung, die problemlos für das Abrufen von Daten konfiguriert werden kann, die über die DataWedge IP-Ausgabe über das Netzwerk gesendet werden. Informationen zur Installation und Konfiguration auf einem Host-Computer finden Sie im IPWedge-Benutzerhandbuch. So aktivieren Sie die IP-Ausgabe, um erfasste Daten an einen Remote-Computer zu senden, der mit IPWedge installiert ist:

1. Berühren Sie unter IP Output (IP-Ausgabe) die Option Enabled (Aktiviert).

Im Kontrollkästchen wird ein Häkchen angezeigt.

- 2. Stellen Sie sicher, dass die Option **Remote Wedge** aktiviert ist.
- 3. Berühren Sie Protocol (Protokoll).
- Wählen Sie im Dialogfeld Choose protocol (Protokoll auswählen) dasselbe Protokoll aus, das f
  ür die IPWedge-Computeranwendung ausgewählt wurde. (TCP ist die Standardeinstellung.)

#### Abbildung 56 Protokollauswahl

Choose protocol	
• ТСР	
	CANCEL

- 5. Berühren Sie IP Address (IP-Adresse).
- 6. Geben Sie im Dialogfeld Enter IP Address (IP-Adresse eingeben) die IP-Adresse des Host-Computers ein, an den Daten gesendet werden sollen.





- 7. Berühren Sie Port.
- 8. Geben Sie im Dialogfeld **Enter port number** (Portnummer eingeben) die gleiche Portnummer ein, die für die IPWedge-Computeranwendung ausgewählt wurde.

#### Abbildung 58 Eingabe der Portnummer

Enter port number		
58627		
	CANCEL	ОК

 Konfigurieren Sie die Plug-ins f
ür die erweiterte Datenformatierung und f
ür die grundlegende Datenformatierung, falls 
Änderungen an erfassten Daten vor dem Senden an einen Remote-Computer erforderlich sind.

### Verwenden der IP-Ausgabe ohne IPWedge

Das IP-Ausgabe-Plug-in kann verwendet werden, um erfasste Daten von DataWedge ohne Verwendung von IPWedge an ein Remote-Gerät oder einen Host-Computer zu senden. Auf der Datenempfängerseite sollte der Host-Computer oder das mobile Gerät über eine Anwendung verfügen, die TCP- oder UDP-Daten abhört, die von einem konfigurierten Port und einer IP-Adresse im IP-Ausgabe-Plug-in stammen. So aktivieren Sie die IP-Ausgabe, um erfasste Daten an einen Remote-Computer zu senden:

1. Berühren Sie unter **IP Output** (IP-Ausgabe) die Option **Enabled** (Aktiviert).

Im Kontrollkästchen wird ein Häkchen angezeigt.

- 2. Stellen Sie sicher, dass die Option Remote Wedge deaktiviert ist.
- 3. Berühren Sie Protocol (Protokoll).
- 4. Wählen Sie im Dialogfeld **Choose protocol** (Protokoll auswählen) dasselbe Protokoll aus, das in der Client-Anwendung ausgewählt wurde. (TCP ist die Standardeinstellung.)

Abbildung 59 Protokollauswahl

Choose protocol	
	CANCEL

- 5. Berühren Sie IP Address (IP-Adresse).
- 6. Geben Sie im Dialogfeld **Enter IP address** (IP-Adresse eingeben) die IP-Adresse des Host-Computers ein, an den Daten gesendet werden sollen.

### Abbildung 60 Eingabe der IP-Adresse

Enter IP addr	ess	
0.0.0.0		
	CANCEL	ОК

7. Berühren Sie Port.

8. Geben Sie im Dialogfeld **Enter port number** (Portnummer eingeben) die Portnummer ein, die von der Host-Computeranwendung überwacht wird.

Enter port number		
58627		
	CANCEL	ОК

 Konfigurieren Sie die Plug-ins f
ür die erweiterte Datenformatierung und f
ür die grundlegende Datenformatierung, falls 
Änderungen an erfassten Daten vor dem Senden an einen Remote-Computer erforderlich sind.

# Erstellen von Regeln für die erweiterte Datenformatierungsregel

Mit dem Plug-in für die erweiterte Datenformatierung werden Regeln (Aktionen, die auf Grundlage definierter Kriterien durchgeführt werden sollen) auf die über ein Eingabe-Plug-in empfangenen Daten angewendet, bevor sie an ein Ausgabe-Plug-in übergeben werden.

- Regeln: Das Plug-in für die ADF-Verarbeitung umfasst eine oder mehrere Regeln. DataWedge formatiert die Ausgabedaten gemäß der ersten übereinstimmenden Regel. Eine Regel ist eine Kombination aus Kriterien und einer Reihe von Aktionen, die ausgeführt werden müssen, wenn die in der Regel festgelegten Kriterien erfüllt sind.
- Kriterien: Die Kriterien können nach Eingabe-Plug-in, Symbologie, übereinstimmender Zeichenfolge innerhalb der Daten (an einer festgelegten Position) und/oder Datenlänge festgelegt werden. Empfangene Daten müssen mit den definierten Kriterien übereinstimmen, damit die Daten verarbeitet werden können.
- Aktionen: Eine Reihe von Verfahren, die zur Formatierung von Daten definiert werden. Es gibt vier Arten von Aktionen, mit denen Vorgaben zum Formatieren der Cursorbewegung, zur Datenänderung, zum Senden von Daten und zur Verzögerung festgelegt werden können. Eine Aktion kann definiert werden, um die erste Anzahl von Zeichen an das Ausgabe-Plug-in zu senden, die Ausgabedaten mit Leerzeichen oder Nullen aufzufüllen, Leerzeichen in Daten zu entfernen usw.

## Konfigurieren des ADF-Plug-ins

Zum Konfigurieren des ADF-Plug-ins wird eine Regel erstellt, die Kriterien und Aktionen definiert.

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **k**.
- 2. Berühren Sie ein DataWedge-Profil.

3. Berühren Sie unter **Keystroke Output** (Tastenanschlag-Ausgabe) die Option **Advanced data formatting** (Erweiterte Datenformatierung).

Abbildung 62 Bildschirm für die erweiterte Datenformatierung



4. Berühren Sie das Kontrollkästchen Enable (Aktivieren), um ADF zu aktivieren.

## **Erstellen einer Regel**



HINWEIS: Standardmäßig ist Rule0 (Regel 0) die einzige Regel in der Regelliste.

- 1. Berühren Sie :
- 2. Berühren Sie New rule (Neue Regel).
- 3. Berühren Sie das Textfeld Enter rule name (Regelnamen eingeben).
- 4. Geben Sie im Textfeld einen Namen für die neue Regel ein.
- 5. Berühren Sie OK.

## **Definieren einer Regel**

1. Berühren Sie die neu erstellte Regel in der Liste Rules (Regeln).

### Abbildung 63 Bildschirm mit der Regelliste

Rule: Rule0	
Rule enabled Enable/disable this rule	
Criteria	
Criteria Set the criteria for this rule	
Actions	
Actions Configure actions	

2. Berühren Sie das Kontrollkästchen Rule enabled (Regel aktiviert), um die aktuelle Regel zu aktivieren.

### Definieren von Kriterien

1. Berühren Sie Criteria (Kriterien).

Abbildung 64 Kriterienbildschirm



- 2. Berühren Sie **String to check for** (Zu prüfende Zeichenfolge), um die Zeichenfolge anzugeben, die in den Daten enthalten sein muss.
- 3. Geben Sie im Dialogfeld **Enter the string to check for** (Zu prüfende Zeichenfolge eingeben) die entsprechende Zeichenfolge ein.
- 4. Berühren Sie OK.
- 5. Berühren Sie die Option String position (Zeichenfolgeposition), um die Position der Zeichenfolge anzugeben, die mit der Option String to check for (Zu pr
  üfende Zeichenfolge) angegeben wurde. Die ADF-Regel wird nur angewendet, wenn die unter String to check for (Zu pr
  üfende Zeichenfolge) angegebene Zeichenfolge an der festgelegten Zeichenfolgeposition gefunden wird (Null f
  ür den Start der Zeichenfolge).
- 6. Berühren Sie + oder zum Ändern des Werts.
- 7. Berühren Sie **OK**.
- 8. Berühren Sie die Option **String length** (Zeichenfolgenlänge), um eine Länge für die empfangenen Daten anzugeben. Die ADF-Regel gilt nur für die Barcode-Daten mit der angegebenen Länge.
- 9. Berühren Sie + oder zum Ändern des Werts.
- 10.Berühren Sie **OK**.
- 11.Berühren Sie die Option **Source criteria** (Quellkriterien), um der ADF-Regel ein Eingabegerät zuzuweisen. Die ADF-Regel gilt nur für Daten, die von zugewiesenen Eingabegeräten empfangen werden.
- 12.Berühren Sie Barcode input (Barcode-Eingabe). Die Optionen variieren je nach Gerätekonfiguration.
- 13. Berühren Sie das Kontrollkästchen Source enabled (Quelle aktiviert), um Daten von dieser Quelle zu akzeptieren.

#### Abbildung 65 Bildschirm für die Barcode-Eingabe

	💎 📋 11:39 AM
Source criteria: Barco	ode input
Source enabled Accept data from this source	
All label IDs enabled Allow all UDI label IDs	
Label IDs	
All decoders enabled Allow all barcode symbologies	s 🗹
Decoders	

- 14. Berühren Sie für allgemeine Barcode-Eingaben das Kontrollkästchen **All decoders enabled** (Alle Decoder aktiviert) zur Auswahl aller Barcode-Symbologien. Deaktivieren Sie das Kontrollkästchen **All decoders enabled** (Alle Decoder aktiviert), um die Symbologien einzeln auszuwählen.
- 15.Berühren Sie **〈**, bis der Bildschirm **Rule** (Regel) angezeigt wird.
- 16. Wiederholen Sie bei Bedarf diese Schritte, um eine weitere Regel zu erstellen.
- 17.Berühren Sie **〈**, bis der Bildschirm **Rule** (Regel) angezeigt wird.

## **Definieren einer Aktion**



HINWEIS: Standardmäßig befindet sich die Aktion Send remaining (Verbleibende senden) in der Liste Actions (Aktionen).

- 1. Berühren Sie .
- 2. Berühren Sie New action (Neue Aktion).
- 3. Wählen Sie im Menü **New action** (Neue Aktion) eine Aktion aus, die der Liste **Actions** (Aktionen) hinzugefügt werden soll.
- 4. Für einige Aktionen sind zusätzliche Informationen erforderlich. Berühren Sie die Aktion, um zusätzliche Informationsfelder anzuzeigen.
- 5. Wiederholen Sie diese Schritte, um weitere Aktionen zu erstellen.
- 6. Berühren Sie **<**.
- 7. Berühren Sie **<**.

### Löschen einer Regel

- 1. Berühren und halten Sie eine Regel gedrückt, bis das Kontextmenü angezeigt wird.
- 2. Berühren Sie Delete rule (Regel löschen), um die Regel aus der Liste Rules (Regeln) zu löschen.



**HINWEIS:** Wenn für das ADF-Plug-in keine Regel verfügbar ist oder alle Regeln deaktiviert sind, leitet DataWedge decodierte Daten an das Ausgabe-Plug-in weiter, ohne die Daten zu verarbeiten.

## Sortieren der Regelliste



**HINWEIS:** Wenn keine Regeln definiert sind, leitet das ADF-Plug-in die erfassten Daten unverändert weiter. Wenn Regeln definiert wurden, diese aber alle deaktiviert sind, leitet das ADF-Plug-in hingegen keine erfassten Daten weiter.

Regeln werden der Reihenfolge nach von oben nach unten verarbeitet. Die Regeln, die in der Liste oben stehen, werden zuerst verarbeitet. Verwenden Sie das Symbol neben der Regel, um sie an eine andere Position in der Liste zu verschieben.

Тур	Aktionen	Beschreibung
Cursorbe- Vorspringen wegung		Bewegt den Cursor um eine bestimmte Anzahl von Zeichen nach vorn. Geben Sie die Anzahl der Zeichen ein, um die der Cursor nach vorne bewegt werden soll.
	Zurückspringen	Bewegt den Cursor um eine bestimmte Anzahl von Zeichen zurück. Geben Sie die Anzahl der Zeichen ein, um die der Cursor zurückbewegt werden soll.
	Zum Start springen	Bewegt den Cursor an den Anfang der Daten.
	Verschieben zu	Bewegt den Cursor vorwärts, bis die angegebene Zeichenfolge gefunden wird. Geben Sie die Zeichenfolge in das Datenfeld ein.
	Verschieben hinter	Bewegt den Cursor über die angegebene Zeichenfolge hinaus. Geben Sie die Zeichenfolge in das Datenfeld ein.

### Tabelle 6 Von ADF unterstützte Aktionen

Тур	Aktionen	Beschreibung
Datenände- rung	Leerzeichen reduzieren	Entfernt Leerzeichen zwischen Wörtern und entfernt Leerzeichen am Anfang und Ende der Daten.
	Reduzieren der Leerzeichen stoppen	Stoppt das Reduzieren von Leerzeichen. Dadurch wird die letzte Aktion vom Typ <b>Leerzeichen reduzieren</b> deaktiviert.
	Alle Leerzeichen entfernen	Entfernt alle Leerzeichen in den Daten.
	Entfernen der Leerzeichen stoppen	Beendet das Entfernen von Leerzeichen. Dadurch wird die letzte Aktion vom Typ <b>Alle Leerzeichen entfernen</b> deaktiviert.
	Voranstehende Nullen entfernen	Entfernt alle Nullen am Anfang der Daten.
	Entfernen von Nullen stoppen	Beendet das Entfernen von Nullen am Anfang der Daten. Dadurch wird die letzte Aktion vom Typ <b>Voranstehende Nullen entfernen</b> deaktiviert.
	Mit Nullen auffüllen	Die Daten werden auf der linken Seite mit Nullen aufgefüllt, um die angegebene Länge zu erreichen. Geben Sie die Anzahl der Nullen ein, die aufgefüllt werden sollen.
	Auffüllen mit Nullen stoppen	Stoppt das Auffüllen mit Nullen. Dadurch wird die vorherige Aktion vom Typ <b>Mit Nullen auffüllen</b> deaktiviert.
	Mit Leerzeichen auffüllen	Die Daten werden auf der linken Seite mit Leerzeichen aufgefüllt, um die angegebene Länge zu erreichen. Geben Sie die Anzahl der Leerzeichen ein, die aufgefüllt werden sollen.
	Auffüllen mit Leerzeichen stoppen	Stoppt das Auffüllen mit Leerzeichen. Dadurch wird die vorherige Aktion vom Typ <b>Mit Leerzeichen auffüllen</b> deaktiviert.
	Ersatzzeichenfolge	Ersetzt eine angegebene Zeichenfolge durch eine neue Zeichenfolge. Geben Sie die zu ersetzende Zeichenfolge und die Zeichenfolge ein, mit der sie ersetzt werden soll.
	Alle Ersatzzeichenfolgen stoppen	Stoppt alle Aktionen vom Typ Ersatzzeichenfolge.
Senden von Daten	Nächste senden	Sendet die angegebene Anzahl von Zeichen ab der aktuellen Cursorposition. Geben Sie die Anzahl der zu sendenden Zeichen ein.
	Verbleibende senden	Sendet alle Daten, die ab der aktuellen Cursorposition verbleiben.
	Senden bis zu	Sendet alle Daten bis zu einer angegebenen Zeichenfolge. Geben Sie die Zeichenfolge ein.
	Pause beim Senden	Macht eine Pause entsprechend der angegebenen Anzahl von Millisekunden, bevor die nächste Aktion fortgesetzt wird. Geben Sie die Zeitdauer in Millisekunden ein.
	Zeichenfolge senden	Sendet eine angegebene Zeichenfolge. Geben Sie die zu sendende Zeichenfolge ein.
	Zeichen senden	Sendet ein angegebenes ASCII-/Unicode-Zeichen. Geben Sie einen Zeichenwert ein. Der maximale Unicode-Zeichenwert, der eingegeben werden kann, ist U-10FFFF (= 1114111 in Dezimalschreibweise).

Tabelle 6	Von ADF unterstützte Aktionen	(Fortsetzung)
-----------	-------------------------------	---------------

## Löschen einer Aktion

- 1. Berühren und halten Sie den Namen der Aktion.
- 2. Wählen Sie **Delete action** (Aktion löschen) im Kontextmenü aus.

## **ADF-Beispiel**

Im Folgenden wird ein Beispiel für die Erstellung einer erweiterten Datenformatierung (Advanced Data Formatting, ADF) dargestellt:

Ein Benutzer scannt einen Barcode mit den folgenden Kriterien:

- Code 39-Barcode
- Länge: 12 Zeichen
- Enthält 129 an der Startposition

Ändern Sie die Daten wie folgt:

- Füllen Sie alle Sendeaktionen mit Nullen bis zu einer Länge von 8 Zeichen ein.
- Senden Sie alle Daten bis zum Zeichen X.
- Senden Sie ein Leerzeichen.

So erstellen Sie eine ADF-Regel für das obige Beispiel:

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **k**.
- 2. Berühren Sie Profile0 (Profil 0).
- 3. Berühren Sie unter **Keystroke Output** (Tastenanschlag-Ausgabe) die Option **Advanced data formatting** (Erweiterte Datenformatierung).
- 4. Berühren Sie Enable (Aktivieren).
- 5. Berühren Sie Rule0 (Regel 0).
- 6. Berühren Sie Criteria (Kriterien).
- 7. Berühren Sie String to check for (Zu prüfende Zeichenfolge).
- 8. Geben Sie im Textfeld Enter the string to check for (Zu prüfende Zeichenfolge eingeben) 129 ein, und berühren Sie dann **OK**.
- 9. Berühren Sie String position (Zeichenfolgenposition).
- 10. Ändern Sie den Wert in 0.
- 11.Berühren Sie OK.
- 12. Berühren Sie String length (Zeichenfolgenlänge).
- 13.Ändern Sie den Wert in 12.
- 14. Berühren Sie OK.
- 15. Berühren Sie Source criteria (Quellenkriterien).
- 16. Berühren Sie Barcode input (Barcode-Eingabe).
- 17. Berühren Sie All decoders enabled (Alle Decoder aktiviert), um alle Decoder zu deaktivieren.

- 18. Berühren Sie Code 39.
- 19. Drücken Sie dreimal **〈**.
- 20.Berühren Sie Actions (Aktionen).
- 21. Halten Sie die Regel Send remaining (Verbleibende senden) gedrückt, bis ein Menü angezeigt wird.
- 22. Berühren Sie Delete action (Aktion löschen).
- 23.Berühren Sie :
- 24. Berühren Sie New action (Neue Aktion).
- 25. Wählen Sie Pad with zeros (Mit Nullen auffüllen).
- 26. Berühren Sie die Regel Pad with zeros (Mit Nullen auffüllen).
- 27.Berühren Sie How many (Wie viele).
- 28.Ändern Sie den Wert in 8, und berühren Sie dann OK.
- 29. Drücken Sie 🗸.
- 30. Berühren Sie .
- 31.Berühren Sie New action (Neue Aktion).
- 32. Wählen Sie Send up to (Senden bis).
- 33. Berühren Sie die Regel Send up to (Senden bis).
- 34. Berühren Sie String (Zeichenfolge).
- 35.Geben Sie im Textfeld Enter a string (Zeichenfolge eingeben) ein x ein.
- 36. Berühren Sie OK.
- 37.Berühren Sie **〈**.
- 38.Berühren Sie .
- 39. Berühren Sie New action (Neue Aktion).
- 40. Wählen Sie Send char (Zeichen senden).
- 41. Berühren Sie die Regel Send char (Zeichen senden).
- 42. Berühren Sie Character code (Zeichencode).
- 43.Geben Sie in das Textfeld Enter character code (Zeichencode eingeben) 32 ein.
- 44. Berühren Sie OK.
- 45.Berühren Sie **⊲**.

#### Abbildung 66 ADF-Beispielbildschirm

Actions: Rule0	:
Pad with zeros	≡
Send up to	≡
Send char	≡

46. Stellen Sie sicher, dass auf dem Gerät eine Anwendung geöffnet ist und sich ein Textfeld im Fokus befindet (Textcursor in Textfeld).

47. Zielen Sie mit dem Scanfenster auf den Barcode.

#### Abbildung 67 Beispielbarcode



48. Halten Sie die Scantaste gedrückt.

Das rote LED-Fadenkreuz wird aktiviert, um Sie beim Zielen zu unterstützen. Achten Sie darauf, dass sich der Barcode innerhalb des Zielbereichs befindet. Die LED leuchtet rot auf und zeigt so an, dass die Datenerfassung ausgeführt wird.

49. Die LED leuchtet grün, ein Signalton ertönt, und das Gerät vibriert standardmäßig, um anzuzeigen, dass der Barcode erfolgreich decodiert wurde. Die LED leuchtet grün, und es ertönt standardmäßig ein Signalton, um anzuzeigen, dass der Barcode erfolgreich decodiert wurde. Die formatierten Daten 000129X<Leerzeichen> werden im Textfeld angezeigt.

Beim Scannen eines Code 39-Barcodes von 1299X15598 wurden keine Daten übertragen (Regel wird ignoriert), da die Barcode-Daten nicht den Längenkriterien entsprachen.

#### Abbildung 68 Formatierte Daten

← Edit:	Î
00001299	

# DataWedge-Einstellungen

Der Bildschirm "DataWedge Settings" (DataWedge-Einstellungen) bietet Zugriff auf allgemeine, nicht profilbezogene Optionen. Berühren Sie **Settings** (Einstellungen).

Abbildung 69 Fenster "Datawedge-Einstei	ellungen
---	----------

DataWedge enabled Enable/disable DataWedgeEnable logging Enable debug output to logcatIgnore disabled profiles Stop switching to disabled profilesDisabled app list Data capture disabled app listImport Import DataWedge configurationExport Export current DataWedge profileImport Profile Import a DataWedge profile	DataWedge Settings	
Enable logging Enable debug output to logcatIgnore disabled profiles Stop switching to disabled profilesDisabled app list Data capture disabled app listImport Import DataWedge configurationExport Export current DataWedge profileImport Profile Import a DataWedge profile	DataWedge enabled Enable/disable DataWedge	
Ignore disabled profiles       □         Stop switching to disabled profiles       □         Disabled app list       □         Data capture disabled app list       □         Import       □         Import DataWedge configuration       □         Export       □         Export current DataWedge configuration       □         Import Profile       □         Import a DataWedge profile       □	Enable logging Enable debug output to logcat	
Disabled app list         Data capture disabled app list         Import         Import DataWedge configuration         Export         Export current DataWedge configuration         Import Profile         Import a DataWedge profile	Ignore disabled profiles Stop switching to disabled profiles	
Import         Import DataWedge configuration         Export         Export current DataWedge configuration         Import Profile         Import a DataWedge profile	Disabled app list Data capture disabled app list	
Export Export current DataWedge configuration Import Profile Import a DataWedge profile	Import Import DataWedge configuration	
Import Profile Import a DataWedge profile	Export Export current DataWedge configuration	
	Import Profile Import a DataWedge profile	

- DataWedge enabled (DataWedge aktiviert): Aktiviert oder deaktiviert DataWedge. Um DataWedge zu deaktivieren, deaktivieren Sie diese Option (Standardeinstellung: aktiviert).
- **Enable logging** (Protokollierung aktivieren): Aktiviert oder deaktiviert die Debug-Ausgabedatei für Logcat. Um die Protokollierung zu aktivieren, aktivieren Sie diese Option (Standardeinstellung: deaktiviert).

- Ignore disabled profiles (Deaktivierte Profile ignorieren): Verhindert, dass DataWedge zu einem Profil wechselt, das nicht aktiviert ist. In solchen Fällen wird der Profilwechsel ignoriert, und das aktuelle Profil bleibt aktiv. Profil 0 muss deaktiviert werden, um diese Funktion zu verwenden (Standardeinstellung: deaktiviert).
- **Disable app list** (Liste der zu deaktivierenden Apps): Deaktiviert Scanfunktionen für ausgewählte Anwendungen oder Aktivitäten.
- **Import**: Ermöglicht den Import einer DataWedge-Konfigurationsdatei. Die importierte Konfiguration ersetzt die aktuelle Konfiguration.
- Export: Ermöglicht den Export der aktuellen DataWedge-Konfiguration.
- Import Profile (Profil importieren): Ermöglicht das Importieren einer DataWedge-Konfigurationsdatei.
- Export Profile (Profil exportieren): Ermöglicht das Exportieren einer DataWedge-Konfigurationsdatei.
- Restore (Wiederherstellen): Die aktuelle Konfiguration wird auf die Werkseinstellungen zurückgesetzt.
- **Reporting** (Berichterstellung): Konfiguriert die Berichtsoptionen.

### Importieren einer Konfigurationsdatei

- 1. Kopieren Sie die Konfigurationsdatei in den Ordner /Android/data/com.symbol.datawedge/files auf der microSD-Karte.
- 2. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **k**.
- 3. Berühren Sie .
- 4. Berühren Sie Settings (Einstellungen).
- 5. Berühren Sie Import (Importieren).
- Berühren Sie den Namen der zu importierenden Datei.
   Die Konfigurationsdatei (datawedge.db) wird importiert und ersetzt die aktuelle Konfiguration.

## Exportieren einer Konfigurationsdatei

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **k**.
- 2. Berühren Sie :
- 3. Berühren Sie Settings (Einstellungen).
- 4. Berühren Sie Export (Exportieren).
- 5. Wählen Sie im Dialogfeld **Export to** (Exportieren nach) den Speicherort aus, an dem die Datei gespeichert werden soll.
- 6. Berühren Sie **Export** (Exportieren). Die Konfigurationsdatei (datawedge.db) wird am ausgewählten Speicherort gespeichert.

# Importieren einer Profildatei



HINWEIS: Ändern Sie nicht den Dateinamen der Profildatei. Wenn der Dateiname geändert wird, wird die Datei nicht importiert.

- 1. Kopieren Sie die Profildatei in den Ordner /Android/data/com.symbol.datawedge/files.
- 2. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie k.
- 3. Berühren Sie
- 4. Berühren Sie Settings (Einstellungen).
- 5. Berühren Sie Import Profile (Profil importieren).
- 6. Berühren Sie die zu importierende Profildatei.
- 7. Berühren Sie **Import** (Importieren). Die Profildatei (**dwprofile\_x.db**, wobei x = Name des Profils) wird importiert und in der Profilliste angezeigt.

## **Exportieren eines Profils**

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **k**.
- 2. Berühren Sie .
- 3. Berühren Sie Settings (Einstellungen).
- 4. Berühren Sie Export Profile (Profil exportieren).
- 5. Berühren Sie das zu exportierende Profil.
- Berühren Sie Export (Exportieren).
   Die Profildatei (dwprofile\_x.db, wobei x = Name des Profils) wird im Stammverzeichnis des Gerätespeichers abgelegt.

## Wiederherstellen von DataWedge

So stellen Sie die werkseitige Standardkonfiguration von DataWedge wieder her:

- Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie k.
- 2. Berühren Sie
- 3. Berühren Sie Settings (Einstellungen).
- 4. Berühren Sie Restore (Wiederherstellen).
- 5. Berühren Sie Yes (Ja).

# Konfigurations- und Profildateiverwaltung

Die Konfigurations- oder Profileinstellungen für DataWedge können in einer Datei zur Verteilung an andere Geräte gespeichert werden.

Exportieren Sie die neue Konfiguration oder das neue Profil nach Konfigurationsänderungen in das Stammverzeichnis des Gerätespeichers. Die erstellte Konfigurationsdatei trägt automatisch den Namen datawedge.db. Die erstellte Profildatei trägt automatisch den Namen dwprofile\_x.db, wobei x der Profilname ist. Die Dateien können dann in den Gerätespeicher anderer Geräte kopiert und auf diesen Geräten in DataWedge importiert werden. Durch Importieren einer Konfiguration oder eines Profils werden die vorhandenen Einstellungen ersetzt.

# **Enterprise-Ordner**

Der interne Speicher enthält den Enterprise-Ordner (/enterprise). Der Enterprise-Ordner ist persistent und verwaltet Daten nach einem Enterprise-Reset. Nach einem Enterprise-Reset prüft DataWedge, ob im Ordner /enterprise/device/settings/datawedge/enterpriserset/ eine Konfigurationsdatei mit dem Namen datawedge.db oder eine Profildatei mit dem Namen dwprofile\_x.db vorhanden ist. Wenn die Datei gefunden wird, so wird die Datei importiert und ersetzt vorhandene Konfigurationen oder Profile.



HINWEIS: Bei der Zurücksetzung auf die Werkseinstellungen werden alle Dateien im Enterprise-Ordner gelöscht.

## **Automatischer Import**

DataWedge unterstützt die Remote-Bereitstellung von Konfigurationen auf Geräten mithilfe von Tools wie handelsüblichen MDM-Systemen (Mobile Device Management) von Drittanbietern. DataWedge überwacht den Ordner /enterprise/device/settings/datawedge/autoimport in Bezug auf die DataWedge-Konfigurationsdatei (datawedge.db) oder eine Profildatei (dwprofile\_x.db). Dieser Ordner wird bei jedem Start von DataWedge überprüft. Wenn eine Konfigurations- oder Profildatei gefunden wird, importiert es die Datei, um vorhandene Konfigurationen oder Profile zu ersetzen. Nachdem die Datei importiert wurde, wird sie aus dem Ordner gelöscht.

Während DataWedge ausgeführt wird, erhält es eine Benachrichtigung vom System, dass eine Datei im Ordner /enterprise/device/settings/datawedge/autoimport abgelegt wurde. In diesem Fall importiert DataWedge diese neue Konfiguration oder dieses neue Profil, ersetzt die vorhandene Konfiguration bzw. das vorhandene Profil und löscht die Datei. DataWedge verwendet die importierte Konfiguration sofort.



**HINWEIS:** Bei der Zurücksetzung auf die Werkseinstellungen werden alle Dateien im Ordner **/enterprise** gelöscht. Es wird dringend empfohlen, DataWedge vor der Remote-Bereitstellung einer Konfiguration oder eines Profils zu beenden. Die Dateiberechtigungen müssen auf 666 gesetzt sein.

Der Ordner **/enterprise** kann nicht über die App **Dateien** oder andere Benutzer-Tools angezeigt werden. Das Verschieben von Dateien in und aus den Ordnern **/autoimport** oder **/enterprisereset** muss programmgesteuert oder über eine Staging-Client-App oder MDM erfolgen.

## Hinweise zur Programmierung

Die folgenden Abschnitte enthalten spezifische Informationen zur Programmierung bei Verwendung von DataWedge.
# Erfassen von Daten und Aufnehmen von Fotos in derselben Anwendung

So können Sie in derselben Anwendung Barcode-Daten erfassen und Fotos aufnehmen:

- Erstellen Sie ein DataWedge-Profil für die Aufnahme von Bildern in Ihrer Anwendung, das Scanvorgänge deaktiviert, und verwenden Sie Android SDK-APIs zum Steuern der Kamera.
- Das DataWedge-Standardprofil ist f
  ür den Scanvorgang in der Anwendung zust
  ändig. Sie k
  önnten ein weiteres DataWedge-Profil f
  ür alle speziellen Scananforderungen erstellen, die mit der Scanaktivit
  ät Ihrer Anwendung verbunden sind.

# Deaktivieren von DataWedge auf dem Gerät und Verwenden der Massenbereitstellung

So deaktivieren Sie DataWedge und stellen es auf mehreren Geräten bereit:

- 1. Wischen Sie auf dem Startbildschirm von unten nach oben, und berühren Sie DataWedge.
- 2. Berühren Sie
- 3. Berühren Sie Settings (Einstellungen).
- 4. Deaktivieren Sie das Kontrollkästchen DataWedge enabled (DataWedge aktiviert).
- Exportieren Sie die DataWedge-Konfiguration. Weitere Informationen entnehmen Sie Exportieren einer Konfigurationsdatei auf Seite 106. Weitere Informationen zur Verwendung der automatischen Importfunktion finden Sie unter Konfigurations- und Profildateiverwaltung auf Seite 108.

# DataWedge-APIs

DataWedge-APIs funktionieren hauptsächlich über Android-Intents – spezifische Befehle, die von anderen Anwendungen zur Steuerung der Datenerfassung verwendet werden können, ohne dass ein direkter Zugriff auf die DataWedge-UI erforderlich ist. Weitere Informationen finden Sie unter http://techdocs.zebra.com/datawedge/6-8/guide/api/

# **Berichterstellung**

DataWedge 6.6 (und höher) kann Berichte zu den Importergebnissen von Geräteprofilen erstellen. Diese HTML-Berichte zeigen Einstellungsunterschiede zwischen der Ursprungsdatenbank (Quelldatenbank) und dem Zielgerät an. Dadurch können Administratoren Unterschiede einfach erkennen und Anpassungen vornehmen, um Missverhältnisse in den Hardware- oder Softwarefunktionen von einem Gerät zum anderen auszugleichen. In Berichten wird immer das Zielgerät als Grundlage für den Vergleich eingehender Einstellungsdateien verwendet.

So aktivieren Sie die Berichterstellung:

- 1. Wischen Sie auf dem Bildschirm von unten nach oben, und berühren Sie **k**.
- 2. Berühren Sie
- 3. Berühren Sie Settings (Einstellungen).
- 4. Berühren Sie Reporting (Berichterstellung).
- 5. Aktivieren Sie das Kontrollkästchen Reporting enabled (Berichterstellung aktiviert).

## Soft-Scanauslöser

Mit DataWedge kann der Scanauslöser über eine native Android-Anwendung programmgesteuert in den Zustand "Starten", "Stoppen" oder "Umschalten" versetzt werden. Die Anwendung kann einen Android Broadcast-Intent ausgeben, um den Scanner zu steuern, ohne dass die Scantaste gedrückt werden muss. Das aktive DataWedge-Profil ist erforderlich, um alle Parameter während eines Scanvorgangs zu steuern.

## Funktionsprototyp

```
Intent i = new Intent();
i.setAction("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.SOFT_SCAN_TRIGGER", "<parameter>");
```

# Scanner-Eingabe-Plug-in

Mit dem API-Befehl ScannerInputPlugin kann das Scanner-Plug-in, das vom derzeit aktiven Profil verwendet wird, aktiviert bzw. deaktiviert werden. Wenn Sie das Scanner-Plug-in deaktivieren, wird das Scannen in diesem Profil deaktiviert, unabhängig davon, ob es sich um ein zugewiesenes Profil handelt oder nicht. Dies gilt nur, wenn die Barcode-Eingabe im aktiven Profil aktiviert ist.



**HINWEIS:** Durch die Verwendung dieser API wird nur der Laufzeitstatus des Scanners geändert; es werden keine dauerhaften Änderungen am Profil vorgenommen.

# Funktionsprototyp

Intent i = new Intent(); i.setAction(ACTION); i.putExtra(EXTRA\_DATA, "<parameter>");

#### Parameter

action: String "com.symbol.datawedge.api.ACTION\_SCANNERINPUTPLUGIN"

extra\_data: String "com.symbol.datawedge.api.EXTRA\_PARAMETER"

**arameter>:** Der Parameter als Zeichenfolge, wobei eine der folgenden Optionen verwendet wird:

- "ENABLE\_PLUGIN": aktiviert das Plug-in
- "DISABLE\_PLUGIN": deaktiviert das Plug-in

#### Rückgabewerte

Keine.

Fehler- und Debug-Meldungen werden im Android-Protokollaufzeichnungssystem erfasst, das dann mit dem Befehl logcat angezeigt und gefiltert werden kann. Sie können logcat über eine ADB-Shell ausführen, um die Protokollmeldungen anzuzeigen, z. B.: \$ adb logcat -s DWAPI

Fehlermeldungen werden für ungültige Aktionen und Parameter protokolliert.

## **Beispiel**

```
// Aktions- und Datenstrings definieren
String scannerInputPlugin = "com.symbol.datawedge.api.ACTION_SCANNERINPUTPLUGIN";
String extraData = "com.symbol.datawedge.api.EXTRA_PARAMETER";

public void onResume() {
    // Intent erstellen
    Intent i = new Intent();
    // Auszuführende Aktion auswählen
    i.setAction(scannerInputPlugin);
    // zusätzliche Informationen hinzufügen
    i.putExtra(extraData, "DISABLE_PLUGIN");
    // Intent an DataWedge senden
    context.this.sendBroadcast(i);
}
```

## Kommentare

Mit diesem API-Intent für die Datenerfassung kann das Scanner-Plug-in für das aktuelle Profil aktiviert oder deaktiviert werden. Zum Beispiel wird Aktivität A gestartet und wechselt über das API-Intent zur Datenerfassung zu Profil A, in dem das Scanner-Plug-in aktiviert ist. Zu einem bestimmten Zeitpunkt deaktiviert sie dann über die Datenerfassungs-API das Scanner-Plug-in und Aktivität B wird gestartet. In DataWedge ist Profil B Aktivität B zugewiesen. DataWedge wechselt zu Profil B. Wenn Aktivität A über die Methode onResume wieder im Vordergrund ausgeführt werden soll, muss Aktivität A über das API-Intent zur Datenerfassung zurück zu Profil A wechseln und dann erneut über das API-Intent zur Datenerfassung das Scanner-Plug-in deaktivieren, um in den Zustand zurückzukehren, in dem es sich befand.



**HINWEIS:** Durch die Verwendung dieser API wird nur der Laufzeitstatus des Scanners geändert; es werden keine dauerhaften Änderungen am Profil vorgenommen.

Im oben genannten Beispiel wird davon ausgegangen, dass Profil A mit keiner Anwendung oder Aktivität verknüpft ist. Wenn der Fokus also wieder zu Aktivität A wechselt, wechselt DataWedge nicht automatisch zu Profile A. Daher muss Aktivität A mit der onResume-Methode zurück zu Profil A wechseln. Da DataWedge das Profil automatisch wechselt, wenn eine Aktivität angehalten wird, empfehlen wir, diese API-Funktion über die onResume-Methode der Aktivität aufzurufen.

## Scanner auflisten

Verwenden Sie den API-Befehl enumerateScanners, um eine Liste der für das Gerät verfügbaren Scanner abzurufen.

## Funktionsprototyp

```
Intent i = new Intent();
```

```
i.setAction("com.symbol.datawedge.api.ACTION");
```

```
i.putExtra("com.symbol.datawedge.api.ENUMERATE_SCANNERS", "");
```

## Parameter

ACTION [String]: "com.symbol.datawedge.api.ENUMERATE\_SCANNERS"

## Rückgabewerte

Die Aufzählungsliste der Scanner wird über ein Broadcast-Intent zurückgegeben. Die Broadcast-Intent-Aktion lautet "com.symbol.datawedge.api.ACTION\_ENUMERATEDSCANNERLIST" und die Liste der Scanner wird als Zeichenfolgenarray zurückgegeben (siehe Beispiel unten).

Fehler- und Debug-Meldungen werden im Android-Protokollaufzeichnungssystem erfasst, das dann mit dem Befehl logcat angezeigt und gefiltert werden kann. Sie können logcat über eine ADB-Shell ausführen, um die Protokollmeldungen anzuzeigen, z. B.:

\$ adb logcat -s DWAPI

Fehlermeldungen werden für ungültige Aktionen und Parameter protokolliert.

## Beispiel

11

```
// Vor dem Senden der Aufzählungsabfrage abrufen
11
public void registerReciever(){
   IntentFilter filter = new IntentFilter();
    filter.addAction("com.symbol.datawedge.api.RESULT_ACTION");//RESULT_ACTION
    filter.addCategory(Intent.CATEGORY DEFAULT);
    registerReceiver(enumeratingBroadcastReceiver, filter);
}
//
// Aufzählungsbefehl an DataWedge senden
11
public void enumerateScanners(){
    Intent i = new Intent();
    i.setAction("com.symbol.datawedge.api.ACTION");
    i.putExtra("com.symbol.datawedge.api.ENUMERATE_SCANNERS", "");
    this.sendBroadcast(i);
}
public void unRegisterReciever(){
    unregisterReceiver(enumeratingBroadcastReceiver);
}
//
// Broadcast-Empfänger für den Empfang des Aufzählungsergebnisses erstellen
11
private BroadcastReceiver enumeratingBroadcastReceiver = new BroadcastReceiver() {
    @Override
    public void onReceive(Context context, Intent intent) {
        String action = intent.getAction();
        Log.d(TAG, "Action: " + action);
        if(action.equals("com.symbol.datawedge.api.RESULT_ACTION")){
            11
            // Scanner auflisten
            11
            if(intent.hasExtra("com.symbol.datawedge.api.RESULT_ENUMERATE_SCANNERS")) {
            ArrayList<Bundle> scannerList = (ArrayList<Bundle>)
intent.getSerializableExtra("com.symbol.datawedge.api.RESULT_ENUMERATE_SCANNERS");
            if((scannerList != null) && (scannerList.size() > 0)) {
                for (Bundle bunb : scannerList){
                    String[] entry = new String[4];
                    entry[0] = bunb.getString("SCANNER NAME");
                    entry[1] = bunb.getBoolean("SCANNER_CONNECTION_STATE")+"";
                    entry[2] = bunb.getInt("SCANNER_INDEX")+"";
                    entry[3] = bunb.getString("SCANNER_IDENTIFIER");
                   Log.d(TAG, "Scanner:" + entry[0] + " Connection:" + entry[1] + " Index:" + entry[2] + " ID:" + entry[3]);
                    }
                }
            }
        }
    }
};
```

#### Kommentare

Der Scanner und seine Parameter werden basierend auf dem aktuell aktiven Profil festgelegt.

## Standardprofil festlegen

Mit der API-Funktion setDefaultProfile können Sie ein angegebenes Profil als Standardprofil festlegen.

#### Standardprofile: Wiederholung

Profil 0 ist das generische Profil, das verwendet wird, wenn keine vom Benutzer erstellten Profile mit einer Anwendung verknüpft sind.

Profil 0 kann bearbeitet, aber nicht mit einer Anwendung verknüpft werden. Das heißt, DataWedge ermöglicht die Bearbeitung von Plug-in-Einstellungen für Profil 0, erlaubt jedoch keine Zuweisung einer im Vordergrund ausgeführten Anwendung. Mit dieser Konfiguration kann DataWedge Ausgabedaten an alle Vordergrundanwendungen senden, die nicht mit benutzerdefinierten Profilen verknüpft sind, wenn Profil 0 aktiviert ist.

Profil 0 kann deaktiviert werden, damit DataWedge nur Ausgabedaten an Anwendungen senden kann, die mit benutzerdefinierten Profilen verknüpft sind. Sie können beispielsweise ein Profil erstellen, das einer bestimmten Anwendung zugeordnet ist, Profil 0 deaktivieren und dann den Scan durchführen. DataWedge sendet nur Daten an die Anwendung, die in dem vom Benutzer erstellten Profil angegeben ist. Dies erhöht die Sicherheit von DataWedge und ermöglicht, dass Daten nur an bestimmte Anwendungen gesendet werden.

#### Nutzungsszenario

Eine Startanwendung verfügt über eine Liste von Apps, die von Benutzern gestartet werden können, und keiner der aufgeführten Apps ist ein DataWedge-Profil zugewiesen. Nachdem eine Benutzer eine App ausgewählt hat, muss das Startprogramm das entsprechende DataWedge-Profil für die ausgewählte App festlegen. Über setDefaultProfile kann das Standardprofil auf das erforderliche Profil festgelegt werden. Wenn der Benutzer dann die ausgewählte App startet, wechselt die automatische Profilwechselfunktion von DataWedge zum Standardprofil (jetzt das erforderliche Profil für diese App).

Wenn der gestarteten App aus irgendeinem Grund ein DataWedge-Profil zugewiesen ist, wird das festgelegte Standardprofil überschrieben.

Wenn die Steuerung an die Startanwendung zurückgegeben wird, kann **resetDefaultProfile** verwendet werden, um das Standardprofil zurückzusetzen.

#### Funktionsprototyp

```
Intent i = new Intent();
i.setAction("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.SET_DEFAULT_PROFILE", "<profile name>");
```

## Parameter

ACTION [String]: "com.symbol.datawedge.api.ACTION"

EXTRA\_DATA [String]: "com.symbol.datawedge.api.SET\_DEFAULT\_PROFILE"

<profile name>: Der Profilname (eine Zeichenfolge mit Beachtung von Groß-/Kleinschreibung), der als Standardprofil festgelegt werden soll.

#### Rückgabewerte

Keine.

Fehler- und Debug-Meldungen werden im Android-Protokollaufzeichnungssystem erfasst, das dann mit dem Befehl logcat angezeigt und gefiltert werden kann. Sie können logcat über eine ADB-Shell ausführen, um die Protokollmeldungen anzuzeigen, z. B.:

```
$ adb logcat -s DWAPI
```

Fehlermeldungen werden für ungültige Aktionen, Parameter und Fehler protokolliert (z. B. nicht gefundene oder mit einer Anwendung verknüpfte Profile).

## **Beispiel**

```
// Aktions- und Datenstrings definieren
String setDefaultProfile = "com.symbol.datawedge.api.ACTION";
String extraData = "com.symbol.datawedge.api.SET_DEFAULT_PROFILE";
public void onResume() {
    // Intent erstellen
    Intent i = new Intent();
    // Auszuführende Aktion auswählen
    i.setAction(setDefaultProfile);
    // Zusätzliche Informationen (Name) hinzufügen
    i.putExtra(extraData, "myProfile");
    // Intent an DataWedge senden
    this.sendBroadcast(i);
}
```

## Kommentare

Der API-Befehl hat keine Auswirkung, wenn das angegebene Profil nicht vorhanden ist oder das angegebene Profil bereits einer Anwendung zugeordnet ist. Da DataWedge das Profil automatisch wechselt, wenn eine Aktivität angehalten wird, empfehlen wir, dass diese API-Funktion über die onResume-Methode der Aktivität aufgerufen wird.

Zebra empfiehlt, dieses Profil so zu erstellen, dass es für alle Anwendungen/Aktivitäten geeignet ist, die andernfalls standardmäßig Profil 0 verwenden würden. Dadurch wird sichergestellt, dass diese Anwendungen/Aktivitäten weiterhin mit einer konsistenten Konfiguration funktionieren.

# Standardprofil zurücksetzen

Mit der API-Funktion resetDefaultProfile können Sie das Standardprofil wieder auf Profil 0 zurücksetzen.

## Funktionsprototyp

```
Intent i = new Intent();
```

i.setAction("com.symbol.datawedge.api.ACTION");

i.putExtra("com.symbol.datawedge.api.RESET\_DEFAULT\_PROFILE", "");

## Parameter

ACTION [String]: "com.symbol.datawedge.api.ACTION"

EXTRA\_DATA [String]: "com.symbol.datawedge.api.RESET\_DEFAULT\_PROFILE".

#### Rückgabewerte

Keine.

Fehler- und Debug-Meldungen werden im Android-Protokollaufzeichnungssystem erfasst, das dann mit dem Befehl logcat angezeigt und gefiltert werden kann. Sie können logcat über eine ADB-Shell ausführen, um die Protokollmeldungen anzuzeigen, z. B.:

\$ adb logcat -s DWAPI

Fehlermeldungen werden für ungültige Aktionen, Parameter und Fehler protokolliert (z. B. nicht gefundene oder mit einer Anwendung verknüpfte Profile).

## **Beispiel**

```
::javascript
// Aktionsstring definieren
String action = "com.symbol.datawedge.api.ACTION";
String extraData = "com.symbol.datawedge.api.RESET_DEFAULT_PROFILE";
public void onResume() {
    // Intent erstellen
    Intent i = new Intent();
    // Auszuführende Aktion auswählen
    i.setAction(action);
    i.putExtra(extraData, ""); // leer, da kein Name erforderlich ist
    this.sendBroadcast;
}
```

## Kommentare

Keine.

# Zu Profil wechseln

Mit der API-Aktion SwitchToProfile können Sie zum angegebenen Profil wechseln.

## Wiederholung: Profile

DataWedge basiert auf Profilen und Plug-ins. Ein Profil enthält Informationen darüber, wie sich DataWedge in Bezug auf verschiedene Anwendungen verhalten soll.

Die Profilinformationen umfassen:

- Zugeordnete Anwendungen
- Konfigurationen des Eingabe-Plug-ins
- Konfigurationen des Ausgabe-Plug-ins
- Konfigurationen des Verarbeitungs-Plug-ins

DataWedge enthält das Standardprofil Profil 0, das beim ersten Ausführen von DataWedge automatisch erstellt wird.

Mithilfe von Profilen kann für jede Anwendung eine spezifische DataWedge-Konfiguration definiert werden. Beispielsweise kann jede Benutzeranwendung ein Profil aufweisen, das gescannte Daten im erforderlichen Format ausgibt, wenn diese Anwendung im Vordergrund ausgeführt wird. DataWedge kann so konfiguriert werden, dass derselbe Satz erfasster Daten je nach Anforderungen der jeweiligen Anwendung unterschiedlich verarbeitet wird.



**HINWEIS:** Durch die Verwendung dieser API wird nur der Laufzeitstatus des Scanners geändert; es werden keine dauerhaften Änderungen am Profil vorgenommen.

Ein einzelnes Profil kann mit einer oder mehreren Aktivitäten/Anwendungen verknüpft sein. Eine bestimmte Aktivität kann jedoch immer nur mit einem Profil verknüpft sein.

#### Nutzungsszenario

Eine Anwendung weist zwei Aktivitäten auf. Aktivität A setzt voraus, dass nur EAN13-Barcodes gescannt werden. Aktivität B setzt voraus, dass nur Code 128-Barcodes gescannt werden. Das Profil "EAN13" ist so konfiguriert, dass nur EAN13-Barcodes gescannt werden, und weist keine Zuordnung auf. Das Profil "Code128" ist für das Scannen von Code 128 konfiguriert und weist keine Zuordnung auf. Beim Start von Aktivität A wird mithilfe von SwitchToProfile das Profil "EAN13" aktiviert. Ebenso wird beim Start von Aktivität B mithilfe von switchToProfile das Profil "Code128" aktiviert.

Wenn eine andere Aktivität/Anwendung im Vordergrund ausgeführt werden soll, wird beim automatischen Profilwechsel von DataWedge das DataWedge-Profil entweder auf das Standardprofil oder auf ein zugeordnetes Profil eingestellt.

Wenn Aktivität A (oder Aktivität B) wieder in den Vordergrund zurückkehrt, wird switchToProfile verwendet, um das Profil wieder auf Profil B (oder Profil M) zurückzusetzen.

## Funktionsprototyp

```
Intent i = new Intent();
i.setAction("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.SWITCH_TO_PROFILE", "<profile name>");
```

## Parameter

ACTION [String]: "com.symbol.datawedge.api.ACTION"

EXTRA\_DATA [String]: "com.symbol.datawedge.api.SWITCH\_TO\_PROFILE"

**<profile name>**: Der Profilname (eine Zeichenfolge, bei der zwischen Groß- und Kleinschreibung unterschieden wird), der als aktives Profil festgelegt werden soll.

## Rückgabewerte

Keine.

Fehler- und Debug-Meldungen werden im Android-Protokollaufzeichnungssystem erfasst, das dann mit dem Befehl logcat angezeigt und gefiltert werden kann. Sie können logcat über eine ADB-Shell ausführen, um die Protokollmeldungen anzuzeigen, z. B.:

\$ adb logcat -s DWAPI

Fehlermeldungen werden für ungültige Aktionen, Parameter und Fehler protokolliert (z. B. nicht gefundene oder mit einer Anwendung verknüpfte Profile).

## Beispiel

```
// Aktions- und Datenstrings definieren
String switchToProfile = "com.symbol.datawedge.api.ACTION";
String extraData = "com.symbol.datawedge.api.SWITCH_TO_PROFILE";
public void onResume() {
    super.onResume();
    // Intent erstellen
    Intent i = new Intent();
    // Auszuführende Aktion auswählen
    i.setAction(switchToProfile);
    // zusätzliche Informationen hinzufügen
    i.putExtra(extraData, "myProfile");
    // Intent an DataWedge senden
    this.sendBroadcast(i);
}
```

118

## Kommentare

Diese API-Funktion hat keine Auswirkung, wenn das angegebene Profil nicht vorhanden ist oder bereits mit einer Anwendung verknüpft ist.

DataWedge weist eine Eins-zu-Eins-Beziehung zwischen Profilen und Aktivitäten auf; ein Profil kann nur mit einer einzelnen Aktivität verknüpft werden. Wenn ein Profil zum ersten Mal erstellt wird, ist es keiner Anwendung zugeordnet und wird erst aktiviert, wenn es zugewiesen wurde. Dadurch können mehrere nicht verknüpfte Profile erstellt werden.

Mit dieser API-Funktion können solche Profile aktiviert werden.

Beispiel: Profil A ist nicht zugewiesen, und Profil B ist mit Aktivität B verknüpft. Wenn Aktivität A gestartet wird und die Funktion **SwitchToProfile** verwendet, um zu Profil A zu wechseln, ist Profil A immer dann aktiv, wenn Aktivität A im Vordergrund ausgeführt wird. Wenn Aktivität B aktiviert wird, wechselt DataWedge automatisch zu Profil B.

Wenn Aktivität A wieder aktiviert wird, muss die App **SwitchToProfile** erneut verwenden, um zurück zu Profil A zu wechseln. Dies geschieht über die für Aktivität A festgelegte Methode **onResume**.



**HINWEIS:** Durch die Verwendung dieser API wird nur der Laufzeitstatus des Scanners geändert; es werden keine dauerhaften Änderungen am Profil vorgenommen.

## Hinweise

Da DataWedge automatisch das Profil wechselt, wenn eine Aktivität angehalten wird, empfiehlt Zebra, diese API-Funktion über die onResume-Methode der Aktivität aufzurufen.

Nach dem Wechsel zu einem Profil wird dieses nicht zugewiesene Profil nicht mit der Anwendung/Aktivität verknüpft und kann in Zukunft mit einer anderen Anwendung/Aktivität verwendet werden.

Aus Gründen der Abwärtskompatibilität ist der automatische Profilwechsel in DataWedge nicht von den oben genannten API-Befehlen betroffen. Daher funktionieren die Befehle nur mit nicht zugewiesenen Profilen und Apps.

Der automatische Profilwechsel in DataWedge funktioniert wie folgt:

Jede Sekunde ...

- Wird newProfileId auf die zugewiesene Profil-ID der aktuellen Vordergrundaktivität festgelegt.
- Wenn kein zugewiesenes Profil gefunden wird, wird newProfileId auf die zugewiesene Profil-ID der aktuellen Vordergrund-App gesetzt.
- Wenn kein zugewiesenes Profil gefunden wird, wird newProfileId auf das aktuelle Standardprofil gesetzt (das nicht Profil 0 sein muss).
- Wird newProfileId mit currentProfileId abgeglichen. Wenn sich die beiden unterscheiden:
  - wird das aktuelle Profil deaktiviert
  - wird das neue Profil aktiviert (newProfileId)
  - wird currentProfileId = newProfileId festgelegt

# Anwendungsinstallation

# Einführung

In diesem Kapitel werden die Funktionen in Android beschrieben, darunter neue Sicherheitsfunktionen, das Packen von Anwendungen und die Verfahren zum Bereitstellen von Anwendungen auf dem Gerät.

# Sicherheit

Das Gerät implementiert eine Reihe von Sicherheitsrichtlinien, die bestimmen, ob eine Anwendung ausgeführt werden darf und, falls zulässig, mit welcher Vertrauensstufe dies erfolgt. Um eine Anwendung zu entwickeln, müssen Sie die Sicherheitskonfiguration des Geräts kennen und wissen, wie die jeweilige Anwendung mit dem entsprechenden Zertifikat signiert wird, damit die Anwendung (mit der erforderlichen Vertrauensstufe) ausgeführt werden kann.



**HINWEIS:** Vergewissern Sie sich, dass das Datum korrekt eingestellt ist, bevor Sie Zertifikate installieren oder auf sichere Websites zugreifen.

# Sichere Zertifikate

Wenn die VPN- oder WLAN-Netzwerke sichere Zertifikate benötigen, erwerben Sie die Zertifikate, und speichern Sie sie im sicheren Anmeldedatenspeicher des Geräts, bevor Sie den Zugriff auf die VPN- oder WLAN-Netzwerke konfigurieren.

Wenn Sie die Zertifikate von einer Website herunterladen, legen Sie ein Kennwort für den Anmeldedatenspeicher fest. Das Gerät unterstützt X.509-Zertifikate, die in PKCS#12-Schlüsselspeicherdateien mit der Erweiterung .p12 gespeichert sind (wenn der Schlüsselspeicher eine PFX- oder eine andere Erweiterung aufweist, ändern Sie diese zu .p12).

Auch alle zugehörigen privaten Schlüssel- oder Zertifizierungsstellenzertifikate, die im Schlüsselspeicher enthalten sind, werden auf dem Gerät installiert.

# Installieren eines sicheren Zertifikats

So installieren Sie ein sicheres Zertifikat:

 Kopieren Sie das Zertifikat vom Host-Computer in das Stammverzeichnis der microSD-Karte oder in den internen Speicher des Geräts. Weitere Informationen zum Anschließen des Geräts an einen Host-Computer und zum Kopieren von Dateien finden Sie unter USB/Ethernet-Kommunikation.

- Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend .
- 3. Berühren Sie Security & Location (Sicherheit und Standort) > Encryption & Credentials (Verschlüsselung und Anmeldedaten).
- 4. Berühren Sie Install from storage (Aus Speicher installieren).
- 5. Navigieren Sie zum Speicherort der Zertifikatdatei.
- 6. Berühren Sie den Dateinamen des zu installierenden Zertifikats.
- Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort f
  ür den Anmeldedatenspeicher ein. Wenn kein Kennwort f
  ür den Anmeldedatenspeicher festgelegt wurde, geben Sie das Kennwort zweimal ein, und ber
  ühren Sie dann OK.
- 8. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort des Zertifikats ein, und berühren Sie OK.
- Geben Sie einen Namen f
  ür das Zertifikat ein, und w
  ählen Sie in der Drop-down-Liste "Credential use:" (Verwendung der Anmeldedaten:) die Option VPN and apps (VPN und Apps) oder Wi-Fi (WLAN) aus.

Abbildung 70 Dialogfeld "Name the Certificate" (Zertifikat benennen)

Name the certificate		
Certificate name:		
Credential use: VPN and apps The package contains:		•
one user certificate	CANCEL	ок

10. Berühren Sie OK.

Das Zertifikat kann jetzt verwendet werden, wenn eine Verbindung zu einem sicheren Netzwerk hergestellt wird. Aus Sicherheitsgründen wird das Zertifikat von der microSD-Karte oder aus dem internen Speicher gelöscht.

# Konfigurieren der Speichereinstellungen für Anmeldedaten

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- Berühren Sie Security & Location > Encryption & Credentials (Sicherheit und Standort > Verschlüsselung und Anmeldedaten).
  - **Trusted credentials** (Vertrauenswürdige Anmeldedaten): Zeigt das vertrauenswürdige System und die Anmeldedaten des Benutzers an.
  - Install from storage (Aus Speicher installieren): Ermöglicht die Installation eines sicheren Zertifikats von der microSD-Karte oder aus dem internen Speicher.
  - Clear credentials (Anmeldedaten löschen): Löscht alle sicheren Zertifikate und die zugehörigen Anmeldeinformationen.

# **Entwicklungstools**

# Android

Android-Entwicklungstools sind unter developer.android.com verfügbar.

Um Anwendungen für das Gerät zu entwickeln, laden Sie das Entwicklungs-SDK und die Eclipse IDE herunter. Die Entwicklung kann auf den Betriebssystemen Microsoft® Windows®, Mac® OS X® oder Linux® erfolgen.

Anwendungen werden in Java programmiert, jedoch in der Dalvik VM kompiliert und ausgeführt (eine nicht Java-basierte virtuelle Maschine). Sobald der Java-Code ordnungsgemäß kompiliert wurde, stellen die Entwicklertools sicher, dass das Anwendungspaket, einschließlich der AndroidManifest.xml-Datei, ordnungsgemäß erstellt wird.

Das Entwicklungs-SDK wird als ZIP-Datei verteilt, die in ein Verzeichnis auf der Festplatte des Host-Computers entpackt wird. Das SDK umfasst:

- android.jar
  - Java-Archivdatei, die alle SDK-Klassen für die Entwicklung enthält, die zum Kompilieren einer Anwendung erforderlich sind.
- documention.html und docs-Verzeichnis
  - Die SDK-Dokumentation wird lokal und im Internet bereitgestellt. Sie ist größtenteils in Form von JavaDocs erhältlich und erleichtert die Navigation durch die zahlreichen Pakete im SDK. Die Dokumentation enthält außerdem einen allgemeinen Entwicklungsleitfaden und Links zur Community.
- Samples-Verzeichnis
  - Das Unterverzeichnis "samples" enthält den vollständigen Quellcode für eine Vielzahl von Anwendungen, einschließlich API-Demos mit Informationen zur Nutzung vieler APIs. Die Beispiele im samples-Verzeichnis sind ein guter Ausgangspunkt, um mit der Anwendungsentwicklung zu starten.
- Tools-Verzeichnis
  - Enthält alle Befehlszeilentools zum Erstellen von Anwendungen. Das am häufigsten verwendete und nützlichste Tool ist das ADB-Dienstprogramm.
- usb\_driver
  - Dieses Verzeichnis enthält die erforderlichen Treiber, um die Entwicklungsumgebung mit einem aktivierten Gerät zu verbinden. Diese Dateien sind nur für Entwickler erforderlich, die die Windows-Plattform verwenden.

Öffnen Sie den Bildschirm **Developer options** (Entwickleroptionen), um entwicklungsbezogene Einstellungen festzulegen.

Standardmäßig sind die Entwickleroptionen ausgeblendet. Wischen Sie am Gerät von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.

Berühren Sie **System > About Phone** (Telefoninfo). Scrollen Sie nach unten zu **Build number** (Build-Nummer). Tippen Sie sieben Mal auf **Build number** (Build-Nummer) bis **You are now a developer** (Sie sind jetzt ein Entwickler) angezeigt wird.

Berühren Sie **System > Developer Options** (Entwickleroptionen). Schieben Sie den Schalter in die Position **ON** (EIN), um die Entwickleroptionen zu aktivieren.

## **EMDK für Android**

EMDK für Android bietet Entwicklern eine umfassende Sammlung von Tools zur einfachen Erstellung leistungsstarker geschäftsbereichsspezifischer Anwendungen für Mobilcomputer in Unternehmen. Es wurde für das Android SDK und Android Studio von Google entwickelt und umfasst Klassenbibliotheken, Beispielanwendungen mit Quellcode und die gesamte zugehörige Dokumentation, damit Sie für Ihre Anwendungen alle Funktionen nutzen können, die Geräte von Zebra zu bieten haben.

Das Kit enthält außerdem den Profile Manager, ein GUI-basiertes Gerätekonfigurationstool, das einen exklusiven Zugriff auf das MX-Geräteverwaltungs-Framework von Zebra bietet. So können Entwickler Zebra-Geräte über ihre Anwendungen in kürzerer Zeit, mit weniger Aufwand und mit weniger Fehlern konfigurieren.

Weitere Informationen finden Sie unter: techdocs.zebra.com.

## **StageNow**

StageNow ist die neueste Generation der Android Staging-Lösung von Zebra, die die Betriebssysteme Android Lollipop, KitKat® und Jelly Bean unterstützt und auf der MX 4.3/4.4/5.x/6.0-Plattform basiert. Sie ermöglicht die schnelle und einfache Erstellung von Geräteprofilen und kann auf Geräten einfach durch Scannen eines Barcodes, Einlesen eines Tags oder die Wiedergabe einer Audiodatei bereitgestellt werden.

Die StageNow Staging-Lösung umfasst die folgenden Komponenten:

- Das StageNow Workstation-Tool wird auf der Staging-Workstation (dem Host-Computer) installiert und ermöglicht dem Administrator die einfache Erstellung von Bereitstellungsprofilen zur Konfiguration von Gerätekomponenten. Zudem können weitere Staging-Aktionen wie die Überprüfung des Zustands eines Zielgeräts durchgeführt werden, um die Eignung für Software-Upgrades oder andere Aktivitäten zu ermitteln. Die StageNow-Workstation speichert Profile und andere erstellte Inhalte zur späteren Verwendung.
- Der StageNow-Client befindet sich auf dem Gerät und bietet eine Benutzeroberfläche, über die die Bereitstellung gestartet werden kann. Der Bediener verwendet eine der gewünschten Bereitstellungsmethoden (Drucken und Scannen eines Barcodes, Lesen eines NFC-Tags oder Wiedergeben einer Audiodatei), um die Staging-Daten auf das Gerät zu übertragen.

Weitere Informationen finden Sie unter: techdocs.zebra.com.

# ADB-Setup über USB

Zur Verwendung der ADB müssen Sie den USB-Treiber installieren. Dies setzt voraus, dass das Entwicklungs-SDK auf dem Host-Computer installiert wurde. Details zum Einrichten des Entwicklungs-SDK finden Sie unter <u>developer.android.com/sdk/index.html</u>.

ADB-Treiber für Windows und Linux sind auf der Support-Website von Zebra verfügbar unter <u>www.zebra.com/support</u>. Laden Sie das Setup-Paket für ADB- und USB-Treiber herunter. Befolgen Sie die Anweisungen für das entsprechende Paket, um die ADB- und USB-Treiber für Windows und Linux zu installieren.

# Aktivieren von USB-Debugging

Standardmäßig ist USB-Debugging deaktiviert. So aktivieren Sie das USB-Debugging:

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🏟.
- 2. Berühren Sie **System > About phone** (Telefoninfo).
- 3. Scrollen Sie nach unten zu Build number (Build-Nummer).
- 4. Tippen Sie sieben Mal auf **Build number** (Build-Nummer). Die Meldung **You are now a developer!** (Sie sind jetzt ein Entwickler!) wird angezeigt.
- 5. Berühren Sie <a></a>.
- 6. Berühren Sie Developer options (Entwickleroptionen).
- 7. Schieben Sie den Schieberegler USB debugging (USB-Debugging) in die Position ON (EIN).
- 8. Berühren Sie OK.
- Schließen Sie das Gerät mit dem robusten Ladekabel/USB-Kabel an einen Host-Computer an. Das Dialogfeld Allow USB debugging? (USB-Debugging zulassen?) wird angezeigt.
- 10. Berühren Sie auf dem Gerät OK.
- 11. Navigieren Sie auf dem Host-Computer zum Ordner platform-tools.
- 12.Geben Sie adb devices ein.

Folgende Anzeige erscheint:

List of devices attached



**HINWEIS:** Wenn die Gerätenummer nicht angezeigt wird, vergewissern Sie sich, dass die ADB-Treiber ordnungsgemäß installiert sind.

13. Berühren Sie O.

# Anwendungsinstallation

Nachdem eine Anwendung entwickelt wurde, kann sie mit einer der folgenden Methoden auf dem Gerät installiert werden:

- USB-Anschluss, siehe Installieren von Anwendungen über die USB-Verbindung auf Seite 125.
- Android Debug Bridge, siehe Installieren von Anwendungen mithilfe von Android Debug Bridge auf Seite 126.
- microSD-Karte, siehe Installieren von Anwendungen über eine microSD-Karte auf Seite 127.
- MDM-Plattformen (Mobile Device Management) mit Anwendungsbereitstellung. Ausführliche Informationen hierzu finden Sie in der Dokumentation der MDM-Software.

# Installieren von Anwendungen über die USB-Verbindung



**VORSICHT:** Beim Anschließen des Geräts an einen Host-Computer und Einsetzen der microSD-Karte sind die für den Host-Computer geltenden Anweisungen zum Anschließen und Trennen von USB-Geräten zu befolgen, um die Beschädigung oder Zerstörung von Dateien zu vermeiden.

- 1. Schließen Sie das Gerät mit dem robusten Ladekabel/USB-Kabel an einen Host-Computer an.
- 2. Ziehen Sie das Benachrichtigungsfeld nach unten, und berühren Sie "**USB connect this device**" (Dieses Gerät über USB verbinden).

#### Abbildung 71 Dialogfeld zum Verwenden von USB

Use USB to	
<ul> <li>Connect this device</li> </ul>	
◯ Transfer files	
○ Transfer photos (PTP)	
○ Use device as MIDI	
	CANCEL

- 3. Berühren Sie Transfer files (Dateien übertragen).
- 4. Öffnen Sie auf dem Host-Computer eine Dateianwendung.
- 5. Kopieren Sie auf dem Host-Computer die .apk-Datei der Anwendung vom Host-Computer auf das Gerät.



**VORSICHT:** Befolgen Sie die für den Host-Computer geltenden Anweisungen zum Deaktivieren der microSD-Karte, und trennen Sie die USB-Geräte ordnungsgemäß, um Informationsverluste zu vermeiden.

- 6. Trennen Sie das Gerät vom Host-Computer.
- 7. Berühren Sie "Home" (Start), wischen Sie dann auf dem Bildschirm nach oben, und wählen Sie 🕒 aus, um Dateien auf der microSD-Karte oder im internen Speicher anzuzeigen.
- 8. Suchen Sie die .apk-Datei der Anwendung.
- 9. Berühren Sie die Anwendungsdatei.

Abbildung 72 Dialogfeld zum Erteilen der Installationsberechtigung



10.Berühren Sie **Continue** (Fortfahren), um die App zu installieren, oder **Cancel** (Abbrechen), um die Installation zu beenden.

•	User Manual	
Do you want to install this application? It does not require any special access.		
	CANCEL INSTALL	

- 11.Um die Installation zu bestätigen und die Auswirkungen der Anwendung zu akzeptieren, berühren Sie **Install** (Installieren), andernfalls **Cancel** (Abbrechen).
- 12. Berühren Sie **Open** (Öffnen), um die Anwendung zu öffnen, oder **Done** (Fertig), um den Installationsvorgang zu beenden. Die Anwendung wird in der App-Liste angezeigt.

## Installieren von Anwendungen mithilfe von Android Debug Bridge

Verwenden Sie die ADB-Befehle, um die Anwendung auf dem Gerät zu installieren.



**VORSICHT:** Beim Anschließen des Geräts an einen Host-Computer und Einsetzen der microSD-Karte sind die für den Host-Computer geltenden Anweisungen zum Anschließen und Trennen von USB-Geräten zu befolgen, um die Beschädigung oder Zerstörung von Dateien zu vermeiden.

Stellen Sie sicher, dass die ADB-Treiber auf dem Host-Computer installiert sind. Siehe ADB-Setup über USB auf Seite 123.

- 1. Verbinden Sie das Gerät über USB mit einem Host-Computer.
- Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend \$\$.
- 3. Berühren Sie System > Developer options (Entwickleroptionen).
- 4. Schieben Sie den Schalter in die Position ON (EIN).
- 5. Berühren Sie **USB Debugging** (USB-Debugging). Im Kontrollkästchen wird ein Häkchen angezeigt. Das Dialogfeld **Allow USB debugging?** (USB-Debugging zulassen?) wird angezeigt.
- 6. Berühren Sie OK.

7. Öffnen Sie auf dem Host-Computer ein Befehlszeilenfenster, und führen Sie den folgenden adb-Befehl aus: adb install <application>

wobei: <application> = Pfad und Dateiname der APK-Datei.

8. Trennen Sie das Gerät vom Host-Computer.

# Installieren von Anwendungen über eine microSD-Karte



**VORSICHT:** Beim Anschließen des Geräts an einen Host-Computer und Einsetzen der microSD-Karte sind die für den Host-Computer geltenden Anweisungen zum Anschließen und Trennen von USB-Geräten zu befolgen, um die Beschädigung oder Zerstörung von Dateien zu vermeiden.

- 1. Verbinden Sie das Gerät über USB mit einem Host-Computer.
- 2. Kopieren Sie die APK-Anwendungsdatei vom Host-Computer auf die microSD-Karte.
- 3. Entfernen Sie die microSD-Karte vom Host-Computer.
- 4. Setzen Sie die microSD-Karte in das Gerät ein.
- 5. Berühren Sie "Home" (Start), wischen Sie dann auf dem Bildschirm nach oben, und wählen Sie 🗅 aus, um Dateien auf der microSD-Karte anzuzeigen.
- 6. Berühren Sie **SD card** (SD-Karte).
- 7. Suchen Sie die .apk-Datei der Anwendung.
- 8. Berühren Sie die Anwendungsdatei.

#### Abbildung 74 Dialogfeld zum Erteilen der Installationsberechtigung



9. Berühren Sie **Continue** (Fortfahren), um die App zu installieren, oder **Cancel** (Abbrechen), um die Installation zu beenden.

#### Abbildung 75 Bildschirm zum Akzeptieren der Installation



- 10.Um die Installation zu bestätigen und die Auswirkungen der Anwendung zu akzeptieren, berühren Sie **Install** (Installieren), andernfalls **Cancel** (Abbrechen).
- 11.Berühren Sie **Open** (Öffnen), um die Anwendung zu öffnen, oder **Done** (Fertig), um den Installationsvorgang zu beenden. Die Anwendung wird in der App-Liste angezeigt.

## Deinstallieren einer Anwendung

So deinstallieren Sie eine Anwendung:

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Apps & Notifications (Apps und Benachrichtigungen).
- 3. Berühren Sie See all apps (Alle Apps anzeigen), um alle Apps in der Liste anzuzeigen.
- 4. Scrollen Sie durch die Liste, bis Sie die App gefunden haben.

5. Berühren Sie die App. Der Bildschirm App info (App-Info) wird angezeigt.

Abbildung 76 Bildschirm "App Info" (App-Info)



- 6. Berühren Sie Uninstall (Deinstallieren).
- 7. Berühren Sie **OK**, um den Vorgang zu bestätigen.

# Durchführen einer Systemaktualisierung

Systemaktualisierungspakete können entweder teilweise oder komplette Aktualisierungen für das Betriebssystem enthalten. Zebra stellt die Systemaktualisierungspakete auf der Support- und Downloads-Website bereit. Führen Sie die Systemaktualisierung entweder über eine microSD-Karte oder über ADB aus.

## Herunterladen des Systemaktualisierungspakets

So laden Sie das Systemaktualisierungspaket herunter:

- 1. Besuchen Sie die Support- und Downloads-Website von Zebra unter www.zebra.com/support.
- 2. Laden Sie das entsprechende Aktualisierungspaket auf einen Host-Computer herunter.

## Verwenden der microSD-Karte

- 1. Kopieren Sie die ZIP-Datei für die Systemaktualisierung in das Stammverzeichnis der microSD-Karte.
  - Kopieren Sie die ZIP-Datei mithilfe eines Host-Computers auf eine microSD-Karte, und setzen Sie die microSD-Karte dann in das Gerät ein (weitere Informationen finden Sie unter Einsetzen der microSD-Karte auf Seite 21).
  - Verbinden Sie das Gerät mit einer bereits installierten microSD-Karte mit dem Host-Computer, und kopieren Sie die ZIP-Datei auf die microSD-Karte. Trennen Sie das Gerät vom Host-Computer.

- Halten Sie die Reset-Taste gedrückt, bis die Option "Restart" (Neu starten) angezeigt wird. Lassen Sie die Reset-Taste los, wenn die Option angezeigt wird. Das Gerät wird neu gestartet, wenn die Taste länger als 3 Sekunden gedrückt wird.
- 3. Berühren Sie Restart (Neu starten).
- 4. Halten Sie die Taste Nr. 1 gedrückt. Der Bildschirm "System Recovery" (Systemwiederherstellung) wird angezeigt.
- 5. Drücken Sie die Taste Nr. 2, um zu **Apply upgrade from SD card** (Aktualisierung von SD-Karte übernehmen) zu navigieren.
- 6. Drücken Sie die Taste Nr. 1.
- 7. Navigieren Sie mit den Tasten Nr. 1 und Nr. 2 zur Systemaktualisierungsdatei.
- 8. Navigieren Sie mit der Taste Nr. 2 zur Systemaktualisierungsdatei.
- 9. Drücken Sie die Taste Nr. 1. Die Systemaktualisierung wird installiert, und das Gerät kehrt zum Wiederherstellungsbildschirm zurück.
- 10. Drücken Sie die Taste Nr. 1, um das Gerät neu zu starten.



**HINWEIS:** Wenn Sie die GMS-Software auf einem Gerät ohne GMS-Software oder Nicht-GMS-Software auf einem Gerät mit GMS-Software installieren, führen Sie ein Reset auf die Werkseinstellungen oder ein Enterprise-Reset (behält Unternehmensdaten bei) durch.

# Verwenden von ADB

So aktualisieren Sie das System mithilfe von ADB:

- 1. Verbinden Sie das Gerät mit dem robusten Lade-/USB-Kabel.
- 2. Schließen Sie das Kabel an den Host-Computer an.
- 3. Wischen Sie am Gerät von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 4. Berühren Sie System > Developer options (Entwickleroptionen).
- 5. Schieben Sie den Schalter in die Position ON (EIN).
- 6. Wenn **USB Debugging** (USB-Debugging) nicht auf **ON** (EIN) gesetzt ist, berühren Sie **USB Debugging** (USB-Debugging). Das Dialogfeld **Allow USB debugging**? (USB-Debugging zulassen?) wird angezeigt.
- 7. Berühren Sie **OK**.
- 8. Öffnen Sie auf dem Host-Computer ein Befehlszeilenfenster, und führen Sie den folgenden adb-Befehl aus: adb devices

Folgende Anzeige erscheint:

List of devices attached



**HINWEIS:** Wenn die Gerätenummer nicht angezeigt wird, vergewissern Sie sich, dass die ADB-Treiber ordnungsgemäß installiert sind.

9. Geben Sie Folgendes ein:

adb reboot recovery

- 10. Drücken Sie die Eingabetaste. Der Bildschirm System Recovery (Systemwiederherstellung) wird angezeigt.
- 11. Drücken Sie die Taste Nr. 2, um zu **Apply upgrade from SD card** (Aktualisierung von SD-Karte übernehmen) zu navigieren.
- 12. Geben Sie im Befehlszeilenfenster des Host-Computers Folgendes ein:

adb sideload <Datei>

wobei: <Datei> = Pfad und Dateiname der ZIP-Datei.

- 13. Drücken Sie die Eingabetaste. Die Systemaktualisierung wird installiert (der Fortschritt in Prozent wird im Befehlszeilenfenster angezeigt), und anschließend wird der Wiederherstellungsbildschirm angezeigt.
- 14. Drücken Sie die Taste Nr. 1, um das Gerät neu zu starten.



**HINWEIS:** Wenn Sie die GMS-Software auf einem Gerät ohne GMS-Software oder Nicht-GMS-Software auf einem Gerät mit GMS-Software installieren, führen Sie ein Reset auf die Werkseinstellungen oder ein Enterprise-Reset (behält Unternehmensdaten bei) durch.

# Überprüfen der Systemaktualisierungsinstallation

So überprüfen Sie, ob die Systemaktualisierung ordnungsgemäß installiert wurde:

- 1. Wischen Sie am Gerät von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie System > About phone (Telefoninfo).
- 3. Scrollen Sie nach unten zu Build number (Build-Nummer).
- 4. Stellen Sie sicher, dass die Build-Nummer mit der Nummer der neuen Systemaktualisierungspaketdatei übereinstimmt.

# **Durchführen eines Enterprise-Reset**

Bei einem Enterprise-Reset werden alle Benutzerdaten in der Partition /data gelöscht, einschließlich der Daten an primären Speicherorten (/sdcard und emulierter Speicher).

Stellen Sie vor dem Durchführen eines Enterprise-Reset alle erforderlichen Konfigurationsdateien bereit, und stellen Sie sie nach dem Zurücksetzen wieder her.

Führen Sie das Enterprise-Reset entweder über eine microSD-Karte oder über ADB durch.

## Herunterladen des Enterprise-Reset-Pakets

So laden Sie das Systemaktualisierungspaket herunter:

- 1. Besuchen Sie die Support- und Downloads-Website von Zebra unter www.zebra.com/support.
- 2. Laden Sie die Enterprise-Reset-Datei auf einen Host-Computer herunter.

## Verwenden der microSD-Karte

- 1. Kopieren Sie die ZIP-Datei für das Enterprise-Reset in das Stammverzeichnis der microSD-Karte.
  - Kopieren Sie die ZIP-Datei mithilfe eines Host-Computers auf eine microSD-Karte, und setzen Sie dann die microSD-Karte in das Gerät ein (siehe Einsetzen der microSD-Karte auf Seite 21).
  - Verbinden Sie das Gerät mit einer bereits installierten microSD-Karte mit dem Host-Computer, und kopieren Sie die ZIP-Datei auf die microSD-Karte. Trennen Sie das Gerät vom Host-Computer.
- 2. Halten Sie die Reset-Taste gedrückt, bis die Option "Restart" (Neu starten) angezeigt wird, und lassen Sie die Reset-Taste dann los.
- 3. Berühren Sie Restart (Neu starten).
- 4. Halten Sie die Taste Nr. 1 gedrückt. Der Bildschirm "System Recovery" (Systemwiederherstellung) wird angezeigt.
- 5. Drücken Sie die Taste Nr. 2, um zu "Apply upgrade from SD card" (Aktualisierung von SD-Karte übernehmen) zu navigieren.
- 6. Drücken Sie die Taste Nr. 1. Die Systemaktualisierung wird installiert, und das Gerät kehrt zum Wiederherstellungsbildschirm zurück.
- 7. Navigieren Sie mit der Taste Nr. 2 zur Systemaktualisierungsdatei.
- 8. Drücken Sie die Taste Nr. 1. Die Systemaktualisierung wird installiert, und das Gerät kehrt zum Wiederherstellungsbildschirm zurück.
- 9. Drücken Sie die Taste Nr. 1, um das Gerät neu zu starten.

# Verwenden von ADB

So führen Sie ein Enterprise-Reset über ADB durch:

- 1. Verbinden Sie das Gerät mit dem robusten Lade-/USB-Kabel.
- 2. Schließen Sie das Kabel an den Host-Computer an.
- 3. Wischen Sie am Gerät von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 4. Berühren Sie System > Developer options (Entwickleroptionen).
- 5. Schieben Sie den Schalter in die Position ON (EIN).
- 6. Berühren Sie **USB Debugging** (USB-Debugging). Im Kontrollkästchen wird ein Häkchen angezeigt. Das Dialogfeld **Allow USB debugging?** (USB-Debugging zulassen?) wird angezeigt.
- 7. Berühren Sie OK.
- 8. Öffnen Sie auf dem Host-Computer ein Befehlszeilenfenster, und geben Sie Folgendes ein:

adb devices.

Folgende Anzeige erscheint:

List of devices attached



**HINWEIS:** Wenn die Gerätenummer nicht angezeigt wird, vergewissern Sie sich, dass die ADB-Treiber ordnungsgemäß installiert sind.

9. Geben Sie Folgendes ein:

adb reboot recovery

- 10. Drücken Sie die Eingabetaste. Der Bildschirm "System Recovery" (Systemwiederherstellung) wird angezeigt.
- 11. Drücken Sie die Tasten Nr. 1 und Nr. 2, um zu apply from adb (Von ADB übernehmen) zu navigieren.
- 12. Geben Sie im Befehlszeilenfenster des Host-Computers Folgendes ein:

adb sideload <Datei>

wobei: <Datei> = Pfad und Dateiname der ZIP-Datei.

13. Drücken Sie die Eingabetaste. Das Enterprise-Reset-Paket wird installiert, und anschließend wird der Wiederherstellungsbildschirm angezeigt.

# Zurücksetzen auf die Werkseinstellungen (Factory-Reset)

Beim Zurücksetzen auf die Werkseinstellungen werden alle Daten in den Partitionen /data und /enterprise im internen Speicher sowie alle Geräteeinstellungen gelöscht. Beim Zurücksetzen auf die Werkseinstellungen wird das Gerät auf das zuletzt installierte Betriebssystemabbild zurückgesetzt. Um zu einer früheren Betriebssystemversion zurückzukehren, müssen Sie das entsprechende Betriebssystemabbild neu installieren. Weitere Informationen sind unter Durchführen einer Systemaktualisierung auf Seite 129 zu finden.

# Herunterladen des Factory-Reset-Pakets

So laden Sie das Paket zum Zurücksetzen auf die Werkseinstellungen herunter:

- 1. Besuchen Sie die Support- und Downloads-Website von Zebra unter www.zebra.com/support.
- 2. Laden Sie die entsprechende Datei mit den Werkseinstellungen auf einen Host-Computer herunter.

# Verwenden der microSD-Karte

- 1. Kopieren Sie die ZIP-Datei für die Werkseinstellungen in das Stammverzeichnis der microSD-Karte.
  - Kopieren Sie die ZIP-Datei mithilfe eines Host-Computers auf eine microSD-Karte, und setzen Sie dann die microSD-Karte in das Gerät ein (siehe Einsetzen der microSD-Karte auf Seite 21).
  - Verbinden Sie das Gerät mit einer bereits installierten microSD-Karte mit dem Host-Computer, und kopieren Sie die ZIP-Datei auf die microSD-Karte. Trennen Sie das Gerät vom Host-Computer.
- 2. Wechseln Sie in den Wiederherstellungsmodus, indem Sie die Taste Nr. 1 auf der Rückseite 3 Sekunden lang gedrückt halten, während Sie das Gerät aus- und wieder einschalten.
- 3. Drücken Sie die Tasten Nr. 1 und Nr. 2, um zu **apply update from sdcard** (Update von der SD-Karte übernehmen) zu navigieren.

Mit dieser Option können Benutzer ein Betriebssystem-Upgrade mit vollständigen OTA-Paketen, OTA-Paketen, die nur den veränderten Code enthalten, oder Wiederherstellungspaketen von einer SD-Karte aus durchführen.

# Verwenden von ADB

So setzen Sie ein Gerät mithilfe von ADB auf die Werkseinstellungen zurück:

- 1. Verbinden Sie das Gerät mit dem robusten Lade-/USB-Kabel.
- 2. Schließen Sie das Kabel an den Host-Computer an.
- 3. Wischen Sie am Gerät von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 4. Berühren Sie System > Developer options (Entwickleroptionen).
- 5. Schieben Sie den Schalter in die Position **ON** (EIN).
- 6. Berühren Sie **USB Debugging** (USB-Debugging). Im Kontrollkästchen wird ein Häkchen angezeigt. Das Dialogfeld **Allow USB debugging?** (USB-Debugging zulassen?) wird angezeigt.
- 7. Berühren Sie OK.
- 8. Öffnen Sie auf dem Host-Computer ein Befehlszeilenfenster, und führen Sie den folgenden adb-Befehl aus: adb reboot recovery
- 9. Drücken Sie die Eingabetaste. Der Bildschirm "System Recovery" (Systemwiederherstellung) wird angezeigt.
- 10. Drücken Sie die Tasten zum Erhöhen und zum Verringern der Lautstärke, um zu **apply from adb** (Von ADB übernehmen) zu navigieren.
- 11. Öffnen Sie auf dem Host-Computer ein Befehlszeilenfenster, und führen Sie den folgenden adb-Befehl aus:

adb devices.

Folgende Anzeige erscheint:

List of devices attached



**HINWEIS:** Wenn die Gerätenummer nicht angezeigt wird, vergewissern Sie sich, dass die ADB-Treiber ordnungsgemäß installiert sind.

12. Geben Sie Folgendes ein:

adb reboot recovery

- 13. Drücken Sie die Eingabetaste. Der Bildschirm "System Recovery" (Systemwiederherstellung) wird angezeigt.
- 14. Drücken Sie die Tasten zum Erhöhen und zum Verringern der Lautstärke, um zu **apply from adb** (Von ADB übernehmen) zu navigieren.
- 15. Geben Sie im Befehlszeilenfenster des Host-Computers Folgendes ein:

adb sideload <Datei>

wobei: <Datei> = Pfad und Dateiname der ZIP-Datei.

16.Drücken Sie die Eingabetaste. Das Factory-Reset-Paket wird installiert, und anschließend wird der Wiederherstellungsbildschirm angezeigt.

# Speicher

Das Gerät bietet vier Arten von Dateispeicher:

- Speicher mit direktem Zugriff (Random Access Memory, RAM)
- Interner Speicher
- Externer Speicher (microSD-Karte)
- Enterprise-Ordner

# Speicher mit direktem Zugriff (Random Access Memory, RAM)

Bei der Ausführung von Programmen werden Daten über den RAM gespeichert. Im RAM gespeicherte Daten gehen beim Zurücksetzen verloren. Das Betriebssystem steuert, wie der RAM von Anwendungen verwendet wird. Es erlaubt Anwendungen, Komponentenprozessen und Diensten nur dann einen Zugriff auf RAM, wenn dies erforderlich ist. Es kann kürzlich verwendete Prozesse im RAM zwischenspeichern, sodass sie beim erneuten Öffnen schneller neu gestartet werden können. Allerdings wird der Zwischenspeicher gelöscht, wenn der RAM für neue Aktivitäten benötigt wird.

- 1. Um die Größe des freien und belegten Arbeitsspeichers anzuzeigen, wischen Sie am Gerät von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend **‡**.
- 2. Berühren Sie System > Developer options (Entwickleroptionen) > Memory (Arbeitsspeicher).

÷	Memory	
	3 hours	~
	Average memory use	
	Performance	Normal
	Total memory	3.9 GB
	Average used (%)	45%
	Free	2.2 GB
	Memory used by apps 85 apps used memory in the las	st 3 hours

Abbildung 77 Bildschirm "Memory" (Arbeitsspeicher)

Der Bildschirm zeigt die Größe des verwendeten und freien RAM an.

## **Interner Speicher**

Das Gerät verfügt über einen internen Speicher. Der Inhalt des internen Speichers kann angezeigt und Dateien können auf das und von dem Gerät kopiert werden, wenn es an einen Host-Computer angeschlossen ist. Einige Anwendungen sind so konzipiert, dass sie im internen Speicher und nicht im internen Arbeitsspeicher abgelegt werden. So zeigen Sie den belegten und verfügbaren Speicherplatz im internen Speicher an:

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Storage (Speicher).

Abbildung 78 Bildschirm "Storage" (Speicher)

÷	Storage	
	Device storage	
	<b>14.81</b> GB	
	Total used of 32.00 GB	
	Internal shared storage 14.81 GB used of 32.00 GB	
	Portable storage	
	SanDisk SD card 1.03 GB used of 7.94 GB	<b>▲</b>

• Internal Storage (Interner Speicher): Zeigt den insgesamt verfügbaren und den belegten Speicherplatz im internen Datenspeicher an.

Berühren Sie **Internal shared storage** (Interner freigegebener Speicher), um den Speicherplatz anzuzeigen, der von Apps, Fotos, Videos, Audio und anderen Dateien verwendet wird.

Abbildung 79 Bildschirm "Internal Storage" (Interner Speicher)

<del>\</del>	Storage	
	7.09 GB Used of 16 GB FREE UP SPACE	44% used
	Storage manager	
<b></b>	Photos & videos	0.00 GB
ſ	Music & audio	0.00 GB
+-	Games	0.00 GB
HINE!	Movie & TV apps	0.00 GB

# **Externer Speicher**

Das Gerät kann mit austauschbarer microSD-Karte betrieben werden. Der Inhalt der microSD-Karte kann angezeigt und Dateien können auf die Karte und von der Karte kopiert werden, wenn das Gerät an einen Host-Computer angeschlossen ist.

So zeigen Sie den verwendeten und verfügbaren Speicherplatz auf der microSD-Karte an:

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Storage (Speicher).

Abbildung 80	Bildschirm "Storag	e" (Speicher)
--------------	--------------------	---------------



Der externe Speicher zeigt den Gesamtspeicherplatz und den auf der installierten microSD-Karte belegten Speicherplatz an.

Um die Verbindung zur microSD-Karte zu trennen, berühren Sie A.

Berühren Sie SD card (SD-Karte), um den Inhalt der Karte anzuzeigen.

## Formatieren der microSD-Karte

So formatieren Sie eine in das Gerät eingesetzte microSD-Karte als externen Speicher:

- 1. Berühren Sie **SD card** (SD-Karte).
- 2. Berühren Sie : > Storage settings (Speichereinstellungen).

Abbildung 81 Bildschirm mit SD-Karten-Einstellungen

<b>1.03</b> GB Used of 7.94 GB
Format
Format as internal
EJECT

3. Berühren Sie Format (Formatieren).

Abbildung 82 Bildschirm für die Formatierung



- 4. Berühren Sie ERASE & FORMAT (Löschen und Formatieren).
- 5. Berühren Sie DONE (Fertig).

## Formatieren als internen Speicher

Sie können eine microSD-Karte als internen Speicher formatieren, um den internen Speicher des Geräts zu vergrößern. Nach dem Formatieren kann die microSD-Karte nur von diesem Gerät gelesen werden. So formatieren Sie eine in das Gerät eingesetzte microSD-Karte als internen Speicher:

- 1. Berühren Sie SD card (SD-Karte).
- 2. Berühren Sie **Storage settings** (Speichereinstellungen).

Abbildung 83 Bildschirm mit SD-Karten-Einstellungen

SanDisk SD card	
1.03 GB Used of 7.94 GB Format Format as internal	
EJECT	

3. Berühren Sie Format as internal (Als intern formatieren).

Abbildung 84 Bildschirm für die Formatierung



- 4. Berühren Sie ERASE & FORMAT (Löschen und Formatieren).
- 5. Berühren Sie DONE (Fertig).

# **Enterprise-Ordner**

Der Enterprise-Ordner (innerhalb des internen Flash-Speichers) ist ein persistenter Speicher, in dem Daten auch nach einem Reset oder einem Enterprise-Reset dauerhaft verbleiben. Der Enterprise-Ordner wird während eines Zurücksetzens auf die Werkseinstellungen gelöscht. Der Enterprise-Ordner wird für die Bereitstellung und für gerätespezifische Daten verwendet. Der Enterprise-Ordner hat eine Größe von ca. 128 MB (formatiert). Anwendungsdaten können nach einem Enterprise-Reset beibehalten werden, indem die Daten im Enterprise-/User-Ordner gespeichert werden. Der Ordner ist ext4-formatiert und kann nur über einen Host-Computer mit ADB oder über ein MDM aufgerufen werden.

# Anwendungsverwaltung

Anwendungen verwenden zwei Arten von Speicher: Datenspeicher und RAM. Anwendungen nutzen den Datenspeicher für sich selbst und alle Dateien, Einstellungen und andere Daten, die sie verwenden. Wenn Anwendungen ausgeführt werden, verwenden sie auch den RAM.

- 1. Wischen Sie von der Statusleiste nach unten, um das Schnellzugriffsfeld zu öffnen, und berühren Sie anschließend 🌣.
- 2. Berühren Sie Apps & Notifications (Apps und Benachrichtigungen).

Abbildung 85 Bildschirm "Apps & Notifications" (Apps und Benachrichtigungen)



3. Berühren Sie See all XX apps (Alle XX Apps anzeigen), um alle Apps auf dem Gerät anzuzeigen.

#### Abbildung 86 Bildschirm "App Info" (App-Info)



- 4. Berühren Sie > Show system (System anzeigen), um Systemprozesse in die Liste aufzunehmen.
- 5. Berühren Sie eine App, einen Prozess oder einen Dienst in der Liste, um einen Bildschirm mit Details zu dieser App zu öffnen. Je nach Element können Sie Einstellungen, Berechtigungen und Benachrichtigungen ändern oder das Beenden der App erzwingen sowie die App deinstallieren.

# **Anzeigen von App-Details**

Apps weisen verschiedene Arten von Informationen und Steuerelementen auf, umfassen jedoch in der Regel:

- Force stop (Beenden erzwingen): Beenden einer App.
- Disable (Deaktivieren): Deaktivieren einer App.
- Uninstall (Deinstallieren): Entfernen der App und aller zugehörigen Daten und Einstellungen vom Gerät. Informationen zum Deinstallieren von Apps finden Sie unter Deinstallieren einer Anwendung auf Seite 128.
- Storage (Speicher): Zeigt an, wie viele Informationen gespeichert sind, und enthält eine Schaltfläche zum Löschen.
- Data usage (Datennutzung): Bietet Informationen zu Daten (WiFi), die von einer App verwendet werden.
- Permissions (Berechtigungen): Listet die Bereiche auf dem Gerät auf, auf die die App zugreifen kann.
- Notifications (Benachrichtigungen): Ermöglicht das Einrichten von Benachrichtigungseinstellungen f
  ür die App.
- **Open by default** (Standardmäßig öffnen): Wenn Sie eine App so konfiguriert haben, dass bestimmte Dateitypen standardmäßig gestartet werden, können Sie diese Einstellung hier löschen.
- Memory (Arbeitsspeicher): Zeigt die durchschnittliche Arbeitsspeicherverwendung durch die App an.
- Erweitert
  - Draw over other apps (Über anderen Apps einblenden): Ermöglicht das Anzeigen einer App über anderen Apps.

# Verwalten von Downloads

Dateien und Apps, die mit dem Browser oder per E-Mail heruntergeladen wurden, werden auf der microSD-Karte oder im internen Speicher im Download-Verzeichnis gespeichert. Verwenden Sie die Downloads-App, um heruntergeladene Elemente anzuzeigen, zu öffnen oder zu löschen.

- 1. Wischen Sie auf dem Bildschirm nach oben, und berühren Sie 🗅.
- 2. Berühren Sie **= > Downloads**.

Abbildung 87 Bildschirm "Files - Downloads" (Dateien – Downloads)



Berühren und halten Sie ein Element, wählen Sie die zu löschenden Elemente aus, und berühren Sie 
 . Das Element wird vom Gerät gelöscht.

# Wartung und Fehlerbehebung

# Einführung

Dieses Kapitel enthält Anweisungen zur Reinigung und Lagerung des Geräts sowie Lösungen zur Fehlerbehebung bei potenziellen Problemen während des Betriebs.

# Wartung des Geräts

Um einen störungsfreien Betrieb zu gewährleisten, sollten Sie bei der Verwendung des Geräts folgende Tipps beachten:

- Um ein Verkratzen des Bildschirms zu vermeiden, verwenden Sie Stifte mit Kunststoffspitze, die für die Verwendung mit Touchscreens geeignet sind. Verwenden Sie für den Bildschirm des Geräts auf keinen Fall einen Kugelschreiber, Bleistift oder anderen spitzen Gegenstand.
- Der Touchscreen des Geräts besteht aus Glas. Achten Sie darauf, dass das Gerät nicht herunterfällt oder starken Stößen ausgesetzt wird.
- Schützen Sie das Gerät vor extremen Temperaturen. Lassen Sie es an heißen Tagen nicht auf dem Armaturenbrett im Auto liegen, und halten Sie es von Wärmequellen fern.
- · Lagern und verwenden Sie das Gerät nicht in staubigen, feuchten oder nassen Umgebungen.
- Verwenden Sie zum Reinigen des Geräts ein weiches Brillenreinigungstuch. Falls die Displayoberfläche des Geräts verschmutzt ist, reinigen Sie sie mit einem weichen, mit einem zugelassenen Reinigungsmittel getränkten Reinigungstuch. Eine Liste der zugelassenen Reinigungsmittel finden Sie unter Zulässige Wirkstoffe in Reinigungsmitteln auf Seite 144.

# Reinigungshinweise



VORSICHT: Tragen Sie immer einen Augenschutz.

Beachten Sie die Warnhinweise für Alkoholprodukte, bevor Sie diese verwenden. Wenn Sie aus medizinischen Gründen eine andere Lösung verwenden müssen, wenden Sie sich bitte an den globalen Kundendienst, um weitere Informationen zu erhalten.



**WARNUNG:** Vermeiden Sie es, dieses Produkt mit heißem Öl oder anderen brennbaren Flüssigkeiten in Kontakt zu bringen. Ziehen Sie bei einer solchen Exposition den Netzstecker aus der Steckdose, und reinigen Sie das Produkt sofort gemäß diesen Richtlinien.

# Zulässige Wirkstoffe in Reinigungsmitteln

100 % der Wirkstoffe in Reinigungsmitteln müssen aus einem oder mehreren der folgenden Stoffe bestehen: Isopropanol, Bleichmittel/Natriumhypochlorit<sup>1</sup> (siehe den wichtigen Hinweis unten), Wasserstoffperoxid, Ammoniumchlorid oder mildes Geschirrspülmittel.



WICHTIG: Verwenden Sie im Voraus befeuchtete Tücher, und vermeiden Sie jegliche Ansammlungen von Flüssigreiniger.

<sup>1</sup> Befolgen Sie bei der Verwendung von Produkten, die auf Natriumhypochlorit (Bleichmittel) basieren, immer die empfohlenen Anweisungen des Herstellers: Verwenden Sie Handschuhe beim Auftragen, und entfernen Sie anschließend die Rückstände mit einem alkoholhaltigen feuchten Tuch oder Wattestäbchen, um einen längeren Hautkontakt beim Umgang mit dem Gerät zu vermeiden.

Da Natriumhypochlorit ein starkes Oxidationsmittel ist, neigen die metallischen Oberflächen des Geräts zum Oxidieren (Korrosion), wenn sie dieser Chemikalie in flüssiger Form (einschließlich Feuchttüchern) ausgesetzt sind. Falls derartige Desinfektionsmittel mit dem Metall des Geräts in Berührung kommen, ist die sofortige Entfernung mithilfe von mit Alkohol angefeuchteten Tüchern oder Wattestäbchen nach dem Reinigungsschritt sehr wichtig.

# Schädliche Inhaltsstoffe

Die folgenden chemischen Stoffe gelten als schädlich für die Kunststoffteile des Geräts und sollten nicht mit dem Gerät in Berührung kommen: Aceton, Ketone, Äther, aromatische und chlorierte Kohlenwasserstoffe, wässrige oder alkoholische alkalische Lösungen, Ethanolamin, Toluol, Trichlorethylen, Benzol, Karbolsäure und TB-Lysoform.

Viele Vinylhandschuhe enthalten Phthalatzusätze, die häufig nicht für medizinische Zwecke empfohlen werden und bekanntermaßen das Gehäuse des Geräts beschädigen.

# Reinigungshinweise für das Gerät

Tragen Sie keine Flüssigkeit direkt auf das Gerät auf. Befeuchten Sie ein weiches Tuch, oder verwenden Sie bereits angefeuchtete Tücher. Wickeln Sie das Gerät nicht in ein Tuch oder einen Wischlappen, sondern wischen Sie es vorsichtig ab. Achten Sie darauf, dass sich keine Flüssigkeit um das Anzeigefenster oder an anderen Stellen sammelt. Lassen Sie das Gerät vor der nächsten Verwendung an der Luft trocknen.



HINWEIS: Zur gründlichen Reinigung empfiehlt es sich, gegebenenfalls zuerst alle Zubehörteile zu entfernen.

# **Besondere Reinigungshinweise**

Das Gerät darf nicht mit Vinylhandschuhen berührt werden, die Phthalate enthalten, oder bevor die Hände gewaschen werden, um Schmutzrückstände nach dem Entfernen der Handschuhe zu entfernen.

Falls Produkte verwendet werden, die einen oder mehrere der oben genannten schädlichen Stoffe enthalten, z. B. Ethanolamin-haltige Handdesinfektionsmittel, müssen die Hände vor der Bedienung des Geräts vollständig trocken sein, um Schäden am Gerät zu vermeiden.



**WICHTIG:** Wenn das Gerät mit Reinigungs-/Desinfektionsmittel in Berührung kommt, ist es wichtig, die Anweisungen des Herstellers des Reinigungs-/Desinfektionsmittels zu beachten.
#### Erforderliche Reinigungsmaterialien

- Alkoholgetränkte Tücher
- Objektiv-Reinigungstuch
- Applikatoren mit Baumwollspitze
- Isopropylalkohol
- Druckluftdose mit Rohr

#### Reinigungshäufigkeit

Die Reinigungshäufigkeit ist vom Kunden unter Berücksichtigung der unterschiedlichen Umgebungen, in denen die mobilen Computer eingesetzt werden, nach eigenem Ermessen festzulegen (d. h. so häufig wie nötig). Wenn Schmutz sichtbar ist, wird empfohlen, den mobilen Computer zu reinigen, um die Ablagerung von Partikeln zu vermeiden, durch die das Gerät später schwerer zu reinigen ist.

Zur Erzielung einer hohen Konsistenz und optimalen Bilderfassung wird empfohlen, das Kamerafenster regelmäßig zu reinigen, insbesondere beim Einsatz in Umgebungen mit hohem Staub- oder Schmutzaufkommen.

#### Reinigen des Geräts

#### Gehäuse

Wischen Sie das Gehäuse, einschließlich aller Tasten und Auslöser, mit einem zugelassenen Alkohol-Reinigungstuch ab.

#### Display

Das Display kann mit einem zugelassenen Alkohol-Reinigungstuch gereinigt werden, doch ist darauf zu achten, dass sich an den Rändern des Displays keine Flüssigkeit ansammelt. Das Display muss anschließend sofort mit einem weichen, nicht scheuernden Tuch getrocknet werden, um Streifen zu vermeiden.

#### Kamera und Scanfenster

Reinigen Sie die Kamera und das Scanfenster regelmäßig mit einem Objektiv-Reinigungstuch oder einem anderen geeigneten Material für optische Geräte wie beispielsweise Brillen.

## Fehlerbehebung

In den folgenden Tabellen sind typische Probleme, die auftreten können, sowie die entsprechenden Lösungen zur Behebung des jeweiligen Problems angegeben.

Problem	Ursache	Lösung
Während der Datenkommuni- kation mit einem Host-Computer wurden keine Daten	Das Gerät wird während der Kommunikation vom Host-Computer getrennt.	Schließen Sie das Kommunikationskabel wieder an, um erneut zu übertragen.
übertragen, oder die Datenübertragung war nicht vollständig	Falsche Kabelkonfiguration.	Wenden Sie sich an Ihren Systemadministrator.
war mont vonetarraig.	Kommunikationssoft- ware wurde falsch installiert oder konfiguriert.	Führen Sie die Einrichtung durch.
Während der Datenkommuni-	WLAN-Funkgerät ist nicht eingeschaltet.	Schalten Sie das WLAN-Funkgerät ein.
kation über WLAN wurden keine Daten übertragen, oder die Datenübertragung war nicht vollständig.	Sie haben sich außerhalb des Bereichs eines Access Points bewegt.	Gehen Sie näher an einen Access Point heran.
Während der Datenkommuni- kation über Bluetooth wurden keine Daten übertragen, oder die Datenübertragung war nicht vollständig.	Bluetooth-Funkgerät ist nicht eingeschaltet.	Schalten Sie das Bluetooth-Funkgerät ein.
	Sie haben sich außerhalb der Reichweite eines anderen Bluetooth-Geräts bewegt.	Bewegen Sie sich innerhalb von 10 Metern in der Nähe des anderen Geräts.
Kein Ton.	Die Lautstärke ist niedrig oder ausgeschaltet.	Passen Sie die Lautstärke an.
Das Gerät schaltet sich aus.	Das Gerät ist inaktiv.	Das Display schaltet sich nach einer bestimmten Zeit der Inaktivität aus. Stellen Sie diesen Zeitraum auf 15 Sekunden, 30 Sekunden, 1, 2, 5, 10 oder 30 Minuten ein.
Durch Tippen auf die Fensterschaltflächen oder -symbole wird die entsprechende Funktion nicht aktiviert.	Das Gerät reagiert nicht.	Setzen Sie das Gerät zurück.

Problem	Ursache	Lösung
Es wird eine Meldung angezeigt, dass der Speicher des Geräts voll ist.	Es wurden zu viele Dateien auf dem Gerät gespeichert.	Löschen Sie nicht verwendete Memos und Datensätze. Speichern Sie diese Datensätze bei Bedarf auf dem Host-Computer (oder verwenden Sie eine SD-Karte als zusätzlichen Speicher).
	Es sind zu viele Anwendungen auf dem Gerät installiert.	Entfernen Sie benutzerinstallierte Anwendungen vom Gerät, um Speicherplatz freizugeben. Wählen Sie 🌣 > Storage (Speicher) > FREE UP SPACE (Speicherplatz freigeben) > REVIEW RECENT ITEMS (Kürzlich verwendete Elemente prüfen). Wählen Sie das bzw. die nicht verwendeten Programme aus, und berühren Sie FREE UP (Freigeben).
Das Gerät decodiert keine Barcodes beim Lesen.	Die Scananwendung ist nicht geladen.	Laden Sie eine Scan-Anwendung auf das Gerät, oder aktivieren Sie DataWedge. Wenden Sie sich an Ihren Systemadministrator.
	Der Barcode ist nicht lesbar.	Überprüfen Sie den Barcode auf Fehler.
	Falscher Abstand zwischen Scanfenster und Barcode.	Positionieren Sie das Gerät im richtigen Scanbereich.
	Das Gerät ist nicht für den Barcode programmiert.	Programmieren Sie das Gerät für das Lesen des zu scannenden Barcodetyps. Weitere Informationen finden Sie in der EMDK- oder DataWedge-Anwendung.
	Das Gerät ist nicht so programmiert, dass ein Signalton erzeugt wird.	Wenn das Gerät nach erfolgreicher Decodierung keinen Signalton ausgibt, müssen Sie die Anwendung entsprechend einrichten.
Das Gerät findet keine Bluetooth-Geräte in	Zu weit von anderen Bluetooth-Geräten entfernt.	Bewegen Sie sich innerhalb einer Reichweite von 10 Metern näher zu den anderen Bluetooth-Geräten.
der Umgebung.	Die Bluetooth-Geräte in der Nähe sind nicht eingeschaltet.	Schalten Sie das/die Bluetooth-Gerät(e) ein, um es/sie zu finden.
	Die Bluetooth-Geräte befinden sich nicht im Erkennungsmodus.	Stellen Sie das/die Bluetooth-Gerät(s) auf den Erkennungsmodus ein. Falls erforderlich, finden Sie weitere Informationen in der Benutzerdokumentation des Geräts.
Das Gerät lässt sich nicht entsperren.	Der Benutzer gibt ein falsches Kennwort ein.	Wenn der Benutzer acht Mal ein falsches Kennwort eingibt, wird er aufgefordert, einen Code einzugeben, bevor er es erneut versuchen kann.
		Wenn der Benutzer das Kennwort vergessen hat, wenden Sie sich an den Systemadministrator.

Tabelle 7	Fehlerbehebung des Geräts	(Fortsetzung)
		1

## **Technische Daten**

## Einführung

Dieses Kapitel enthält die technischen Daten sowie die Decodierabstände für den CC600 und den CC6000.

## **Technische Daten**

#### CC6000

Element	Beschreibung
Gerätemerkmale	
Abmessungen	Querformat: 10,9 Zoll x 7,9 Zoll x 1,4 Zoll
	27,8 cm x 20,1 cm x 3,6 cm
	Hochformat: 7,2 Zoll x 11,6 Zoll x 1,4 Zoll
	18,3 cm x 29,6 cm x 3,6 cm
Gewicht	980 g
Display	10,1 Zoll PCAP Multitouch
Aktiver Bildschirmbereich	217 mm B x 136 mm T
Seitenverhältnis	16:10
Auflösung	1280 x 800 bei 60 Hz
Tastenfeld	Virtuell
Konnektivität	USB-Host: 2 USB 2.0 Typ A Anschlüsse für Zubehör
	USB OTG: 1 USB-C OTG
	Ethernet Gigabit-kompatibel: RJ45
	Externer Audioeingang: 3,5 mm-Stecker
Audio	Audio zwei Mikrofone; zwei nach vorne gerichtete Lautsprecher (2 W gesamt)
Erweiterungsmöglichkeiten	Micro SD-Card-Steckplatz, unterstützt Klasse 2 bis Klasse 10 und UHS-1 SD-Speicherkarten
Stromversorgung	Unternehmensgerechte Stromversorgung: 5,4 V DC/3 A; 110/220 V
	Unterstützung für integriertes 802.3at Power-over-Ethernet (PoE)

 Tabelle 8
 Technische Daten des CC6000

Tabelle 8	Technische	Daten des	CC6000	(Fortsetzung)
-----------	------------	-----------	--------	---------------

Element	Beschreibung
Leistungsmerkmale	
Display-Helligkeit	300 Nits
CPU	Qualcomm Snapdragon ™ 660
Betriebssystem	Android Oreo, Google GMS
Speicher	RAM: 4 GB
	Interner Speicher: 32 GB
Benutzerumgebung	
Betriebstemperatur	0 °C bis 40 °C
Lagerungstemperatur	-40 °C bis 70 °C
Luftfeuchtigkeit	5 bis 95 % (nicht kondensierend)
Verwaltung	
Verwaltungswerkzeuge	Integration in standardmäßige Mobile Device Management (MDM)-Lösungen zur Konfiguration von Einstellungen und Bereitstellung von Software-Updates per Fernzugriff
Datenerfassung/-ausgabe	
Integrierter Scanner	1D/2D Zebra SE4710 decodierter Scanner
Kamera an der Vorderseite	5 MP
Video	1080p
Netzwerke	
WLAN	Dualband 802.11 a/b/g/n/ac/d/h/r/k/w/i (unterstützt 2,4 GHz und 5,2 GHz)
WPAN	Bluetooth 5.0; integrierte Antenne
Ethernet	Gigabit-Ethernet über RJ45-Schnittstelle mit Aktivitäts-LEDs
Peripheriegeräte und Zuber	nör
Zubehör	Länderspezifisches Kabel für Wechselstromleitung.
	Weiteres Zubehör kann mithilfe von USB- und der Bluetooth-Schnittstelle integriert werden
Montageoptionen	Integrierte Montagemöglichkeit nach VESA-Standard; entspricht dem VESA-Montagestandard von 100 mm x 100 mm für handelsübliche Montagelösungen von Drittanbietern; vier (4) M4 x 8 mm maximaler Einsatzabstand
Technische Daten der 2D-Imager-Engine (SE4710)	
Sichtfeld	Horizontal – 42,0°
	Vertikal – 28,0°
Bildauflösung	1280 x 800 Pixel (H x V)
Drehung	360°
Neigungswinkel	±60° von der Ausgangsposition
Schwenktoleranz	±60° von der Ausgangsposition
Umgebungslicht	Sonnenlicht: 10.764 lx

Tabelle 8	Technische D	aten des C	CC6000 (I	Fortsetzung)
-----------	--------------	------------	-----------	--------------

Element	Beschreibung
Fokusdistanz	Ab Engine-Vorderseite: 19,4 cm
Zielelement	610 nm gelber LED-Punkt
Beleuchtungssystem	Rote LED-Anzeige

## CC600

Element	Beschreibung
Gerätemerkmale	
Abmessungen	6,6 Zoll x 4,6 Zoll x 1,4 Zoll 16,9 cm x 11,6 cm x 3,5 cm
Gewicht	320 g
Display	5,0 Zoll PCAP Multitouch
Aktiver Bildschirmbereich	110 mm B x 62 mm T
Seitenverhältnis	16:10
Auflösung	1280 x 720 bei 60 Hz
Tastenfeld	Virtuell
Konnektivität	USB OTG: 1 USB-C OTG Ethernet Gigabit-kompatibel: RJ45
Audio	Zwei Mikrofone, ein nach vorn gerichteter Lautsprecher (2 W gesamt)
Erweiterungsmöglichkeiten	Micro SD-Card-Steckplatz, unterstützt Klasse 2 bis Klasse 10 und UHS-1 SD-Speicherkarten
Stromversorgung	Unternehmensgerechte Stromversorgung: 5,4 V DC/3 A; 110/220 V Unterstützung für integriertes 802.3at Power-over-Ethernet (PoE)
Leistungsmerkmale	
Display-Helligkeit	480 Nits
CPU	Qualcomm Snapdragon ™ 660
Betriebssystem	Android Oreo, Google GMS
Speicher	RAM: 4 GB
	Interner Speicher: 32 GB
Benutzerumgebung	
Betriebstemperatur	0 °C bis 40 °C
Lagerungstemperatur	-40 °C bis 70 °C
Luftfeuchtigkeit	5 bis 95 % (nicht kondensierend)
Verwaltung	
Verwaltungswerkzeuge	Integration in standardmäßige Mobile Device Management (MDM)-Lösungen zur Konfiguration von Einstellungen und Bereitstellung von Software-Updates per Fernzugriff

#### Tabelle 9 Technische Daten des CC600

Tabelle 9	Technische Daten de	les CC600 (Fortsetzung)	
-----------	---------------------	-------------------------	--

Element	Beschreibung
Datenerfassung/-ausgabe	
Integrierter Scanner	1D/2D Zebra SE2100 Scanner
Netzwerke	
WLAN	Dualband 802.11 a/b/g/n/ac/d/h/r/k/w/i (unterstützt 2,4 GHz und 5,2 GHz)
WPAN	Bluetooth 5.0; integrierte Antenne
Ethernet	Gigabit-Ethernet über RJ45-Schnittstelle mit Aktivitäts-LEDs
Peripheriegeräte und Zubeh	iör
Zubehör	Weiteres Zubehör kann mithilfe von USB- und der Bluetooth-Schnittstelle integriert werden
Montageoptionen	Integrierte Montagemöglichkeit nach VESA-Standard; entspricht dem VESA-Montagestandard von 75 mm x 75 mm für handelsübliche Montagelösungen von Drittanbietern; vier (4) M4 x 8 mm maximaler Einsatzabstand
Technische Daten der 2D-In	nager-Engine (SE 2100)
Sichtfeld	Horizontal – 41,5°
	Vertikal – 31,7°
Bildauflösung	640 horizontale x 480 vertikale Pixel
Drehung	360°
Neigungswinkel	±60° von der Ausgangsposition
Schwenktoleranz	±60° von der Ausgangsposition
Umgebungslicht	Sonnenlicht: 10.764 lx
Fokusdistanz	Ab Engine-Vorderseite: 10,7 cm
Zielelement	Keine
Beleuchtungssystem	Ultraweiße LED

Tabelle 10	Für die Datenerfassung	unterstützte S	ymbologien
------------	------------------------	----------------	------------

Element	Beschreibung
1D-Barcodes	Code 128, EAN-8, EAN-13, GS1 DataBar Expanded, GS1 128, GS1 DataBar Coupon, UPCA, Interleaved 2 aus 5, UPC Coupon Code
2D-Barcodes	PDF-417, QR Code, Digimarc, DotCode (nur CC6000)

#### Decodierabstände

#### CC6000 – SE4710 Scan-Engine

In Tabelle 11 sind die typischen Abstände für die ausgewählten Barcodedichten beim Scannen mit dem CC6000 aufgeführt. Die Mindestbreite des Elements (oder "Symboldichte") ist die Breite des schmalsten Elements (Balken oder Zwischenraum) im Symbol in Mil.

Barcadatun	Nahbereich	Fernbereich				
Barcodetyp	Typisch	Typisch				
4 mil	3,3 Zoll / 8,4 cm	8,8 Zoll / 22,4 cm				
Code 39						
5 mil	2,8 Zoll / 7,1 cm	8,2 Zoll / 20,8 cm				
Code 128						
5 mil	2,0 Zoll / 5,08 cm	13,5 Zoll / 34,3 cm				
Code 39						
5 mm	3,1 Zoll / 7,9 cm	7,5 Zoll / 19,0 cm				
PDF417						
10 mil	2,9 Zoll / 7,4 cm	10,1 Zoll / 25,7 cm				
DataMatrix						
100 % UPCA	1,8 Zoll / 4,6 cm*	24,0 Zoll / 60,9 cm				
20,0 mil	2,0 Zoll / 5,08 cm*	26 Zoll / 66,0 cm				
Code 39						

Tabelle 11	CC6000 – SE4710 Decodierbereiche
------------	----------------------------------

\* Begrenzt durch die Breite des Barcodes im Sichtfeld.

Hinweis: Barcode fotografischer Qualität bei 15 ° Neigungswinkel unter einer Umgebungsbeleuchtung von 30 fcd.

#### CC600 – SE2100 Scan-Engine

In Tabelle 12 sind die typischen Abstände für die ausgewählten Barcodedichten beim Scannen mit dem CC600 aufgeführt. Die Mindestbreite des Elements (oder "Symboldichte") ist die Breite des schmalsten Elements (Balken oder Zwischenraum) im Symbol in Mil.

Paradatun	Nahbereich	Fernbereich				
Barcouetyp	Typisch	Typisch				
5 mil	2,0 Zoll / 51 mm	4,8 Zoll / 122 mm				
Code 128						
5 mil	1,7 Zoll / 43 mm	5,8 Zoll / 147 mm				
Code 39						
6,6 mil	1,6 Zoll / 41 mm	4,9 Zoll / 124 mm				
PDF417						
10 mil	1,2 Zoll / 30 mm	4,9 Zoll / 124 mm				
DataMatrix						
100 % UPCA	2,0 Zoll / 51 mm	10,6 Zoll / 269 mm				
20,0 mil	2,1 Zoll / 53 mm*	13,6 Zoll / 345 mm				
Code 39						
10,0 mil	1,1 Zoll / 28 mm	5,2 Zoll / 132 mm				
QR-Code						
* Begrenzt durch die Breite des Barco	odes im Sichtfeld					

Hinweis: Barcode fotografischer Qualität bei 15 ° Neigungswinkel unter einer Umgebungsbeleuchtung von 30 fcd.

# Index

#### А

Apps	
RxLogger43	3
RxLogger-Dienstprogramm	)

#### В

Barcode-Eingabe	 	 								. 70
Aktiviert	 	 	• •	•			•	•		. 70

#### D

Data Capture Plus	68
Aktivierung bei Unterbrechung beibehalten       1         APIs       1         Ausgabe-Plug-ins       1         Automatischer Import       1         Barcode-Eingabe       1         bei Freignis automatisch auf Standard       1	87 09 63 08 70
umschalten	70
Berichterstellung1	09
Data Capture Plus	68
Deaktivieren	65
Decoder	71
Einführung	61
Eingabe-Plug-ins	63
Einstellungen1	05
Enterprise-Ordner1	80
Erstellen eines neuen Profils	65
Erweiterte Datenformatierungsregeln	96
Exportieren einer Konfigurationsdatei1	06
grundlegendes Scannen	61
Hinweise zur Programmierung	80
Importieren einer Konfigurationsdatei	06
	90
	92
Konfigurations- und Profildateiverwaltung	08
	90
	02 65
	05

Plug-ins
Profil0
Profil-Bildschirm64
Profile
Profilkonfiguration 66
Profil-Kontextmenü 64
Scannerauswahl
Scan-Parameter
Spracheingabe
Tastenanschlag-Ausgabe
Überblick über Intents
UDI-Parameter
UPC/EAN-Parameter
Verarbeitungs-Plug-ins
Zuordnen von Anwendungen
Dateiübertragung
Decoder
Decoder-Parameter
Code39
Code11
Code128
Codabar
Code93 76
Composite AB
Decodierungslängen
Discrete 2 of 55
GS1 DataBar Limited
HAN XIN
Interleaved 2 of 5
Matrix 2 of 5
MSI
Triontic39 79
UK Postal 79
UPCA 79
UPCE0 79
UPCE1 79
US Planet 80
Decodierbereiche 152 153

#### Е

Einstellungen

## Index

DataWedge	105
Erweiterte Datenformatierungsregeln	. 96

## F

Fehlerbehebung	146
Fotoübertragung	57
Funktionsbeschreibungen	
Touchscreen	. 20

## G

Gerätemontage	21
Google	
Kontoeinrichtung	28

## L

Lesegerät-Parameter	2
---------------------	---

## R

Reinigen
Display
Gehäuse145
Kamera und Scanfenster
Reinigung
Häufigkeit145
Hinweise
Materialien
Reinigungshinweise
RxLogger
Dienstprogramm
Konfiguration
Konfigurationsdatei
Protokolldateien extrahieren
Protokollierung aktivieren
Protokollierung deaktivieren

## S

Scan-Parameter	. 86
Schädliche Inhaltsstoffe	144
Schreibkonventionen	. 14
Softwareversion	. 13
Spracheingabe	. 87
Symbologien	151

## Т

Touchscreen	
Trennen vom Host-Computer	

## U

Übertragen von Dateien über USB	.56
UDI-Parameter	.87
UPC/EAN-Parameter	.80
USB	.56

## W

N/antura	
vartung	3
Besondere Reinigungshinweise	4
Display reinigen14	5
Erforderliche Reinigungsmaterialien14	5
Gehäuse reinigen14	5
Gerät pflegen	3
Kamera und Scanfenster reinigen14	5
Reinigungshäufigkeit14	5
Reinigungshinweise14	3
Reinigungshinweise für das Gerät14	4
Schädliche Inhaltsstoffe14	4
Zulässige Wirkstoffe in Reinigungsmitteln 14	4
Vi-Fi Direct	8

## Ζ

Zulässige Wirkstoffe in Reinigungsmitteln				.144
Zulässiges Reinigungsmittel				.144



www.zebra.com