TC25

Rugged Smartphone



Integrator Guide
for Android ™ 8.1.0 Oreo

ZEBRA

MN-003307-02 Rev. A

Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. Google, Android, Google Play and other marks are trademarks of Google LLC; Oreo is a trademark of Mondelez International, Inc. group. All other trademarks are the property of their respective owners. ©2019 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to www.zebra.com/copyright.

WARRANTY: For complete warranty information, go to www.zebra.com/warranty.

END USER LICENSE AGREEMENT: For complete EULA information, go to www.zebra.com/eula.

Terms of Use

- Proprietary Statement

  This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.
- Product Improvements

  Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.
- Liability Disclaimer

  Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.
- Limitation of Liability

  In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	1/2019	Initial release.
-02 Rev. A	8/2019	Remove Imager as Camera section from DataWedge chapter.

Table of Contents

Copyright 2
Terms of Use 2
Revision History 2

About This Guide 11
Introduction 11
Configurations 11
Software Versions 11
Chapter Descriptions 12
Notational Conventions 12
Related Documents 12
Service Information 13
Provide Documentation Feedback 13

Getting Started 14
Introduction 14
Setup 14
- Installing a microSD Card 14
- Installing the SIM Card 16
- Charging the Battery 18
- Charging Indicators 20

Replacing the microSD Card 20
Replacing the SIM Card 22
Resetting the TC25 24
- Performing a Soft Reset 24
- Performing a Hard Reset 24

Accessories 25
Introduction 25

Accessories 25
1-Slot Base Charge Only Cradle 28
Setup 28
Cable Routing 28
Connecting Cradles Together 29
Charging the Device 30
Battery Charging 30
Charging Temperature 31
1-Slot Ethernet Charge Cradle 32
Ethernet Bracket Installation 32
USB/Ethernet Communication 36
Ethernet LED Indicators 37
Ethernet Settings 37
Configuring Ethernet Proxy Settings 37
Configuring Ethernet Static IP Address 38
Charging the Device 39
Battery Charging 40
Charging Temperature 40
5-Slot Charge Only Cradle 41
Charging the TC25 41
Battery Charging 42
Charging Temperature 42
Extended Power Pack 43
Installation 43
Charging 43
Power Pack Charging 45
Charging Temperature 46
Check Power Level 46
Resetting the Extended Power Pack 47
Vehicle Cradle 48
Assembling the Mount 48
Installing on the Windshield 48
Installing the Dash Mount 49
Installing the Device 49
Connecting Power 50
Removing the Device 51
5-Slot Cradle Rack Installation 52
Rack Mount Installation 55
Wall Installation 58
Bottom Tray Assembly 58
Bracket Wall Mounting 58

USB Communication 60
Introduction 60
Transferring Files 60
Transferring Photos 61
Disconnect from the Host Computer 61

DataWedge 62
Introduction 62
Basic Scanning 62
Profiles 62
Profile0 63
Plug-ins 63
Input Plug-ins 63
Process Plug-ins 64
Output Plug-ins 64
Profiles Screen 64
Profile Context Menu 65
Options Menu 65
Disabling DataWedge 66
Creating a New Profile 66
Profile Configuration 66
Associating Applications 67
Data Capture Plus 69
Barcode Input 71
Enabled 71
Scanner Selection 71
Auto Switch to Default on Event 71
Decoders 72
Decoder Params 74
Codabar 74
UPC EAN Params 79
Reader Params 81
Scan Params 84
UDI Params 85
Multibarcode params 85
Voice Input 85
Keystroke Output 86
Intent Output 88
Intent Overview 89
IP Output 90
Usage 91
Using IP Output with IPWedge 91
Using IP Output without IPWedge 92

Generating Advanced Data Formatting Rules 94
Configuring ADF Plug-in 94
Creating a Rule 94
Defining a Rule 95
Defining an Action 95
Deleting a Rule 95
Order Rules List 96
Deleting an Action 97
ADF Example 97
DataWedge Settings 100
Importing a Configuration File 101
Exporting a Configuration File 101
Importing a Profile File 101
Exporting a Profile 102
Restoring DataWedge 102
Configuration and Profile File Management 102
Enterprise Folder 102
Auto Import 102
Programming Notes 103
Overriding Trigger Key in an Application 103
Capture Data and Taking a Photo in the Same Application 103
Disabling DataWedge 103
Soft Scan Trigger 103
Function Prototype 104
Scanner Input Plugin 104
Function Prototype 104
Parameters 104
Return Values 104
Example 105
Comments 105
Enumerate Scanners 105
Function Prototype 105
Parameters 106
Return Values 106
Example 107
Comments 107
Set Default Profile 108
Default Profile Recap 108
Usage Scenario 108
Function Prototype 108
Parameters 108
Return Values 108
Example 109
Comments 109
Reset Default Profile 109

Function Prototype 110
Parameters 110
Return Values 110
Example 110
Comments 110
Switch To Profile 111
Profiles Recap 111
Usage Scenario 111
Function Prototype 111
Parameters 111
Return Values 112
Example 112
Comments 112
Notes 113

Settings 114
Introduction 114
WLAN Configuration 114
Configuring a Secure Wi-Fi Network 114
Manually Adding a Wi-Fi Network 115
Configuring for a Proxy Server 116
Configuring the Device to Use a Static IP Address 117
Wi-Fi Preferences 118
Additional Wi-Fi Settings 119
Setting Screen Lock 119
Setting Screen Lock Using PIN 120
Setting Screen Unlock Using Password 121
Setting Screen Unlock Using Pattern 121
Passwords 122
Accounts 122
Language Usage 122
Changing the Language Setting 123
Adding Words to the Dictionary 123
Keyboard Settings 123
Button Remapping 123
Remapping a Button 124
PTT Express Configuration 125
RxLogger 125
RxLogger Configuration 126
RxLogger Settings 127
ANR Module 127
Kernel Module 127
Logcat Module 128

LTS Module 129
Qxdm Module 129
Ramoops Module 130
Resource Module 130
Snapshot Module 130
TCPDump Module 131
Tombstone Module 131
Configuration File 131
Enabling Logging 131
Disabling Logging 132
Extracting Log Files 132
RxLogger Utility 132
App View 132
Viewing Logs 133
RxLogger Utility 134
Archive Data 135
Overlay View 135
Initiating the Main Chat Head 135
Removing the Main Chat Head 135
Viewing Logs 136
Removing a Sub Chat Head Icon 137
Backup 137
About Phone 137

Application Deployment 139
Introduction 139
Security 139
Secure Certificates 139
Installing a Secure Certificate 139
Configuring Credential Storage Settings 140
Development Tools 140
Android Application Development 140
Development Workstation 140
Target Device 141
EMDK for Android 141
StageNow 141
ADB USB Setup 141
Enabling USB Debugging 142
Application Installation 142
Installing Applications Using the USB Connection 142
Installing Applications Using the Android Debug Bridge 144
Installing Applications Using a microSD Card 145
Uninstalling an Application 146

Performing a System Update 147
Downloading the System Update Package 147
Using microSD Card 147
Using ADB 148
Verify System Update Installation 149
Performing an Enterprise Reset 149
Downloading the Enterprise Reset Package 149
Using microSD Card 149
Using ADB 150
Performing a Factory Reset 151
Downloading the Factory Reset Package 151
Using microSD Card 151
Using ADB 151
Storage 152
Random Access Memory 152
Internal Storage 153
External Storage 154
Formatting a microSD Card or USB Drive as Portable Storage 155
Formatting a microSD Card as Internal Memory 157
Enterprise Folder 158
App Management 158
Viewing App Details 159
Managing Downloads 160

Maintenance and Troubleshooting 161
Introduction 161
Maintaining the TC25 161
Display Best Practices 161
Image Retention 161
Cleaning Instructions 162
Approved Cleanser Active Ingredients 162
Harmful Ingredients 162
Cleaning Instructions 162
Special Cleaning Notes 162
Cleaning Materials Required 162
Cleaning Frequency 163
Cleaning the TC25 163
Housing 163
Display 163
Camera and Exit Window 163
Connector Cleaning 163

Cleaning Cradle Connectors 163
Troubleshooting 165
TC25 165
1-Slot Base Charge Only Cradle 167
1-Slot Ethernet Cradle 168
5-Slot Charge Only Cradle Troubleshooting 169

Technical Specifications 170
TC25 170
Decode Distances 173
2-Pin I/O Connector Pin-Outs 174
1-Slot Base Charge Only Cradle Technical Specifications 175
1-Slot Ethernet Cradle Technical Specifications 175
5-Slot Charge Only Cradle Technical Specifications 176
Trigger Handle Technical Specifications 177
Extended Power Pack Technical Specifications 177

Index 178

About This Guide

Introduction

This guide provides information about using the TC25 rugged smartphone and accessories.

NOTE: Screens and windows pictured in this guide are samples and can differ from actual screens.

Configurations

This guide covers the following configurations:

Table 1 *Configurations*

Configuration	Radios	Operating System Android 7.1	Memory RAM/Flash	Data Capture	8 MP Camera	Access Door
TC25AJ-10B101xx	WAN/LAN/PAN	GMS	2 GB/16 GB	SE2100	Yes	Blank
TC25AJ-10C102xx	WAN/LAN/PAN	GMS	2 GB/16 GB	SE4710	No	2-Pin
TC25BJ-10B101xx	WAN/LAN/PAN	GMS	2 GB/16 GB	SE2100	Yes	Blank
TC25BJ-10C102xx	WAN/LAN/PAN	GMS	2 GB/16 GB	SE4710	No	2-Pin

Software Versions

To determine the current software versions:

1. Swipe down from the Status bar to open the Quick Settings bar.
2. Touch ⚙ > **System**.
3. Touch **About phone**.

4. Scroll to view the following information:
   - **Model**
   - **Android version**
   - **Android security patch version**
   - **Kernel version**
   - **Build number**.

To determine the device serial number, touch **About phone > Status**.

- **Serial number**

Chapter Descriptions

Topics covered in this guide are as follows:

- Getting Started provides information on getting the TC25 up and running for the first time.
- Accessories describes the available accessories and how to use them with the TC25.
- DataWedge describes how to use and configure the DataWedge application.
- USB Communication describes how to transfer files with a host computer.
- Settings provides the settings for configuring the TC25.
- Application Deployment provides information for developing and managing applications.
- Maintenance and Troubleshooting includes instructions on cleaning and storing the TC25, and provides troubleshooting solutions for potential problems during TC25 operation.
- Technical Specifications provides the technical specifications for the TC25.

Notational Conventions

The following conventions are used in this document:

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Button names on a screen.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (for example, lists that describe step-by-step procedures) appear as numbered lists.

Related Documents

- TC25 Quick Start Guide, p/n MN-003052-xx.
- TC25 Regulatory Guide, p/n MN-003053-xx.
- TC25 Rugged Smartphone User Guide for Android Version 8.1.0, p/n MN-003308-xx.

For the latest version of this guide and all guides, go to: www.zebra.com/support.

Service Information

If you have a problem with your equipment, please use the Self-Help support resources available at www.zebra.com. If the support provided via the Self-Help resources is not sufficient, you may contact Zebra Global Customer Support for your region. Contact information is available at: zebra.com/support.

When contacting support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number.

Zebra responds to calls by email, telephone or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Customer Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your Zebra business product from a Zebra business partner, contact that business partner for support.

Provide Documentation Feedback

If you have comments, questions, or suggestions about this guide, send an email to EVM-Techdocs@zebra.com.

Getting Started

Introduction

This chapter provides information for getting the device up and running for the first time.

Setup

Perform this procedure to start using the TC25 for the first time.

1. Install a micro secure digital (SD) card (optional).
2. Installing a nano SIM card
3. Charge the TC25.
4. Power on the TC25.

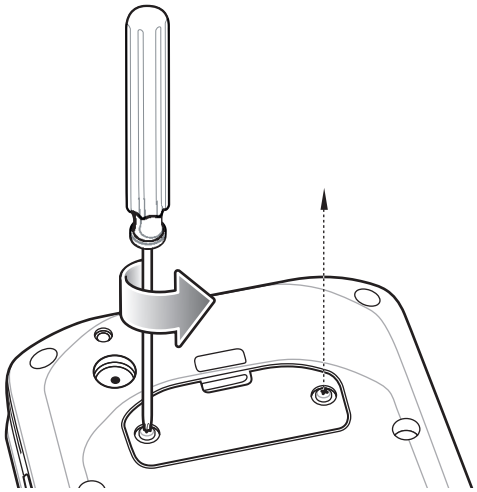
Installing a microSD Card

The microSD card slot provides secondary non-volatile storage. The slot is located under the access door. Refer to the documentation provided with the card for more information, and follow the manufacturer's recommendations for use.

CAUTION: Use proper electrostatic discharge (ESD) precautions to avoid damaging the microSD card. Proper ESD precautions include, but are not limited to, working on an ESD mat and ensuring that the operator is properly grounded.

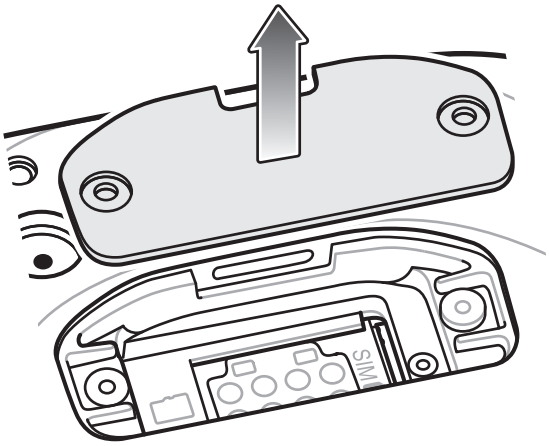
1. Using a 0# Phillips screwdriver, remove two screws securing the access door.

Figure 1 Remove Access Door



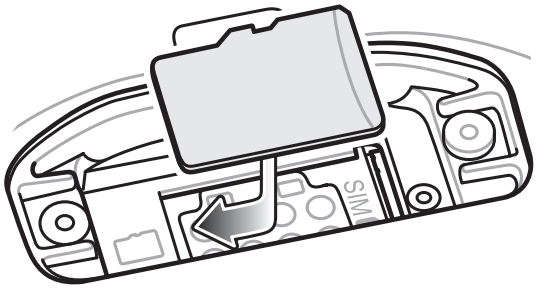
2. Remove access door.

Figure 2 Remove Access Door



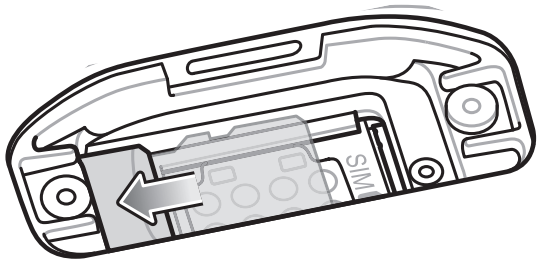
3. Align the microSD card with the SD card slot.

Figure 3 Align microSD Card



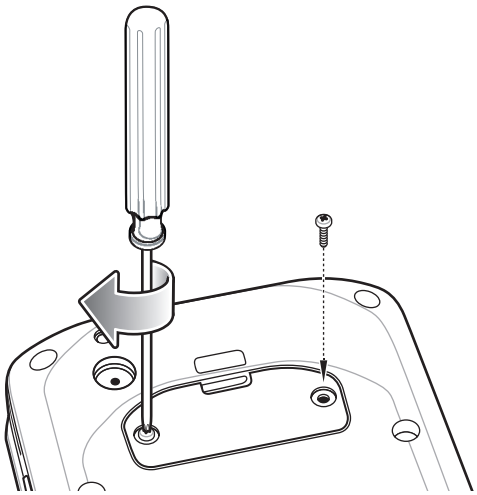
4. Push the microSD card into the SD card slot.

Figure 4 Push microSD Card into the SD Card Slot



5. Replace the access Door.
6. Secure the access door using the two screws.

Figure 5 Secure Access Door



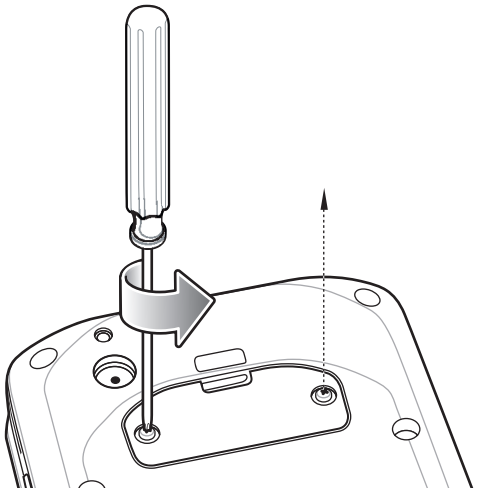
Installing the SIM Card

NOTE: Only use a nano SIM card.
Only use nano SIM cards that meet the ESTI TS102.221 standard for nano SIM cards, form factor 4FF (0.67 mm thick). Do not use SIM cards that are cut from thicker mini or micro SIM cards.

CAUTION: Use proper electrostatic discharge (ESD) precautions to avoid damaging the SIM card. Proper ESD precautions include, but not limited to, working on an ESD mat and ensuring that the user is properly grounded.

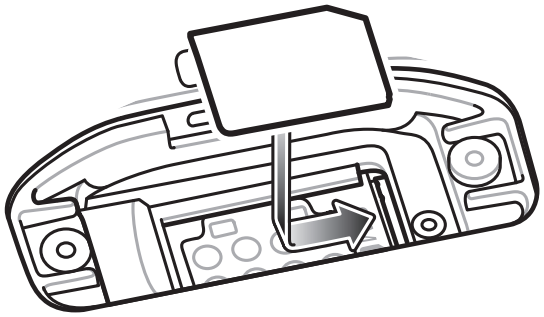
1. Using a 0# Phillips screwdriver, remove two screws securing the access door.

Figure 6 Remove Access Door



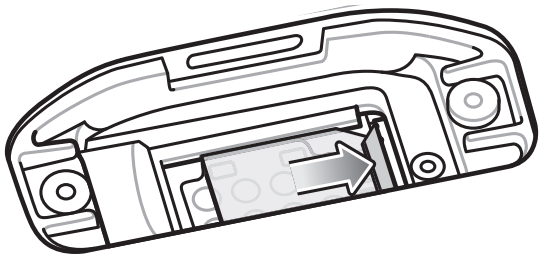
2. Align the SIM card with the SIM card slot with the contacts facing down and the cut edge toward the top of the device.

Figure 7 Align SIM Card with Slot



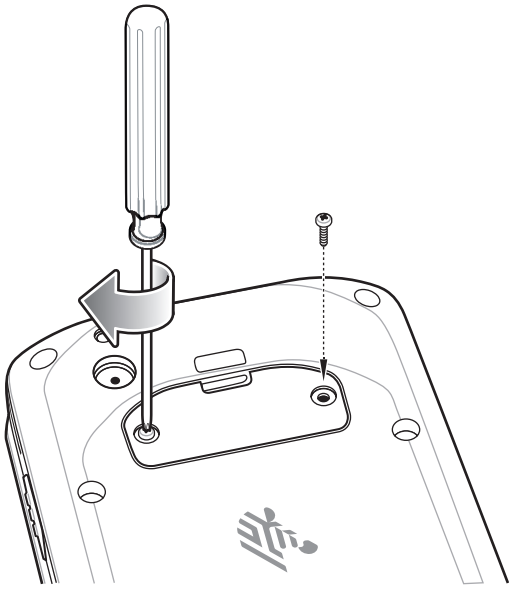
3. Push the SIM card in until it locks into the slot.

Figure 8 Push SIM Card into Slot



4. Re-install the access door.

Figure 9 Replace Access Door



Charging the Battery

Before using the TC25 for the first time, charge the internal battery until the green Charging/Notification light emitting diode (LED) remains lit. To charge the TC25 use a USB-C cable or a cradle with the appropriate power supply. For information about the accessories available for the TC25 see Accessories on page 25 for more information.

The internal battery charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.

NOTE: In many cases the 90% charge provides plenty of charge for daily use. A full 100% charge lasts for approximately 10 hours of use.
Use only Zebra charging accessories and batteries. Charge batteries at room temperature with the TC25 in sleep mode.

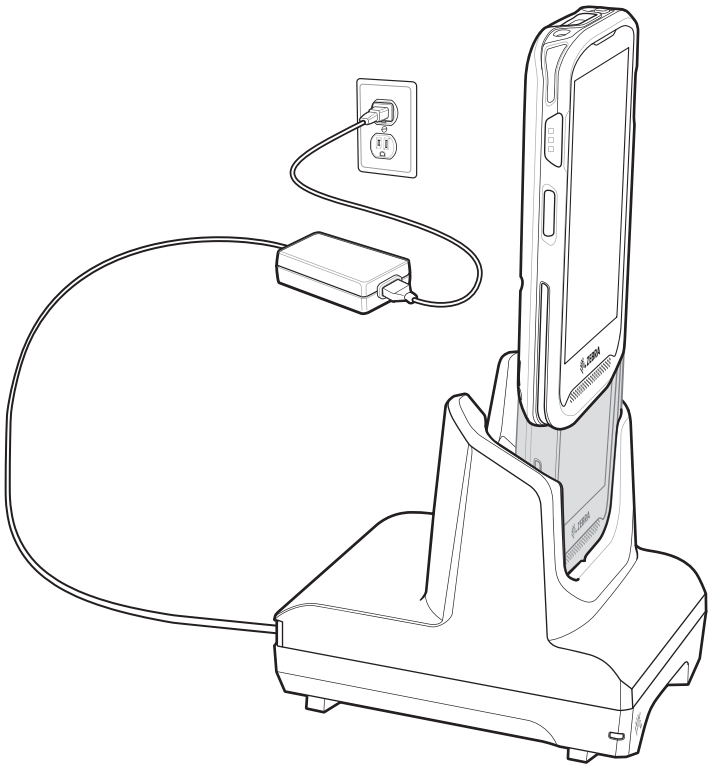
Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The TC25 or accessory always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the TC25 or accessory may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The TC25 or accessory indicates when charging is disabled due to abnormal temperatures via its LED and a notification appears on the display.

To charge the main battery:

1. Connect the charging accessory to the appropriate power source.

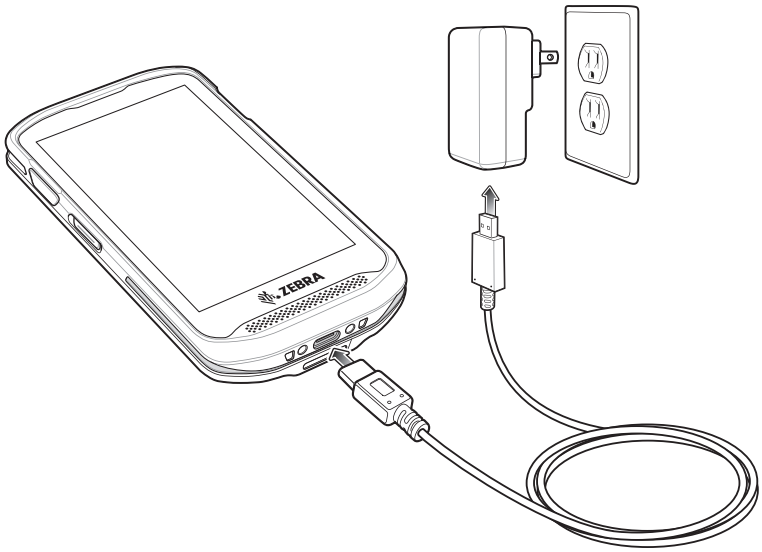
2. Insert the TC25 into a cradle or attach to a cable. The TC25 turns on and begins charging. The Charging/Notification LED blinks amber while charging, then turns solid green when fully charged.

Figure 10 Charging with Cradle



IMPORTANT: Use only the Zebra USB-C Cable for charging.

Figure 11 Charging with USB Cable



Charging Indicators

Table 2 *Charging/Notification LED Charging Indicators*

State	LED	Indication
Off		TC25 is not charging. TC25 is not inserted correctly in the cradle or connected to a power source. Charger/cradle is not powered.
Slow Blinking Amber (1 blink every 4 seconds)		TC25 is charging.
Slow Blinking Red (1 blink every 4 seconds)		TC25 is charging but the battery is at end of useful life. See system administrator for battery replacement services.
Solid Green		Charging complete.
Solid Red		Charging complete but the battery is at end of useful life. See system administrator for battery replacement services.
Fast Blinking Amber (2 blinks/second)		Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).
Fast Blinking Red (2 blinks/second)		Charging error but the battery is at end of useful life., e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours). See system administrator for battery replacement services.

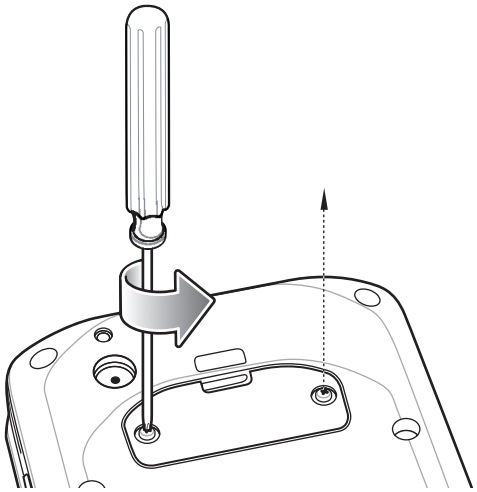
Replacing the microSD Card

To replace the microSD card:

1. Press the Power button until the menu appears.
2. Touch **Power off**.
3. Touch **OK**.
4. If hand strap is attached, remove the hand strap.
5. Using a #0 Phillips screwdriver, remove two screws securing the access door.

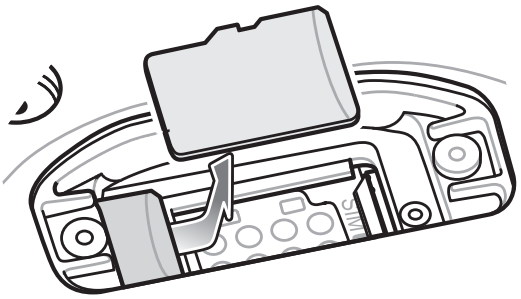
6. Remove access door.

Figure 12 Remove Access Door



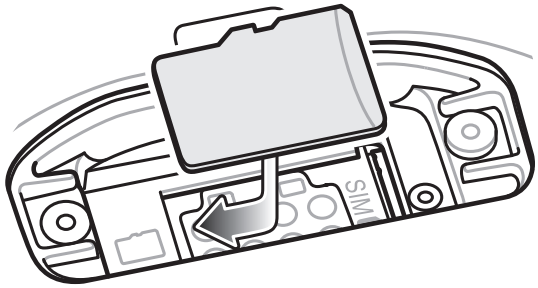
7. Slide the microSD card out of the SD card slot.

Figure 13 Align microSD Card



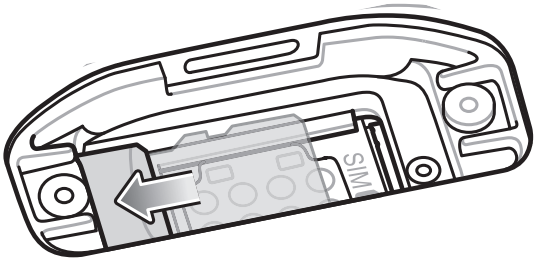
8. Lift the microSD card.
9. Align the replacement microSD card with the SD card slot.

Figure 14 Align microSD Card



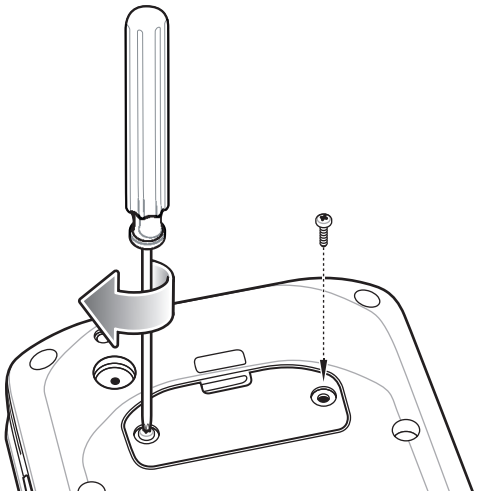
10. Push the microSD card into the SD card slot.

Figure 15 Push microSD Card into the SD Card Slot



11. Replace the access Door.
12. Secure the access door using the two screws.

Figure 16 Secure Access Door



13. Replace the hand strap, if required.
14. Press and hold the Power button to turn on the device.

Replacing the SIM Card

NOTE: Only use a nano SIM card.

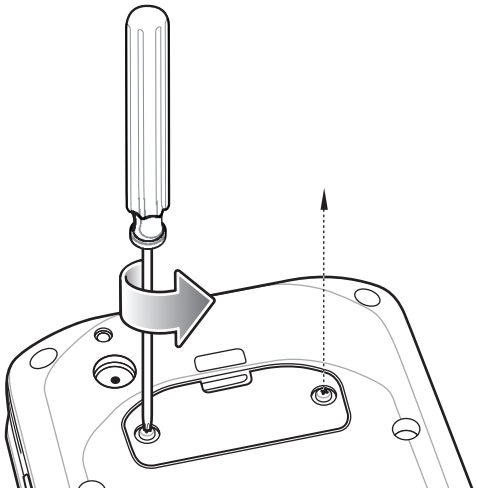
CAUTION: Access door must be replaced and securely seated to ensure proper device sealing. TC25 must be powered off when replacing the SIM card.

To replace the SIM card:

1. Press the Power button until the menu appears.
2. Touch **Power off**.
3. Touch **OK**.
4. If hand strap is attached, slide the hand strap clip up toward the top of the TC25 and then lift.

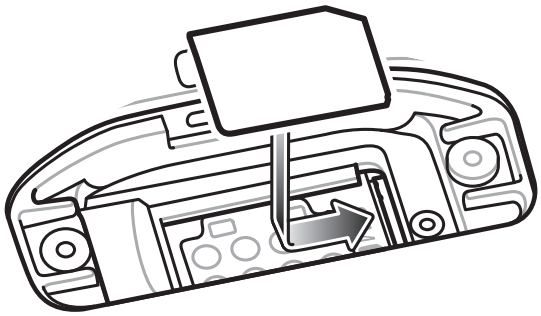
5. Using a 0# Phillips screwdriver, remove two screws securing the access door.

Figure 17 Remove Access Door



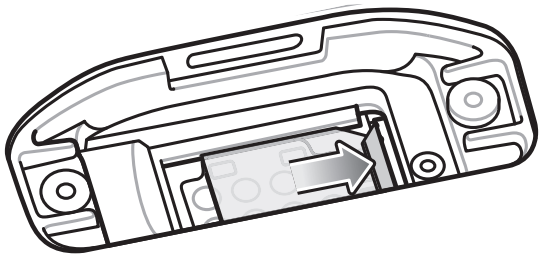
6. Push the SIM card in to eject the card.
7. Remove the SIM card from the slot.
8. Align the replacement SIM card with the SIM card slot with the contacts facing down and the cut edge toward the top of the device.

Figure 18 Align SIM Card with Slot



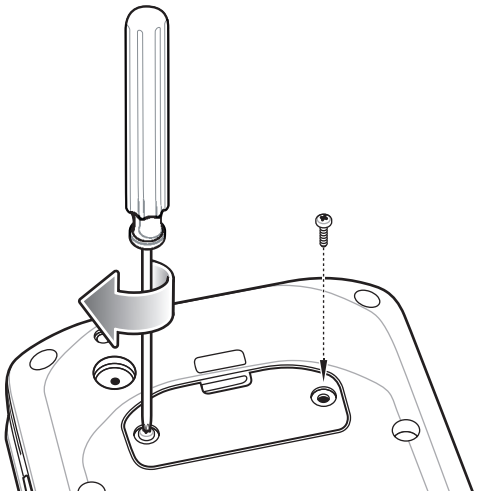
9. Push the SIM card in until it locks into the slot.

Figure 19 Push SIM Card into Slot



10. Re-install the access door.

Figure 20 Replace Access Door



11. Replace the hand strap, if required.
12. Press and hold the Power button to turn on the TC25.

Resetting the TC25

There are four reset functions:

- Soft reset
- Hard reset
- Enterprise reset. See Performing an Enterprise Reset on page 149.
- Factory reset See Performing a Factory Reset on page 151.

Performing a Soft Reset

Perform a soft reset if applications stop responding.

1. Press and hold the Power button until the menu appears.
2. Touch **Reset**.
3. The device reboots.

Performing a Hard Reset

CAUTION: Performing a hard reset with a SD card installed in the TC25 may cause damage or data corruption to the SD card.

Perform a hard reset if the TC25 stops responding.

1. Simultaneously press the Power and Volume Up buttons for at least five seconds.
2. When the screen turns off, release the buttons.
3. The TC25 reboots.

Accessories

Introduction

This chapter provides information for using the accessories for the device.

Accessories

This table lists the accessories available for the TC25.

Table 3 *TC25 Accessories*

Accessory	Part Number	Description
Cradles		
1-Slot Base Charge Only Cradle	CRD-TC2X-BS1CO-01	Provides charging for device and Extended power pack. Requires power supply (PWR-WUA5V12W0xx), and USB-C cable.
1-Slot Ethernet Cradle	CRD-TC2X-SE1ET-01	Provides device charging and communication, and charging for Extended Power Pack. Requires power supply (PWR-BGA12V50W0WW), DC line cord (CBL-DC-388A1-01), and country-specific AC line cord.
5-Slot Charge Only Cradle	CRD-TC2X-SE5CO-01	Charges up to five devices. Requires power supply (PWR-BGA12V108W0WW), DC line cord (CBL-DC-382A1-01), and country-specific AC line cord.
Cradle Mount	BRKT-SCRD-SMRK-01	Mounts the 5-Slot Charge Only Cradle to a wall or rack.
Batteries and Chargers		
Extended Power Pack	BTRY-TC2X-PRPK1-01	Charges the TC25 internal battery to provide additional power and extend the shift time.

Table 3 *TC25 Accessories (Continued)*

Accessory	Part Number	Description
Vehicle Solutions		
Cigarette Light Adapter Auto Charge Cable	CHG-AUTO-USB1-01	Provides power to the device from a cigarette lighter socket.
Vehicle Cradle	CRD-TC2X-VCH1-01	Provides mounting solution for the device in a vehicle.
Miscellaneous		
Trigger Handle	TRG-TC2X-SNP1-01	Adds gun-style handle with a scanner trigger for comfortable and productive scanning.
Screen Protector	KT-TC20-SCRNP1-01	Add additional screen protection.
SmartDEX Solution	DX30	Provides wireless DEX communications to the TC25.
Ethernet Bracket	BRKT-TC51-ENET1-01	Use to connect the USB/Ethernet Adapter to the 1-Slot Ethernet Cradle.
USB/Ethernet Module	MOD-MT2-EU1-01	Use with 1-Slot Ethernet Cradle to provide Ethernet connectivity.
Cradle Mating Adapter	KIT-TC2X-BS1FT-05	Use the optional mating adapter to connect two or more cradles together. Each cradle still requires a power supply (5-pack).
Carrying Solutions		
TC2X Soft Holster	SG-TC2X-HLSTR1-01	Use to hold the device on hip. Accepts TC25 device with Trigger Handle.
TC2X Hand Strap	SG-TC2X-HSTRP1-01	Replacement hand strap (3–pack).
Wrist/Arm Mount	SG-TC2X-ARMNT-01	Use to mount the TC25 to the forearm.
Small Wrist Mount Strap	SG-WT4023221-03R	Replacement small wrist mount strap
Large Wrist Mount Strap	SG-WT4023221-04R	Replacement long wrist mount strap.
Power Supplies		
Power Supply	PWR-BGA12V50W0WW	Provides power to the 1-Slot Ethernet Cradle. Requires DC Line Cord, p/n CBL-DC-388A1-01 and country specific three wire grounded AC line cord sold separately.
Power Supply	PWR-BGA12V108W0WW	Provides power to the 5-Slot Charge Only cradle. Requires DC Line Cord, p/n CBL-DC-382A1-01 and country specific three wire grounded AC line cord sold separately.

Table 3 *TC25 Accessories (Continued)*

Accessory	Part Number	Description
Power Supply	PWR-WUA5V12W0US	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in the United States.
Power Supply	PWR-WUA5V12W0GB	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in the European Union.
Power Supply	PWR-WUA5V12W0EU	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in the United Kingdom.
Power Supply	PWR-WUA5V12W0AU	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in Australia.
Power Supply	PWR-WUA5V12W0CN	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in China.
Power Supply	PWR-WUA5V12W0BR	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in Brazil.
Power Supply	PWR-WUA5V12W0KR	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in Korea.
Power Supply	PWR-WUA5V12W0IN	Provides 5 VDC, 2.5 A power to the USB-C cable. Includes plug adapter for use in India.
DC Line Cord	CBL-DC-382A1-01	Provides power from the power supply (PWR-BGA12V108W0WW) to the 5-Slot Charge Only Cradle.
DC Line Cord	CBL-DC-388A1-01	Provides power from the power supply (PWR-BGA12V50W0WW) to the 1-Slot Ethernet Cradle.
2-Way DC Line Cord	CBL-DC-377A1-01	Use to charge two 5-Slot Charge only Cradles with one power supply.
2-Way DC Line Cord	CBL-DC-379A1-01	Use to charge one 1-Slot Ethernet Cradle and one 5-Slot Charge Only Cradle with one power supply.
4-Way DC Line Cord	CBL-DC-380A1-01	Use to charge four 1-Slot Ethernet Cradles with one power supply.
US AC Line Cord	23844-00-00R	7.5 feet long, grounded, three wire for power supply.
USB-C Cable	CBL-TC2X-USBC-01	The USB cable used to connect PC to single slot USB cradle.

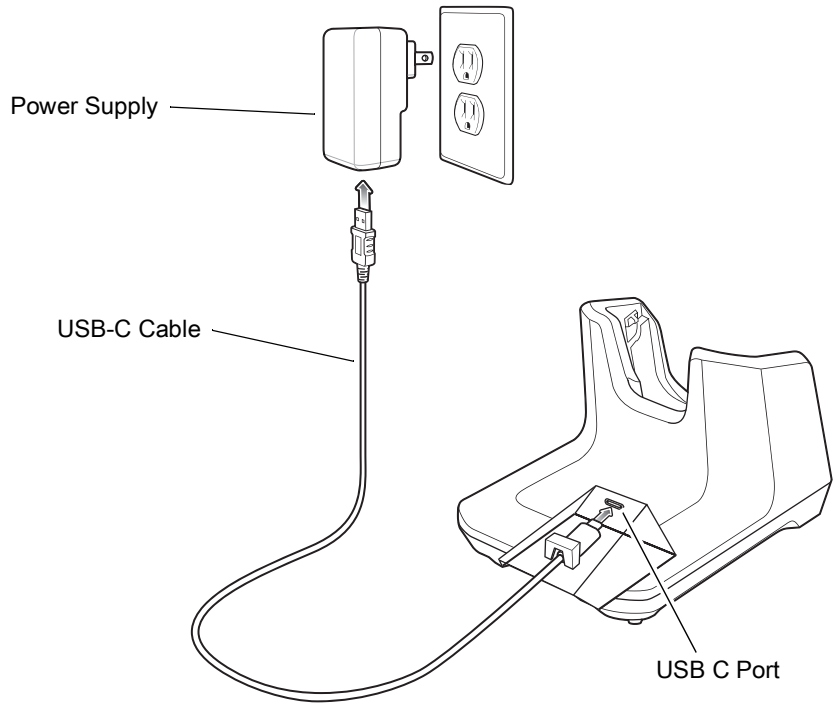
1-Slot Base Charge Only Cradle

The 1-Slot Base Charge Only Cradle provide 5 VDC for charging:

- TC25
- Extended Power Pack
- TC25 and Extended Power Pack
- TC25 with Trigger Handle.

Setup

Figure 21 1-Slot Base Charge Only Cradle Setup

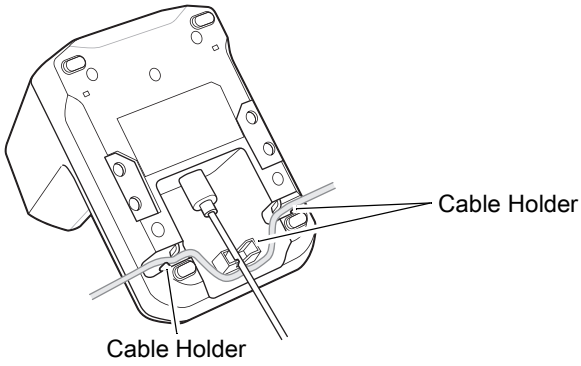


Cable Routing

To cradle provides three ways to route the USB cable:

- Rear
- Left side
- Right side.

Figure 22 USB Cable Routing



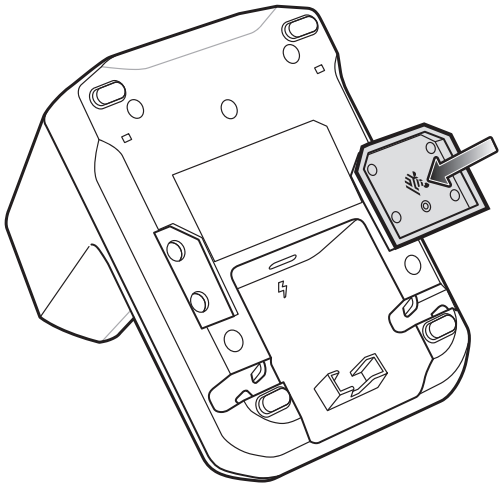
Insert the USB-C cable connector into the USB port. Routing the cable to the rear, left, or right and use cable holders to secure cable.

Connecting Cradles Together

The 1-Slot Base Charge Only Cradle can be connected together to form a row of cradles using the optional mounting brackets.

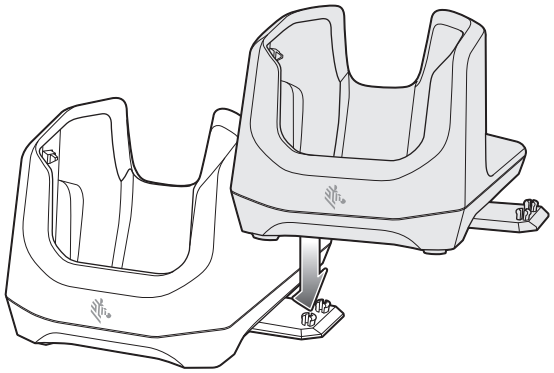
1. Align a mounting bracket on either side of cradle.

Figure 23 Align Mounting Bracket



2. Press the mounting bracket into the cradle.
3. Place cradle on flat surface.
4. Align second cradle.

Figure 24 Align Cradles



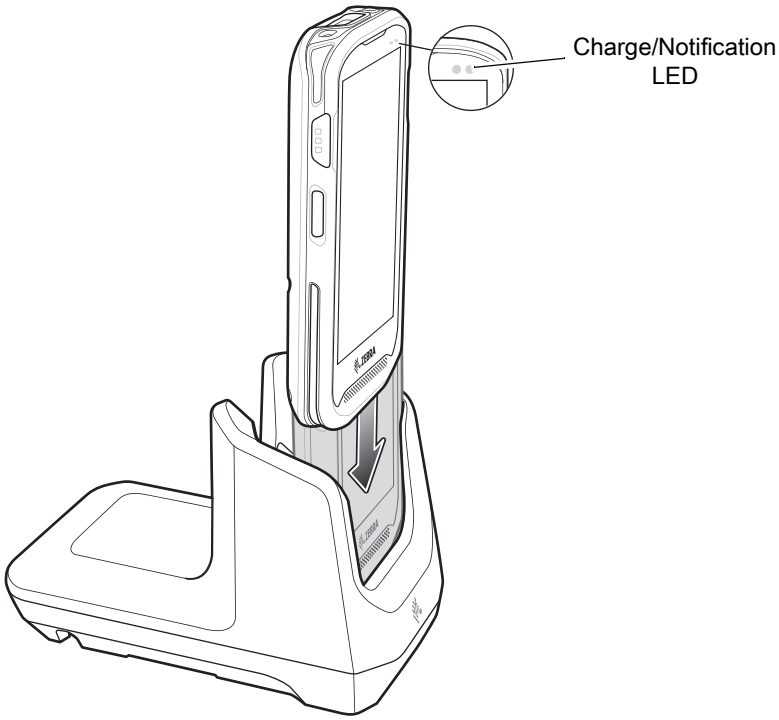
5. Press the cradle down ensuring that the bracket studs snap into the receiving holes in the cradle.

Charging the Device

To charge a device:

1. Insert the device into the slot to begin charging.

Figure 25 Battery Charging



2. Ensure the device is seated properly.

Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See Table 2 on page 20 for device charging status. The battery charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.

NOTE: In many cases the 90% charge provides plenty of charge for daily use. A full 100% charge lasts for approximately 10 hours of use.

Use only Zebra charging accessories and batteries. Charge batteries at room temperature with the TC25 in sleep mode.

Charging Temperature

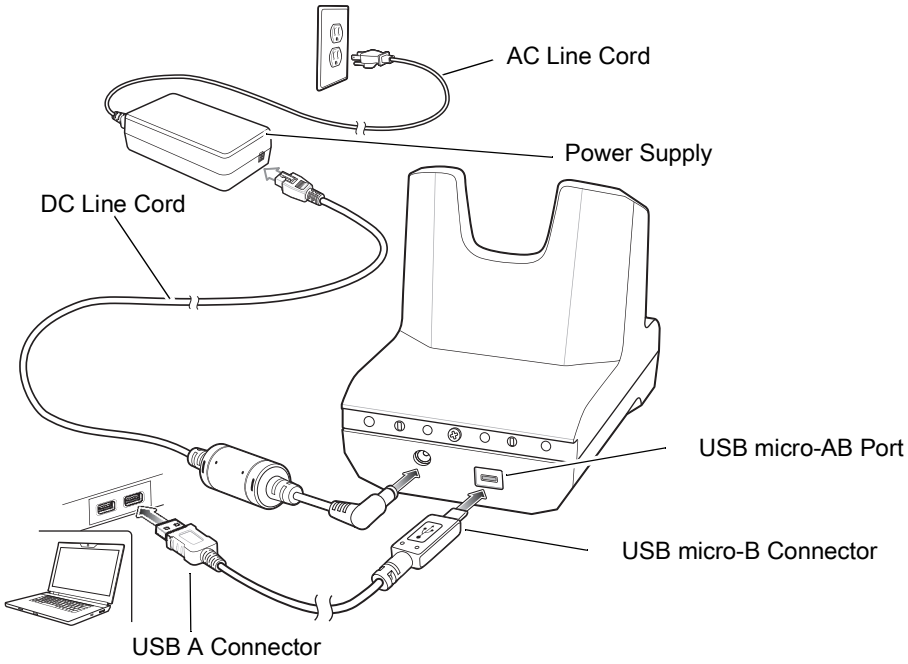
Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

1-Slot Ethernet Charge Cradle

The 1-Slot USB Charge Cradle:

- Provides 5 VDC power for operating the device.
- Charges the device's battery.
- Provides USB communication with host computer.
- Provides USB and Ethernet communication using the Ethernet Bracket and Module adapter.

Figure 26 1–Slot USB Charge Cradle Setup

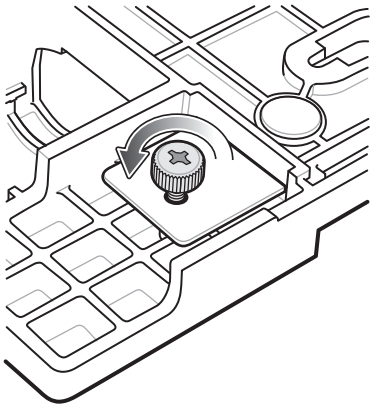


Ethernet Bracket Installation

To install the Ethernet Bracket:

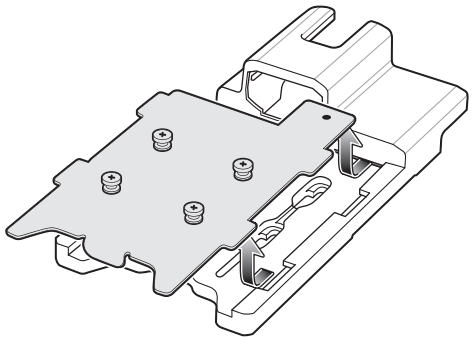
1. Turn over the Ethernet Bracket.
2. Remove the thumbscrew securing the plate to the bracket.

Figure 27 Remove Thumbscrew



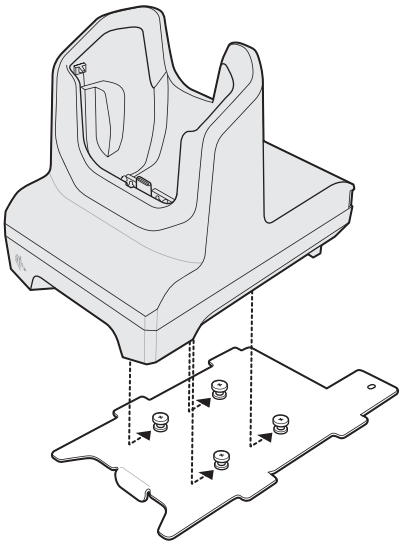
3. Turn over the bracket and remove plate.

Figure 28 Remove Plate



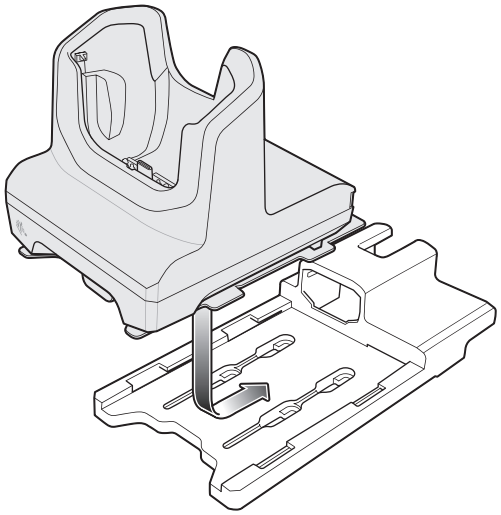
4. Align the 1-Slot Ethernet Cradle with the plate.

Figure 29 Align Cradle with Plate



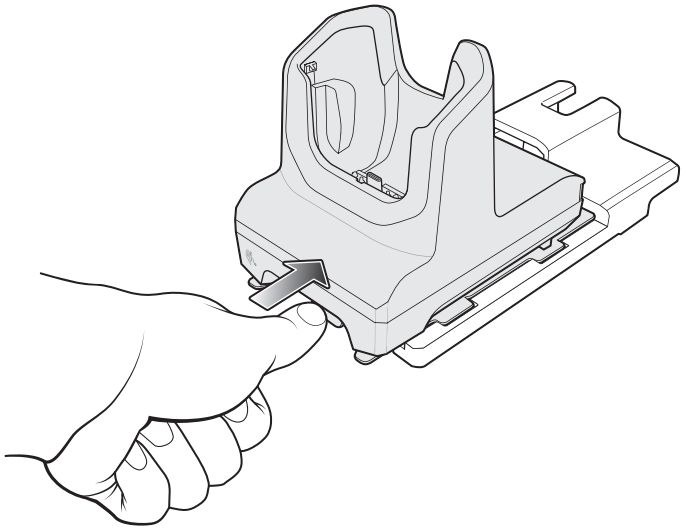
5. Slide the plate and cradle into the bracket.

Figure 30 Align Cradle/Plate with Bracket



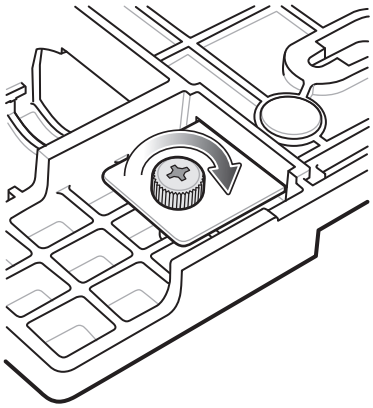
6. Push the plate into the bracket.

Figure 31 Push Plate into Bracket



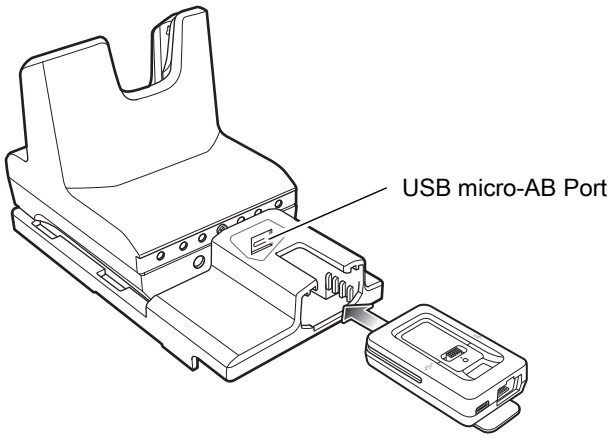
7. Turn over the bracket and cradle.
8. Secure the thumbscrew.

Figure 32 Secure Screw



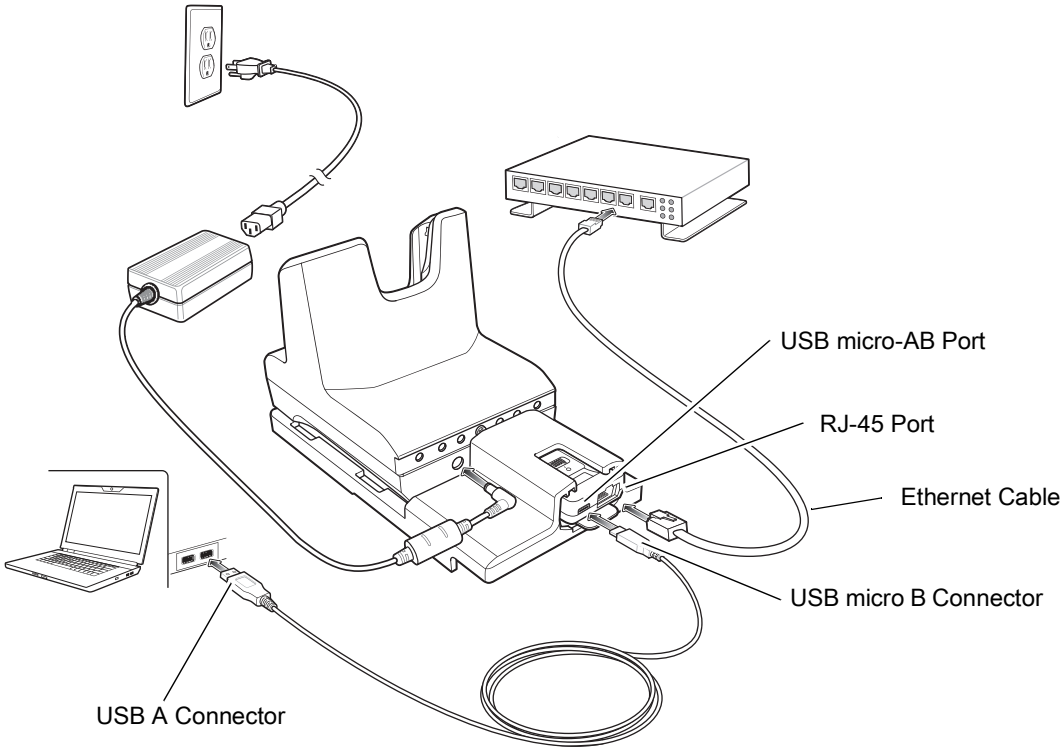
9. Insert the Ethernet Module into the bracket.

Figure 33 Insert Module



10. Push module in until it is seated properly. The USB micro-B connector on the Ethernet module plugs into the USB micro-AB port on the cradle.

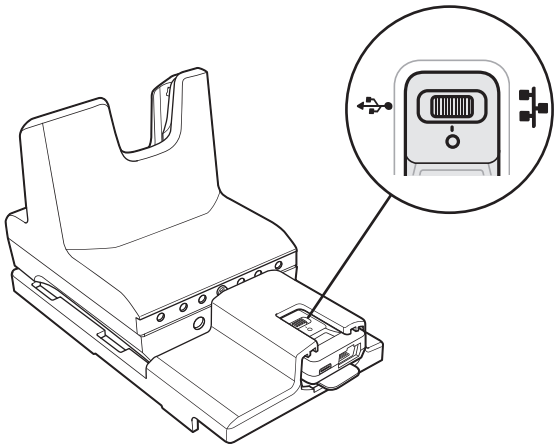
Figure 34 Ethernet Bracket Setup



USB/Ethernet Communication

The 1-Slot Ethernet Cradle provides both Ethernet communication with a network and USB communication with a host computer. Prior to using the cradle for Ethernet or USB communication. Ensure that the switch on the USB/Ethernet module is set properly.

Figure 35 Ethernet Cradle Module Switch



For Ethernet communication, slide the switch to the position.

For USB communication, slide the switch to the position.

Place the switch in the center position to disable communications.

Ethernet LED Indicators

There are two LEDs on the USB/Ethernet Module RJ-45 port. The green LED lights to indicate that the transfer rate is 100 Mbps. When the LED is not lit the transfer rate is 10 Mbps. The yellow LED blinks to indicate activity, or stays lit to indicate that a link is established. When it is not lit it indicates that there is no link.

Figure 36 LED Indicators

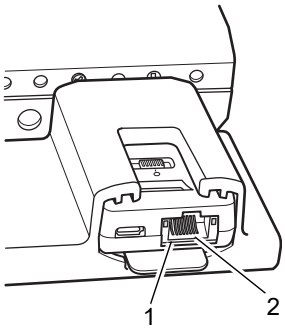


Table 4 *USB/Ethernet Module LED Data Rate Indicators*

Data Rate	(1) Amber LED	(2) Green LED
100 Mbps	On/Blink	On
10 Mbps	On/Blink	Off

Ethernet Settings

The following settings can be configured when using Ethernet communication:

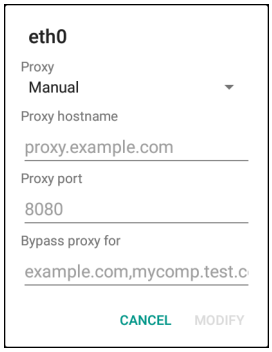
- Proxy Settings
- Static IP.

Configuring Ethernet Proxy Settings

The TC25 includes Ethernet cradle drivers. After inserting the TC25, configure the Ethernet connection:

1. Swipe down from the status bar and then touch .
2. Touch **Ethernet**.
3. Place the TC25 into the Ethernet cradle slot.
4. Slide the switch to the **ON** position.
5. Touch and hold **Eth0** until the menu appears.
6. Touch **Modify Proxy**.
7. Touch the **Proxy** drop-down list and select **Manual**.

Figure 37 Ethernet Proxy Settings



8. In the **Proxy hostname** field, enter the proxy server address.
9. In the **Proxy port** field, enter the proxy server port number.

NOTE: When entering proxy addresses in the Bypass proxy for field, do not use spaces or carriage returns between addresses.

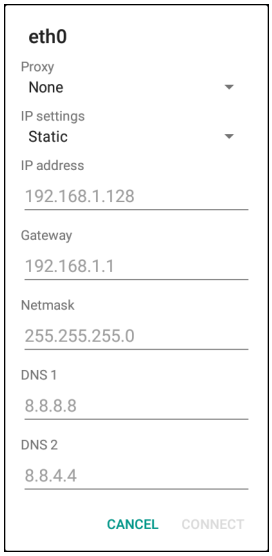
10. In the **Bypass proxy for** text box, enter addresses for web sites that do not require to go through the proxy server. Use the separator "|" between addresses.
11. Touch **MODIFY**.
12. Touch ○.

Configuring Ethernet Static IP Address

The TC25 includes Ethernet cradle drivers. After inserting the TC25, configure the Ethernet connection:

1. Swipe down from the status bar and then touch ⚙.
2. Touch ⟨···⟩ **Ethernet**.
3. Place the TC25 into the Ethernet cradle slot.
4. Slide the switch to the **ON** position.
5. Touch **Eth0**.
6. Touch **Disconnect**.
7. Touch **Eth0**.
8. Touch and hold the IP settings drop-down list and select **Static**.

Figure 38 Static IP Settings



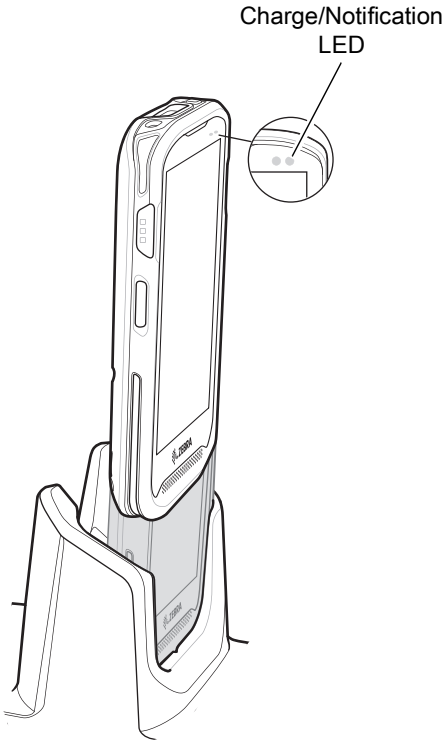
9. In the **IP** address field, enter the proxy server address.
10. If required, in the **Gateway** field, enter a gateway address for the device.
11. If required, in the **Netmask** field, enter the network mask address.
12. If required, in the **DNS address** fields, enter a Domain Name System (DNS) addresses.
13. Touch **CONNECT**.
14. Touch ○.

Charging the Device

To charge a device:

1. Insert the device into the slot to begin charging.

Figure 39 Battery Charging



2. Ensure the device is seated properly.

Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See Table 2 on page 20 for device charging status. The internal battery charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.

NOTE: In many cases the 90% charge provides plenty of charge for daily use. A full 100% charge lasts for approximately 10 hours of use.

Use only Zebra charging accessories and batteries. Charge batteries at room temperature with the TC25 in sleep mode.

Charging Temperature

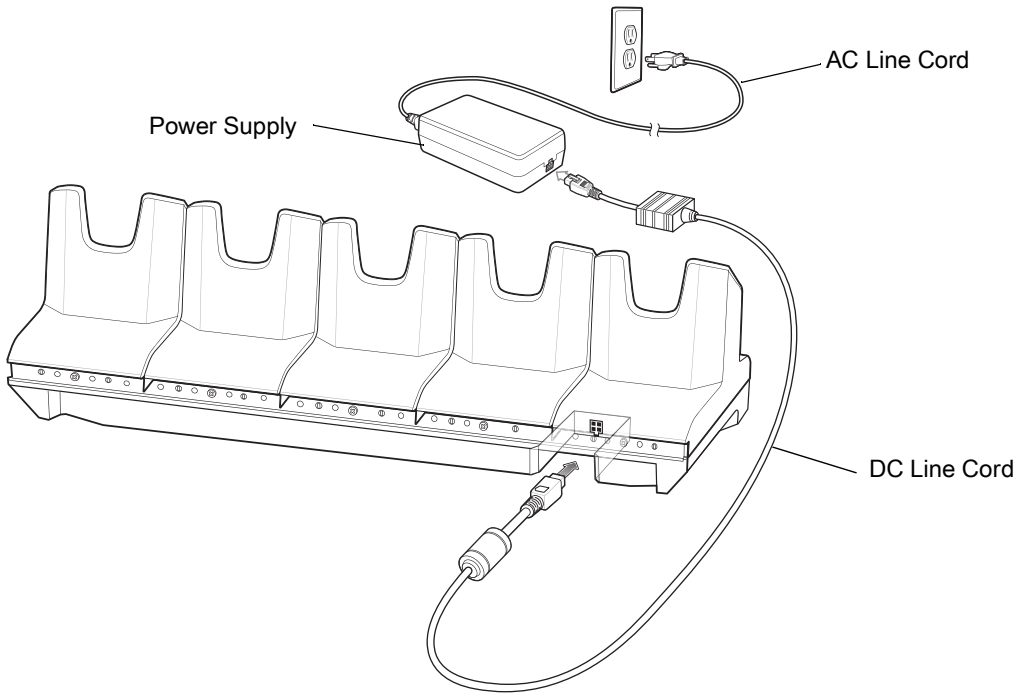
Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

5-Slot Charge Only Cradle

The 5-Slot Charge Only Cradle:

- Provides 5 VDC power for operating the TC25.
- Simultaneously charges up to five TC25s.

Figure 40 5-Slot Charge Only Cradle Setup

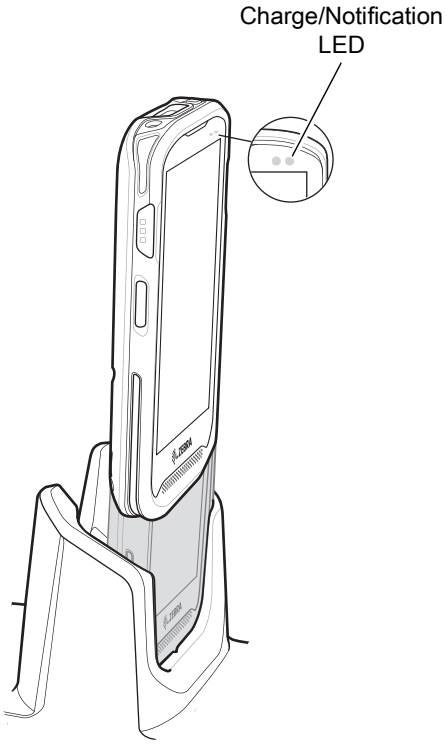


Charging the TC25

To charge a device:

1. Insert the TC25 into a slot to begin charging.

Figure 41 TC25 Battery Charging



2. Ensure the TC25 is seated properly.

Battery Charging

The device's Charging/Notification LED indicates the status of the battery charging in the device. See Table 2 on page 20 for device charging status. The internal battery charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.

NOTE: In many cases the 90% charge provides plenty of charge for daily use. A full 100% charge lasts for approximately 10 hours of use.

Use only Zebra charging accessories and batteries. Charge batteries at room temperature with the TC25 in sleep mode.

Charging Temperature

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The device and cradle indicates when charging is disabled due to abnormal temperatures via its LED.

Extended Power Pack

The Extended Power Pack provides additional power for charging the TC25 battery.

For best performance it is recommended that the Power Pack should always be installed on the device and that both the Power Pack and device are fully charged at the start of each work shift.

Figure 42 Extended Power Pack Front View

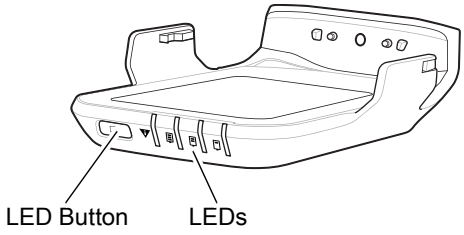
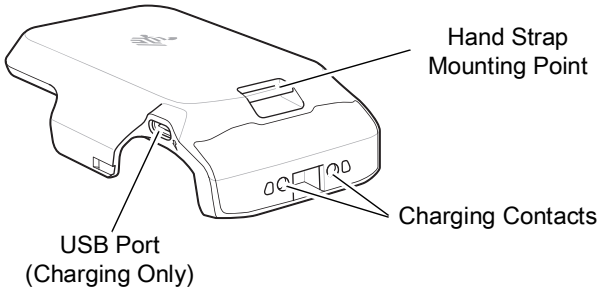


Figure 43 Extended Power Pack Back View

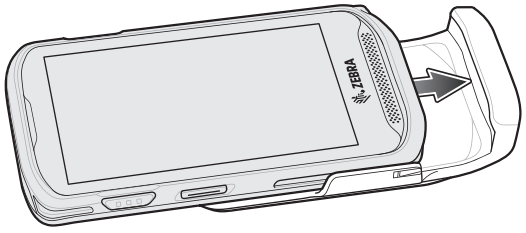


Installation

To install the Power Pack:

1. Align the Power Pack with the TC25.

Figure 44 Align Power Pack with TC25



2. Slide the power pack up onto the TC25 until it snaps into place.

Charging

Charge the Extended Power Pack:

- In a cradle
- In a cradle attached to the TC25
- using a USB cable.

Figure 45 Charging Power Pack in Cradle

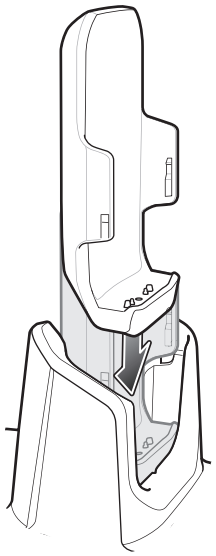
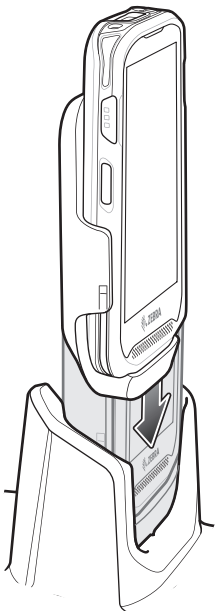
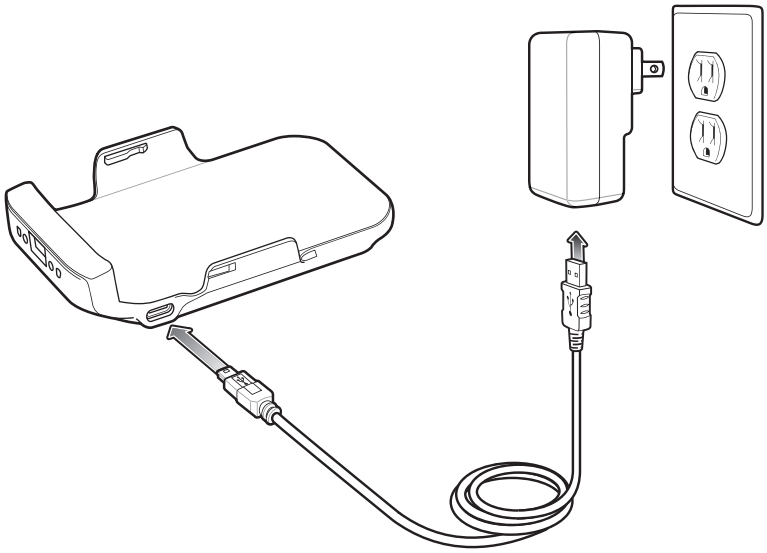


Figure 46 Charging TC25 and Power Pack in Cradle



IMPORTANT: Use only the Zebra USB-C Cable for charging.

Figure 47 Charging with USB Cable



Power Pack Charging

The Power Pack Charging LEDs indicate the status of charging. See Table 5 on page 45 for charging status. The power pack charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.

Figure 48 Power Pack LEDs

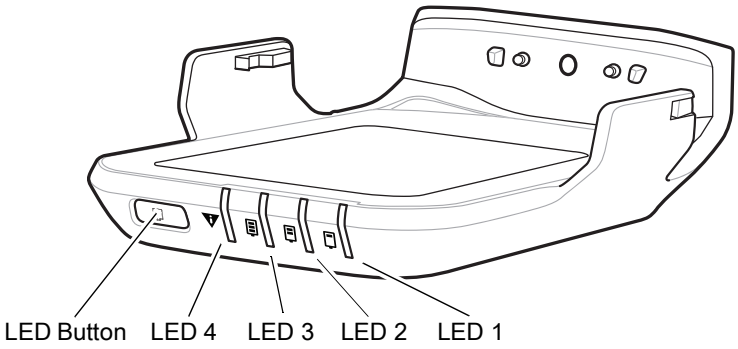


Table 5 *LED Charging Indicators*

LED State				
LED 1	**LED 2**	**LED 3**	**LED 4**	**Indication**
				Not charging.
Flashing				Charge level is between 0% and 33%.

Table 5 *LED Charging Indicators (Continued)*

LED State				
LED 1	**LED 2**	**LED 3**	**LED 4**	**Indication**
 Solid	 Flashing			Charge level is between 33% and 66%.
 Solid	 Solid	 Flashing		Change level is between 66% and 95%.
 Solid	 Solid	 Solid		Fully charged (95-100%).
			 Flashing	Charging error, e.g.: Temperature is too low or too high. Charging has gone on too long without completion (typically 10 hours).

Charging Temperature

Charge batteries in temperatures from 0°C to 40°C (32°F to 104°F). The device or cradle always performs battery charging in a safe and intelligent manner. At higher temperatures (e.g. approximately +37°C (+98°F)) the device or cradle may for small periods of time alternately enable and disable battery charging to keep the battery at acceptable temperatures. The power pack indicates when charging is disabled due to abnormal temperatures via its LED.

Check Power Level

To check the power level of the power pack, press the LED button. The LEDs light indicating the charge level. After five seconds the LEDs turn off.

Figure 49 Check Power Level

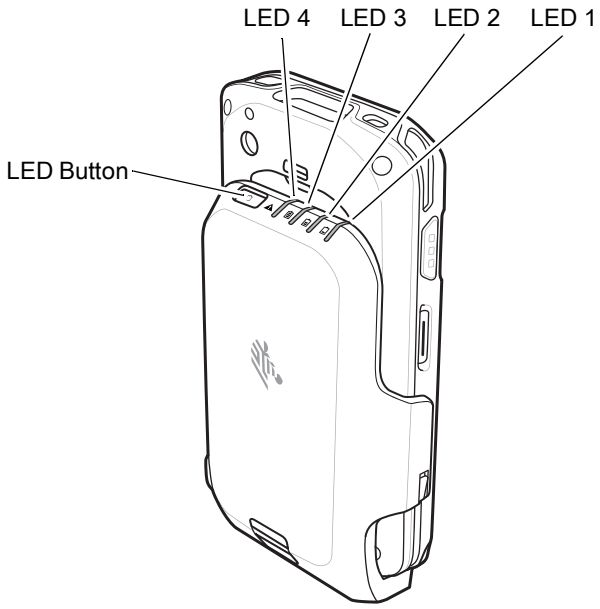


Table 6 *LED Charge State Indicators*

LED State				
LED 1	**LED 2**	**LED 3**	**LED 4**	**Indication**
				No charge.
Flashing				Charge level is between 0% and 33%.
Solid	Flashing			Charge level is between 33% and 66%.
Solid	Solid	Flashing		Change level is between 66% and 95%.
Solid	Solid	Solid		Fully charged (95-100%).

Resetting the Extended Power Pack

If the user thinks that the pack is not operating properly, reset the pack:

Press and hold the button for 10 seconds. All four LEDs flash three times.

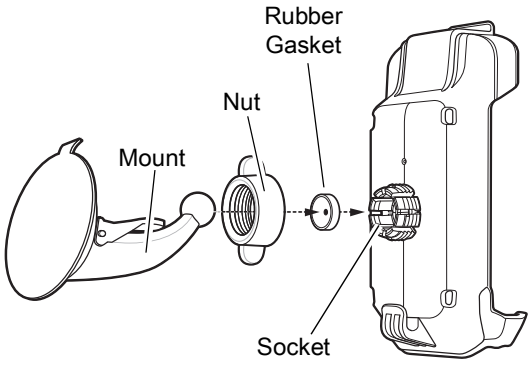
Vehicle Cradle

Install the vehicle mount on a surface of your vehicle that is flat and free of dirt and oil. Clean the mounting surface with a glass cleaner and a clean cotton cloth. Install the vehicle mount on the windshield or other flat car surface using the supplied disc.

Assembling the Mount

1. Remove all parts from plastic bags.
2. Insert the rubber gasket into the socket with the flat side against the holder.
3. Insert the arm ball through the nut and into the socket on the holder.
4. Secure nut but do not tighten at this time.
5. Remove protective plastic from suction cup.

Figure 50 Cradle Assembly

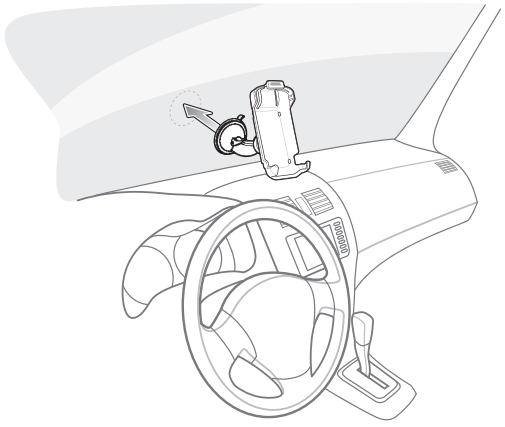


Installing on the Windshield

To install the cradle on the windshield:

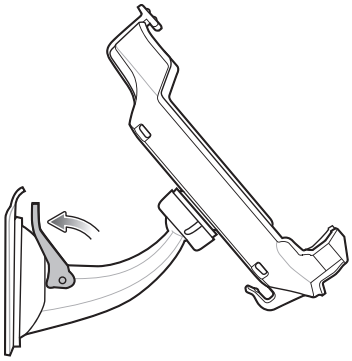
1. Fix the suction cup mount to the selected area with the suction lever facing up.

Figure 51 Windshield Mount



2. Push the lever towards the base to create a vacuum between the suction cup and the windshield.

Figure 52 Lock Level



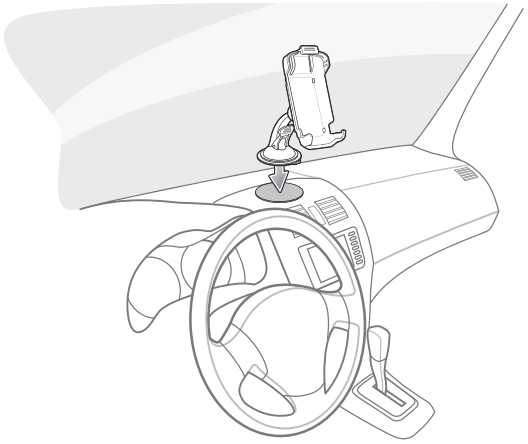
3. Make sure that the suction bond is strong enough before installing the device.

Installing the Dash Mount

To install the cradle on the dashboard:

1. Install the disc using the instructions provided with the disc.
2. Remove protective plastic from top of disc.
3. Fix the suction cup mount to the disc with the suction lever facing you.

Figure 53 Attach Suction Cup to Disk



4. Push the lever towards the base to create a vacuum between the suction cup and the disc.
5. Make sure that the suction bond is strong enough before installing the device.

Installing the Device

To install the device into the cradle:

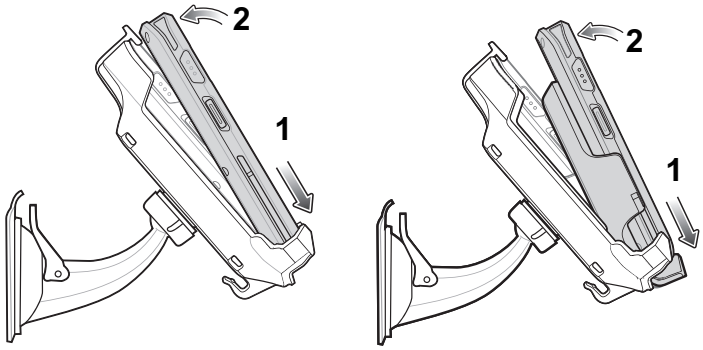
NOTE: The cradle accommodates the device with or without the Extended Power Pack.

Do not leave the device in direct sunlight for a long period of time as it may cause the device to exceed proper operating temperature.

1. Place the device bottom first into the cradle.

2. Rotate the top of the device into the cradle and push in until the retention tab closes over the device.

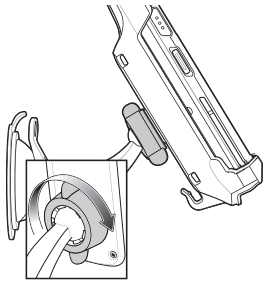
Figure 54 Install Device into Cradle



Without Power Pack With Power Pack

1. Position the device for best viewing.
2. Tighten the nut to lock the cradle in place.

Figure 55 Tighten Nut

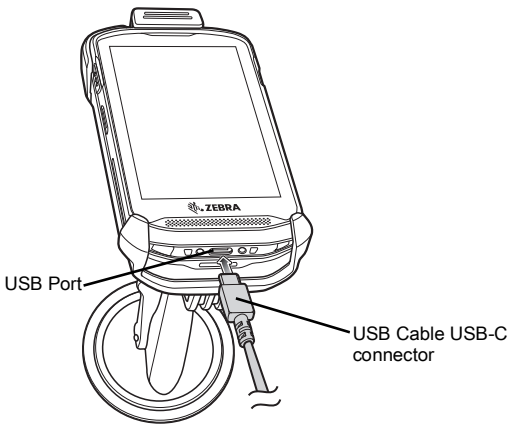


Connecting Power

To connect power to the device:

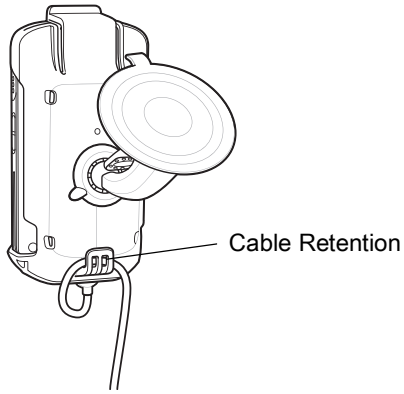
1. Plug the USB-C connector on the USB cable into the bottom of the device.

Figure 56 Connect USB-C Cable



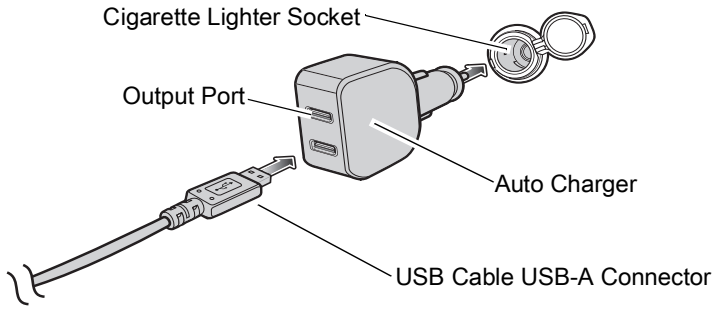
2. Use the cable retention feature to secure the cable.

Figure 57 Secure Cable on Retention Feature



3. Plug the Auto Charger into the cigarette lighter socket.

Figure 58 Connect Power



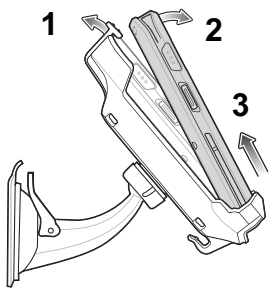
4. Plug the USB A connector into one of the output ports.
   The device LED flashes green indicating the device is charging.
5. Route the USB cable so that it does not interfere with driving.

Removing the Device

To remove the device from the cradle:

1. Press the retention tab.
2. Pull the top of the device out of the cradle.
3. Lift the device up and out of the cradle.

Figure 59 Remove Device from Cradle



5-Slot Cradle Rack Installation

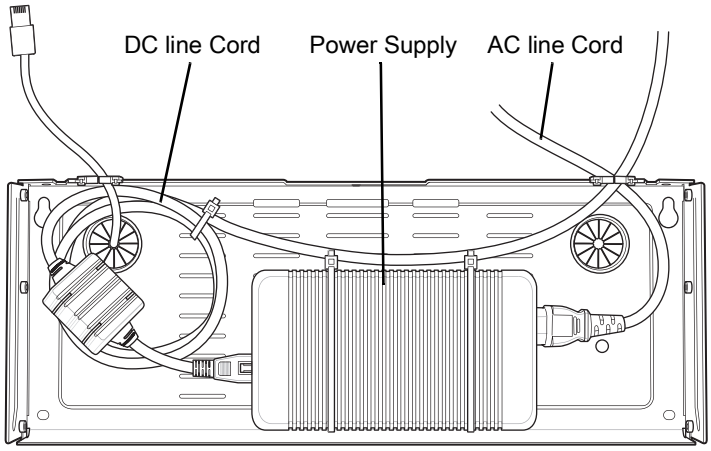
Use the Rack/Wall Mount Bracket to mount a 5-slot cradle on a rack. When installing on a rack, first assemble the bracket and cradles/chargers and then install the assembly on the rack.

1. Place the power supply in bottom tray.
2. Connect AC line cord to power supply.
3. Connect DC line cord to power supply.
4. Secure power supply and cables to bottom tray with tie wraps.

NOTE: Ensure tie wrap buckle is on side of power supply. Tie wrap buckle on top of power supply interferes with top tray.

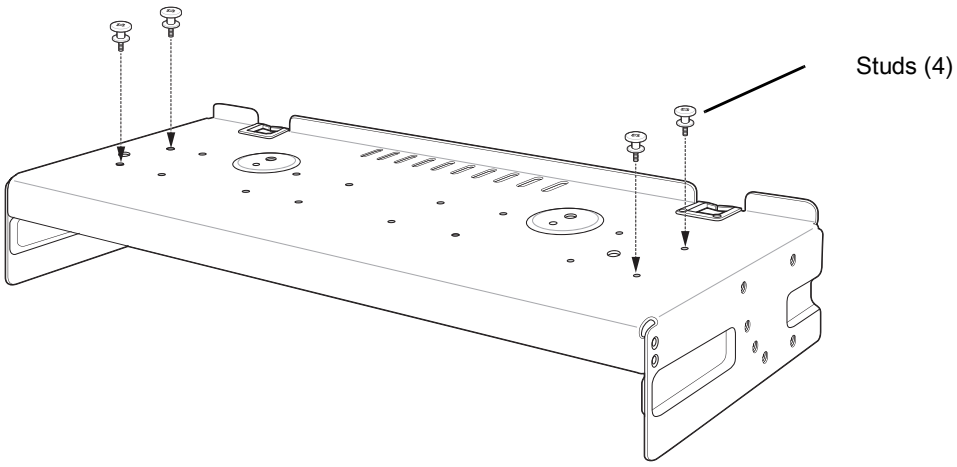
5.Route cables through cable slots.

Figure 60 Power Supply in Bottom Tray



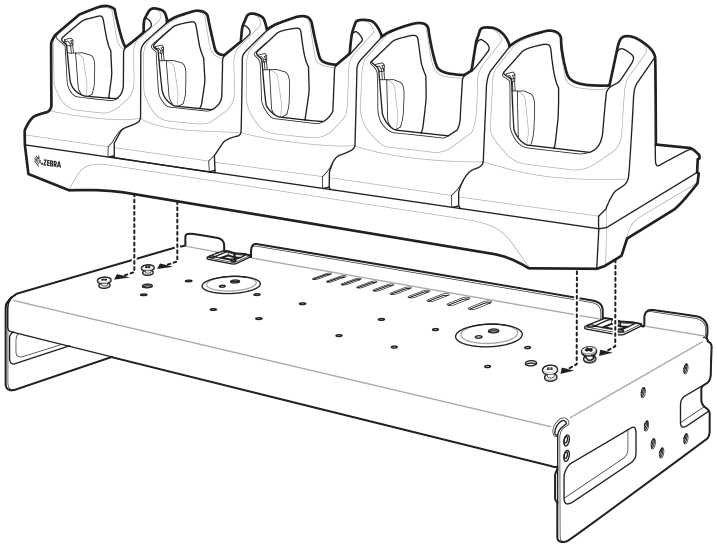
6. Secure four M2.5 studs to top tray as shown.

Figure 61 Install Studs



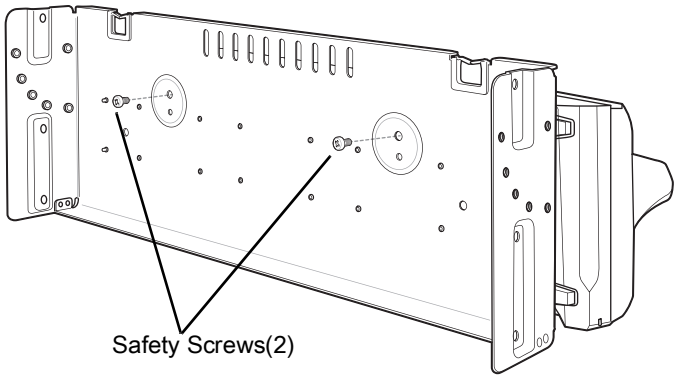
7. Align and install 5-Slot cradle onto studs of top tray.

Figure 62 Align Cradle on Studs



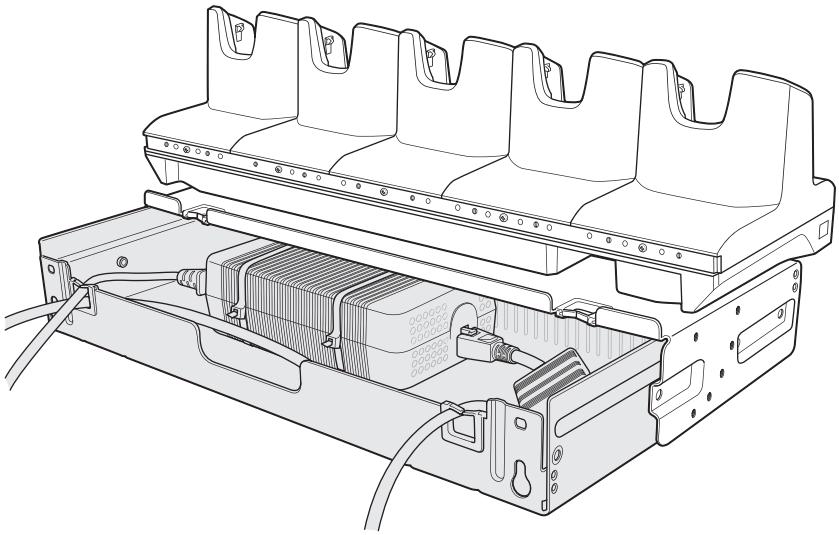
8. Secure cradle to top tray with two M2.5 safety screws.

Figure 63 Secure Cradle



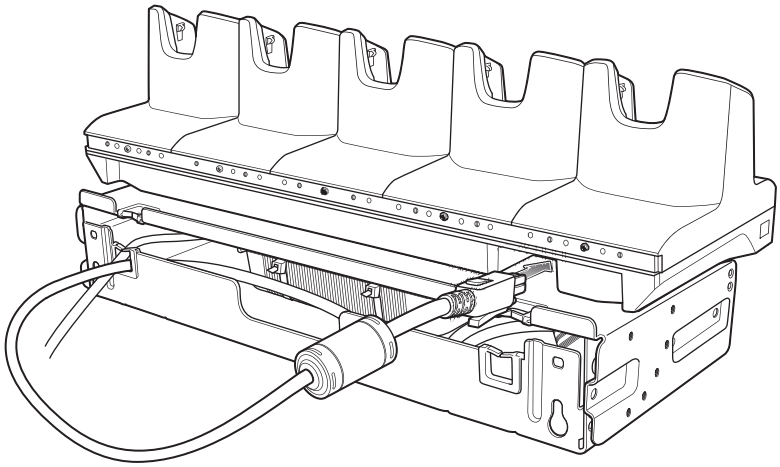
9. Slide top tray onto bottom tray.

Figure 64 Slide Top Tray onto Bottom Tray



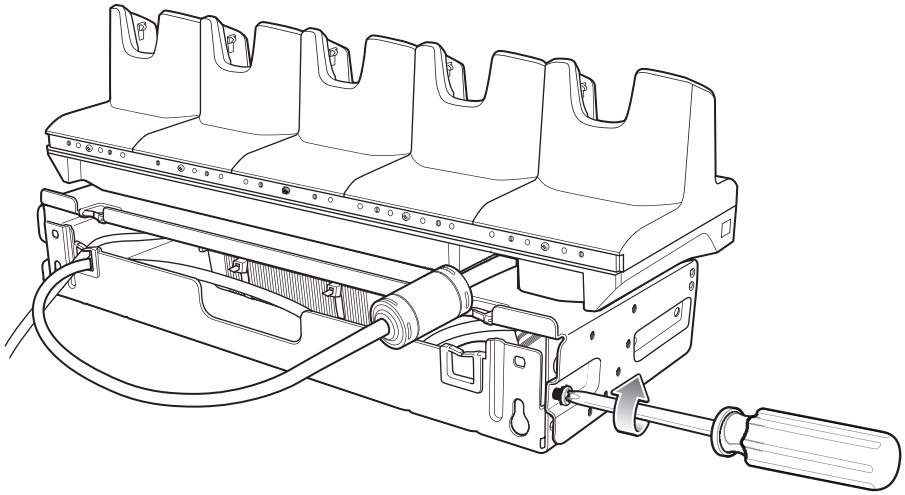
10. Connect cables to cradle.

Figure 65 Connect Cables



11. Secure top tray to bottom tray with 4 M5 screws (two on each side).

Figure 66 Secure Top and Bottom Tray



See Rack Mount Installation on page 55 for installing the bracket assembly onto a rack.

Rack Mount Installation

NOTE: Use screws provided with rack system. Refer to rack user documentation for instructions.

1. Secure mounting brackets to both sides of top tray with four M5 screws (two on each side).

Figure 67 Flange Horizontal Position

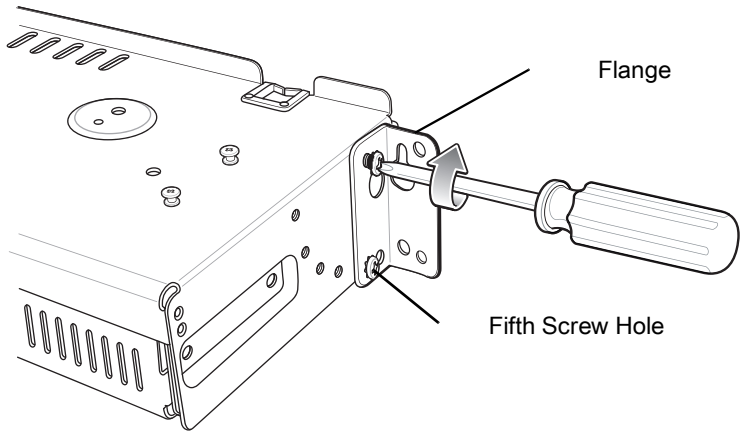
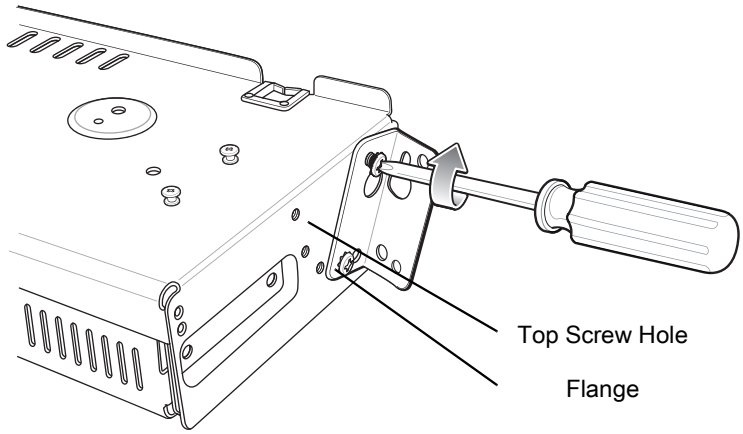


Figure 68 Flange 25° Position



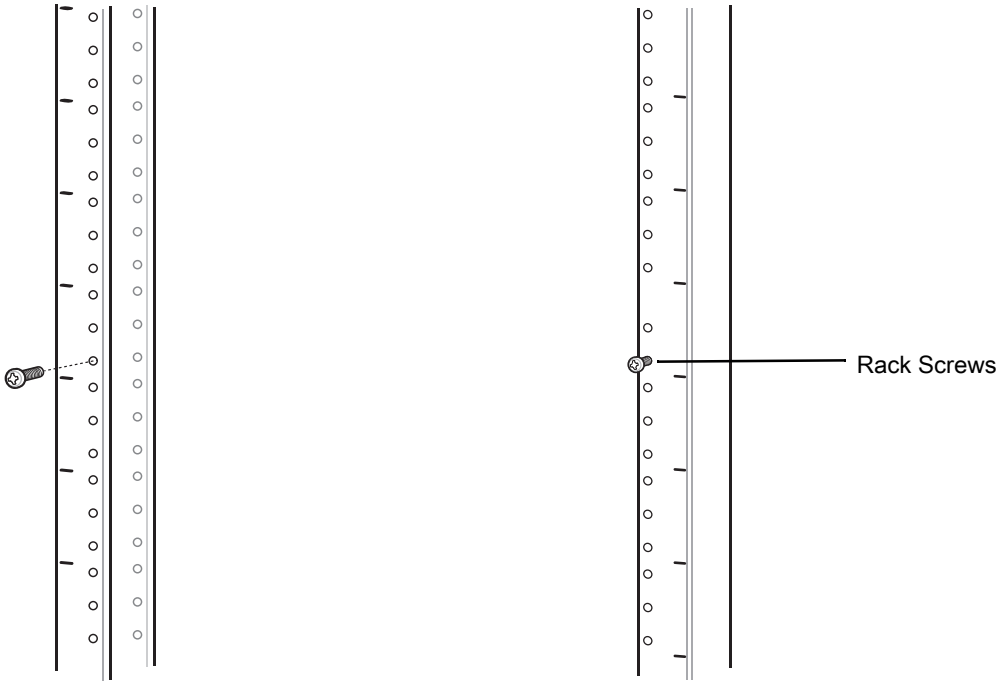
CAUTION: Install mounting bracket with 5-Slot cradle at a maximum height of four feet from ground.

NOTE: Distance between two horizontal mounted brackets should be at least 14.5” apart (from top of one flange to the top of the next flange).

Distance between two 25° mounted brackets should be at least 12” apart (from top of one flange to the top of the next flange).

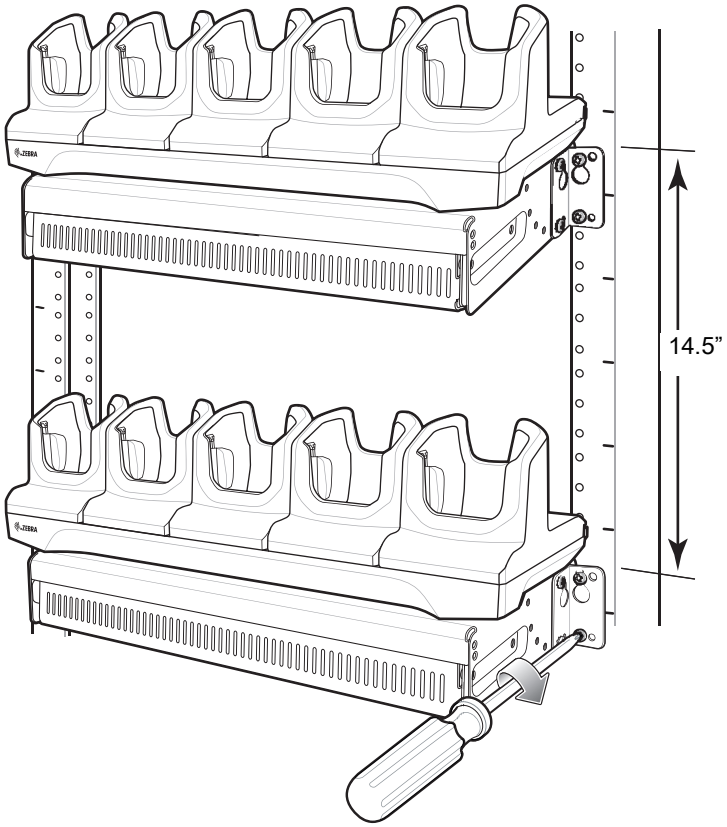
2. Install two rack system screws for top of mounting brackets. The screw heads should protrude half way from the rail.

Figure 69 Install Rack System Screws



3. Align the mounting bracket's top mounting key holes with the screws.
4. Place the brackets on the screws.

Figure 70 Secure Bracket to Rack (Horizontal Position Shown)



5. Secure the top screws.

6. Install bottom screws and tighten screws.
7. Route cables and connect to power source.

CAUTION: Installer should ensure that all building codes are followed when connecting the power supplies to an AC power source.

While installing the brackets, power supplies and cables:

- Use tie wraps to secure cables to the bracket and rails.
- Coil cables wherever possible.
- Route power cables along the rails.
- Route inter-cradle cables to the side rails and then from the rails to the bracket.

Wall Installation

Use the Rack/Wall Mount Bracket to mount a 5-Slot Charge Only cradle on a wall. When installing on a wall, first assemble the bottom tray, install the bottom tray on the wall and then assemble the top tray.

Use mounting hardware (screws and/or anchors) appropriate for the type of wall mounting the bracket onto. The Mount Bracket mounting slots dimensions are 5 mm (0.2 in.). Fasteners must be able to hold a minimum of 20 Kg (44 lbs.)

For proper installation consult a professional installer. Failure to install the bracket properly can possibly result in damage to the hardware.

CAUTION: Install mounting bracket with 5-Slot Charge Only cradle at a maximum height of four feet from ground.

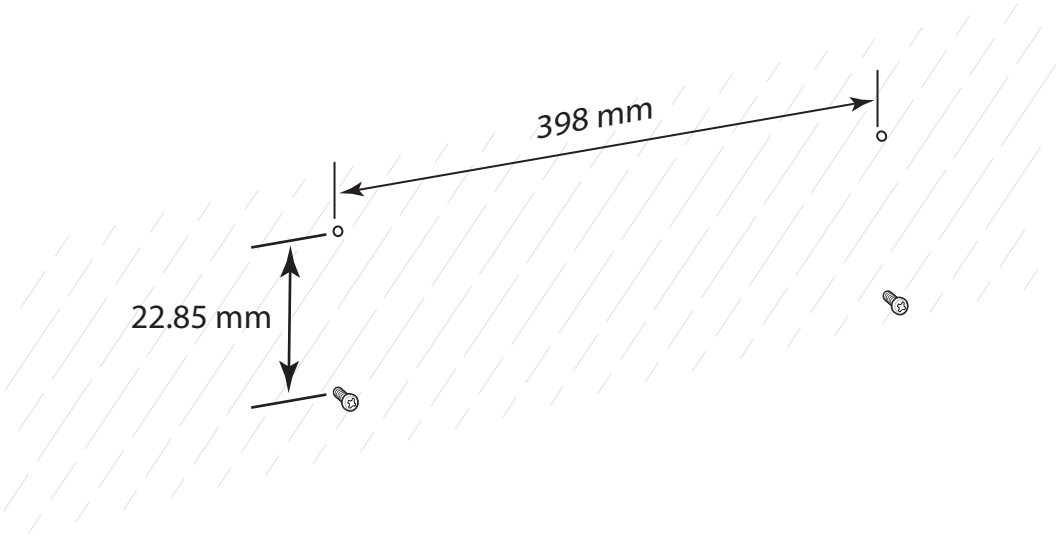
Bottom Tray Assembly

See steps 1 through 5 on page 52 for instructions.

Bracket Wall Mounting

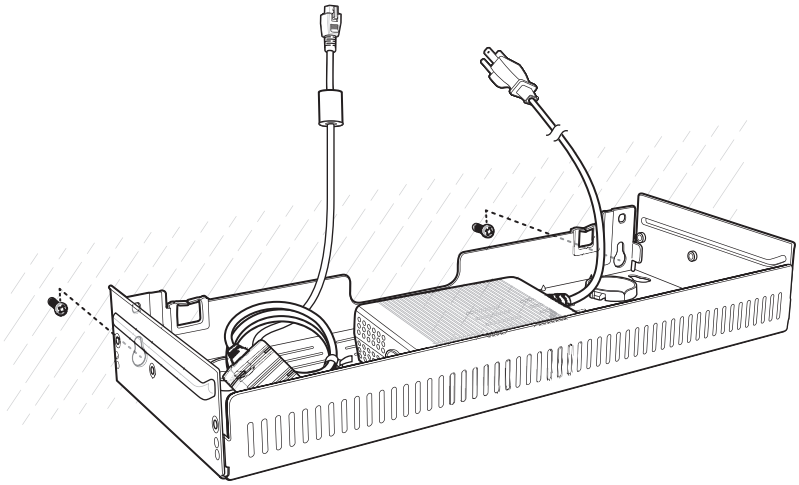
1. Drill holes and install anchors according to the template supplied with the bracket.
2. Install two screws for bottom of bracket. The screw heads should protrude 2.5 mm (0.01”) from the wall.

Figure 71 Horizontal Mounting Template



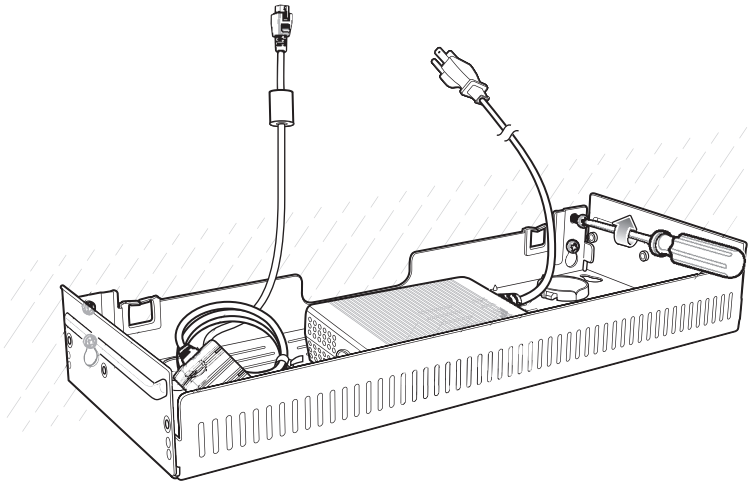
3. Align the mounting bracket’s bottom mounting key holes with the screws.
4. Hang the bracket on the screws.

Figure 72 Horizontal Installation



5. Install two top screws.
6. Tighten all screws.

Figure 73 Horizontal Installation - Tighten Screws



7. Assembly the 5-Slot Charge Only cradle onto the bracket. See steps 7 through 11 on page 52.
8. Route cables and connect to power source.

CAUTION: Installer should ensure that all building codes are followed when connecting the power supplies to an AC power source.

While installing the brackets, power supplies and cables:

- Use tie wraps to secure cables to the bracket and rails.
- Coil cables wherever possible.
- Route power cables along the rails.
- Route inter-cradle cables to the side rails and then from the rails to the bracket.

USB Communication

Introduction

Connect the TC25 to a host computer using the USB-C Cable, or the 1-Slot Ethernet Cradle with a standard USB B cable to transfer files between the TC25 and the host computer. See Accessories on page 25 for more information.

When connecting the TC25 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

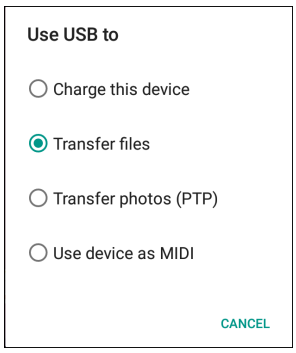
Transferring Files

NOTE Use Transfer files to copy files between the device (internal memory or microSD card) and the host computer.

1. Connect a USB cable to the device or place the device into a USB cradle.
2. Pull down the Notification panel and touch **USB charging this device**.

   By default, **Charge this device** is selected.

Figure 74 Use USB to Dialog Box



3. Touch **Transfer files**.
4. On the host computer, open a file explorer application.
5. Locate the **device** as a portable device.
6. Open the **SD card** or the **Internal storage** folder.
7. Copy files to and from the device or delete files as required.

Transferring Photos

To transfer photos using Photo Transfer Protocol:

NOTE Use Photo Transfer Protocol (PTP) to copy photos from either the microSD card or internal memory to the host computer.

1. Connect USB cable to the device or place the device into a USB cradle. See Accessories on page 25 for setup information.
2. Pull down the Notification panel and touch **USB charging this device**.
3. Touch **Transfer photos (PTP)**.
4. On the host computer, open a file explorer application.
5. Open the **SD card** or the **Internal storage** folder.
6. Copy or delete photos as required.

Disconnect from the Host Computer

To disconnect the device from the host computer:

CAUTION Carefully follow the host computer's instructions to unmount the microSD card and disconnect USB devices correctly to avoid losing information.

1. On the host computer, unmount the device.
2. Remove the USB from the device or remove the device from the cradle.

DataWedge

Introduction

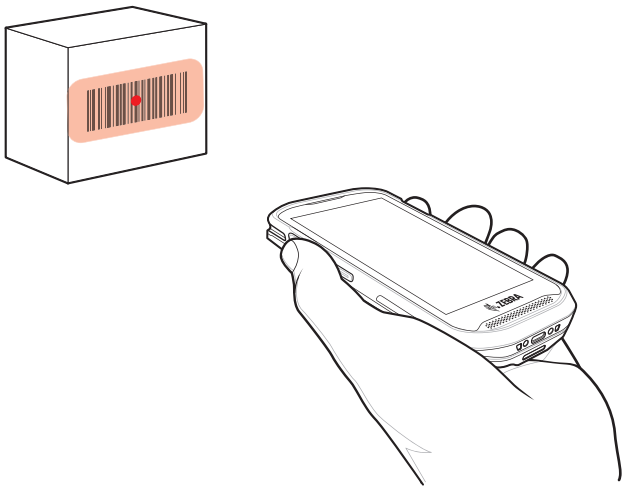
This chapter applies to DataWedge on Android devices. DataWedge is an application that reads data, processes the data and sends the data to an application.

Basic Scanning

To capture bar code data:

1. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
2. Aim the exit window at a bar code.
3. Press and hold the a Scan button. The red aiming pattern turns on to assist in aiming. Ensure that the bar code is within the area formed by the aiming pattern.

Figure 75 TC25 Data Capture



4. The Data Capture LED lights green, a beep sounds and the device vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

Profiles

DataWedge is based on profiles and plug-ins. A profile contains information on how DataWedge should behave with different applications.

Profile information consists of:

- Associated application
- Input plug-in configurations
- Output plug-in configurations
- Process plug-in configurations.

Using profiles, each application can have a specific DataWedge configuration. For example, each user application can have a profile which outputs scanned data in the required format when that application comes to the foreground. DataWedge can be configured to process the same set of captured data differently based on the requirements of each application.

DataWedge includes the following pre-configured profiles which support specific built-in applications:

- Visible profiles:
  - **Profile0** - created automatically the first time DataWedge runs. Generic profile used when there are no user created profiles associated with an application.
  - **Launcher** - enables scanning when the Launcher is in foreground.
  - **DWDemo** - provides support for the DWDemo application.

Some Zebra applications are capable of capturing data by scanning. DataWedge is pre-loaded with private and hidden profiles for this purpose. There is no option to modify the private profiles.

Profile0

Profile0 can be edited but cannot be associated with an application. That is, **DataWedge** allows manipulation of plug-in settings for **Profile0** but it does not allow assignment of a foreground application. This configuration allows **DataWedge** to send output data to any foreground application other than applications associated with user-defined profiles when **Profile0** is enabled.

Profile0 can be disabled to allow **DataWedge** to only send output data to those applications which are associated in user-defined profiles. For example, create a profile associating a specific application, disable **Profile0** and then scan. **DataWedge** only sends data to the application specified in the user-created profile. This adds additional security to **DataWedge** enabling the sending of data only to specified applications.

Plug-ins

A plug-in is a software module utilized in DataWedge to extend its functionality to encompass technologies such as barcode scanning. The plug-ins can be categorized into three types based on their operations:

- Input Plug-ins
- Output Plug-ins
- Process Plug-ins.

Input Plug-ins

An Input Plug-in supports an input device, such as a barcode scanner contained in, or attached to the device. **DataWedge** contains base plug-ins for these input devices.

Barcode Scanner Input Plug-in – The Barcode Scanner Input Plug-in is responsible for reading data from the integrated barcode scanner and supports different types of barcode readers including laser, imager and internal camera. Raw data read from the barcode scanner can be processed or formatted using Process

Plug-ins as required. **DataWedge** has built-in feedback functionality for the barcode scanner to issue user alerts. The feedback settings can be configured according to user requirement.

Process Plug-ins

Process Plug-ins are used in **DataWedge** to manipulate the received data according to the requirement, before sending to the foreground application via the Output Plug-in.

- **Basic Data Formatting Process Plug-in** – The Basic Data Formatting Plug-in allows **DataWedge** to add a prefix and/or a suffix to the captured data before passing it to an Output Plug-in.
- **Advanced Data Formatting Process Plug-in** – The Advanced Data Formatting Plug-in allows **DataWedge** to apply rules (actions to be performed based on defined criteria) to the data received via an input plug-in before passing it to an Output Plug-in.

Output Plug-ins

Output Plug-ins are responsible for sending the data from Input Plug-ins to a foreground application on the device.

- **Keystroke Output Plug-in** – The Keystroke Output Plug-in collects and sends data received from the Input Plug-in to the foreground applications by emulating keystrokes.
- **Intent Output Plug-in** – The Intent Output Plug-in collects and sends data received from the Input Plug-ins to foreground applications using the Android Intent mechanism.
- **IP Output Plug-in** – The IP Output Plug-in collects and sends data received from the Input Plug-ins to a host computer via a network connection. Captured data can be sent over an IP network to a specified IP address and port using either TCP or UDP transport protocols.

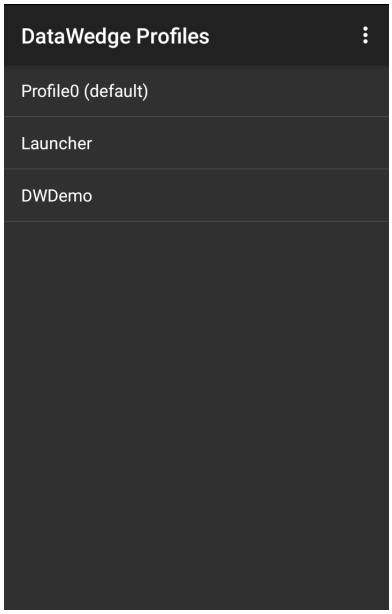
Profiles Screen

To launch DataWedge, swipe up from the bottom of the screen and touch . By default, the following profiles appear:

- **Profile0**
- **Launcher**
- **DWDemo**

Profile0 is the default profile and is used when no other profile can be applied.

Figure 76 DataWedge Profiles Screen



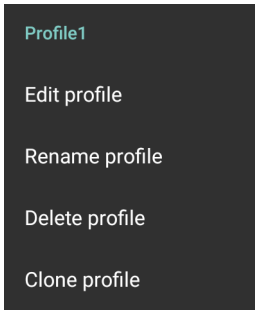
Profile names are color coded. Enabled profiles are white and disabled profiles are gray.

To configure a profile touch the profile name.

Profile Context Menu

Touch and hold a profile to open a context menu that allows additional actions to be performed on the selected profile.

Figure 77 Profile Context Menu

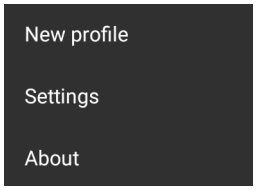


The profile context menu allows the profile to be edited (same as just tapping on a profile), renamed or deleted.

Options Menu

Touch ⋮ to open the options menu.

Figure 78 DataWedge Options Menu



The menu provides options to create a new profile, access to general DataWedge settings and DataWedge version information.

Disabling DataWedge

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **Settings**.
4. Touch **DataWedge enabled**.

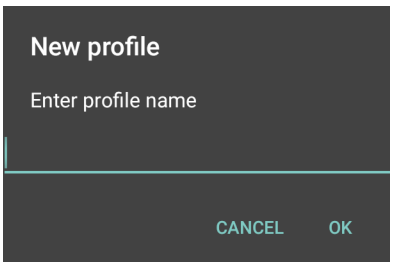
The blue check disappears from the checkbox indicating that DataWedge is disabled.

Creating a New Profile

To create a new profile:

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **New profile**.
4. In the **New profile** dialog box, enter a name for the new profile. It is recommended that profile names be unique and made up of only alpha-numeric characters (A-Z, a-z, 0-9).

Figure 79 New Profile Name Dialog Box



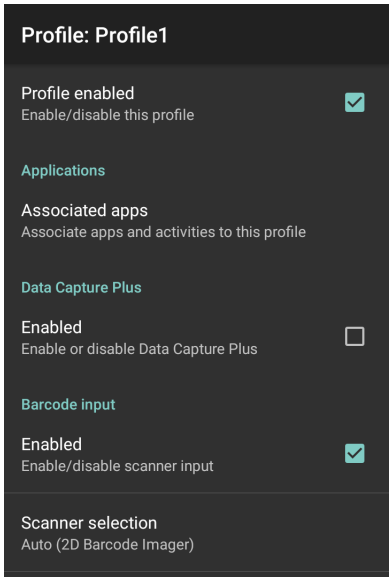
5. Touch **OK**.

The new profile name appears in the **DataWedge profile** screen.

Profile Configuration

To configure the Profile0 or a user-created profile, touch the profile name.

Figure 80 Profile Configuration Screen



The configuration screen lists the following sections:

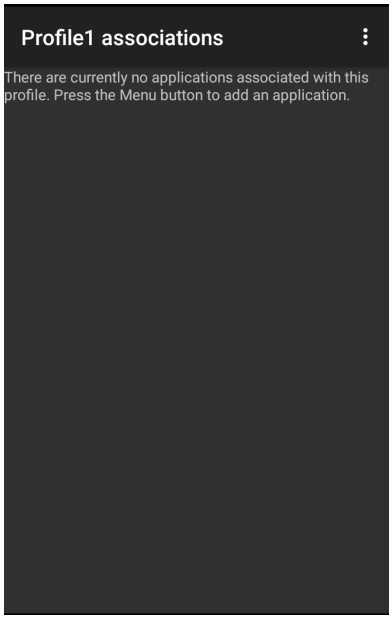
- Profile enabled
- Applications
- Data Capture Plus (DCP)
- Barcode Input
- SimulScan Input
- Keystroke output
- Intent Output
- IP Output.

Associating Applications

Use Applications option to associate applications with this profile. User created profiles should be associated with one or more applications and its activities.

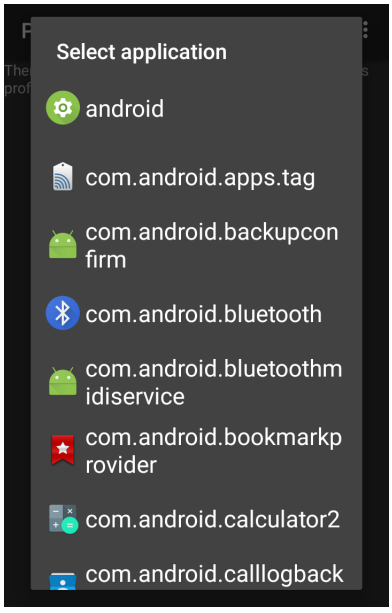
1. Touch **Associated apps**. A list of applications/activities associated with the profile displays. Initially the list does not contain any applications/activities.

Figure 81 Associated Apps Screen



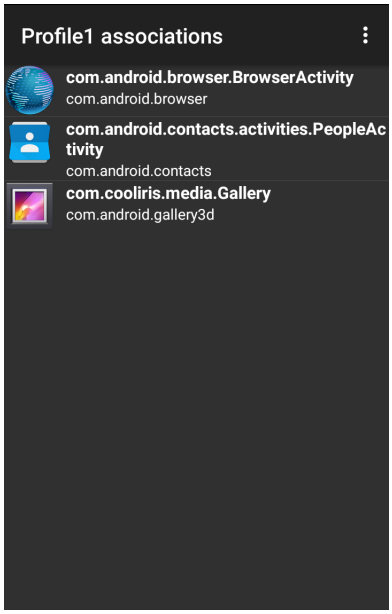
2. Touch ⋮.
3. Touch **New app/activity**.

Figure 82 Select Application Menu



4. In the **Select application** screen, select the desired application from the list.
5. In the **Select activity** menu, selecting the activity adds that application/activity combination to the associated application list for that profile. Selecting * as the activity results in all activities within that application being associated to the profile. During operation, DataWedge tries to match the specific application/activity combinations with the foreground application/activity before trying to match the general application/* combinations.
6. Touch ◁.

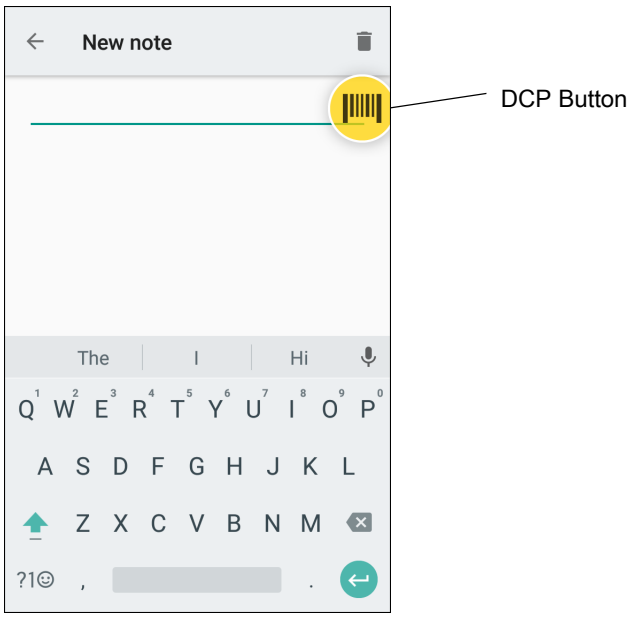
Figure 83 Selected Application/Activity



Data Capture Plus

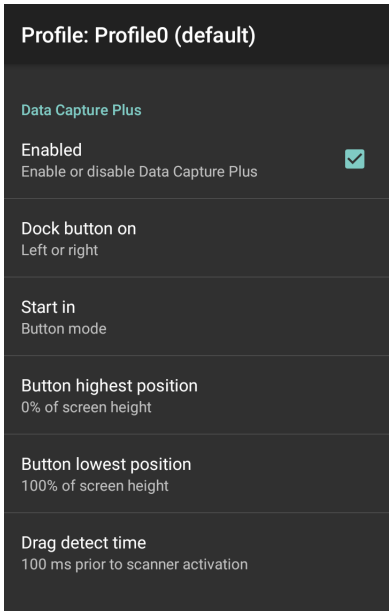
Data Capture Plus (DCP) is a DataWedge feature that enables the user to initiate data capture by touching a designated part of the screen. A variable screen overlay acts like a scan button.

Figure 84 Minimized Data Capture Panel



The DataWedge profile configuration screen allows the user to configure how the DCP appears on the screen once the particular profile is enabled. The DCP is hidden by default. Enabling DCP option displays seven additional configuration parameters.

Figure 85 Data Capture Panel Settings

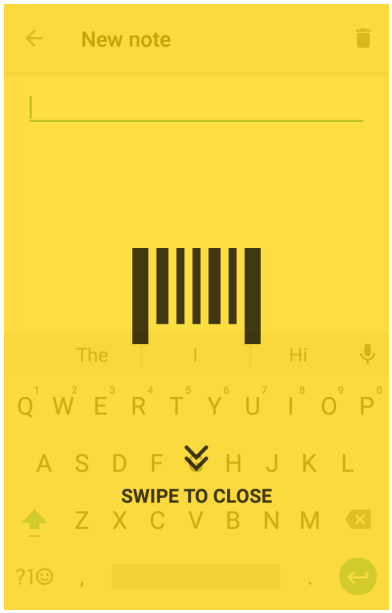


- Enable - Select to enable Data Capture Plus (default - disabled).
- **Dock button on** - Select position of the button.
  - **Left or right** - Allows user to place the button on either the right or left edge of the screen.
  - **Left only** - Places the button on left edge of the screen.
  - **Right only** - Places the button on the right edge of the screen.
- **Start in** - Select the initial DCP state.
  - **Fullscreen mode** - DCP covers the whole screen.
  - **Button mode** - DCP displays as a circular button on the screen and can be switched to fullscreen mode.
  - **Button only mode** - DCP displays as a circular button on the screen and cannot be switched to fullscreen mode.
- **Button highest position** - Select the top of the range the user is allowed to move the DCP, given as a percent of the screen height (default - 0).
- **Button lowest position** - Select the bottom of the range the user is allowed to move the DCP, given as a percent of the screen height (default - 100).
- **Drag detect time** - Select the time in milliseconds that the scanner waits before activating scanner. This allows the user to drag the button without initiating scanner (default - 100 ms, maximum 1000 ms).

NOTE: The DCP does not appear if the scanner is disabled in the profile even though the **Enabled** option is set.

In Button mode, the user can place DCP in full screen mode by dragging the button over **Fullscreen mode**. The overlay covers the screen.

Figure 86 Maximized DCP



Swipe down to return to button mode.

Barcode Input

Use the **Barcode Input** options to configure the Barcode Scanner Input Plug-in for the profile.

Enabled

Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled.

Scanner Selection

Configures which scanning device to use for barcode data capture when the profile is active. For Bluetooth scanners, if the device was not previously paired, a pairing barcode displays prior to automatic connection.

•

Auto Switch to Default on Event

This feature configures DataWedge to select an external scanner as the default scanning device immediately upon connection and revert to a built-in scanner when the external scanner is disconnected. External scanners include those connecting by Bluetooth, serial cable or snap-on module. Disabled by default. This is only available when **Scanner Selection** is set to **Auto**.

This helps reduce scanning workflow interruptions when a Bluetooth scanner is introduced and/or it becomes disconnected due to losing power or moving out of range.

- **Disabled** - No scanner switching occurs when an external scanner is connected or disconnected (default).
- **On connect** - Selects the external scanner as the default scanning device immediately upon connection.
- **On disconnect** - Reverts to a built-in scanner based on its position in an internally managed scanner list (which varies by host device). This is usually the scanner most recently used prior to the external connection (see notes below).

- **On connect/disconnect** - Selects an external scanner as the default scanning device immediately upon connection. Upon disconnection, reverts to the scanner set as the default prior to the external connection.

NOTE: The system selects the default scanner based on the connection state and the scanner's position in an internally managed scanner list. If the newly connected scanner is lower in the scanner list than the one currently selected as the default scanner, the newly connected scanner becomes the default scanner.

On devices with only one built-in scanner or imager, **On disconnect** reverts to that built-in scanner or imager.

Decoders

Configures which barcode decoders are enabled or disabled. For best performance disable all unnecessary decoders.

Touch **Decoders**. The **Barcode input** screen appears. A check in the checkbox indicates that the decoder is enabled. By default the most commonly used decoders are enabled (shown below with an asterisk). The supported decoders are:

NOTE: DataWedge supports the decoders listed below but not all are validated on this device.

Table 7 Supported Decoders

Decoders	Camera	Internal Imager SE2100	Internal Imager SE4710	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
Australian Postal	O	O	O	O	O	O	O	--
Aztec	X	X	X	X	X	X	X	--
Canadian Postal	O	O	O	--	O	--	--	--
Chinese 2 of 5	O	O	O	O	O	O	O	O
Codabar	X	X	X	X	X	X	X	X
Code 11	O	O	O	O	O	O	O	O
Code 128	X	X	X	X	X	X	X	X
Code 39	X	X	X	X	X	X	X	X
Code 93	O	O	O	O	O	O	O	O
Composite AB	O	O	O	O	O	O	O	--
Composite C	O	O	O	O	O	O	O	--
Discrete 2 of 5	O	O	O	O	O	O	O	O
Datamatrix	X	X	X	X	X	X	X	--
Dutch Postal	O	O	O	O	O	O	O	--

Table 7 Supported Decoders (Continued)

Decoders	Camera	Internal Imager SE2100	Internal Imager SE4710	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
DotCode	X	O	O	O	O	O	O	O
EAN13	X	X	X	X	X	X	X	X
EAN8	X	X	X	X	X	X	X	X
Grid Matrix	O	O	O	O	O	O	O	O
GS1 DataBar	X	X	X	X	X	X	X	X
GS1 DataBar Expanded	X	X	X	X	X	X	X	X
GS1 DataBar Limited	O	O	O	O	O	O	O	O
GS1 Datamatrix	O	O	O	--	O	O	O	--
GS1 QRCode	O	O	O	--	O	O	O	--
HAN XIN	O	O	O	--	O	O	O	--
Interleaved 2 of 5	O	O	O	O	O	O	O	O
Japanese Postal	O	O	O	O	O	O	O	--
Korean 3 of 5	O	O	O	O	O	O	O	O
MAIL MARK	X	X	X	--	X	X	X	--
Matrix 2 of 5	O	O	O	O	O	O	O	O
Maxicode	X	X	X	X	X	X	X	--
MicroPDF	O	O	O	O	O	O	O	--
MicroQR	O	O	O	O	O	O	O	--
MSI	O	O	O	O	O	O	O	O
PDF417	X	X	X	X	X	X	X	--
QR Code	X	X	X	X	X	X	X	--
Decoder Signature	O	O	O	O	O	O	--	--
TLC 39	O	O	O	O	O	O	O	O
Trioptic 39	O	O	O	O	O	O	O	O
UK Postal	O	O	O	O	O	O	O	--
UPCA	X	X	X	X	X	X	X	X

Table 7 Supported Decoders (Continued)

Decoders	Camera	Internal Imager SE2100	Internal Imager SE4710	RS507/RS507X	RS6000	DS2278	DS3678	LI3678
UPCE0	X	X	X	X	X	X	X	X
UPCE1	O	O	O	O	O	O	O	O
US4state	O	O	O	O	O	O	O	--
US4state FICS	O	O	O	O	O	O	O	--
US Planet	O	O	O	O	O	O	O	--
US Postnet	O	O	O	O	O	O	O	--

Touch ◁ to return to the previous screen.

Decoder Params

Use **Decode Params** to configure individual decoder parameters.

NOTE: Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

NOTE:

Codabar

- **CLSI Editing** - Enable this parameter to strip the start and stop characters and insert a space after the first, fifth, and tenth characters of a 14-character Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **Length1** - Use to set decode lengths (default - 6). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **NOTIS Editing** - Enable this parameter to strip the start and stop characters from a decoded Codabar symbol. Enable this feature if the host system requires this data format (default - disabled).
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

Code 11

- **Length1** - Use to set decode lengths (default - 4). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Code 11 data with or without the check digit. A check in the checkbox indicates to send Code 11 data with check digit (default - disabled).

- **Verify Check Digit** - Check the integrity of all Code 11 symbols to verify that the data complies with the specified check digit algorithm. This selects the check digit mechanism for the decoded Code 11 barcode.
  - **No Check Digit** - Do not verify check digit.
  - **1 Check Digit** - Barcode contains one check digit (default).
  - **2 Check Digits** - Barcode contains two check digits.

Code128

- **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 barcodes (default - disabled).
- **Ignore Code128 FCN4** - When enabled, and a Code 128 barcode has an embedded FNC4 character, it will be removed from the data and the following characters will not be changed. When the feature is disabled, the FNC4 character will not be transmitted but the following character will have 128 added to it (default - disabled).
- **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT barcodes that are commonly used in pairs. If ISBT128 Concat Mode is set, enable Check ISBT Table to concatenate only those pairs found in this table. Other types of ISBT codes are not concatenated. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Enable GS1-128** - Set the GS1 128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **Enable ISBT128** - Set the ISBT128 subtype. A check in the checkbox indicates that the option is enabled (default - enabled).
- **Enable Plain Code128** - Set the Plain Code128 subtype. Enables other (non-EAN or ISBT) Code 128 subtypes. A check in the checkbox indicates that the option is enabled (default - enabled).
- **ISBT128 Concatenation Mode** - Select an option for concatenating pairs of ISBT code types:
  - **Concat Mode Never** - Do not concatenate pairs of ISBT codes encountered (default).
  - **Concat Mode Always** - There must be two ISBT codes in order to decode and perform concatenation. Does not decode single ISBT symbols.
  - **Concat Mode Auto** - Decodes and concatenates pairs of ISBT codes immediately. If only a single ISBT symbol is present, the device must decode the symbol the number of times set via DataWedge Configuration 4 - 11 Redundancy - Code128 before transmitting its data to confirm that there is no additional ISBT symbol.
- **Length1** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Security Level** - The scanner offers four levels of decode security for Code 128 barcodes. Select increasing levels of security for decreasing levels of barcode quality. There is an inverse relationship between security and scanner aggressiveness, so choose only that level of security necessary for any given application.
  - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” barcodes.
  - **Security Level 1** - This setting eliminates most misdecodes (default).
  - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
  - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec barcodes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the barcodes.

Code39

- **Code39 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 barcodes (default - disabled).
- **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate barcode below to enable or disable converting Code 39 to Code 32 (default - disabled).
- **Full ASCII**- Code 39 Full ASCII is a variant of Code 39 that pairs characters to encode the full ASCII character set. To enable or disable Code 39 Full ASCII (default - disabled),
- **Length1** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths 4 (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Report Check Digit** - Transmit Code 39 data with or without the check digit. A check in the checkbox indicates to send Code 39 data with check digit (default - disabled).
- **Report Code32 Prefix** - Scan the appropriate barcode to enable or disable adding the prefix character “A” to all Code 32 barcodes (default - disabled).
- **Security Level** - Options: **Security level 0**, **Security Level 1**, **Security Level 2** and **Security Level 3** (default - Security level 1).
  - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” barcodes.
  - **Security Level 1** - This setting eliminates most misdecodes (default).
  - **Security Level 2** - Select this option if Security level 1 fails to eliminate misdecodes.
  - **Security Level 3** - If Security Level 2 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec barcodes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the barcodes.
- **Verify Check Digit** - Enable this feature to check the integrity of all Code 39 symbols to verify that the data complies with a specified check digit algorithm. The digital scanner decodes only those Code 39 symbols that include a modulo 43 check digit. Enable this feature only if the Code 39 symbols contain a modulo 43 check digit (default - disabled).

Code93

- **Length1** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).

Composite AB

- **UCC Link Mode**
  - **Link Flag ignored** - 1D component is transmitted regardless of whether a 2D component is detected.
  - **Always Linked** - 1D and the 2D components are transmitted. If 2D is not present, the 1D component is not transmitted.
  - **Auto Discriminate** - the digital scanner determines if there is a 2D portion, then transmits the 1D component, as well as the 2D portion if present. (default).

Discrete 2 of 5

- **Length1** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 14). See Decode Lengths for more information.

- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).

GS1 DataBar Limited

- **GS1 Limited Security Level**
  - **GS1 Security Level 1** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” barcodes.
  - **GS1 Security Level 2** - This setting eliminates most misdecodes (default).
  - **GS1 Security Level 3** - Select this option if Security level 2 fails to eliminate misdecodes.
  - **GS1 Security Level 4** - If Security Level 3 is selected and misdecodes still occur, select this security level. Be advised, selecting this option is an extreme measure against mis-decoding severely out of spec barcodes. Selecting this level of security significantly impairs the decoding ability of the scanner. If this level of security is needed, try to improve the quality of the barcodes.

HAN XIN

- **HAN XIN Inverse**
  - **Disable** - Disables decoding of HAN XIN inverse barcodes (default).
  - **Enable** - Enables decoding of HAN XIN inverse barcodes.
  - **Auto** - Decodes both HAN XIN regular and inverse barcodes.

Interleaved 2 of 5

- **Check Digit**
  - **No Check Digit** - A check digit is not used. (default)
  - **USS Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Uniform Symbology Specification (USS) check digit algorithm.
  - **OPCC Check Digit** - Select to check the integrity of all Interleaved 2 of 5 symbols to verify the data complies with either the Optical Product Code Council (OPCC) check digit algorithm.
- **Length1** - Use to set decode lengths (default - 14). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 10). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit Interleaved 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Interleaved 2 of 5 data with check digit (default - disabled).
- **I2of5 Security Level** - Options: **I2of5 Security level 0**, **I2of5 Security Level 1**, **I2of5 Security Level 2** and **I2of5 Security Level 3** (default - I2of5 Security level 1).
- **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 barcodes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 barcode must be enabled and must have a leading zero and a valid EAN-13 check digit. A check in the checkbox indicates that the option is enabled (default - disabled).
- **I2of5 Reduced Quiet Zone** - Enables decoding of margin-less I2of5 barcodes (default - disabled).

Matrix 2 of 5

- **Length1** - Use to set decode lengths (default - 10). See Decode Lengths for more information.
- **Length2** - Use to set decode lengths (default - 0). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Report Check Digit** - Transmit Matrix 2 of 5 data with or without the check digit. A check in the checkbox indicates to send Matrix 2 of 5 data with check digit (default - enabled).

- **Verify Check Digit** - Enable this feature to check the integrity of all Matrix 2 of 5 symbols to verify that the data complies with a specified check digit algorithm (default - enabled).

MSI

- **Check Digit** - With MSI symbols, one check digit is mandatory and always verified by the reader. The second check digit is optional.
  - **One Check Digit** - Verify one check digit (default).
  - **Two Check Digits** - Verify two check digits.
- **Check Digit Scheme** - Two algorithms are possible for the verification of the second MSI check digit. Select the algorithm used to encode the check digit.
  - **Mod-11-10** - First check digit is MOD 11 and second check digit is MOD 10 (default).
  - **Mod-10-10** - Both check digits are MOD 10.
- **Length 1** - Use to set decode lengths (default - 4). See Decode Lengths for more information.
- **Length 2** - Use to set decode lengths (default - 55). See Decode Lengths for more information.
- **Redundancy** - Sets the reader to read the barcode twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
- **Report Check Digit** - Transmit MSI data with or without the check digit. A check in the checkbox indicates to send MSI data with check digit (default - disabled).

UK Postal

- **Report Check Digit** - Transmit UK Postal data with or without the check digit. A check in the checkbox indicates to send UK Postal data with check digit (default - disabled).

UPCA

- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

  There are three options for transmitting a UPCA preamble:
  - **Preamble None** - Transmit no preamble.
  - **Preamble Sys Char** - Transmit System Character only (default).
  - **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA). Select the appropriate option to match the host system.
- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - enabled).

UPCE0

- **Convert UPCE0 To UPCA** - Enable to convert UPCE0 (zero suppressed) decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable to transmit UPCE0 decoded data as UPCE0 data, without conversion (default - disabled).
- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

  There are three options for transmitting a UPCE0 preamble:
  - **Preamble None** - Transmit no preamble (default).
  - **Preamble Sys Char** - Transmit System Character only.
  - **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA).

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

UPCE1

- **Convert UPCE1 To UPCA** - Enable this to convert UPCE1 decoded data to UPC-A format before transmission. After conversion, the data follows UPC-A format and is affected by UPC-A programming selections. Disable this to transmit UPCE1 decoded data as UPCE1 data, without conversion (default - disabled).
- **Preamble** - Preamble characters are part of the UPC symbol consisting of Country Code and System Character. Select the appropriate option to match the host system.

  There are three options for transmitting a UPCE1 preamble:

  - **Preamble None** - Transmit no preamble (default).
  - **Preamble Sys Char** - Transmit System Character only.
  - **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA).
- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

US Planet

- **Report Check Digit** - The check digit is the last character of the symbol used to verify the integrity of the data. Enables or disables this option. A check in the checkbox indicates that the option is enabled (default - disabled).

Decode Lengths

The allowable decode lengths are specified by options **Length1** and **Length2** as follows:

- Variable length: Decode symbols containing any number of characters.
  - Set both **Length1** and **Length2** to 0.
- Range: Decode a symbol with a specific length range (from *a* to *b*, including *a* and *b*).
  - Set **Length1** to *a* and set **Length2** to *b*.
- Two Discrete Lengths: Decode only symbols containing either of two selected lengths.
  - Set both **Length1** or **Length2** to the specific lengths. **Length1** must be greater than **Length2**.
- One Discrete Length: Decode only symbols containing a specific length.
  - Set both **Length1** and **Length2** to the specific length.

UPC EAN Params

Allows the configuration of the parameters that apply to more than one UPC or EAN decoder.

NOTE: Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

- **Convert DataBar To UPC EAN** - If this is set it converts DataBar barcodes to UPC/EAN format. For this setting to work UPC/EAN symbologies must be enabled. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC barcodes. (default - disabled)
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled. (default - disabled).

- **Bookland Format -** If Bookland EAN is enabled, select one of the following formats for Bookland data:
  - **Format ISBN-10 -** The decoder reports Bookland data starting with 978 in traditional 10-digit format with the special Bookland check digit for backward-compatibility. Data starting with 979 is not considered Bookland in this mode. (default)
  - **Format ISBN-13** - The decoder reports Bookland data (starting with either 978 or 979) as EAN-13 in 13-digit format to meet the 2007 ISBN-13 protocol.
- **Coupon** - Enables Coupon code decoding. Note that in order to successfully decode Coupon codes, all of the correct decoders must be enabled. A check in the checkbox indicates that the option is enabled. (default - disabled).
- **Coupon Report Mode** - Traditional coupon symbols are composed of two barcode: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded barcode. The new format offers more options for purchase values (up to $999.999) and supports complex discount offers as a second purchase requirement. An interim coupon symbol also exists that contain both types of barcodes: UPC/EAN and Databar Expanded. This format accommodates both retailers that do not recognize or use the additional information included in the new coupon symbol, as well as those who can process new coupon symbols.
  - **Old Coupon Report Mode** - Scanning an old coupon symbol reports both UPC and Code 128, scanning is interim coupon symbol reports UPC, and scanning a new coupon symbol reports nothing (no decode).
  - **New Coupon Report Mode** - Scanning an old coupon symbol reports either UPC or Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded.
  - **Both Coupon Report Modes** - Scanning an old coupon symbol reports both UPC and Code 128, and scanning an interim coupon symbol or a new coupon symbol reports Databar Expanded. (default)
- **Ean Zero Extend** – Enable this parameter to add five leading zeros to decoded EAN-8 symbols to make them compatible in format to EAN-13 symbols. Disable this to transmit EAN-8 symbols as is. Default – disabled.
- **Linear Decode** - This option applies to code types containing two adjacent blocks, for example, UPC-A, EAN-8, EAN-13. Enable this parameter to transmit a bar code only when both the left and right blocks are successfully decoded within one laser scan. Enable this option when bar codes are in proximity to each other (default - enabled).
- **Retry Count** - Retry count for auto-discriminating for supplementals. Possible values are 2 to 20 inclusive. Note that this flag is only considered if Supplemental Mode - UPC EAN is set to one of the following values: **Supplementals Auto**, **Supplementals Smart**, **Supplementals 378-379**, **Supplementals 978-979**, **Supplementals 977** or **Supplementals 414-419-434-439** (2 to 20, default 10).
- **Security Level** - The scanner offers four levels of decode security for UPC/EAN barcodes. Select higher security levels for lower quality barcodes. There is an inverse relationship between security and decode speed, so be sure to choose only that level of security necessary for the application.
  - **Level 0** - This default setting allows the scanner to operate fastest, while providing sufficient security in decoding “in-spec” UPC/EAN barcodes.
  - **Level 1** - As barcode quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed barcodes, and the misdecodes are limited to these characters, select this security level. (default).
  - **Level 2** - If the scanner is misdecoding poorly printed barcodes, and the misdecodes are not limited to characters 1, 2, 7, and 8, select this security level.
  - **Level 3** - If the scanner is still misdecoding, select this security level. Be advised, selecting this option is an extreme measure against misdecoding severely out of spec barcodes. Selecting this level of security can significantly impair the decoding ability of the scanner. If this level of security is necessary, try to improve the quality of the barcodes.
- **Supplemental2** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.

- **Supplemental5** - Enables or disables this option. A check in the checkbox indicates that the option is enabled.
- **Supplemental Mode**
  - **No Supplementals** - the scanner is presented with a UPC/EAN plus supplemental symbol, the scanner decodes UPC/EAN and ignores the supplemental characters (default).
  - **Supplemental Always** - the scanner only decodes UPC/EAN symbols with supplemental characters, and ignores symbols without supplementals.
  - **Supplements Auto** - the scanner decodes UPC/EAN symbols with supplemental characters immediately. If the symbol does not have a supplemental, the scanner must decode the barcode the number of times set via UPC/EAN Supplemental Redundancy before transmitting its data to confirm that there is no supplemental.
  - **Supplemental Smart** - Enables smart supplementals. In this mode the decoder returns the decoded value of the main block right away if it does not belong to one of the following supplemental types: 378, 379, 977, 978, 979, 414, 419, 434 or 439. If the barcode starts with one of the prefixes it searches the image more aggressively for a supplemental. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
  - **Supplemental 378-379** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 378 or 379. Disables reading of supplementals for any other UPC/EAN barcode not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
  - **Supplemental 978-979** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 978 or 979. Disables reading of supplementals for another UPC/EAN barcode not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
  - **Supplemental 414-419-434-439** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 414, 419, 434 or 439. Disables reading of supplementals for another UPC/EAN barcode 4 - 16 not starting with 414, 419, 434 or 439. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.
  - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN barcode not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main barcode is returned.

Reader Params

Allows the configuration of parameters specific to the selected barcode reader.

NOTE: Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

- **Character Set Configuration** - Used to support the GB2312 Chinese characters encoding.
  - **Character Set Selection** - Allows the user to convert the barcode data if different from default encoding type.
    - **Auto Character Set Selection (Best Effort)** - Automatic character convert option. Tries to decode data from the Preferred selection. The first correct decodable character set is used to convert the data and is sent.
    - **ISO-8859-1** - Part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
    - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
    - **GB18030** - Chinese coded character set that defines the required language and character support necessary for software in China.

- **UTF-8** - A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).

- **Auto Character Set Preferred Order** - In **Auto Character Set Selection** mode, the system will try to decode the data in a preference order of character sets. The algorithm used is a best effort one. That is, there could be cases where the data can be decoded from more than one character set. The first character set from the preferred list which can decode the data successfully will be chosen to decode the data and sent to the user. Any other character set that is in the list but lower in the preferred order, would not be considered, even if the data could be successfully decoded using such character set.

  The preferred character set and its preference order is configurable to the user through the **Auto Character Set Preferred Order** menu. Users can change the order by dragging the icon for that menu item. To delete an item, long press on an item and the **Delete** option will appear. To add a new item, tap the menu icon at top right corner and options to add UTF-8 and GB2312 will appear.

  - **UTF-8 -** A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
  - **GB2312 -** Character set of the People's Republic of China, used for simplified Chinese characters.

- **Auto Character Set Failure Option** - If the system cannot find a character set from the preferred list that can be used to successfully decode the data, the character set selected in **Auto Character Set Failure Option** is used to decode the data and send to the user. If **NONE** is used, Null data is returned as string data.

  - **NONE**
  - **UTF-8 -** A character encoding capable of encoding all possible characters, or code points, defined by Unicode (default).
  - **ISO-8859-1 -** Part of the ISO/IEC 8859 series of ASCII-based standard character encodings. It is generally intended for Western European languages.
  - **Shift_JIS** - Shift Japanese Industrial Standards (JIS) is a character encoding for the Japanese language.
  - **GB18030 -** Chinese coded character set that defines the required language and character support necessary for software in China.

- **1D Quiet Zone Level** - Sets the level of aggressiveness in decoding barcodes with a reduced quiet zone (the area in front of and at the end of a barcode), and applies to symbologies enabled by a Reduced Quiet Zone parameter. Because higher levels increase the decoding time and risk of misdecodes, Zebra strongly recommends enabling only the symbologies which require higher quiet zone levels, and leaving Reduced Quiet Zone disabled for all other symbologies.

  Options are:

  - **0** - The scanner performs normally in terms of quiet zone.
  - **1** - The scanner performs more aggressively in terms of quiet zone (default).
  - **2** - The scanner only requires one side EB (end of barcode) for decoding.
  - **3** - The scanner decodes anything in terms of quiet zone or end of barcode.

- **Adaptive Scanning -** When adaptive scanning is enabled, the scan engine toggles between wide and narrow, allowing the scan engine to decode barcodes based on the distance.

  - **Disable**
  - **Enable** (default).

- **Beam Width** - Beam Width is applicable only with linear scanners.

  - **Narrow**
  - **Normal** (default)
  - **Wide**

- **Aim mode** - Turns the scanner cross-hairs on or off.
  - **On** - Cross-hair is on (default).
  - **Off** - Cross-hair is off.
- **Aim Timer** - Sets the maximum amount of time that aiming remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the aim to stay on indefinitely (default - 500).
- **Aim Type** - Set the aiming usage.
  - **Trigger** - A trigger event activates decode processing, which continues until the trigger event ends or a valid decode occurs (default).
  - **Timed Hold** - A trigger pull and hold activates the laser for aiming, which continues until the trigger is released, a valid decode, or the decode session time-out is expired.
  - **Timed Release** - A trigger pull activates the laser for aiming, which continues until a valid decode or the remaining decode session time has expired.
  - **Press and Release** - A trigger pull and release activates the laser for aiming, which continues until a trigger is pressed again, a valid decode, or the decode session time-out is expired.
  - **Continuous Read** - A trigger pull activates a decode session which continues until the Beam Timer expires or the trigger is released. Barcodes are continuously decoded while the session is active.
  - **Press and Sustain** - A trigger pull activates decode processing which continues until the Beam Timer expires or a barcode is decoded.
- **Beam Timer** - Sets the maximum amount of time that the reader remains on (0 - 60,000 ms in increments of 100 ms). A value of 0 sets the reader to stay on indefinitely (default -5000).
- **Time Delay to Low Power** - Sets the time the decoder remains active after decoding. After a scan session, the decoder waits this amount of time before entering Low Power Mode. Options: **1 Second** (default), **30 Seconds**, **1 Minute** or **5 Minutes**.
- **Different Symbol Timeout** - Controls the time the scanner is inactive between decoding different symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.
- **Digimarc Decoding** - Enables/disables support for Digimarc, which encodes and invisibly integrates traditional barcode data onto product packaging. Supported with internal imager only. (default - Enabled).
- **Illumination Brightness** - Sets the brightness of the illumination by altering LED power. The default is 10, which is maximum LED brightness. For values from 1 to 10, LED brightness varies from lowest to highest level of brightness.
- **Illumination mode** - Turns imager illumination on and off. This option is only available when **Bluetooth Scanner** is selected in the **Barcode input**, **Scanner selection** option.
  - **Off** - Illumination is off.
  - **On** - Illumination is on (default).
- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D barcodes.
  - **Disable** - Disables decoding of inverse 1D barcodes (default).
  - **Enable** - Enables decoding of only inverse 1D barcodes.
  - **Auto** - Allows decoding of both twice positive and inverse 1D barcodes.
- **Keep Pairing Info After Reboot**
  - **Disable** - Disables the ability to keep pairing info after reboot.
  - **Enable** - Enables the ability to keep pairing info after reboot. (default).
- **LCD Mode** - Enables or disables LCD mode. LCD mode enhances the ability of the imager to read barcodes from LCD displays such as cellphones.
  - **Disable** - Disables the LCD mode (default).
  - **Enable** - Enables LCD mode.

- **Linear Security Level** - Sets the number of times a barcode is read to confirm an accurate decode.
  - **Security Short or Codabar** - Two times read redundancy if short barcode or Codabar (default).
  - **Security All Twice** - Two times read redundancy for all barcodes.
  - **Security Long and Short** - Two times read redundancy for long barcodes, three times for short barcodes.
  - **Security All Thrice** - Three times read redundancy for all barcodes.
- **HW Engine Low Power Timeout** - Time (0 - 1,000 ms in increments of 50 ms) of inactivity before scanner enters low-power mode from (default - 250).
- **Picklist** - Allows the imager to decode only the barcode that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple barcodes may appear in the field of view during a decode session and only one of them is targeted for decode.
  - **Disabled** – Disables Picklist mode. Any barcode within the field of view can be decoded (default).
  - **Enabled** – Enables Picklist mode so that only the barcode under the projected reticle can be decoded.
- **Poor Quality Decode Effort** - Enable poor quality barcode decoding enhancement feature.
- **Same Symbol Timeout** - Controls the time the scanner is inactive between decoding same symbols. Programmable in 500 msec increments from 0 to 5 seconds. The default is 500 msec.
- **Scanning Modes** - Scanning options available on the device.
  - **Single** - Set to scan general barcodes (default).
  - **UDI** - Set to scan healthcare specific barcodes.
  - **MultiBarcode** - Set to scan multiple barcodes. When this option is selected, the **Multibarcode params** can be set to read from 2 to 10 barcodes on a single scan.

Scan Params

Allows the configuration of Code ID and decode feedback options.

NOTE: Not all parameter options are available with all scanners. See the DataWedge app on each device for the available scanners and parameter options.

- **Code ID Type** - A Code ID character identifies the code type of a scanned barcode. This is useful when the reader is decoding more than one code type. Select a code ID character to insert between the prefix and the decoded symbol.
  - **Code ID Type None** - No prefix (default)
  - **Code ID Type AIM** - Insert AIM Character prefix.
  - **Code ID Type Symbol** - Insert Symbol character prefix.
- **Engine Decode LED** - Use to turn on scanner red LED when the scan beam is emitting either by scanner trigger or using soft scan button.
- **BT Disconnect On Exit** - Bluetooth connection is disconnected when data capture application is closed .
- **Connection Idle Time** - Set connection idle time. The Bluetooth connection disconnects after being idle for set time.
- **Display BT Address Barcode** - Enable or disable displaying Bluetooth Address bar code if there is no Bluetooth scanner being paired when application tries to enable the Bluetooth scanner.
- **Establish Connection Time** - The timeout which the device will try to enable or reconnect to the Bluetooth scanner when the Bluetooth scanner is not in the vicinity or not paired.

- **Audio Feedback Mode** - Select good decode audio indication.
  - **Local Audio Feedback** - Good decode audio indication on device only.
  - **Remote Audio Feedback** - Good decode audio indication.
  - **Both** - Good decode audio indication on device and scanner (default).
  - **Disable** - No good decode audio indication on either device or scanner.
- **LED Feedback Mode** - Select good decode LED indication.
  - **Local LED Feedback** - Good decode LED indication on device only.
  - **Remote LED Feedback** - Good decode LED indication on scanner.
  - **Both** - Good decode LED indication on device and scanner (default).
  - **Disable** - No good decode LED indication on either device or scanner.
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode (default optimized-beep).
- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).
- **Decode Feedback LED Timer** - Set the amount of time (in milliseconds) that the green Data Capture LED stays lit after a good decode. (default - 75 msec.)
- **Beep Volume Control** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.



NOTE: Not all ringtones are fully supported as decode tones and those of longer length may be truncated when used as a decode tone. The recommendation is to test the selected tone for operation before deployment to a customer site.

  - **Ringer** - Uses Ringer audio stream to play the decode beep.
  - **Music and Media** - Uses Media audio stream to play the decode beep.
  - **Alarms** - Uses Alarms audio stream to play the decode beep.
  - **Notifications** - Uses Notifications audio stream to play the decode beep. (default)

UDI Params

Allows the configuration of parameters specific to healthcare barcodes.

- **Enable UDI-GSI** - Enable UDI using GS1 standards (default - enabled).
- **Enable UDI-HIBCC** - Enable UDI using HIBCC standards (default - enabled).
- **Enable UDI-ICCBBA** - Enable UDI using ICCBBA standards (default - enabled).

Multibarcode params

Set the number of barcodes that the device can read on a single scan from 2 to 10. Must also enable **Reader Params** > **Scanning Modes** > **MultiBarcode** option.

Keep enabled on suspend

Keep Bluetooth scanner enabled after suspend (default-disabled).

Voice Input

Zebra GMS devices have a built in Google speech recognition engine. By making use of the speech engine capabilities, DataWedge has extended automated data capturing to user applications through voice. Currently, DataWedge does not capture data for Voice Input.

Voice data capturing starts after you speak the predefined start phrase and it stops after you speak the data or speak the end phrase, if one was defined.

IMPORTANT:

- Simultaneous use of Voice Input in DataWedge and Google Voice is not supported.
- Voice Input is not supported if the Enterprise Home Screen (EHS) is in restricted mode. However, enabling all of the privilege settings in EHS reinstates Voice Input.
- Voice Input is not supported if the device language is changed to another language, for example Chinese.

Use **Voice Input** to configure the Voice Input Plug-in.

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled.
- **Data capture start phrase** - Starts data capture with the phrase entered in this field.This field is mandatory. (Default - **start**).

  Providing numbers and other special characters as the data capture start phrase is not supported.
- **Data capture end phrase** - Ends data capture with the phrase entered in this field or keep it blank if not required. This field is not mandatory. (Default - Blank).
- **Tab command** - Enables the Tab command, which sends a tab key when the user speaks the command **`send tab`**. The commands are supported only when the device is at the **`Waiting for start phrase`** state.
- **Enter command** - Enables the Enter command, which sends an enter key when the user speaks the command **`send enter`**. The commands are supported only when the device is at the **`Waiting for start phrase`** state.
- **Data type** - Allows the user to configure the data type. Set the data type to limit the data capture according to the preferences specified. Available options:
  - **Any** - Scanning a barcode of ABC123, returns ABC123.
  - **Alpha** - Scanning a barcode of ABC123, returns ABC only.
  - **Numeric** - Scanning a barcode of ABC, returns 123 only.
- **Start phrase waiting tone** - Enables or disables this option. Enables audio feedback for **`Waiting for start`**. This option notifies the user that the device is waiting to start the speech engine if you miss the toast message and the **`Waiting for start`** state changes.
- **Data capture waiting tone** - Enables or disables this option. Enables audio feedback for **`Waiting for data`**. This option notifies the user that the device is waiting to capture data if you miss the toast message.
- **Validation window** - Enables or disables the **Validate captured data** window. Enable this option to validate the result that you speak. The window displays the data spoken and the data can be edited on the same screen if any modification is needed. This is very useful when used with the offline mode, since the results receive at this moment might not be accurate.
- **Offline speech recognition** - Enables or disables speech recognition. Enable this option to use Voice Input when you do not have access to the Internet. This option uses an offline recognition speech engine to detect the data you speak.

Keystroke Output

DataWedge supports Keystroke Output.

Use to configure the Keystroke Output Plug-in for the profile.

- **Enabled** — Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - enabled).

- **Action key character** - Enables decoding of a special character embedded within a barcode data for use in native Android applications. This feature is helpful when populating or executing a form.
  - **None** - Action key character feature is disabled (default).
  - **Tab** - Tab character code in a barcode is processed. When DataWedge detects this character code in a barcode, move the focus to the next field.
  - **Line feed** - Line feed character code in a barcode is processed. When DataWedge detects this character code in a barcode, move the focus to the next field.
  - **Carriage return** - Carriage return character code in a barcode is processed. When DataWedge detects this character code in a barcode, move the focus to the next field.
- **Inter character delay** - Set the delay between keystrokes (in milliseconds).
- **Delay Multibyte characters only** - If Inter character delay is set, enable Delay Multbyte characters only to delay only the multibyte characters.
- **Multi byte character display** - Set the amount of time (in milliseconds) of the inter character delay for multi byte characters. (default - 0.)
- **Key event delay** - Set the amount of time (in milliseconds) of the wait time for control characters. (default - 0.)
- **Data formatting and ordering** - Allows formatting and ordering of UDI and Multibarcode data.
  - **UDI specific** - Allows the output order of acquired UDI data to be adjusted and the optional insertion of a tab, line feed, or carriage return character between tokens.
    - **Send tokens -** Set to select the output format for UDI data. (default - disabled)
    - **Token separator** - Set to select a separator character. If no separator character is selected when Send tokens is set to Barcodes and tokens, two instances of the same data are sent. (default - none)
    - **Token order** - Set to include or exclude Tokens from the output and adjust their output order.
  - **Multibarcode specific** - Allows the optional insertion of a tab, line feed, or carriage return between each barcode.
    - **Barcode separator** - Set to select a separator character. If no separator character is selected, the data set is sent as a single string.
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See Generating Advanced Data Formatting Rules for more information.

- **Basic data formatting** - Allows the configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled, any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Output

Allows configuration of the Intent Output Plug-in for the profile. The Intent Output Plug-in allows the captured data to be sent to an application in the form of an implicit Intent. Refer to the Android Developer web site for more information, developer.android.com.

- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Intent action** - Enter the Intent Action name (required).
- **Intent category** - Enter the Intent Category name (required).
- **Intent delivery** - Select the method by which the intent is delivered:
  - Send via StartActivity
  - Send via startService (default)
  - Broadcast intent
- **Receiver foreground flag** - Set Broadcast intent flag in Intent delivery. (DS3678).
- **Advanced data formatting** - is a way to customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See Generating Advanced Data Formatting Rules for more information.

- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Intent Overview

The core components of an Android application (its activities, services, and broadcast receivers) are activated by intents. An intent is a bundle of information (an Intent object) describing a desired action - including the data to be acted upon, the category of component that should perform the action, and other pertinent instructions. Android locates an appropriate component to respond to the intent, launches a new instance of the component if one is needed, and passes it the Intent object.

Components advertise their capabilities, the kinds of intents they can respond to, through intent filters. Since the system must learn which intents a component can handle before it launches the component, intent filters are specified in the manifest as <intent-filter>elements. A component may have any number of filters, each one describing a different capability. For example, if the manifest contains the following:

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

In the Intent output plug-in configuration, the **Intent action** would be:
android.intent.action.DEFAULT
and the Intent category would be:
android.intent.category.MAIN.

The **Intent delivery** option allows the method by which the intent is delivered to be specified. The delivery mechanisms are **Send via startActivity**, **Send via startService** or **Broadcast intent**.

The decode related data added to the Intent’s bundle can be retrieved using the **`Intent.getStringExtra()`** and **`Intent.getSerializableExtra()`** calls, using the following String tags:

- String LABEL_TYPE_TAG = “com.symbol.emdk.datawedge.label_type”;
  - String contains the label type of the barcode.

- String DATA_STRING_TAG = “com.symbol.datawedge.data_string”;
  - String contains the output data as a String. In the case of concatenated barcodes, the decode data is concatenated and sent out as a single string.
- String DECODE_DATA_TAG = “com.symbol.datawedge.decode_data”;
  - Decode data is returned as a list of byte arrays. In most cases there will be one byte array per decode. For barcode symbologies that support concatenation, for example, Codabar, Code128, MicroPDF, etc., the decoded data is stored in multiple byte arrays (one byte array per barcode). Clients can get data in each byte array by passing an index.

Most scanning applications might want the user to be able to decode data and for that decode data to be sent to the ***current*** activity but not necessarily displayed. If this is the case, then the activity needs to be marked as ‘singleTop’ in its AndroidManifest.xml file. If your activity is not defined as singleTop, then on every decode, the system will create another copy of your Activity and send the decode data to this second copy.

Finally there will be a configuration option for each process plug-in so that the process plug-in can be configured specifically for the intent output, which in this case is the basic data formatting process plug-in.

IP Output

NOTE: IPWedge application is required on a host computer. Download the IPWedge application from the Support Central web site: www.zebra.com/support.

IP Output allows DataWedge to send captured data to a host computer via a network connection. Captured data can be sent over an IP network to a specified IP address and port using either TCP or UDP transport protocols.

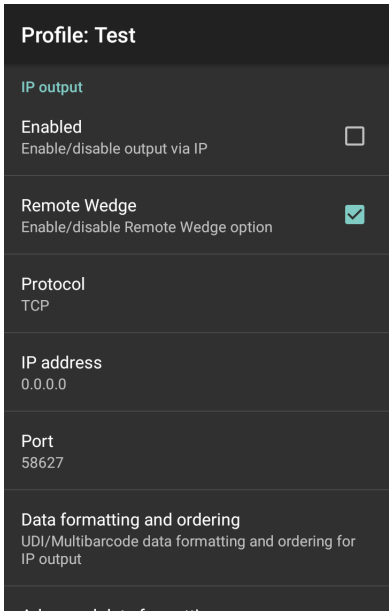
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol used by the remote application. Options: **TCP** (default) or **UDP**.
- **IP address** - Enter the IP address used by the remote application (default - 0.0.0.0).
- **Port** - Enter the port number used by the remote application (default - 58627).
- **Data formatting and ordering** - Allows formatting and ordering of UDI and Multibarcode data.
  - **UDI specific** - Allows the output order of acquired UDI data to be adjusted and the optional insertion of a tab, line feed, or carriage return character between tokens.
    - **Send tokens -** Set to select the output format for UDI data. (default - disabled)
    - **Token separator** - Set to select a separator character. If no separator character is selected when Send tokens is set to Barcodes and tokens, two instances of the same data are sent. (default - none)
    - **Token order** - Set to include or exclude Tokens from the output and adjust their output order.
- **Advanced data formatting** - is a way of customizing data before transmission. Use advanced data formatting (ADF) to edit scan data to suit requirements.
  - **Enable** - Enables or disables ADF. A check in the checkbox indicates that ADF is enabled (default - disabled).
  - **Rules** - ADF uses rules to customize data. These rules perform detailed actions when the data meets certain criteria. One rule may consist of single or multiple criteria applied to single or multiple actions. See Generating Advanced Data Formatting Rules for more information.

- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.
  - **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
  - **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
  - **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Usage

This section provides information on how to configure IP Output using the DataWedge configuration user interface. To use IP Output in a particular DataWedge profile (for example: **Profile0**), scroll downward on **IP Output**.

Figure 87 IP Output Screen



Using IP Output with IPWedge

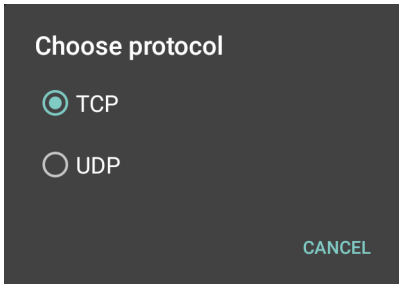
IPWedge is a computer application that can be easily configured to retrieve data sent over network by DataWedge IP Output. Refer to the IPWedge User Manual on how to install and configure in a host computer. To enable IP Output to send captured data to a remote computer that is installed with IPWedge:

1. In **IP Output**, touch **Enabled**.

   A check appears in the checkbox.

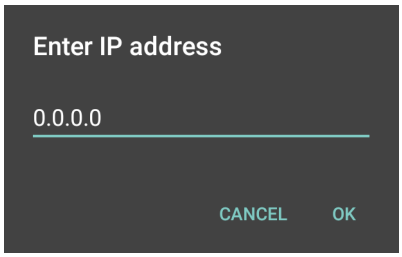
2. Ensure **Remote Wedge** option is enabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected for the IPWedge computer application. (TCP is the default).

Figure 88 Protocol Selection



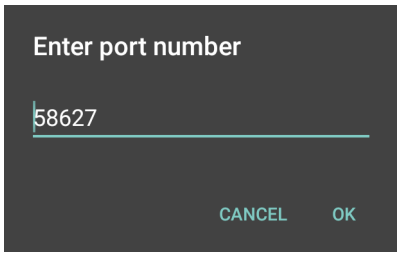
5. Touch **IP Address**.
6. In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.

Figure 89 IP Address Entry



7. Touch **Port**.
8. In the **Enter port number** dialog box, enter same port number selected for IPWedge computer application.

Figure 90 Port Number Entry



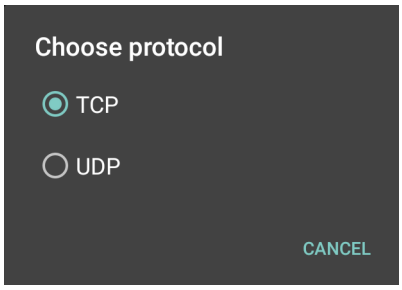
9. Configure **Advanced data formatting** and **Basic data formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

Using IP Output without IPWedge

IP Output Plug-in can be used to send captured data from DataWedge to a remote device or host computer without using IPWedge. At the data receiving end, the host computer or mobile device should have an application, that listens to TCP or UDP data coming from a configured port and IP address in the IP Output plug-in. To enable IP Output to send captured data to a remote computer:

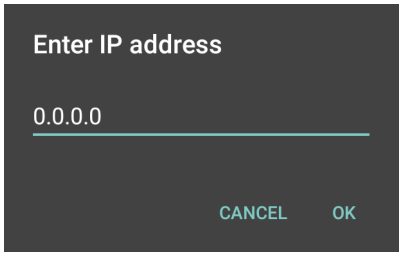
1. In **IP Output**, touch **Enabled**.
   A check appears in the checkbox.
2. Ensure **Remote Wedge** option is disabled.
3. Touch **Protocol**.
4. In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).

Figure 91 Protocol Selection



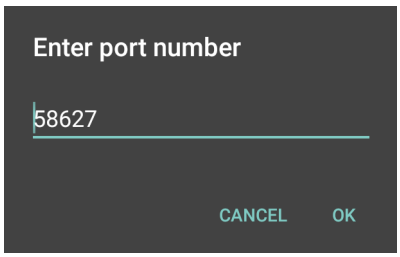
5. Touch **IP Address**.
6. In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.

Figure 92 IP Address Entry



7. Touch **Port**.
8. In the **Enter port number** dialog box, enter the port number that the host computer application is listening on.

Figure 93 Port Number Entry



9. Configure **Advanced Data Formatting** and **Basic Data Formatting** Plug-in if any required modification to be done to captured data before sending to remote computer.

Generating Advanced Data Formatting Rules

The ADF plug-in applies rules (actions to be performed based on defined criteria) to the data received via an input plug-in before sending it to the output plug-in.

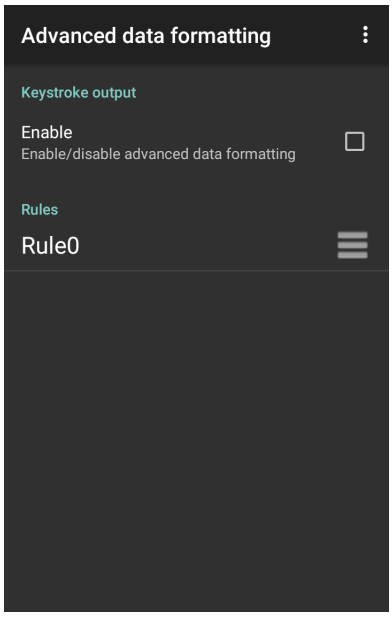
- Rules - The ADF process plug-in consists of one or more rules. DataWedge formats the output data according to the first matching rule. A rule is a combination of criteria and a set of actions to be performed, upon fulfillment of the criteria set in the rule.
- Criteria - Criteria can be set according to Input plug-in, symbology, matching string within the data (at the specified position) and/or data length. Received data must match the defined criteria in order for the data to be processed.
- Actions - A set of procedures defined to format data. There are four types of actions which are for formatting cursor movement, data modification, data sending and delay specifications. An action can be defined to send the first number of characters to the Output plug-in, pad the output data with spaces or zeros, remove spaces in data, etc.

Configuring ADF Plug-in

Configuring the ADF plug-in consists of creating a rule, defining the criteria and defining the actions.

1. Swipe up from the bottom of the screen and touch .
2. Touch a DataWedge profile.
3. In **Keystroke Output**, touch **Advanced data formatting**.

Figure 94 Advanced Data Formatting Screen



4. Touch the **Enable** checkbox to enable ADF.

Creating a Rule

NOTE: By default, **Rule0**, is the only rule in the Rules list.

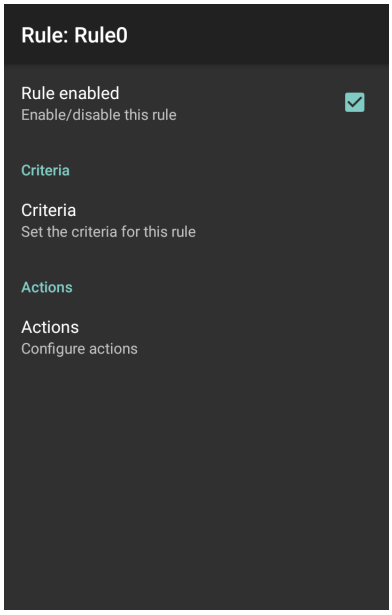
1. Touch .

2. Touch **New rule**.
3. Touch the **Enter rule name** text box.
4. In the text box, enter a name for the new rule.
5. Touch **OK**.

Defining a Rule

1. Touch the newly created rule in the **Rules** list.

Figure 95 Rule List Screen



2. Touch the **Rule enabled** check box to enable the current rule.

Defining an Action

NOTE: By default the **Send remaining** action is in the **Actions** list.

1. Touch ⋮.
2. Touch **New action**.
3. In the **New action** menu, select an action to add to the **Actions** list. See the ADF Supported Actions table for a list of supported ADF actions.
4. Some Actions require additional information. Touch the Action to display additional information fields.
5. Repeat steps to create more actions.
6. Touch ◁.
7. Touch ◁.

Deleting a Rule

1. Touch and hold on a rule until the context menu appears.
2. Touch **Delete rule** to delete the rule from the **Rules** list.

NOTE: When there is no rule available for ADF plug-in or all rules are disabled, DataWedge passes decoded data to the output plug-in without processing the data.

Order Rules List

NOTE: When there are no rules defined, ADF passes the captured data through as is. In contrast, when rules are defined but all are disabled, ADF does not pass any captured data through.

Rules are processed in top-down order. The rules that are on top of the list are processed first. Use the icon next to the rule to move it to another position in the list.

Table 8 ADF Supported Actions

Type	Actions	Description
Cursor Movement	Skip ahead	Moves the cursor forward by a specified number of characters. Enter the number of characters to move the cursor ahead.
	Skip back	Moves the cursor back by a specified number of characters. Enter the number of characters to move the cursor back.
	Skip to start	Moves the cursor to the beginning of the data.
	Move to	Moves the cursor forward until the specified string is found. Enter the string in the data field.
	Move past a	Moves the cursor forward past the specified string. Enter the string in the data field.
Data Modification	Crunch spaces	Remove spaces between words to one and remove all spaces at the beginning and end of the data.
	Stop space crunch	Stops space crunching. This disables the last **Crunch spaces** action.
	Remove all spaces	Remove all spaces in the data.
	Stop space removal	Stop removing spaces. This disables the last **Remove all spaces** action.
	Remove leading zeros	Remove all zeros at the beginning of data.
	Stop zero removal	Stop removing zeros at the beginning of data. This disables the previous **Remove leading zeros** action.
	Pad with zeros	Left pad data with zeros to meet the specified length. Enter the number zeros to pad.
	Stop pad zeros	Stop padding with zeros. This disables the previous **Pad with zeros** action.
	Pad with spaces	Left pad data with spaces to meet the specified length. Enter the number spaces to pad.
	Stop pad spaces	Stop padding with spaces. This disables the previous **Pad with spaces** action.
	Replace string	Replaces a specified string with a new string. Enter the string to replace and the string to replace it with.
	Stop all replace string	Stop all **Replace string** actions.

Table 8 ADF Supported Actions (Continued)

Type	Actions	Description
Data Sending	Send next	Sends the specified number of characters from the current cursor position. Enter the number of characters to send.
	Send remaining	Sends all data that remains from the current cursor position.
	Send up to	Sends all data up to a specified string. Enter the string.
	Send pause	Pauses the specified number of milliseconds before continuing the next action. Enter the amount of time in milliseconds.
	Send string	Sends a specified string. Enter the string to send.
	Send char	Sends a specified ASCII/ Unicode character. Enter a character value. The maximum Unicode character value can be entered is U-10FFFF (= 1114111 in decimal).

Deleting an Action

1. Touch and hold the action name.
2. Select **Delete action** from the context menu.

ADF Example

The following illustrates an example of creating Advanced Data Formatting:

When a user scans a barcode with the following criteria:

- Code 39 barcode.
- length of 12 characters.
- contains 129 at the start position.

Modify the data as follows:

- Pad all sends with zeros to length 8.
- send all data up to character X.
- send a space character.

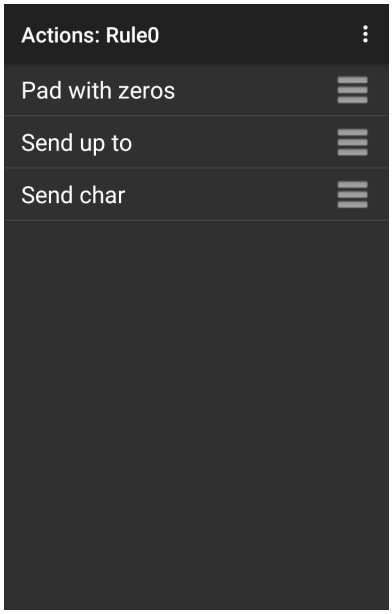
To create an ADF rule for the above example:

1. Swipe up from the bottom of the screen and touch .
2. Touch **Profile0**.
3. Under **Keystroke Output**, touch **Advanced data formatting**.
4. Touch **Enable**.
5. Touch **Rule0**.
6. Touch **Criteria**.
7. Touch **String to check for**.
8. In the **Enter the string to check for** text box, enter `129` and then touch **OK**.
9. Touch **String position**.

10. Change the value to `0`.
11. Touch **OK**.
12. Touch **String length**.
13. Change value to `12`.
14. Touch **OK**.
15. Touch **Source criteria**.
16. Touch **Barcode input**.
17. Touch **All decoders enabled** to disable all decoders.
18. Touch **Code 39**.
19. Press ◁ three times.
20. Touch **Actions**.
21. Touch and hold on the **Send remaining rule** until a menu appears.
22. Touch **Delete action**.
23. Touch ⋮.
24. Touch **New action**.
25. Select **Pad with zeros**.
26. Touch the **Pad with zeros** rule.
27. Touch **How many**.
28. Change value to `8` and then touch **OK**.
29. Press ◁.
30. Touch ⋮.
31. Touch **New action**.
32. Select **Send up to**.
33. Touch **Send up to** rule.
34. Touch **String**.
35. In the **Enter a string** text box, enter `X`.
36. Touch **OK**.
37. Touch ◁.
38. Touch ⋮.
39. Touch **New action**.
40. Select **Send char**.
41. Touch **Send char** rule.
42. Touch **Character code**.

43. In the **Enter character code** text box, enter `32`.
44. Touch **OK**.
45. Touch ◁.

Figure 96 ADF Sample Screen



46. Ensure that an application is open on the device and a text field is in focus (text cursor in text field).
47. Aim the exit window at the barcode.

Figure 97 Sample Barcode



48. Press and hold the scan button.

    The red laser aiming pattern turns on to assist in aiming. Ensure that the barcode is within the area formed by the aiming pattern. The LED light red to indicate that data capture is in process.

49. The LED lights green, a beep sounds and the device vibrates, by default, to indicate the barcode was decoded successfully.The LED lights green and a beep sounds, by default, to indicate the barcode was decoded successfully. The formatted data 000129X<space>appears in the text field.

    Scanning a Code 39 barcode of 1299X15598 does not transmit data (rule is ignored) because the barcode data did not meet the length criteria.

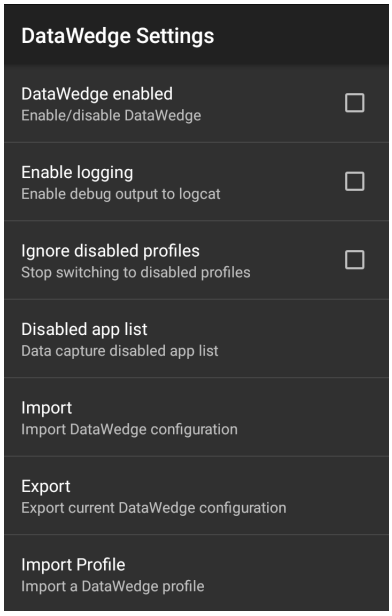
Figure 98 Formatted Data



DataWedge Settings

The DataWedge Settings screen provides access to general, non-profile related options. Touch ⋮ > **Settings**.

Figure 99 DataWedge Settings Window



- **DataWedge enabled** - Enables or disables DataWedge. To disable DataWedge uncheck this option (default - enabled).
- **Enable logging** - Enables or disables debug output file to logcat. To enable logging check this option (default - disabled).

- **Ignore disabled profiles** - Prevents DataWedge from switching to a Profile that is not enabled. In such instances, the Profile switch is ignored and the current Profile remains active Profile0 must be disabled to use this feature (default - disabled).
- **Disable app list** - Disables scanning functions for selected applications or activities.
- **Import** - Allows import of a DataWedge configuration file. The imported configuration replaces the current configuration.
- **Export** - Allows export of the current DataWedge configuration.
- **Import Profile** - Allows import of a DataWedge profile file.
- **Export Profile** - Allows export of a DataWedge profile.
- **Restore** - Return the current configuration back to factory defaults.
- **Reporting** - Configures reporting options.

Importing a Configuration File

1. Copy the configuration file to the microSD card `/Android/data/com.symbol.datawedge/files` folder.
2. Touch ⋮.
3. Touch **Settings**.
4. Touch **Import**.
5. Touch **filename to import**.
   The configuration file (datawedge.db) is imported and replaces the current configuration.

Exporting a Configuration File

1. Touch ⋮.
2. Touch **Settings**.
3. Touch **Export**.
4. In the **Export to** dialog box, select the location to save the file.
5. Touch **Export**. The configuration file (datawedge.db) is saved to the selected location.

Importing a Profile File

NOTE: Do not change the filename of the of the profile file. If the filename is changed, the file will not be imported.

1. Copy the profile file to the On Device Storage `/Android/data/com.symbol.datawedge/files` folder.
2. Touch ⋮.
3. Touch **Settings**.
4. Touch **Import Profile**.
5. Touch the profile file to import.
6. Touch **Import**. The profile file (**dwprofile_x.db**, where x = the name of the profile) is imported and appears in the profile list.

Exporting a Profile

1. Touch ⋮.
2. Touch **Settings**.
3. Touch **Export Profile**.
4. Touch the profile to export.
5. Touch **Export**.
   The profile file (dwprofile_x.db, where x = name of the profile) is saved to the root of the On-device Storage.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

1. Touch ⋮.
2. Touch **Settings**.
3. Touch **Restore**.
4. Touch **Yes**.

Configuration and Profile File Management

The configuration or profile settings for DataWedge can be saved to a file for distribution to other devices.

After making configuration or profile changes, export the new configuration or profile to the root of the On-device Storage. The configuration file created is automatically named datawedge.db. The profile file created is automatically named dwprofile_x.db, where x is the profile name. The files can then the copied to the On-device Storage of other devices and imported into DataWedge on those devices. Importing a configuration or profile replaces the existing settings.

Enterprise Folder

Internal storage contains the Enterprise folder (**`/enterprise`**). The Enterprise folder is persistent and maintains data after an Enterprise reset. After an Enterprise Reset, DataWedge checks folder **`/enterprise/device/settings/datawedge/enterprisereset/`** for a configuration file, datawedge.db or a profile file, dwprofile_x.db. If the file is found, it imports the file to replace any existing configuration or profile.

NOTE: A Factory Reset deletes all files in the Enterprise folder.

Auto Import

DataWedge supports remote deployment of a configuration to a device, using tools such as commercially available third-party Mobile Device Management (MDM) systems. DataWedge monitors the **`/enterprise/device/settings/datawedge/autoimport`** folder for the DataWedge configuration file (datawedge.db) or a profile file (dwprofile_x.db). If a configuration or profile file is found, it imports the file to replace any existing configuration or profile. Once the file has been imported it is deleted from the folder. DataWedge begins using the imported configuration immediately.

NOTE: A Factory Reset deletes all files in the **/enterprise** folder.

It is strongly recommended that the user exits DataWedge before remotely deploying any configuration or profile. It is required that the file permissions are set to 666.

The **/enterprise** folder cannot be seen with **Files** app or other user-level tools. Moving configuration files to and from the **/autoimport** or **/enterprisereset** folders must be done programmatically, or with a staging client app or MDM.

Programming Notes

The following paragraphs provide specific programming information when using DataWedge.

Overriding Trigger Key in an Application

To override the trigger key in an application, create a profile for the application that disables the Barcode input. In the application, use standard APIs, such as onKeyDown() to listen for the KEYCODE_BUTTON_L1 and KEYCODE_BUTTON_R1 presses.

Capture Data and Taking a Photo in the Same Application

To be able to capture bar code data and take a photo in the same application:

- Create a Datawedge profile pertaining to the picture taking Activity in your application that disables scanning and use standard Android SDK APIs to control the Camera.
- The default Datawedge profile takes care of the scanning in the application. You might want to create another DataWedge profile that caters to any specific scanning needs, associated to your Application's Activity pertaining to scanning.

Disabling DataWedge

1. Swipe up from the bottom of the screen and touch .
2. Touch .
3. Touch **Settings**.
4. Touch **DataWedge enabled**.

The blue check disappears from the checkbox indicating that DataWedge is disabled.

Soft Scan Trigger

DataWedge allows a native Android application to programmatically start, stop, or toggle the scan trigger state. The application can issue an Android Broadcast Intent, to control the scanner, without requiring the scan key to be pressed. The active DataWedge profile is required to control all the parameters during a scan operation.

Function Prototype

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

Scanner Input Plugin

The ScannerInputPlugin API command can be used to enable/disable the scanner plug-in being used by the currently active Profile. Disabling the scanner plug-in effectively disables scanning in that Profile, regardless of whether the Profile is associated or unassociated. Valid only when Barcode Input is enabled in the active Profile.

NOTE: Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile.

Function Prototype

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

Parameters

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

extra_data: String "com.symbol.datawedge.api.SCANNER_INPUT_PLUGIN"

<parameter>: The parameter as a string, using either of the following:

- SUSPEND_PLUGIN - suspends the scanner so it is temporarily inactive when switching from the WAITING or SCANNING state. SCANNER_STATUS notification broadcasts IDLE state.
- RESUME_PLUGIN - resumes the scanner when changing from the SUSPEND_PLUGIN suspended state. SCANNER_STATUS notification broadcasts WAITING and SCANNING states, rotating between each depending on whether scanning is taking place. In the WAITING state it is expecting an action from the user such as a trigger press. In the SCANNING state it is actively performing a scan resulting from an action such as a trigger press.
- "ENABLE_PLUGIN" - enables the plug-in the scanner becomes active.
- "DISABLE_PLUGIN" - disables the plug-in the scanner becomes inactive.

Return Values

None.

Error and debug messages will be logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages, for example:

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

Error messages will be logged for invalid actions and parameters.

Example

```
// define action and data strings
String scannerInputPlugin = "com.symbol.datawedge.api.ACTION_SCANNERINPUTPLUGIN";
String extraData = "com.symbol.datawedge.api.EXTRA_PARAMETER";

public void onResume() {
   // create the intent
   Intent i = new Intent();
   // set the action to perform
   i.setAction(scannerInputPlugin);
   // add additional info
   i.putExtra(extraData, "DISABLE_PLUGIN");
   // send the intent to DataWedge
   context.sendBroadcast(i);
}
```

Comments

This intent API allows the scanner plug-in for the current Profile to be enabled or disabled. For example, activity A launches and uses the intent API to switch to ProfileA in which the scanner plug-in is enabled, then at some point it uses the Data Capture API to disable the scanner plug-in. Activity B is launched. In DataWedge, ProfileB is associated with activity B. DataWedge switches to ProfileB. When activity A comes back to the foreground, in the **onResume** method, activity A needs to use the intent API to switch back to ProfileA, then use the intent API again to disable the scanner plug-in, to return back to the state it was in.

NOTE: Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile. The above assumes that ProfileA is not associated with any applications/activities, therefore when focus switches back to activity A, DataWedge will not automatically switch to ProfileA therefore activity A must switch back to ProfileA in its onResume method. Because DataWedge will automatically switch Profile when an activity is paused, it is recommended that this API function be called from the onResume method of the activity.

Enumerate Scanners

Use the enumerateScanners API command to get a list of scanners available on the device.

Function Prototype

```
Intent i = new Intent();
i.setAction("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.ENUMERATE_SCANNERS", "");
```

Parameters

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

Return Values

The enumerated list of scanners will be returned via the broadcast Intent "com.symbol.datawedge.api.ACTION_ENUMERATEDSCANNERLIST". The list of scanners is returned as a string array (see the example below).

Error and debug messages are logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages. For example:

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

Error messages are logged for invalid actions and parameters.

Example

```
//
//  Call before sending the enumeration query
//
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);
}
//
// Send the enumeration command to DataWedge
//
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);
}

//
// Create broadcast receiver to receive the enumeration result
//
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")){
            //
            // enumerate scanners
            //
            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]);
                    }
                }
            }
        }
    }
};
```

Comments

The scanner and its parameters are set based on the currently active Profile.

Set Default Profile

Use the setDefaultProfile API function to set the specified Profile as the default Profile.

Default Profile Recap

Profile0 is the generic Profile used when there are no user created Profiles associated with an application.

Profile0 can be edited but cannot be associated with an application. That is, DataWedge allows manipulation of plug-in settings for Profile0 but it does not allow assignment of a foreground application. This configuration allows DataWedge to send output data to any foreground application other than applications associated with user-defined Profiles when Profile0 is enabled.

Profile0 can be disabled to allow DataWedge to only send output data to those applications which are associated in user-defined Profiles. For example, create a Profile associating a specific application, disable Profile0 and then scan. DataWedge only sends data to the application specified in the user-created Profile. This adds additional security to DataWedge enabling the sending of data only to specified applications.

Usage Scenario

A launcher application has a list of apps that a user can launch and that none of the listed apps has an associated DataWedge Profile. Once the user has selected an app, the launcher needs to set the appropriate DataWedge Profile for the selected app. This could be done by using **`setDefaultProfile`** to set the default Profile to the required Profile. Then when the user launches the selected app, DataWedge auto Profile switching switches to the default Profile (which is now the required Profile for that app).

If, for some reason, the launched app has an associated DataWedge Profile then that will override the set default Profile.

When control is returned to the launcher application, **`resetDefaultProfile`** can be used to reset the default Profile.

Function Prototype

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

Parameters

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

EXTRA_DATA [String]: "com.symbol.datawedge.api.SET_DEFAULT_PROFILE"

<profile name>: The Profile name (a case-sensitive string) to set as the default Profile.

Return Values

None.

Error and debug messages are logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages. For example:

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

Error messages are logged for invalid actions, parameters and failures, for example, Profile not found or associated with an application.

Example

```
// define action and data strings
String setDefaultProfile = "com.symbol.datawedge.api.ACTION";
String extraData = "com.symbol.datawedge.api.SET_DEFAULT_PROFILE";

public void onResume() {
        // create the intent
        Intent i = new Intent();

        // set the action to perform
        i.setAction(setDefaultProfile);

        // add additional info (a name)
        i.putExtra(extraData, "myProfile");

        // send the intent to DataWedge
        this.sendBroadcast(i);
}
```

Comments

The API command has no effect if the specified Profile does not exist or if the specified Profile is already associated with an application. DataWedge automatically switches Profiles when the activity is paused, so it is recommended that this API function is called from the onResume method of the activity.

Zebra recommends that this Profile is created to cater to all applications/activities that would otherwise default to using Profile0. This ensures that these applications/activities continue to work with a consistent configuration.

Reset Default Profile

Use the resetDefaultProfile API function to reset the default Profile back to Profile0.

Function Prototype

```
Intent i = new Intent();
i.setAction("com.symbol.datawedge.api.ACTION");
i.putExtra("com.symbol.datawedge.api.RESET_DEFAULT_PROFILE", "");
```

Parameters

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

EXTRA_DATA [String]: "com.symbol.datawedge.api.RESET_DEFAULT_PROFILE".

Return Values

None.

Error and debug messages are logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages. For example:

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

Error messages are logged for invalid actions, parameters and failures, for example, Profile not found or associated with an application.

Example

```
// define action string
String action = "com.symbol.datawedge.api.ACTION";
String extraData = "com.symbol.datawedge.api.RESET_DEFAULT_PROFILE";

public void onResume() {
    // create the intent
    Intent i = new Intent();

    // set the action to perform
    i.setAction(action);
    i.putExtra(extraData, ""); // empty since a name is not required
    this.sendBroadcast;
}
```

Comments

None.

Switch To Profile

Use the SwitchToProfile API action to switch to the specified Profile.

Profiles Recap

DataWedge is based on Profiles and plug-ins. A Profile contains information on how DataWedge should behave with different applications.

Profile information consists of:

- Associated application
- Input plug-in configurations
- Output plug-in configurations
- Process plug-in configurations

DataWedge includes a default Profile, Profile0, that is created automatically the first time DataWedge runs.

Using Profiles, each application can have a specific DataWedge configuration. For example, each user application can have a Profile which outputs scanned data in the required format when that application comes to the foreground. DataWedge can be configured to process the same set of captured data differently based on the requirements of each application.



NOTE: Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile. A single Profile may be associated with one or many activities/apps, however, given an activity, only one Profile may be associated with it.

Usage Scenario

An application has two activities. Activity A only requires EAN13 bar codes to be scanned. Activity B only requires Code 128 bar codes to be scanned. Profile EAN13 is configured to only scan EAN13 bar codes and is left unassociated. Profile Code128 is configured to scan Code 128 and is left unassociated. When Activity A launches it uses SwitchToProfile to activate Profile EAN13. Similarly, when Activity B launches it uses switchToProfile to activate Profile Code128.

If another activity/app comes to the foreground, DataWedge auto Profile switching sets the DataWedge Profile accordingly either to the default Profile or to an associated Profile.

When Activity A (or Activity B) comes back to the foreground it uses switchToProfile to reset the Profile back to Profile B (or Profile M).

Function Prototype

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

Parameters

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

EXTRA_DATA [String]: "com.symbol.datawedge.api.SWITCH_TO_PROFILE"

<profile name>: The Profile name (a case-sensitive string) to set as the active Profile.

Return Values

None.

Error and debug messages are logged to the Android logging system which then can be viewed and filtered by the logcat command. You can use logcat from an ADB shell to view the log messages. For example:

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

Error messages are logged for invalid actions, parameters and failures, for example, Profile not found or associated with an application.

Example

```
// define action and data strings
String switchToProfile = "com.symbol.datawedge.api.ACTION";
String extraData = "com.symbol.datawedge.api.SWITCH_TO_PROFILE";

public void onResume() {
        super.onResume();

        // create the intent
        Intent i = new Intent();

        // set the action to perform
        i.setAction(switchToProfile);

        // add additional info
        i.putExtra(extraData, "myProfile");

        // send the intent to DataWedge
        this.sendBroadcast(i);
}
```

Comments

This API function has no effect if the specified Profile does not exist or is already associated with an application.

DataWedge has a one-to-one relationship between Profiles and activities; a Profile can be associated only with a single activity. When a Profile is first created, it's not associated with any application, and is not activated until associated. This makes it possible to create multiple unassociated Profiles.

This API function activates such Profiles.

For example, Profile A is unassociated and Profile B is associated with activity B. If activity A is launched and uses **`SwitchToProfile`** function to switch to Profile A, then Profile A is active whenever activity A is in the foreground. When activity B comes to the foreground, DataWedge automatically switches to Profile B.

When activity A returns to the foreground, the app must use **`SwitchToProfile`** again to switch back to Profile A. This would be done in the **`onResume`** method of activity A.

NOTE: Use of this API changes only the runtime status of the scanner; it does not make persistent changes to the Profile.

Notes

Because DataWedge automatically switches Profile when the activity is paused, Zebra recommends that this API function is called from the onResume method of the activity.

After switching to a Profile, this unassociated Profile does not get assigned to the application/activity and is available to use in the future with a different app/activity.

For backward compatibility, DataWedge's automatic Profile switching is not affected by the above API commands. This why the commands work only with unassociated Profiles and apps.

DataWedge auto Profile switching works as follows:

Every second…

- Sets newProfileId to the associated Profile ID of the current foreground activity.
- If no associated Profile is found, sets newProfileId to the associated Profile ID of the current foreground app.
- If no associated Profile is found, sets newProfileId to the current default Profile (which MAY NOT be Profile0).
- Checks the newProfileId against the currentProfileId. If they are different:
  - deactivates current Profile
  - activates new Profile (newProfileId)
  - sets currentProfileId = newProfileId

Settings

Introduction

This chapter describes settings available for configuring the device.

WLAN Configuration

This section provides information on configuring Wi-Fi settings.

Configuring a Secure Wi-Fi Network

To set up a Wi-Fi network:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Network & Internet** > **Wi-Fi**.
3. Slide the switch to the **ON** position.
4. The device searches for WLANs in the area and lists them on the screen.
5. Scroll through the list and select the desired WLAN network.
6. Touch the desired network. If the network security is **Open**, the device automatically connects to the network. For all other network security a dialog box appears.

Figure 100 WLAN WEP Network Security Dialog Box

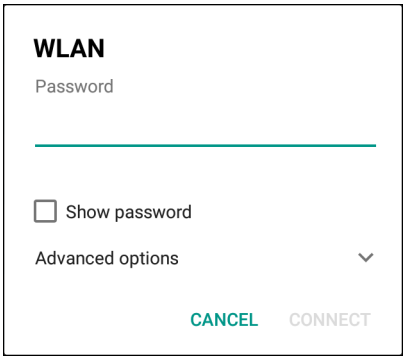
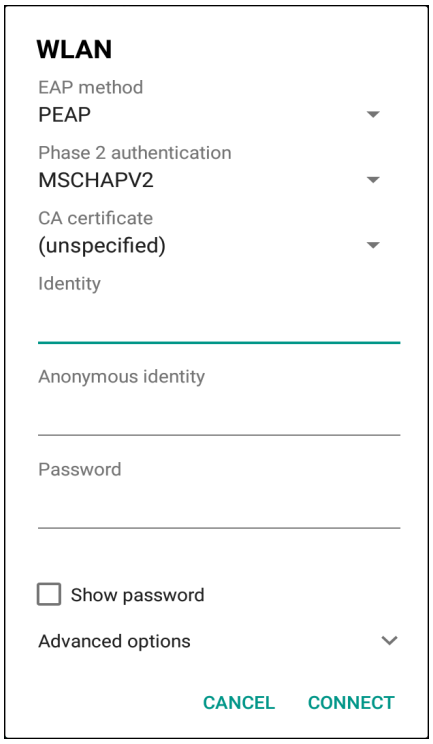


Figure 101 WLAN 802.11 EAP Network Security Dialog Box



7. If the network security is **WEP** or **WPA/WPS2 PSK**, enter the required password and then touch **Connect**.
8. If the network security is 802.1x EAP:
   - Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **or TTLS**.
   - Touch the **Phase 2 authentication** drop-down list and select an authentication method.
   - If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.
   - If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the Location & security settings.
   - If required, in the **Identity** text box, enter the username credentials.
   - If desired, in the **Anonymous identity** text box, enter an anonymous identity username.
   - If required, in the **Password** text box, enter the password for then given identity.

NOTE: By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See Configuring for a Proxy Server for setting connection to a proxy server and see Configuring the Device to Use a Static IP Address for setting the device to use a static IP address.

9. Touch **Connect**.
10. Touch ◯.

Manually Adding a Wi-Fi Network

Manually add a Wi-Fi network if the network does not broadcast its name (SSID) or add a Wi-Fi network when out of range.

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.

2. Touch **Network & Internet** > **Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. Scroll to the bottom of the list and select **Add network**.
5. In the **Network name** text box, enter the name of the Wi-Fi network.
6. In the **Security** drop-down list, set the type of security to:
   - **None**
   - **WEP**
   - **WPA/WPA2 PSK**
   - **802.1x EAP**.
7. If the network security is **None**, touch **Save**.
8. If the network security is **WEP** or **WPA/WPA2 PSK**, enter the required password, and then touch **Save**.
9. If the network security is **802.1x EAP**:
   - Touch the **EAP method** drop-down list and select **PEAP**, **TLS**, **or TTLS**.
   - Touch the **Phase 2 authentication** drop-down list and select an authentication method.
   - If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.
   - If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the **Security** settings.
   - If required, in the **Identity** text box, enter the username credentials.
   - If desired, in the **Anonymous** identity text box, enter an anonymous identity username.
   - If required, in the **Password** text box, enter the password for the given identity.

NOTE: By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See Configuring for a Proxy Server for setting connection to a proxy server and see Configuring the Device to Use a Static IP Address for setting the device to use a static IP address.

10. Touch **Save**. To connect to the saved network, touch and hold on the saved network and select **Connect to network**.
11. Touch ◯.

Configuring for a Proxy Server

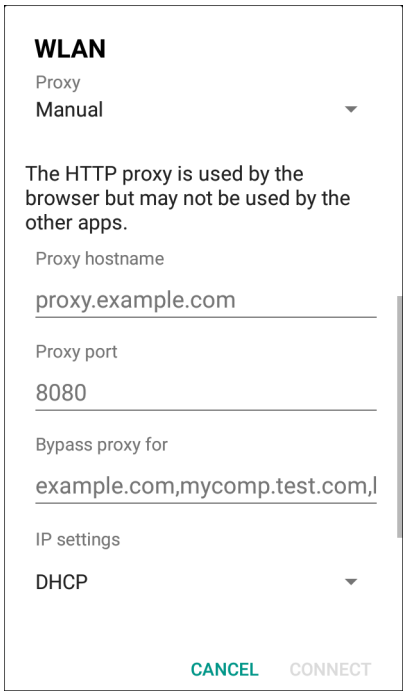
A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server and requests some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

It is important for enterprise customers to be able to set up secure computing environments within their companies, making proxy configuration essential. Proxy configuration acts as a security barrier ensuring that the proxy server monitors all traffic between the Internet and the intranet. This is normally an integral part of security enforcement in corporate firewalls within intranets.

To configure the device for a proxy server:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Network & Internet** > **Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. In the network dialog box, select and touch a network.
5. Touch **Advanced options**.
6. Touch **Proxy** and select **Manual**.

Figure 102 Proxy Settings



7. In the **Proxy hostname** text box, enter the address of the proxy server.
8. In the **Proxy port** text box, enter the port number for the proxy server.
9. In the **Bypass proxy for** text box, enter addresses for web sites that are not required to go through the proxy server. Use a comma "," between addresses. Do not use spaces or carriage returns between addresses.
10. Touch **Connect**.
11. Touch ◯.

Configuring the Device to Use a Static IP Address

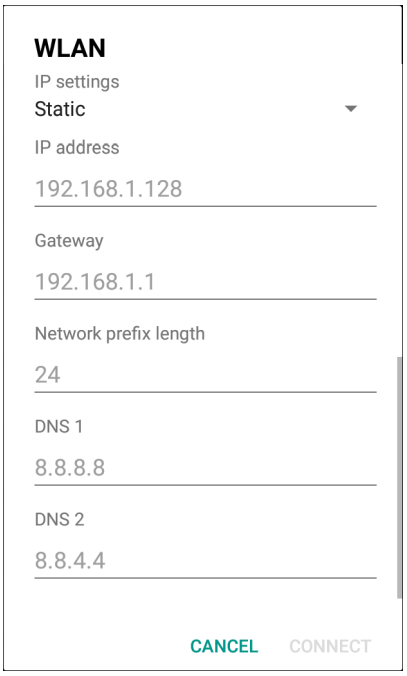
By default, the device is configured to use Dynamic Host Configuration Protocol (DHCP) to assign an Internet protocol (IP) address when connecting to a wireless network.

To configure the device to connect to a network using a static IP address:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Network & Internet** > **Wi-Fi**.

3. Slide the Wi-Fi switch to the **On** position.
4. In the network dialog box, select and touch a network.
5. Touch **Advanced options**.
6. Touch **IP settings** and select **Static**.

Figure 103 Static IP Settings



7. In the **IP address** text box, enter an IP address for the device.
8. If required, in the **Gateway** text box, enter a gateway address for the device.
9. If required, in the **Network prefix length** text box, enter the prefix length.
10. If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.
11. If required, in the **DNS 2** text box, enter a DNS address.
12. Touch **Connect**.
13. Touch ◯.

Wi-Fi Preferences

Use the **Wi-Fi preferences** to configure advanced Wi-Fi settings. From the Wi-Fi screen scroll down to the bottom of the screen and touch **Wi-Fi preferences**.

- **Open network notification** - When enabled, notifies the user when an open network is available.
- **Advanced - Touch to expand options.**
  - **Additional settings** - See Additional Settings.
  - **Install Certificates** – Touch to install certificates.
  - **Network rating provider** - Disabled (AOSP devices). To help determine what constitutes a good Wi-Fi network, Android supports external Network rating providers that provide information about the quality of

open Wi-Fi networks. Select one of the providers listed or **None**. If none are available or selected, the Connect to open networks feature is disabled.

- **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **IP address** - Displays the IP address of the device when connecting to Wi-Fi networks.

Additional Wi-Fi Settings

NOTE: Additional Wi-Fi settings are for the device, not for a specific wireless network.

Use the **Additional Settings** to configure additional Wi-Fi settings. To view the additional Wi-Fi settings, scroll to the bottom of the **Wi-Fi** screen and touch **Wi-Fi Preferences > Advanced > Additional settings.**

- **Regulatory**
  - **Country Selection** - Displays the acquired country code if 802.11d is enabled, else it displays the currently selected country code.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - Set the frequency band to: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
- **Logging**
  - **Advanced Logging** – Touch to enable advanced logging or change the log directory.
- **About**
  - **Version** - Displays the current Fusion information.

Setting Screen Lock

Use the **Device security** settings to set preferences for locking the screen.

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Security & location**.

NOTE: Options vary depending upon the policy of some apps, such as email.

- **Screen lock** - Touch to configure the device to require a slide, pattern, PIN, or password to unlock the screen.
  - **None** - Disable screen unlock security.
  - **Swipe** - Slide the lock icon to unlock the screen.
  - **Pattern** - Draw a pattern to unlock screen. See Setting Screen Unlock Using Pattern for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See Setting Screen Lock Using PIN for more information.
  - **Password** - Enter a password to unlock screen. See Setting Screen Unlock Using Password for more information.

Lock the screen to protect access to data on the device. Some email accounts require locking the screen. The Locking feature functions differently in Single-user versus Multiple-user mode.

When locked, a slide, pattern, PIN or password is required to unlock the device. Press the Power button to lock the screen. The device also locks after a pre-defined time-out.

Press and release the Power button to wake the device. The Lock screen displays.

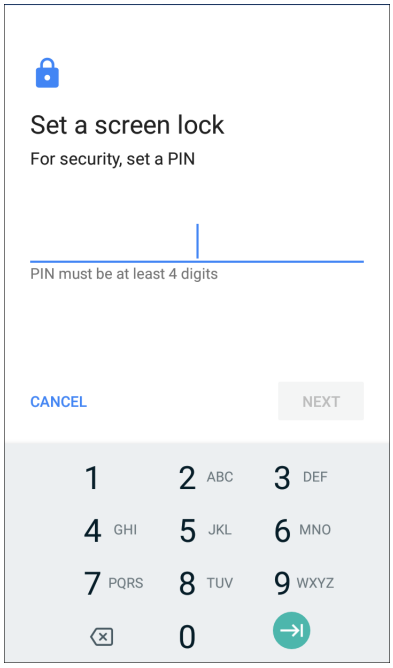
Slide the screen up to unlock. If the Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen.

If the PIN or Password screen unlock feature is enabled, enter the PIN or password after unlocking the screen.

Setting Screen Lock Using PIN

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **PIN**.
5. To require a PIN upon device start up select **Yes**, or select **No** not to require a PIN.

Figure 104 PIN Screen

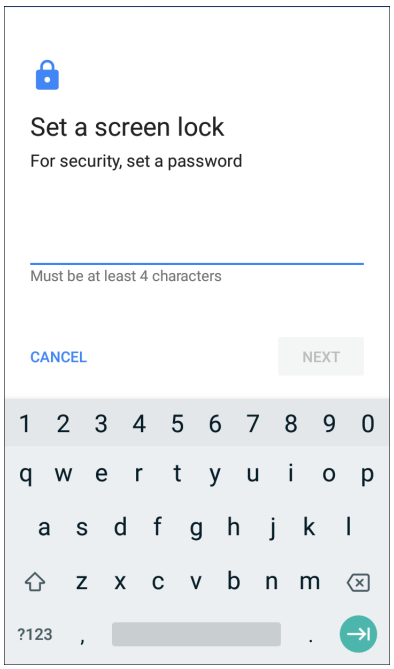


6. Touch in the text field.
7. Enter a PIN (4 numbers), and then touch **Next**.
8. Re-enter PIN and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch ○. The next time the device goes into suspend mode a PIN is required upon waking.

Setting Screen Unlock Using Password

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Password**.
5. To require a password upon device start up select **Yes**, or select **No** not to require a password.
6. Touch in the text field.
7. Enter a password (between 4 and 16 characters), and then touch **Next**.

Figure 105 Password Screen

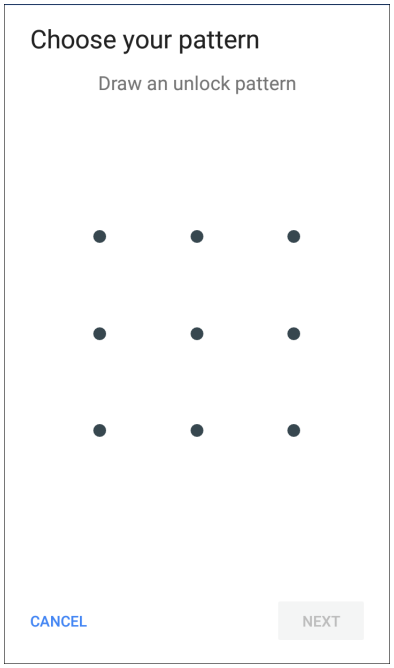


8. Re-enter the password and then touch **Next**.
9. Select the type of notifications that appear when the screen is locked and then touch **Done**.
10. Touch ○. The next time the device goes into suspend mode a password is required upon waking.

Setting Screen Unlock Using Pattern

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **Security & location**.
3. Touch **Screen lock**.
4. Touch **Pattern**.
5. To require a pattern upon device start up select **Yes**, or select **No** not to require a pattern.

Figure 106 Choose Your Pattern Screen



6. Draw a pattern connecting at least four dots.
7. Touch **Continue**.
8. Re-draw the pattern.
9. Touch **Confirm**.
10. Select the type of notifications that appear when the screen is locked, and then touch **Done**.
11. Touch ◯. The next time the device goes into suspend mode a pattern is required upon waking.

Passwords

To set the device to briefly show password characters as the user types:

Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙ > **Security & location**. Slide the **Show passwords** switch to the ON position.

Accounts

Use the **Accounts** settings to add, remove, and manage accounts. Use these settings to control how applications send, receive, and sync data on their own schedules, and whether applications can synchronize user data automatically.

Applications may also have their own settings to control how they synchronize data; see the documentation for those applications for details.

Language Usage

Use the **Language & input** settings to change the device's language, including words added to the dictionary.

Changing the Language Setting

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **System** > **Languages & input**.
3. Touch **Languages**. A list of available languages displays.
4. If the desired language is not listed, touch **Add a language** and select a language from the list.
5. Touch and hold ☰ to the right of the desired language, then drag it to the top of the list.
6. The operating system text changes to the selected language.

Adding Words to the Dictionary

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **System** > **Languages & input** > **Advanced** > **Personal dictionary**.
3. If prompted, select the language where this word or phase is stored.
4. Touch **+** to add a new word or phrase to the dictionary.
5. Enter the word or phrase.
6. In the **Shortcut** text box, enter a shortcut for the word or phrase.
7. Touch ◯.

Keyboard Settings

Use the **Languages & input** settings to configure the on-screen keyboards. The device contains the following keyboard settings:

- Android Keyboard - AOSP devices only
- Enterprise Keyboard
- Gboard - GMS devices only.

Button Remapping

The TC20's buttons and the TC20K buttons and keys can be programmed to perform different functions or shortcuts to installed applications.

NOTE: It is not recommended to remap the scan button.

The center Scan button cannot be remapped.

TC20 buttons:

- Left Scan button (LEFT_TRIGGER_1)
- PTT button (LEFT_TRIGGER_2)
- Right Scan button (RIGHT_TRIGGER_1).

TC20K buttons and keys:

- Left Scan button (LEFT_TRIGGER_1)
- PTT button (LEFT_TRIGGER_2)
- P1 key (SYMBOL_TRIGGER_1)
- P2 key (SYMBOL_TRIGGER_2)
- P3 key (SYMBOL_TRIGGER_3)
- P4 key (SYMBOL_TRIGGER_4)
- Right Scan button (RIGHT_TRIGGER_1).

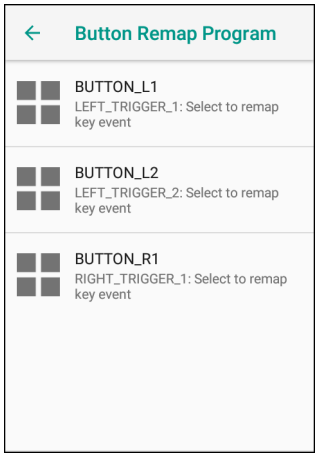
Remapping a Button

Buttons on the device can be programmed to perform different functions or as shortcuts to installed apps.

NOTE: It is not recommended to remap the scan button.

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Key Programmer**. A list of programmable buttons displays.

Figure 107 TC25 Button Remap Program Screen



3. Select the button to remap.

Figure 108 KeyProgrammer Screen



4. Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.
5. Touch a function or application shortcut to map to the button.

NOTE: If you select an application shortcut, the application icon appears next to the button on the Key Programmer screen.

6. Touch ◯.

PTT Express Configuration

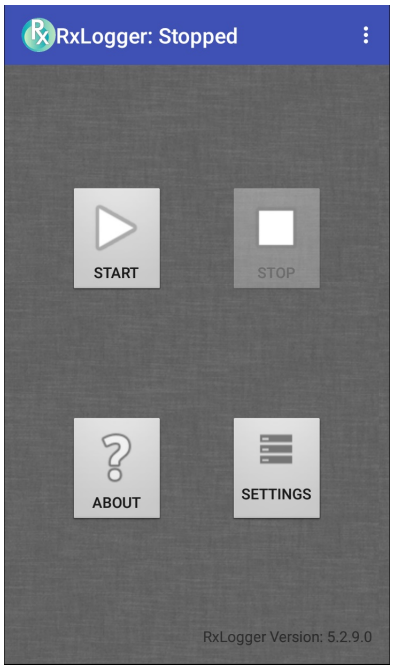
Refer to the PTT Express User Guide at www.zebra.com/support for information on configuring the PTT Express Client application.

RxLogger

RxLogger is a comprehensive diagnostic tool that provides application and system metrics, allows for the creation of custom plug-ins, and diagnoses device and application issues. RxLogger logs the following information: CPU load, memory load, memory snapshots, battery consumption, power states, wireless logging,

cellular logging, TCP dumps, Bluetooth logging, GPS logging, logcat, FTP push/pull, ANR dumps, etc. All generated logs and files are saved onto flash storage on the device (internal or external).

Figure 109 RxLogger

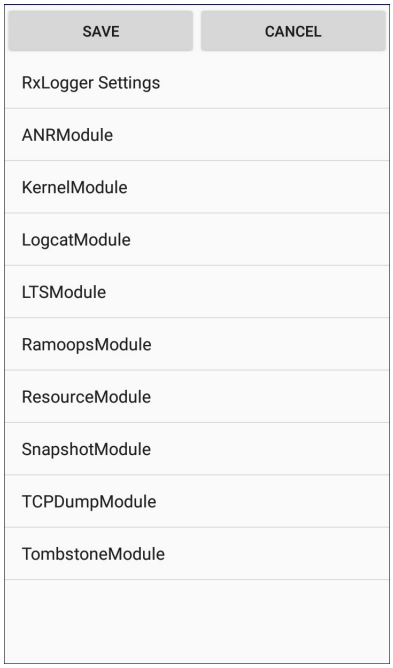


RxLogger Configuration

RxLogger is built with an extensible plug-in architecture and comes packaged with a number of plug-ins already built-in. The included plug-ins are described below.

To open the configuration screen, from the RxLogger home screen touch **Settings**.

Figure 110 RxLogger Configuration Screen



RxLogger Settings

The RxLogger Settings module provides additional RxLogger settings.

- **Enable notifications** - Select to allow RxLogger notifications in the Status bar and Notification panel.
- **Enable debug logs** - Select to enable debug logs.

ANR Module

Application Not Responsive (ANR) indicates that a running application's UI thread is not responding for a specified time period. RxLogger is able to detect this condition and trigger a copy of the call stack trace of the unresponsive application into the log directory. The event is also indicated in the high level CSV log.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the default log path to store the ANR log files.
- **Collect Historic ANRs** - Collects ANR trace files from the system.

Kernel Module

The Kernel Module captures kmsg from the system.

- **Enable Module** - Enables logging for this kernel module.
- **Log path** - Specifies the high level log path for storage of all kernel logs. This setting applies globally to all kernel buffers.
- **Kernel Log filename** - Specifies the base log filename for this kernel buffer. The current file count is appended to this name.
- **Max Kernel log file size** - Specifies the maximum size, in megabytes, of an individual log file.
- **Kernel Log interval** - Sets the interval, in seconds, on which to flush the log buffer to the file.

- **Kernel Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
- **Enable System Timestamp in Kernel Log** - Enables system timestamps in kernel logs.
- **System Timestamp Interval** - Sets the interval, in seconds, between system timestamps.
- **Enable Logcat Integration override** - Enables logcat integration overrides.

Logcat Module

Logcat is an essential debugging tool on Android devices. RxLogger provides the ability to record data from all four of the available logcat buffers. The Logcat plug-in can collect data from multiple logcat buffers provided by the system, which are the main, event, radio, and system buffers. Each of the settings are available for each buffer independently unless otherwise noted.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.
- **Enable main logcat** - Enables logging for this logcat buffer.
  - **Main Log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Main Log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Main Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Main log file size (MB)** - Specifies the maximum size, in megabytes, of an individual log file.
  - **Main log filter** - Custom logcat filter to run on the main buffer.
- **Enable event logcat** - Enables event logging for this logcat buffer.
  - **Event log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Event log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Event log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Event log file size (MB)** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Event log filter** - Custom logcat filter to run on the event buffer.
- **Enable radio logcat** - Enables logging for this logcat buffer.
  - **Radio log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Radio log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Radio log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Radio log file size (MB)** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **Radio log filter** -Custom logcat filter to run on the radio buffer.

- **Enable system logcat** - Enables logging for this logcat buffer.
  - **System log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **System log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **System log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **System log file size (MB)** - Specifies the maximum size, in kilobytes, of an individual log file.
  - **System log filter** - Custom logcat filter to run on the system buffer.
- **Enable crash logcat**- Enables logging for this crash logcat buffer.
  - **Crash log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Crash log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Crash log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Crash log file size (MB)** - Specifies the maximum size, in megabytes, of an individual log file.
  - **Crash log filter** - Custom logcat filter to run on the crash buffer.
- **Enable combined logcat** - Enables logging for this logcat buffer.
  - **Enable main buffer** - Enable or disable the addition of the main buffer into the combined logcat file.
  - **Enable event buffer** - Enable or disable the addition of the event buffer into the combined logcat file.
  - **Enable radio buffer** - Enable or disable the addition of the radio buffer into the combined logcat file.
  - **Enable system buffer** - Enable or disable the addition of the system buffer into the combined logcat file.
  - **Enable crash buffer** - Enable or disable the addition of the crash buffer into the combined logcat file.
  - **Combine log interval (sec)** - Sets the interval, in seconds, on which to flush the log buffer to the file.
  - **Combined log filename** - Specifies the base log filename for this logcat buffer. The current file count is appended to this name.
  - **Combined log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
  - **Combined log file size (MB)** - Specifies the maximum size, in megabytes, of an individual log file.
  - **Combined log filter** - Custom logcat filter to run on the combined buffer.

LTS Module

The LTS (Long Term Storage) Module captures data over a long duration of time without losing any data. Whenever a file is done being written, LTS saves it as a GZ file in an organized path for later use.

- **Enable Module** - Enables logging for this module.
- **Storage Directory** - Specifies the high level log path for storage of all logcat logs. This setting applies globally to all logcat buffers.

Qxdm Module

The Ramoops Module captures Qualcomm Modem Logs from the device.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the storage path for Qxdm files.
- **Qxdm Log Size** - Specifies the maximum size, in kilobytes, of an individual log file.
- **Qxdm test sets to keep** - Specifies the number of test sets to keep. One test set is a start and stop.

- **Choose Log Filter** - Select which filter Qxdm uses to process logs.
- **Path for User Defined Filter** - Specifies the path to a user-defined configuration file.

Ramoops Module

The Ramoops Module captures the last kmsg from the device.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the high level log path for storage of all ramoops logs. This setting applies globally to all Ramoops buffers.
- **Base filename** - Specifies the base log filename for this kernal buffer. The current file count is appended to this name.
- **Ramoops file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the log size option.

Resource Module

The Resource Module captures device information and system statistics at specified intervals. The data is used to determine the health of the device over a period of time.

- **Enable Module** - Enables logging for this module.
- **Log Path** - Specifies the high level log path for storage of all resource logs. This setting applies globally to all resource buffers.
- **Resource Log interval** - Sets the interval, in seconds, on which to flush the log buffer to the file.
- **Resource Log file size** - Specifies the maximum size, in megabytes, of an individual log file.
- **Resource Log file count** - Specifies the number of log files to keep and rotate through. Each log file is subject to the max log size option.
- **Power** - Enables or disables the collection of Battery statistics.
- **System Resource**- Enables or disables the collection of System Resource information.
- **Network** - Enables or disables the collection of Network status.
- **Bluetooth** - Enables or disables the collection of Bluetooth information.
- **Light** - Enables or disables the collection of ambient light level.
- **Heater** - Not supported.

Snapshot Module

The Snapshot Module collects detailed device statistics at an interval to see detailed device information.

- **Enable Module** - Enables logging for this module.
- **Log Path** - Specifies the base path to use to store the snapshot files
- **Log filename** - Specifies the base filename for all the snapshot files. The current file count is appended to this name.
- **Log Interval (sec)** - Specifies the interval, in seconds, on which to invoke a detailed snapshot.
- **Snapshot file count** - The maximum number of Snapshot files to keep at any one time.
- **Top** - Enables or disables the running of the `top` command for data collection.
- **CPU Info** - Enables detailed per process CPU logging in the snapshot.
- **Memory Info** - Enables logging of detailed per process memory usage in the snapshot.
- **Battery Info** - Enables logging of detailed power information including battery life, on time, charging, and wake locks.

- **Wake Locks** - Enables or disables the collection of the sys/fs wake_lock information.
- **Time in State** - Enables or disables the collection of the sys/fs cpufreq for each core.
- **Processes** - Enables dumping the complete process list in the snapshot.
- **Threads** - Enables dumping all processes and their threads in the snapshot.
- **Properties** - Enables dumping of all system properties on the device. This includes build/version information as well as state information.
- **Interfaces** - Enables or disables the running of the **`netcfg`** command for data collection.
- **IP Routing Table** - Enables or disables the collection of the net route for data collection.
- **Connectivity** - Enables or disables the running of the **`dumpsys connectivity`** command for data collection.
- **Wifi** - Enables or disables the running of the **`dumpsys wifi`** command for data collection.
- **File systems** - Enables dumping of the available volumes on the file system and the free storage space for each.
- **Usage stats** - Enables dumping of detailed usage information for each package on the device. This includes the number of starts and duration of each run.

TCPDump Module

The TCPDump Module captures TCP data that happens over the device's networks.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the location to store the TCPDump output log files.
- **Base filename** - Specifies the base filename to use when storing the TCPDump files. The index number of the current log file is appended to the filename.
- **Tcpdump file size (MB)** - Specifies the maximum file size, in megabytes, for each log file created.
- **Tcpdump file count** - Specifies the number of log files to cycle through when storing the network traces.

Tombstone Module

The Tombstone Module collects tombstone (Linux Native Crashes) logs from the device.

- **Enable Module** - Enables logging for this module.
- **Log path** - Specifies the location to store the Tombstone output log files.
- **Collect Historic tombstones** - Collects new and existing tombstone files.

Configuration File

RxLogger configuration can be set using an XML file. The **`config.xml`** configuration file is located on the microSD card in the **`RxLogger\config`** folder. Copy the file from the device to a host computer using a USB connection. Edit the configuration file and then replace the XML file on the device. There is no need to stop and restart the RxLogger service since the file change is automatically detected.

Enabling Logging

To enable logging:

1. Swipe the screen up and select .
2. Touch **Start**.

3. Touch ◯.

Disabling Logging

To disable logging:

1. Swipe the screen up and select .
2. Touch **Stop**.
3. Touch ◯.

Extracting Log Files

1. Connect the device to a host computer using an USB connection.
2. Using a file explorer, navigate to the **RxLogger** folder.
3. Copy the file from the device to the host computer.
4. Disconnect the device from the host computer.

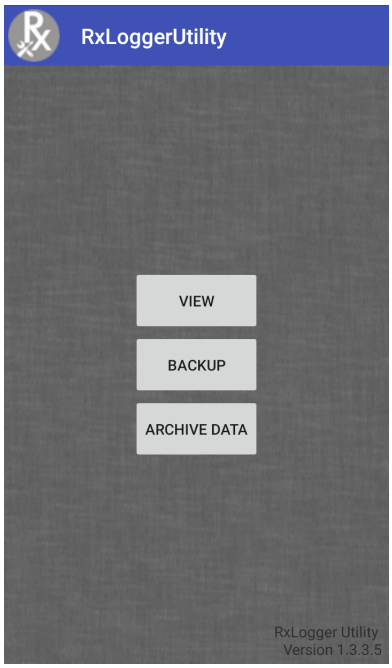
RxLogger Utility

RxLogger Utility is a data monitoring application for viewing logs in the device while RxLogger is running. Logs and RxLogger Utility features are accessed in the App View or the Overlay View.

App View

In App View, the user views logs in the RxLogger Utility.

Figure 111 App View

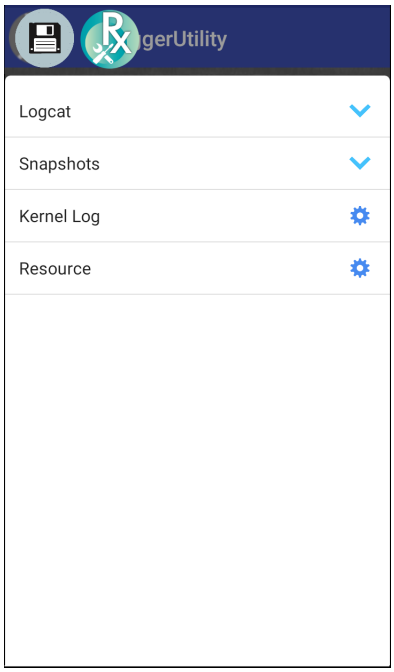


Viewing Logs

To view logs:

1. Touch the Main Chat Head icon. The Overlay View screen appears.

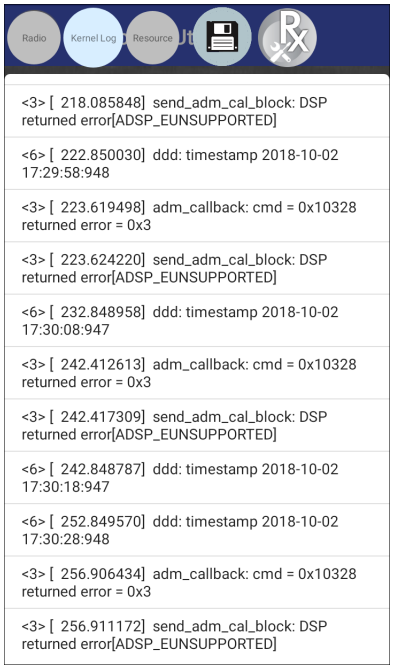
Figure 112 Overlay View Screen



2. Touch a log to open it. The user can open many logs with each displaying a new sub Chat Head.
3. If necessary, scroll left or right to view additional Sub Chat Head icons.

4. Touch a Sub Chat Head to display the log contents.

Figure 113 Log File



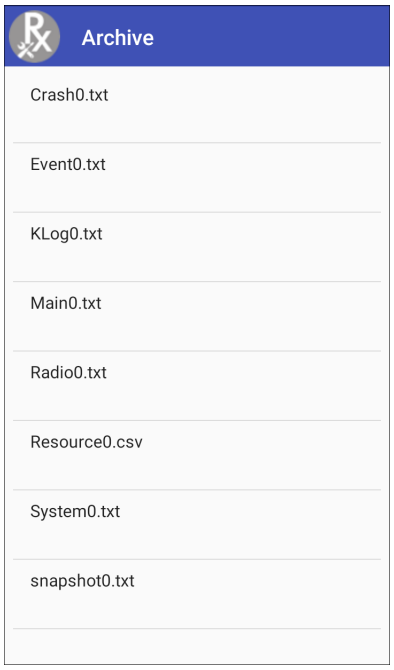
RxLogger Utility

RxLogger Utility is a data monitoring application for viewing logs in the device while RxLogger is running. Logs and RxLogger Utility features are accessed in the App View or the Overlay View.

Archive Data

View all the RxLogger logs stored in the default **RxLogger** directory. Logs viewed in the Archive window are not live.

Figure 114 Archive



To view the log files, touch **ARCHIVE DATA** and then touch a log file.

Overlay View

Use Overlay View to display RxLogger information while using other apps or on the home screen. Overlay View is accessed using the Main Chat Head.

Initiating the Main Chat Head

To initiate the Main Chat Head:

1. Open **RxLogger**.
2. Touch ⋮ > **Toggle Chat Head**. The Main Chat Head icon appears on the screen.
3. Touch and drag the Main Chat head icon to move it around the screen.

Removing the Main Chat Head

To remove the Main Chat Head icon:

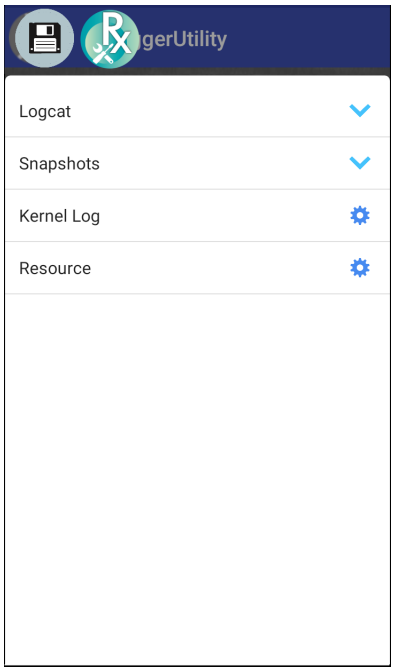
1. Touch and drag the icon. A circle with an X appears.
2. Move the icon over the circle and then release.

Viewing Logs

To view logs:

1. Touch the Main Chat Head icon. The Overlay View screen appears.

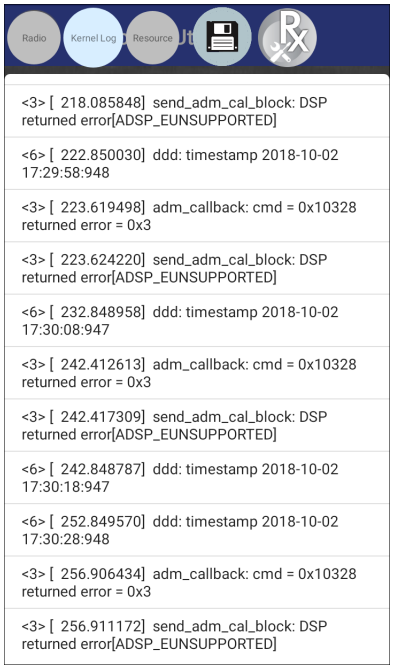
Figure 115 Overlay View Screen



2. Touch a log to open it. The user can open many logs with each displaying a new sub Chat Head.
3. If necessary, scroll left or right to view additional Sub Chat Head icons.

4. Touch a Sub Chat Head to display the log contents.

Figure 116 Log File



Removing a Sub Chat Head Icon

To remove a sub chat Head icon, press and hold the icon until it disappears.

Backup

RxLogger Utility allows the user to make a zip file of the **`RxLogger`** folder in the device, which by default contains all the RxLogger logs stored in the device.

Backup Now icon is always available in the Overlay View.

1. Touch the Backup Now icon. The Backup dialog box appears.
2. Touch **Yes** to create the back up.

About Phone

Use About phone settings to view information about the device. Swipe down with two fingers from the status bar to open the quick access panel and then touch ⚙ > **System** > **About phone**.

- **Status** - Touch to display the following:
  - **Battery status** - Indicates if the battery is charging (on AC power) or discharging (on battery power).
  - **Battery level** - Indicates the battery charge level.
  - **IP address** - Displays the IP address of the device.
  - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
  - **Ethernet MAC address** - Displays the Ethernet driver MAC address.
  - **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
  - **Serial number** - Displays the serial number of the device.
  - **Up time** - Displays the time that the device has been running since being turned on.
- **SW components** - Lists filenames and versions for various software on the device.
- **Battery Management** - Displays information about the battery.
- **Legal information** - Opens a screen to view legal information about the software included on the device.
- **Device Model Number** - Displays the devices model number.
- **Android version** - Displays the operating system version.
- **Android security patch level** - Displays the security patch level date.
- **Baseband version** - Displays WAN radio firmware version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

Application Deployment

Introduction

This chapter describes features in Android including new security features, how to package applications, and procedures for deploying applications onto the device.

Security

The device implements a set of security policies that determine whether an application is allowed to run and, if allowed, with what level of trust. To develop an application, you must know the security configuration of the device, and how to sign an application with the appropriate certificate to allow the application to run (and to run with the needed level of trust).

NOTE: Ensure the date is set correctly before installing certificates or when accessing secure web sites.

Secure Certificates

If the VPN or Wi-Fi networks rely on secure certificates, obtain the certificates and store them in the device's secure credential storage, before configuring access to the VPN or Wi-Fi networks.

If downloading the certificates from a web site, set a password for the credential storage. The device supports X.509 certificates saved in PKCS#12 key store files with a .p12 extension (if key store has a .pfx or other extension, change to .p12).

The device also installs any accompanying private key or certificate authority certificates contained in the key store.

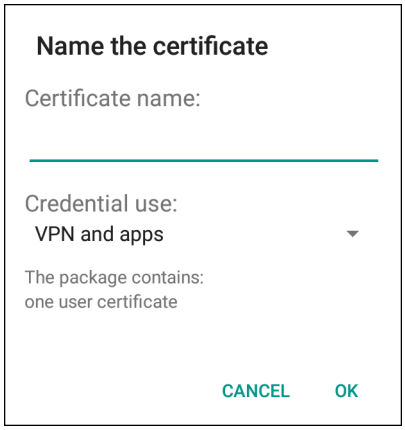
Installing a Secure Certificate

To install a secure certificate:

1. Copy the certificate from the host computer to the root of the microSD card or the device's internal memory. See USB Communication for information about connecting the device to a host computer and copying files.
2. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
3. Touch **Security & location** > **Advanced** > **Encryption & credentials**.
4. Touch **Install from storage**.

5. Navigate to the location of the certificate file.
6. Touch the filename of the certificate to install.
7. If prompted, enter the password for credential storage. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.
8. If prompted, enter the certificate's password and touch **OK**.
9. Enter a name for the certificate and in the Credential use drop-down, select **VPN and apps** or **Wi-Fi**.

Figure 117 Name the Certificate Dialog Box



10. Touch **OK**.

    The certificate can now be used when connecting to a secure network. For security, the certificate is deleted from the microSD card or internal memory.

Configuring Credential Storage Settings

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Security & location** > **Encryption & credentials**.
   - **Trusted credentials** - Touch to display the trusted system and user credentials.
   - **Install from storage** - Touch to install a secure certificate from the microSD card or internal storage.
   - **Clear credentials** - Deletes all secure certificates and related credentials.

Development Tools

Android Application Development

Development Workstation

Android development tools are available at developer.android.com.

To start developing applications for the device, download Android Studio. Development can take place on a Microsoft® Windows®, Mac® OS X®, or Linux® operating system.

Applications are written in the Java language, but compiled and executed in the Dalvik virtual machine. Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

Android Studio contains a full featured IDE as well as SDK components required to develop Android applications.

Target Device

Open the **Developer options** screen to set development related settings.

By default, the Developer Options are hidden. To un-hide the developer options, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

Touch **System > About device**. Scroll down to **Build number**. Tap **Build number** seven times until **You are now a developer appears**.

Touch **System > Developer options**. Slide the switch to the **ON** position to enable developer options.

EMDK for Android

EMDK for Android provides developers with a comprehensive set of tools to easily create powerful line-of-business applications for enterprise mobile computing devices. It's designed for Google's Android SDK and Android Studio, and includes class libraries, sample applications with source code, and all associated documentation to help your applications take full advantage of what Zebra devices have to offer.

The kit also delivers Profile Manager, a GUI-based device configuration tool providing exclusive access to the Zebra MX device management framework. This allows developers to configure Zebra devices from within their applications in less time, with fewer lines of code and with fewer errors.

For more information go to: techdocs.zebra.com.

StageNow

StageNow is Zebra's next-generation Android Staging Solution built on the MX platform. It allows quick and easy creation of device profiles, and can deploy to devices simply by scanning a bar code, reading a tag, or playing an audio file.

The StageNow Staging Solution includes the following components:

- The StageNow Workstation tool installs on the staging workstation (host computer) and lets the administrator easily create staging profiles for configuring device components, and perform other staging actions such as checking the condition of a target device to determine suitability for software upgrades or other activities. The StageNow Workstation stores profiles and other created content for later use.
- The StageNow Client resides on the device and provides a user interface for the staging operator to initiate staging. The operator uses one or more of the desired staging methods (print and scan a bar code, read an NFC tag or play an audio file) to deliver staging material to the device.

For more information go to: techdocs.zebra.com.

ADB USB Setup

To use the ADB, install the USB driver. This assumes that the development SDK has been installed on the host computer. Go to developer.android.com/sdk/index.html for details on setting up the development SDK.

ADB driver for Windows and Linux are available on the Zebra Support Central web site at www.zebra.com/support. Download the ADB and USB Driver Setup package. Follow the instructions with the package to install the ADB and USB drivers for Windows and Linux.

Enabling USB Debugging

By default, USB debugging is disabled. To enable USB debugging:

1. Swipe down from the Status bar to open the Quick Access panel, and then touch ⚙.
2. Touch **System** > **About phone**.
3. Scroll down to **Build number**.
4. Tap **Build number** seven times. The message **You are now a developer!** appears.
5. Touch ◁.
6. Touch **Developer options**.
7. Slide the **USB debugging** switch to the **ON** position.
8. Touch **OK**.
9. Connect the device to the host computer using the Rugged Charge/USB Cable.
   The **Allow USB debugging?** dialog box appears on the device.
10. On the device, touch **OK**.
11. On the host computer, navigate to the `platform-tools` folder.
12. Type `adb devices`.
    The following displays:
    `List of devices attached`
    `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).



NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

13. Touch ○.

Application Installation

After an application is developed, install the application onto the device using one of the following methods:

- USB connection, see Installing Applications Using the USB Connection.
- Android Debug Bridge, see Installing Applications Using the Android Debug Bridge.
- microSD Card, see Installing Applications Using a microSD Card.
- Mobile device management (MDM) platforms that have application provisioning. Refer to the MDM software documentation for details.

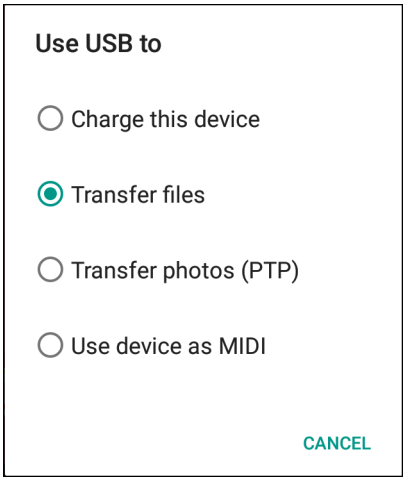
Installing Applications Using the USB Connection



CAUTION: When connecting the device to a host computer and mounting the microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

1. Connect the device to a host computer using the Rugged Charge/USB cable.
2. Pull down the Notification panel and touch **USB for Charging**.

Figure 118 Use USB Dialog Box

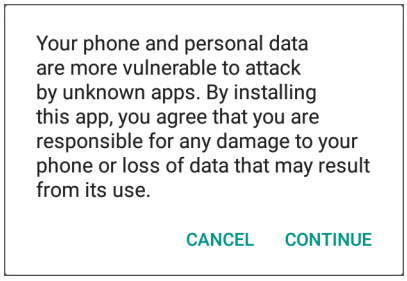


3. Touch **Transfer files**.
4. On the host computer, open a **Files** application.
5. On the host computer, copy the application .apk file from the host computer to the device.

CAUTION: Carefully follow the host computer's instructions to unmount the microSD card and disconnect USB devices correctly to avoid losing information.

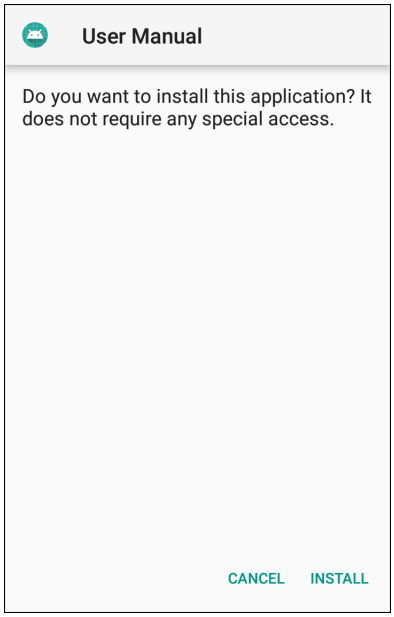
6. Disconnect the device from the host computer.
7. Swipe the screen up and select to view files on the microSD card or Internal Storage.
8. Locate the application .apk file.
9. Touch the application file.

Figure 119 Install App Permission Dialog Box



10. Touch **Continue** to install the app or **Cancel** to stop the installation.

Figure 120 Accept Installation Screen



11. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
12. Touch **Open** to open the application or **Done** to exit the installation process. The application appears in the App list.

Installing Applications Using the Android Debug Bridge

Use ADB commands to install application onto the device.

CAUTION: When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Ensure that the ADB drivers are installed on the host computer. See ADB USB Setup.

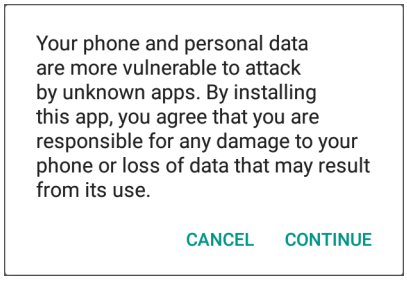
1. Connect the device to a host computer using USB. See USB Communication.
2. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
3. Touch **System** > **Developer options**.
4. Slide the switch to the **ON** position.
5. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
6. Touch **OK**.
7. On the host computer, open a command prompt window and use the adb command:
   `adb install <application>`
   where: <application> = the path and filename of the apk file.
8. Disconnect the device from the host computer. See USB Communication.

Installing Applications Using a microSD Card

CAUTION: When connecting the device to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

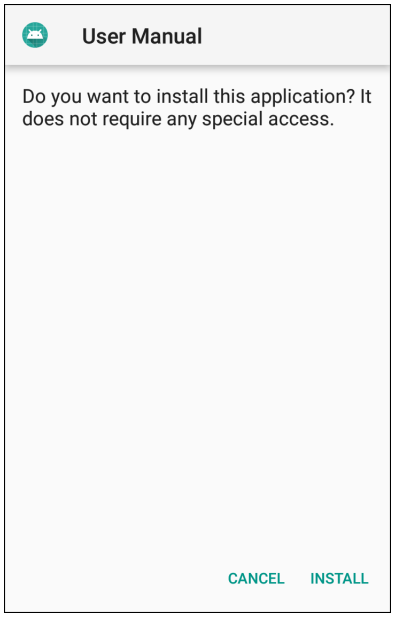
1. Connect the device to a host computer using USB. See USB Communication.
2. Copy the application APK file from the host computer to the microSD card.
3. Remove the microSD card from the host computer.
4. Press and hold the Power button on the device until the menu appears.
5. Touch **Power off**.
6. Press the two battery latches in.
7. Lift the battery from the device.
8. Lift the access door.
9. Insert the microSD card.
10. Replace the access door.
11. Insert the battery, bottom first, into the battery compartment in the back of the device.
12. Press the battery down until the battery release latches snap into place.
13. Press and hold the Power button to turn on the device.
14. Swipe the screen up and select to view files on the microSD card.
15. Touch ≡ > **SD card**.
16. Locate the application .apk file.
17. Touch the application file.

Figure 121 Install App Permission Dialog Box



18. Touch **Continue**. to install the app or **Cancel** to stop the installation.

Figure 122 Accept Installation Screen



19. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.
20. Touch **Open** to open the application or **Done** to exit the installation process. The application appears in the App list.

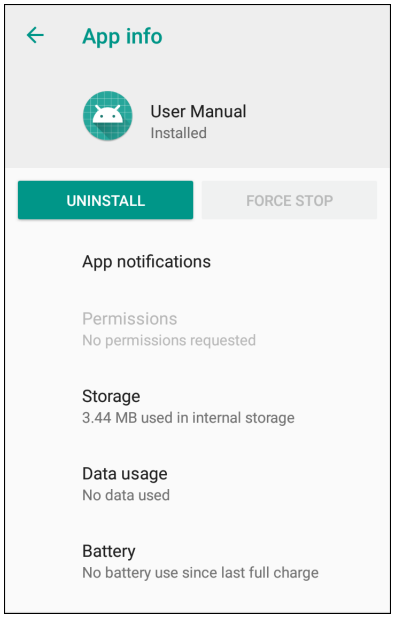
Uninstalling an Application

To uninstall an application:

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Apps & notifications**.
3. Touch **See all apps** to view all apps in the list.
4. Scroll through the list to the app.

5. Touch the app. The **App info** screen appears.

Figure 123 App Info Screen



6. Touch **Uninstall**.
7. Touch **OK** to confirm.

Performing a System Update

System Update packages can contain either partial or complete updates for the operating system. Zebra distributes the System Update packages on the Zebra Support & Downloads web site. Perform system update using either a microSD card or using ADB.

Downloading the System Update Package

To download the system update package:

1. Go to the Zebra Support & Downloads web site, www.zebra.com/support.
2. Download the appropriate System Update package to a host computer.

Using microSD Card

1. Copy the System Update zip file to the root of the microSD card.
   - Copy the zip file to a microSD card using a host computer (see USB Communication for more information), and then installing the microSD card into the device (see Replacing the microSD Card for more information).
   - Connect the device with a microSD card already installed to the host computer, and copy zip file to the microSD card. See USB Communication for more information. Disconnect the device from the host computer.
2. Press and hold the Power button until the menu appears.

3. Touch **Restart**.
4. Touch **OK**. The device resets.
5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.
6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.
7. Press the Power button.
8. Use the Volume Up and Volume Down buttons to navigate to the System Update file.
9. Press the Power button. The System Update installs and then the device returns to the Recovery screen.
10. Press the Power button to reboot the device.

NOTE: If installing GMS software on a device that had Non-GMS software or Non-GMS software on a device that had GMS software, perform a Factory or Enterprise reset (retains enterprise data).

Using ADB

To update the system using ADB:

1. Connect the device to the USB-C Cable or insert the device into the 1-Slot Ethernet Cradle.
2. Connect the cable or cradle to the host computer.
3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
4. Touch **System** > **Developer options**.
5. Slide the switch to the **ON** position.
6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
7. Touch **OK**.
8. On the host computer, open a command prompt window and use the adb command:
   `adb devices`
   The following displays:
   `List of devices attached`
   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

9. Type:
   `adb reboot recovery`
10. Press Enter. The System Recovery screen appears.
11. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.
12. On the host computer command prompt window type:
    `adb sideload <file>`
    where: <file> = the path and filename of the zip file.

13. Press Enter. The System Update installs (progress appears as percentage in the Command Prompt window) and then the Recovery screen appears.
14. Press the Power button to reboot the device.

NOTE: If installing GMS software on a device that had Non-GMS software or Non-GMS software on a device that had GMS software, perform a Factory or Enterprise reset (retains enterprise data).

Verify System Update Installation

To check that the system update installed properly:

1. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **System** > **About phone**.
3. Scroll down to **Build number**.
4. Ensure that the build number matches the new system update package file number.

Performing an Enterprise Reset

An Enterprise Reset erases all user data in the `/data` partition, including data in the primary storage locations (`/sdcard` and emulated storage).

Before performing an Enterprise Reset, provision all necessary configuration files and restore after the reset.

Perform Enterprise Reset using either a microSD card or using ADB.

Downloading the Enterprise Reset Package

To download the system update package:

1. Go to the Zebra Support & Downloads web site, www.zebra.com/support.
2. Download the Enterprise Reset file to a host computer.

Using microSD Card

1. Copy the Enterprise Reset zip file to the root of the microSD card.
   - Copy the zip file to a microSD card using a host computer (see USB Communication for more information) and then installing the microSD card into the device (see Replacing the microSD Card for more information).
   - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See USB Communication for more information. Disconnect the device from the host computer.
2. Press and hold the Power button until the menu appears.
3. Touch **Reboot**.
4. Touch **OK**. The device resets.
5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.

6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.
7. Press the Power button.
8. Use the Volume Up and Volume Down buttons to navigate to the System Update file.
9. Press the Power button. The Enterprise Reset occurs and then the device returns to the Recovery screen.
10. Press the Power button.

Using ADB

To perform an Enterprise Reset using ADB:

1. Connect the device to the USB-C Cable or insert the device into the 1-Slot Ethernet Cradle.
2. Connect the device to the Rugged Charge/USB cable or insert the device into the 1-Slot USB/Charge Only Cradle.
3. Connect the cable or cradle to the host computer.
4. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
5. Touch **System** > **Developer options**.
6. Slide the switch to the **ON** position.
7. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
8. Touch **OK**.
9. On the host computer, open a command prompt window and type:

   `adb devices`.

   The following displays:

   `List of devices attached`

   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).

NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

10. Type:

    `adb reboot recovery`

11. Press Enter. The System Recovery screen appears.
12. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.
13. Press the Power button.
14. On the host computer command prompt window type:

    `adb sideload <file>`

    where: <file> = the path and filename of the zip file.

15. Press Enter. The Enterprise Reset package installs and then the Recovery screen appears.
16. Press the Power button to reboot the device.

Performing a Factory Reset

A Factory Reset erases all data in the **/data** and **/enterprise** partitions in internal storage and clears all device settings. A Factory Reset returns the device to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See Performing a System Update for more information.

Downloading the Factory Reset Package

To download the Factory Reset package:

1. Go to the Zebra Support & Downloads web site, www.zebra.com/support.
2. Download the appropriate Factory Reset file to a host computer.

Using microSD Card

1. Copy the Factory Reset zip file to the root of the microSD card.
   - Copy the zip file to a microSD card using a host computer (see USB Communication for more information) and then installing the microSD card into the device (see Replacing the microSD Card for more information).
   - Connect the device with a microSD card already installed to the host computer and copy zip file to the microSD card. See USB Communication for more information. Disconnect the device from the host computer.
2. Press and hold the Power button until the menu appears.
3. Touch **Reboot**.
4. Touch **OK**. The device resets.
5. Press and hold the PTT button until the device vibrates. The System Recovery screen appears.
6. Press the Volume Up and Volume Down buttons to navigate to **apply from sdcard**.
7.
8.
9.
10. Press the Power button.
11. Use the Volume Up and Volume Down buttons to navigate to the Factory Reset file.
12. Press the Power button. The Factory Reset occurs and then the device returns to the Recovery screen.
13. Press the Power button.

Using ADB

To perform an Factory Reset using ADB:

1. Connect the device to the USB-C Cable or insert the device into the 1-Slot Ethernet Cradle.
2. Connect the cable or cradle to the host computer.

3. On the device, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
4. Touch **System** > **Developer options**.
5. Slide the switch to the **ON** position.
6. Touch **USB Debugging**. A check appears in the check box. The **Allow USB debugging?** dialog box appears.
7. Touch **OK**.
8. On the host computer, open a command prompt window and use the adb command:

   `adb devices`.

   The following displays:

   `List of devices attached`

   `XXXXXXXXXXXXXXX device` (where XXXXXXXXXXXXXXX is the device number).



NOTE: If device number does not appear, ensure that ADB drivers are installed properly.

9. Type:

   `adb reboot recovery`

10. Press Enter. The System Recovery screen appears.
11. Press the Volume Up and Volume Down buttons to navigate to **apply from adb**.
12. Press the Power button.
13. On the host computer command prompt window type:

    `adb sideload <file>`

    where: <file> = the path and filename of the zip file.

14. Press Enter. The Factory Reset package installs and then the Recovery screen appears.
15. Press the Power button to reboot the device.

Storage

The device contains the following types of file storage:

- Random Access Memory (RAM)
- Internal storage
- External storage (microSD card) or
- Enterprise folder.

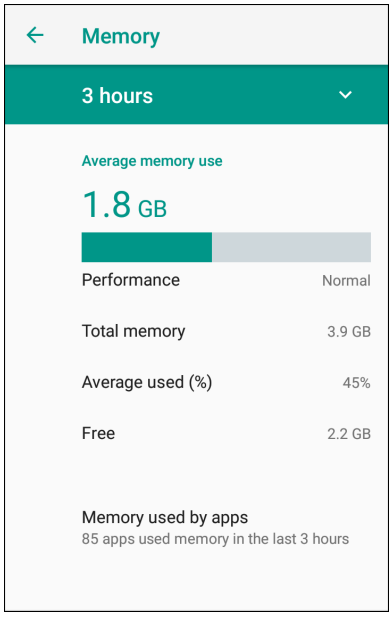
Random Access Memory

Executing programs use RAM to store data. Data stored in RAM is lost upon a reset. The operating system manages how applications use RAM. It only allows applications and component processes and services to use RAM when required. It may cache recently used processes in RAM, so they restart more quickly when opened again, but it will erase the cache if it needs the RAM for new activities.

1. To view the amount of free and used memory, swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

2. Touch **System** > **Developer options** > **Memory**.

Figure 124 Memory Screen



The screen displays the amount of used and free RAM.

- **Performance** - Indicates memory performance.
- **Total memory** - Indicates the total amount of RAM available.
- **Average used (%)** - Indicates the average amount of memory (as a percentage) used during the period of time selected (default - 3 hours).
- **Free** - Indicates the total amount of unused RAM.
- **Memory used by apps** - Touch to view RAM usage by individual apps.

Internal Storage

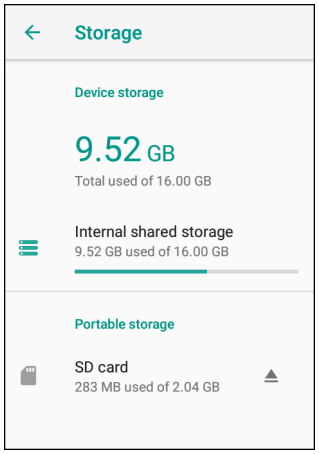
The device has internal storage. The internal storage content can be viewed and files copied to and from when the device is connected to a host computer. Some applications are designed to be stored on the internal storage rather than in internal memory.

To view the used and available space on the internal storage:

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

2. Touch **Storage**.

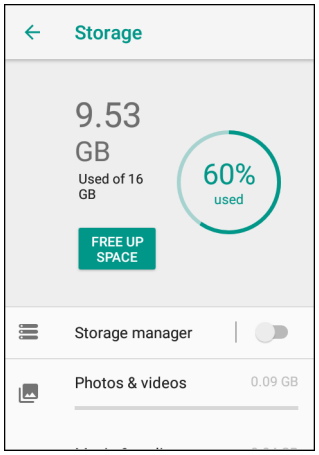
Figure 125 Storage Screen



- **Internal Storage** - Displays the total amount of space on internal storage and amount used.

Touch **Internal shared storage** to display a the amount of storage used by apps, photos, videos, audio and other files.

Figure 126 Internal Storage Screen



External Storage

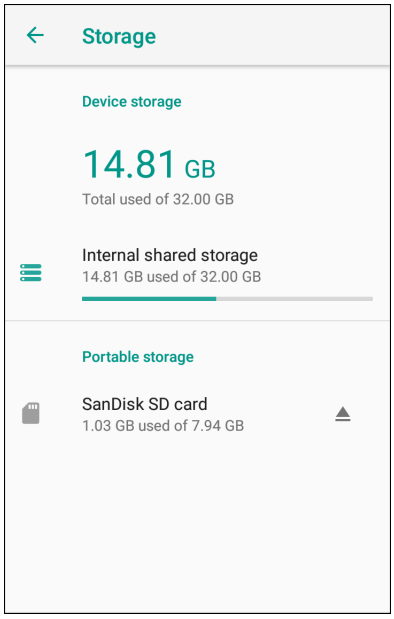
The device can have a removable microSD card. The microSD card content can be viewed and files copied to and from when the device is connected to a host computer.

To view the used and available space on the microSD card:

1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.

2. Touch **Storage**.

Figure 127 External Storage Screen



Portable storage displays the total amount of space on the installed microSD card and the amount used.

To unmount the microSD card, touch ⏏.

Touch **SD card**to view the contents of the card.

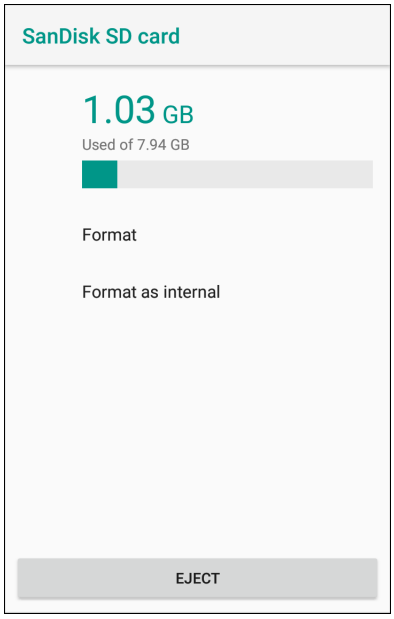
Formatting a microSD Card or USB Drive as Portable Storage

To format an installed microSD card or USB drive as portable storage:

1. Touch **SD card**.

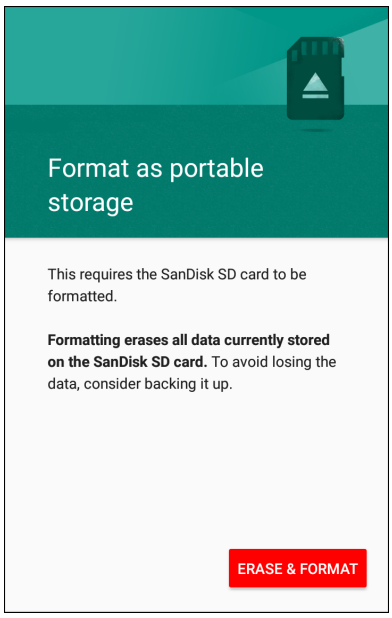
2. Touch ⋮ > **Storage settings**.

Figure 128 SD Card Settings Screen



3. Touch **Format**.

Figure 129 Format Screen



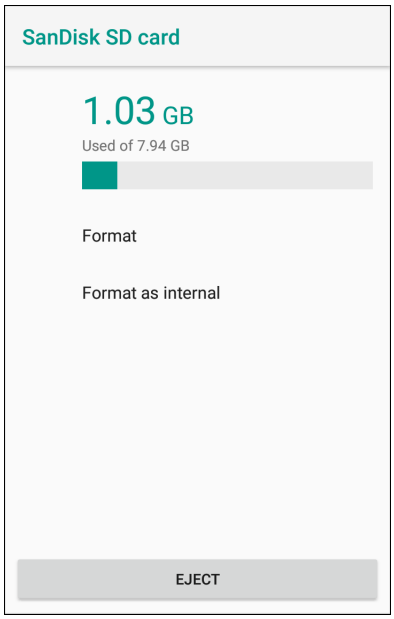
4. Touch **ERASE & FORMAT**.
5. Touch **DONE**.

Formatting a microSD Card as Internal Memory

You can format a microSD card as internal memory to increase the actual amount of the device's internal memory. Once formatted, the microSD card can only be read by this device. To format an installed microSD card as internal memory:

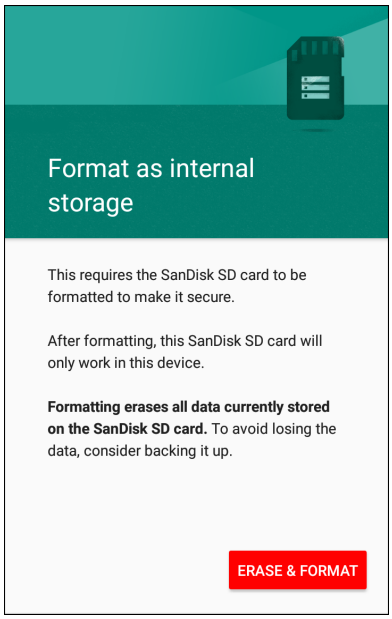
1. Touch **SD card**.
2. Touch ⋮ > **Storage settings**.

Figure 130 SD Card Settings Screen



3. Touch **Format as internal**.

Figure 131 Format Screen



4. Touch **ERASE & FORMAT**.
5. Touch **DONE**.

Enterprise Folder

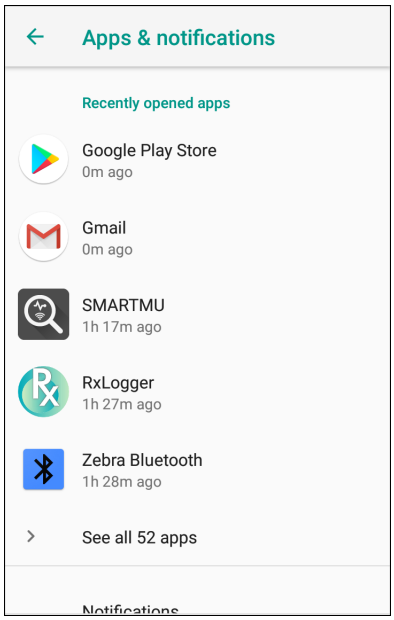
The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 MB (formatted). Applications can persist data after an Enterprise Reset by saving data to the enterprise/user folder. The folder is ext4 formatted and is only accessible from a host computer using ADB or from an MDM.

App Management

Apps use two kinds of memory: storage memory and RAM. Apps use storage memory for themselves and any files, settings, and other data they use. They also use RAM when they are running.

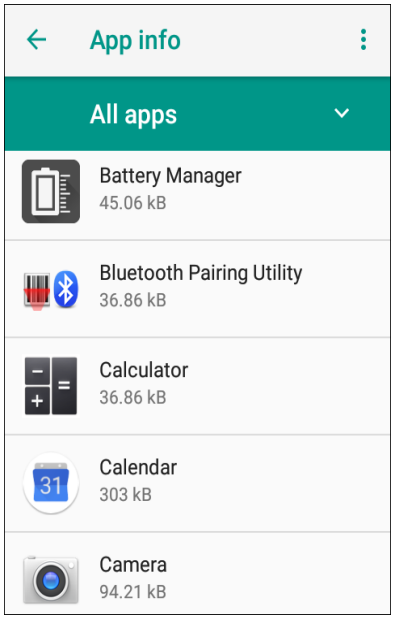
1. Swipe down from the Status bar to open the Quick Access panel and then touch ⚙.
2. Touch **Apps & notifications**.

Figure 132 Apps & Notifications Screen



3. Touch **See all XX apps** to view all apps on the device.

Figure 133 App Info Screen



4. Touch ⋮ > **Show system** to include system processes in the list.
5. Touch an app, process, or service in the list to open a screen to view its details. Depending on the item, you can change its settings, permissions, notifications, and force stop or uninstall the item.

Viewing App Details

Apps have different kinds of information and controls, but commonly include:

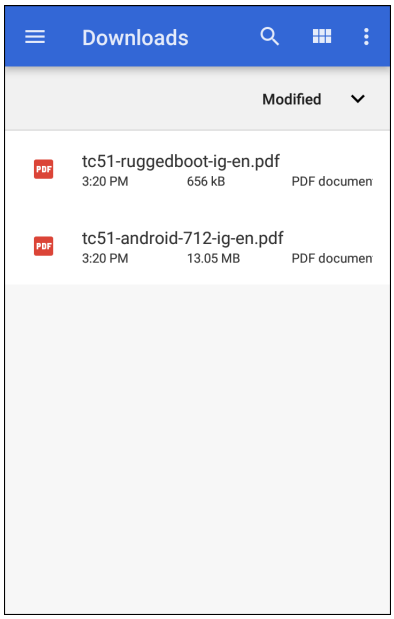
- **Force stop** - stop an app.
- **Disable** - disable an app.
- **Uninstall** - remove the app and all of its data and settings from the device. See Uninstalling an Application for information about uninstalling apps.
- **Storage** - lists how much information is stored, and includes a button for clearing it.
- **Data usage** - provides information about data (Wi-Fi) consumed by an app.
- **Permissions** - lists the areas on the device that the app has access to.
- **Notifications** - set the app notification settings.
- **Open by default** - clears If you have configured an app to launch certain file types by default, you can clear that setting here.
- **Battery** - lists the amount of computing power used by the app.
- **Memory** - lists the average app memory usage.
- Advanced
  - **Draw over other apps** - allows an app to display on top of other apps.

Managing Downloads

Files and apps downloaded using the Browser or Email are stored on the microSD card or Internal storage in the Download directory. Use the Downloads app to view, open, or delete downloaded items.

1. Swipe the screen up and touch .
2. Touch > **Downloads**.

Figure 134 Files - Downloads Screen



3. Touch and hold an item, select items to delete and touch . The item is deleted from the device.

Maintenance and Troubleshooting

Introduction

This chapter includes instructions on cleaning and storing the device, and provides troubleshooting solutions for potential problems during operation.

Maintaining the TC25

For trouble-free service, observe the following tips when using the TC25:

- Do not scratch the screen of the TC25. When working with the TC25, use the optional stylus or plastic-tipped pens intended for use with a touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the TC25 screen.
- The touch-sensitive screen of the TC25 is glass. Do not to drop the TC25 or subject it to strong impact.
- Protect the TC25 from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
- Do not store or use the TC25 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the TC25. If the surface of the TC25 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.

Display Best Practices

Image Retention

Image retention may occur when a static image continuously displays for extended periods of time. A user may see a faint remnant of the image even after a new image displays. To prevent image retention:

- set the display to turn off after a few minutes of idle time.
- rotate background images on a periodic basis.
- turn off the display when the device in not in use.
- use a screen saver with the following characteristics:
  - background color set to black
  - use a small moving image (approximately 2% of the display size).
  - move the image randomly across the screen
  - screen saver should be active as long as the static image is used.

Cleaning Instructions



CAUTION: Always wear eye protection.

Read warning label on compressed air and alcohol product before using.

If you have to use any other solution for medical reasons please contact the Global Customer Support Center for more information.



WARNING: Avoid exposing this product to contact with hot oil or other flammable liquids. If such exposure occurs, unplug the device and clean the product immediately in accordance with these guidelines.

Approved Cleanser Active Ingredients

100% of the active ingredients in any cleaner must consist of one or some combination of the following: isopropyl alcohol, or mild dish soap.

Harmful Ingredients

The following chemicals are known to damage the plastics on the device and should not come in contact with the device: ammonia solutions, compounds of amines or ammonia; acetone; ketones; ethers; aromatic and chlorinated hydrocarbons; acqueous or alcoholic alkaline solutions; ethanolamine; toluene; trichloroethylene; benzene; carbolic acid and TB-lysoform.

Cleaning Instructions

Do not apply liquid directly to the device. Dampen a soft cloth or use pre-moistened wipes. Do not wrap the device in the cloth or wipe, but gently wipe the unit. Be careful not to let liquid pool around the display window or other places. Allow the unit to air dry before use.

Special Cleaning Notes

Many vinyl gloves contain phthalate additives, which are often not recommended for medical use and are known to be harmful to the housing of the device. The device should not be handled while wearing vinyl gloves containing phthalates, or before hands are washed to remove contaminant residue after gloves are removed. If products containing any of the harmful ingredients listed above are used prior to handling the device, such as hand sanitizer that contain ethanolamine, hands must be completely dry before handling the device to prevent damage to the plastics.

Cleaning Materials Required

- Alcohol wipes
- Lens tissue
- Cotton-tipped applicators
- Isopropyl alcohol
- Can of compressed air with a tube.

Cleaning Frequency

The cleaning frequency is up to the customer's discretion due to the varied environments in which the mobile devices are used. They may be cleaned as frequently as required, but it is advisable to clean the camera window periodically when used in dirty environments to ensure optimum performance.

Cleaning the TC25

Housing

Using the alcohol wipes, wipe the housing including buttons.

Display

The display can be wiped down with the alcohol wipes, but care should be taken not to allow any pooling of liquid around the edges of the display. Immediately dry the display with a soft, non-abrasive cloth to prevent streaking.

Camera and Exit Window

Wipe the camera and exit window periodically with a lens tissue or other material suitable for cleaning optical material such as eyeglasses.

Connector Cleaning

To clean the connectors:

1. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
2. Rub the cotton portion of the cotton-tipped applicator back-and-forth across the connector. Do not leave any cotton residue on the connector.
3. Repeat at least three times.
4. Use the cotton-tipped applicator dipped in alcohol to remove any grease and dirt near the connector area.
5. Use a dry cotton-tipped applicator and repeat steps 4 through 6.



CAUTION: Do not point nozzle at yourself and others, ensure the nozzle or tube is pointed away from your face.

6. Spray compressed air on the connector area by pointing the tube/nozzle about ½ inch away from the surface.
7. Inspect the area for any grease or dirt, repeat if required.

Cleaning Cradle Connectors

To clean the connectors on a cradle:

1. Remove the DC power cable from the cradle.

2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton-tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not leave any cotton residue on the connector.
4. All sides of the connector should also be rubbed with the cotton-tipped applicator.



CAUTION: Do not point nozzle at yourself and others, ensure the nozzle or tube is pointed away from your face.

5. Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.
6. Remove any lint left by the cotton-tipped applicator.
7. If grease and other dirt can be found on other areas of the cradle, use a lint-free cloth and alcohol to remove.
8. Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

   If the temperature is low and humidity is high, longer drying time is required. Warm temperature and dry humidity requires less drying time.

Troubleshooting

The following tables provides typical problems that might arise and the solution for correcting the problem.

TC25

Table 9 *Troubleshooting the TC25*

Problem	Cause	Solution
When pressing the power button the TC25 does not turn on.	Battery not charged.	Charge or replace the battery in the TC25.
	System crash.	Perform a reset.
When pressing the power button the TC25 does not turn on but two LEDs blink.	Battery charge is at a level where data is maintained but battery should be re-charged.	Charge or replace the battery in the TC25.
Battery did not charge.	Battery failed.	Replace battery. If the TC25 still does not operate, perform a reset.
	TC25 removed from cradle while battery was charging.	Insert TC25 in cradle. See Charging the Battery on page 18.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0°C (32°F) or above 40°C (104°F).
Cannot see characters on display.	TC25 not powered on.	Press the **Power** button.
During data communication with a host computer, no data transmitted, or transmitted data was incomplete.	TC25 removed from cradle or disconnected from host computer during communication.	Replace the TC25 in the cradle, or reattach the communication cable and re-transmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software was incorrectly installed or configured.	Perform setup.
During data communication over Wi-Fi, no data transmitted, or transmitted data was incomplete.	Wi-Fi radio is not on.	Turn on the Wi-Fi radio.
	You moved out of range of an access point.	Move closer to an access point.

Table 9 *Troubleshooting the TC25 (Continued)*

Problem	Cause	Solution
During data communication over Bluetooth, no data transmitted, or transmitted data was incomplete.	Bluetooth radio is not on.	Turn on the Bluetooth radio.
	You moved out of range of another Bluetooth device.	Move within 10 meters (32.8 feet) of the other device.
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device's user documentation for help.
No sound.	Volume setting is low or turned off.	Adjust the volume.
TC25 shuts off.	TC25 is inactive.	The display turns off after a period of inactivity. Set this period to 15 seconds, 30 seconds, 1, 2, 5, 10 or 30 minutes.
	Battery is depleted.	Replace the battery.
Tapping the window buttons or icons does not activate the corresponding feature.	The device is not responding.	Reset the device. See Resetting the TC25 on page 24.
A message appears stating that the TC25 memory is full.	Too many files stored on the TC25.	Delete unused memos and records. If necessary, save these records on the host computer (or use an SD card for additional memory).
	Too many applications installed on the TC25.	Remove user-installed applications on the TC25 to recover memory. Select > > **Apps** > **Downloaded**. Select the unused program and tap **Uninstall**.

Table 9 *Troubleshooting the TC25 (Continued)*

Problem	Cause	Solution
The TC25 does not decode with reading bar code.	Scanning application is not loaded.	Load a scanning application on the TC25 or enable DataWedge. See the system administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between exit window and bar code is incorrect.	Place the TC25 within proper scanning range.
	TC25 is not programmed for the bar code.	Program the TC25 to accept the type of bar code being scanned. Refer to the EMDK or DataWedge application.
	TC25 is not programmed to generate a beep.	If the TC25 does not beep on a good decode, set the application to generate a beep on good decode.
	Battery is low.	If the scanner stops emitting a laser beam upon a trigger press, check the battery level. When the battery is low, the scanner shuts off before the TC25 low battery condition notification. Note: If the scanner is still not reading symbols, contact the distributor or the Global Customer Support Center.
Cannot unlock TC25.	User enters incorrect password.	If the user enters an incorrect password eight times, the user is requested to enter a code before trying again. If the user forgot the password, contact system administrator.

1-Slot Base Charge Only Cradle

Table 10 *Troubleshooting the 1-Slot Base Charge Only Cradle*

Symptom	Possible Cause	Action
LEDs do not light when TC25 is inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	TC25 is not seated firmly in the cradle.	Remove and re-insert the TC25 into the cradle, ensuring it is firmly seated.

Table 10 *Troubleshooting the 1-Slot Base Charge Only Cradle (Continued)*

Symptom	Possible Cause	Action
TC25 battery is not charging.	TC25 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure TC25 is seated correctly. Confirm main battery is charging. The internal battery charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.
	Battery is faulty.	Verify that other devices charge properly. If so, the replace the device.
	The TC25 is not fully seated in the cradle.	Remove and re-insert the TC25 into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).

1-Slot Ethernet Cradle

Table 11 *Troubleshooting the 1-Slot Ethernet Cradle*

Symptom	Possible Cause	Action
LEDs do not light when TC25 is inserted.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	TC25 is not seated firmly in the cradle.	Remove and re-insert the TC25 into the cradle, ensuring it is firmly seated.
TC25 battery is not charging.	TC25 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure TC25 is seated correctly. Confirm main battery is charging. The internal battery charges from fully depleted to 90% in approximately four hours and from fully depleted to 100% in approximately five hours.
	Battery is faulty.	Verify that other devices charge properly. If so, replace the device.
	The TC25 is not fully seated in the cradle.	Remove and re-insert the TC25 into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).

5-Slot Charge Only Cradle Troubleshooting

Table 12 *Troubleshooting the 5-Slot Charge Only Cradle*

Problem	Cause	Solution
Battery is not charging.	TC25 removed from the cradle too soon.	Replace the TC25 in the cradle. The battery fully charges in approximately six hours.
	Battery is faulty.	Verify that other devices charge properly. If so, replace the device.
	TC25 is not inserted correctly in the cradle.	Remove the TC25 and reinsert it correctly. Verify charging is active. Touch > > **About phone** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between -10 °C (+14 °F) and +60 °C (+140 °F).

Technical Specifications

The following sections provide technical specification for the device.

TC25

Table 13 *TC25 Technical Specifications*

Item	Description
Physical Characteristics	
Dimensions	Length: 134.0 mm (5.3 in.) Width: 71.3 mm (2.8 in.) Depth: 17.9 mm (0.7 in.)
Weight	200 g (7.1 oz)
Display	4.3 in. High Definition (800 x 480) WVGA
Touch Panel	Capacitive Touch Panel; multi-touch
Backlight	Light Emitting Diode (LED) backlight
Internal Battery	Rechargeable 3,000 mAh (typical) / 2,900 mAh (minimum) Li-Ion.
Expansion Slot	User accessible microSD up to 32 GB (SDHC) or up to 128 GB (SDXC) formatted in exFAT.
Connection Interface	One USB OTG (host/client) type C connector
Notification	Audible tone; multi-color LEDs, vibration
Voice and Audio	PTT Pro and PTT Express support. Voice support (internal speaker/microphone). Two microphones; speaker; and audio jack.
Performance Characteristics	
CPU	QCOM MSM8937 64-bit, 8-core, ARM Cortex A53 1.4 GHz, 512 kB L2 cache, power-optimization
Operating System	Android 8.1.0 Oreo
Memory	2 GB RAM/16 GB or 32 GB Flash
Output Power	USB - 5 VDC @ 500 mA max

Table 13 *TC25 Technical Specifications (Continued)*

Item	Description
User Environment	
Operating Temperature	-10°C to 50°C (14°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0° C to 40° C (32°F to 104°F)
Relative Humidity	Operating: 5 to 95% non-condensing
Drop Specification	Multiple 1.2 m (4 ft.) to tile over concrete per MIL-STD at room temperature.
Tumble	300 0.5 m (1.6 ft.) tumbles
Sealing	IP54
Electrostatic Discharge (ESD)	± 20 kVDC air discharge, ± 10 kVDC direct discharge, ± 10 kVDC indirect discharge
Vibration	4 g's peak, 5 Hz to 2 kHz, 1 hour duration per axis
Thermal Shock	-40°C to 70°C (-40°F to 158°F) rapid transition. 10 cycles: (1 cycle = 1.25 hours at -40°C and 1.25 hours at 70°C.
Interactive Sensor Technology (IST)	
Motion Sensor	3-axis accelerometer
Light Sensor	Ambient light sensor to auto adjust display backlight brightness
Proximity Sensor	Automatically detects when the user places the handset against head during a phone call to disable display output and touch input.
Wireless LAN Data and Voice Communications	
Radio	IEEE 802.11 a/b/g/n/ac/d/r/k/w/v/h/i IPv4, IPv6
Data Rates Supported	2.4GHz: 802.11b/g/n - up to 150 Mbps 5GHz: 802.11a/n/ac - up to 433.3 Mbps
Operating Channels	2.4 GHz: Chan 1 - 13; 1 - 11 (US) 5GHz: Chan 36-48, 52-64, 100-140, 149-151, 161-165 Channel Bandwidth: 20, 40, 80 MHz Actual operating channels/frequencies and bandwidth depend on regulatory rules and certification agency.
Security and Encryption	WEP (40 or 104 bit); WPA/WPA2 Personal (TKIP and AES); WPA/WPA2 Enterprise (TKIP and AES) — EAP-TTLS (PAP, MSCHAP, MSCHAPv2), EAP-TLS, PEAPv0-MSCHAPv2.
Certifications	802.11 a/b/g/n/ac; WPA; WPA2
Fast Roam	802.11

Table 13 *TC25 Technical Specifications (Continued)*

Item	Description
Wireless WAN Data and Voice Communications	
Frequency band	Worldwide: LTE: 700/800/900/1800/2100/2600 (FDD 28,20,8,3,1,7); UMTS/HSPA/HSPA+: 850/900/2100; GSM/GPRS/EDGE: 850/900/1800/1900 Note: Indonesian configurations do not support LTE. Americas: LTE: 700/850/1800/1900, (FDD 12,17,5,2,4); UMTS/HSPA/HSPA+: 850/1700/1900 GSM/GPRS/EDGE: 850/900/1800/1900
GPS	Integrated, Autonomous, Assisted GPS (A-GPS), GLONASS, Beidou
Wireless PAN Data and Voice Communications	
Bluetooth	Bluetooth v4.2 Low Energy (LE)
Data Capture Specifications	
2D Imager	SE2100 imager (1D and 2D). SE4710 imager (1D and 2D).
Camera	Rear - 8 MP autofocus; f/2.4 aperture; rear camera flash LED generates balancedwhite light; supports Torch mode. (Available only on TC25 with WSE4710 scan engine).
2D Imager Engine (SE2100) Specifications	
Field of View	Horizontal - 41.5° Vertical - 31.7°
Image Resolution	640 horizontal X 480 vertical pixels
Roll	360°
Pitch Angle	± 60° from normal
Skew Tolerance	± 60° from normal
Ambient Light	Sunlight: 10,000 ft. candles (107,639 lux)
Focal Distance	From front of engine: 10.7 cm (4.2 in.)
Illumination System	LED: Ultra white Pattern Angle: 42° horizontal, 32.0° vertical at 50% intensity
2D Imager Engine (SE4710) Specifications	
Field of View	Horizontal - 42.0° Vertical - 28°
Image Resolution	1280 horizontal X 800 vertical pixels
Roll	360°

Table 13 *TC25 Technical Specifications (Continued)*

Item	Description
Pitch Angle	± 60° from normal
Skew Tolerance	± 60° from normal
Ambient Light	Sunlight: 10,000 ft. candles (107,639 lux)
Focal Distance	From front of engine: 19.4 cm (7.64 in.)
Laser Aiming Element	LED: 610 Aiming Dot Brightness Level: 130 fcd nominal
Illumination System	LEDs: Hyper Red 660 nm Pattern Angle: 53° horizontal, 32° vertical at 50% intensity

Table 14 *Data Capture Supported Symbologies*

Item	Description
1D barcodes	Code 39, Code 128, Code 93, Codabar, MSI, UPC/EAN, Interleaved 2 of 5, RSS
2D barcodes	PDF-417, Micro PDF-417, Composite, TLC-39, Datamatrix, QR Code, Micro QRCode, Maxicode, Postal codes, Aztec Code, Han Xin

Decode Distances

The table below lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.

Table 15 *SE2100 Decode Distances*

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
5.0 mil Code 128	2.0 in. 5.1 cm	4.8 in. 12.2 cm
5 mil Code 39	1.7 in. 4.3 cm	5.8 in. 14.7 cm
6.6 mil PDF417	1.6 in. 4.1 cm	4.9 in. 12.4 cm
10 mil Data Matrix	1.2 in. 3.0 cm	4.9 in. 12.4 cm
100% UPCA	2.0 in. 5.1 cm	10.3 in. 26.2 cm
20 mil Code 39	2.1 in. 5.3 cm*	13.0 in. 33.0 cm

Table 15 *SE2100 Decode Distances (Continued)*

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
10 mil QR Code	1.1 in. 2.8 cm	5.2 in. 13.2 cm
*Limited by width of bar code in field of view. Notes: Photographic quality bar code at 15° tilt pitch angle under 30 fcd ambient illumination. Distances measured from front edge of scan engine chassis.		

Table 16 *SE4710 Decode Distances*

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
5.0 mil Code 128	3.1 in. 8.0 cm	8.3 in. 21.0 cm
5 mil Code 39	2.5 in. 6.3 cm	13.2 in. 33.5 cm
5 mil PDF417	3.8 in. 9.7 cm	8.0 in. 20.3 cm
10 mil Data Matrix	3.4 in. 8.6 cm	9.9 in. 25.1 cm
100% UPCA	1.6 in. 4.1 cm*	21.7 in. 55.2 cm
20 mil Code 39	1.8 in. 4.6 cm*	27.5 in. 69.9 cm
*Limited by width of bar code in field of view. Notes: Photographic quality bar code at 15° tilt pitch angle under 30 fcd ambient illumination. Distances measured from front edge of scan engine chassis.		

2-Pin I/O Connector Pin-Outs

Figure 135 I/O Connector

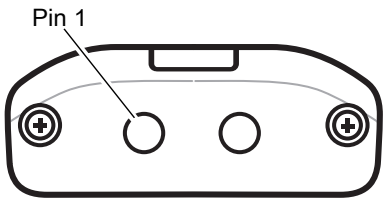


Table 17 *2-Pin I/O Connector Pin-Outs*

Pin	Signal	Description
1	TRIG	Trigger
2	GND	Ground

1-Slot Base Charge Only Cradle Technical Specifications

Table 18 *1-Slot Base Charge Only Cradle Technical Specifications*

Item	Description
Dimensions	Height: 8.9 cm (3.5 in.) Width: 9.7 cm (3.8 in.) Depth: 13.2 cm (5.2 in.)
Weight	147 g (5.2 oz.)
Input Voltage	12 VDC
Power Consumption	up to 15 watts
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0°C to 40°C (32°F to 104°F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10 kV contact +/- 10 kV indirect discharge

1-Slot Ethernet Cradle Technical Specifications

Table 19 *1-Slot Ethernet Cradle Technical Specifications*

Item	Description
Dimensions	Height: 12.2 cm (4.8 in.) Width: 9.8 cm (3.9 in.) Depth: 13.2 cm (5.2 in.)
Weight	391 g (13.8 oz.)
Input Voltage	12 VDC
Power Consumption	up to 15 watts

Table 19 *1-Slot Ethernet Cradle Technical Specifications*

Item	Description
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0°C to 40°C (32°F to 104°F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10 kV contact +/- 10 kV indirect discharge

5-Slot Charge Only Cradle Technical Specifications

Table 20 *5-Slot Charge Only Cradle Technical Specifications*

Item	Description
Dimensions	Height: 12.9 cm (5.1 in.) Width: 48.8 cm (19.2 in.) Depth: 13.2 cm (5.2 in.)
Weight	1,982 g (69.9 oz.)
Input Voltage	12 VDC
Power Consumption	up to 65 watts
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0°C to 40°C (32°F to 104°F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact +/- 10kV indirect discharge

Trigger Handle Technical Specifications

Table 21 *Trigger Handle Technical Specifications*

Item	Description
Dimensions	Height: 12.2 cm (4.8 in.) Width: 7.6 cm (3.0 in.) Depth: 13.1 cm (5.2 in.)
Weight	91 g (3.2 oz.)
Operating Temperature	-20°C to 50°C (-4°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	10% to 95% non-condensing
Drop	1.8 m (6 feet) drops to concrete over temperature range.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

Extended Power Pack Technical Specifications

Table 22 *Extended Power Pack Technical Specifications*

Item	Description
Dimensions	Height: 11.7 cm (4.6 in.) Width: 7.6 cm (3.0 in.) Depth: 2.9 cm (1.1 in.)
Weight	103 g (3.6 oz.)
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0°C to 40°C (32°F to 104°F)
Humidity	0% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 20kV air +/- 10kV contact

Index

Numerics

5-slot charge only cradle kit 25

A

advanced data formatting rules 94
approved cleanser 162
apps
    RxLogger 125
    RxLogger Utility 132, 134
arm mount 26

B

barcode input 71
    enabled 71
battery charging 18

C

cleaning instructions 162
configuration 11
cradle
    connector cleaning 163
cradle mount 25
cradle mounting adapter 26

D

data capture 11
data capture plus 69
datawedge
    advanced data formatting rules 94
    associating applications 67
    auto import 102
    auto switch to default on event 71
    barcode input 71
    configuration and profile file management 102
    configuring ADF plug-in 94
    creating a new profile 66
    data capture plus 69
    decoders 72
    disabling 66, 103
    enterprise folder 102
    exporting a configuration file 101
    importing a configuration file 101
    input plugins 63
    intent output 88
    intent overview 89
    IP output 90
    keep enabled on suspend 85
    keystroke output 86
    multibarcode params 85
    options menu 65
    output plug-ins 64
    plug-ins 63
    process plug-ins 64
    profile configuration 66
    profile context menu 65
    profile0 63
    profiles 62
    profiles screen 64
    programming notes 103
    reader params 81
    scan params 84
    scanner selection 71
    settings 100
    UDI params 85
    UPC EAN params 79
    voice input 85
DC line cord 27
decoder params
    Codabar 74
    Code 11 74
    Code 128 75
    Code 39 76
    Code 93 76
    Composite AB 76
    decode lengths 79
    Discrete 2 of 5 76
    GS1 DataBar Limited 77
    HAN XIN 77
    Interleaved 2 of 5 77

Matrix 2 of 5 77
MSI 78
UK Postal 78
UPCA 78
UPCE0 78
UPCE1 79
US Planet 79
decoders 72
disconnect host computer 61
display
cleaning 163

E

extended power pack 25

F

file transfer 60

H

hand strap 26
harmful ingredients 162

M

memory 11
microSD card 14, 20
multibarcode params 85

O

operating system 11

P

photo transfer 61
power supply 26

R

reader params 81
RxLogger 125
configuration 126
configuration file 131
disable logging 132
enable logging 131
extract log files 132
RxLogger Utility 132, 134

S

scan params 84
screen protector 26
sensors 171
settings
datawedge 100
SIM card 22
soft holster 26
soft reset 24
software version 12
software versions 11
symbologies 173

T

trigger handle 26
troubleshooting 165
TC25 165

U

UDI params 85
UPC EAN params 79

V

voice input 85

W

wrist mount 26