MC18
WITH ANDROID™ OS
PRODUCT REFERENCE GUIDE

MC18 WITH ANDROID™ OS
Product Reference Guide

MN002177A01

Rev. A

July 2015

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an “as is” basis. All software, including firmware, furnished to the user is on a licensed basis. We grant to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission. The user agrees to maintain copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

We reserve the right to make changes to any software or product to improve reliability, function, or design.

We do not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any of our intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in our products.

Zebra Technologies Corporation
3 Overlook Point
Lincolnshire, IL 60069 U.S.A.
http://www.zebra.com

Zebra and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

© 2015 ZIH Corp and/or its affiliates. All rights reserved.

Revision History

Changes to the original manual are listed below:

Change	Date	Description
01 Rev. A	07/2015	Initial release.

TABLE OF CONTENTS

About This Guide

Chapter 1: Getting Started

Chapter 2: Using the MC18

Chapter 3: Wireless

Chapter 8: Administrator Utilities

Chapter 10: Application Deployment

Chapter 11: Settings

Chapter 12: Maintenance and Troubleshooting

Appendix A: Technical Specifications

Index

ABOUT THIS GUIDE

Introduction

This guide provides information about setting up and configuring MC18 mobile computers with Android operating system and installing its accessories.

✓ ***NOTE*** Some screens or windows shown in this guide may differ from the actual screens shown on the MC18.

Documentation Set

The documentation set for the MC18 is divided into guides that provide information for specific user needs.

MC18 documentation includes:

- **MC18 Quick Reference Guide** - describes basic set up and operation of the MC18 and it's cradles. The guide also includes regulatory and safety information.
- **MC18 Product Reference Guide** (this guide) - describes how to set up, operate and program the MC18 with Android operating system and it's accessories.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
MC18	WLAN: 802.11 a/b/g/n WPAN: Bluetooth v4.0	WVGA 4.0" color	1 GB RAM/4 GB Flash	imager	Android Open Source Project (AOSP) 4.4.4.

Software Versions

To determine the current software versions touch ⚙ > **About device**.

- Serial number - Displays the serial number.
- Model number- Displays the model number.
- Android version - Displays the operating system version.
- Kernel version - Displays the kernel version number.
- Build number - Displays the software build number.

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Getting Started*, describes the features and basic operation of the MC18, lists the accessories for the MC18 and explains how to install and charge the batteries and start the MC18 for the first time.
- *Chapter 2, Using the MC18*, provides instructions for connecting the MC18 to a host computer and using the OS desktop of the MC18.
- *Chapter 4, Applications*, provides information on various applications pre-installed on the MC18.
- *Chapter 5, Data Capture*, provides information for capturing bar code data.
- *Chapter 6, Cradle Installation*, provides installation instructions for the MC18 cradles and other accessories.
- *Chapter 7, USB Communication*, provides instructions for connecting the MC18 to a host computer.
- *Chapter 8, Administrator Utilities*, provides information for using the MX Administrator Utilities.
- *Chapter 9, DataWedge*, provides information for configuring DataWedge.
- *Chapter 10, Application Deployment*, provides instructions for downloading software and files to the MC18.
- *Chapter 11, Settings*, provides various setting for the MC18.
- *Chapter 12, Maintenance and Troubleshooting*, includes instructions on cleaning and storing the MC18, and provides troubleshooting solutions for potential problems during MC18 operation.
- *Appendix A, Technical Specifications*, includes a table listing the technical specifications for the MC18 and accessories.

Notational Conventions

The following conventions are used in this document:

- *Italics* are used to highlight the following:
  - Chapters and sections in this guide
  - Related documents

- **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
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential
  - Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

✓ ***NOTE*** This symbol indicates something of special interest or importance to the reader. Failure to read the note will not result in physical harm to the reader, equipment or data.

⚠ ***CAUTION*** This symbol indicates that if this information is ignored, the possibility of data or material damage may occur.

⚠ ***WARNING!*** **This symbol indicates that if this information is ignored the possibility that serious personal injury may occur.**

Related Documents and Software

The following documents provide more information about the MC18 mobile computers.

- *MC18 Quick Reference Guide,* p/n MN000835Axx

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

Service Information

If you have a problem with your equipment, contact Customer Support for your region. Contact information is available at: http://www.zebra.com/support.

When contacting Customer Support, please have the following information available:

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

We respond to calls by E-mail, or telephone within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra 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 business product from a business partner, contact that business partner for support.

CHAPTER 1 GETTING STARTED

Introduction

This chapter describes the features of the MC18 and explains how to install and charge the battery, how to capture data using the integrated Imager and how to reset the MC18.

Unpacking

Carefully remove all protective material from the MC18 and save the shipping container for later storage and shipping.

Verify that box contains all the equipment listed below:

- MC18
- Two Torx screws inside a plastic bag (used for securing the battery cover to the MC18)
- Quick Reference Guide

Inspect the equipment for damage. If you are missing any equipment or if you find any damaged equipment, contact Support immediately. See *Service Information on page xiii* for contact information.

Removing the Screen Protection Film

A screen protection film is applied to the MC18 screen to protect the screen during shipping. To remove the screen protector, carefully lift the thin film off the display.

Features

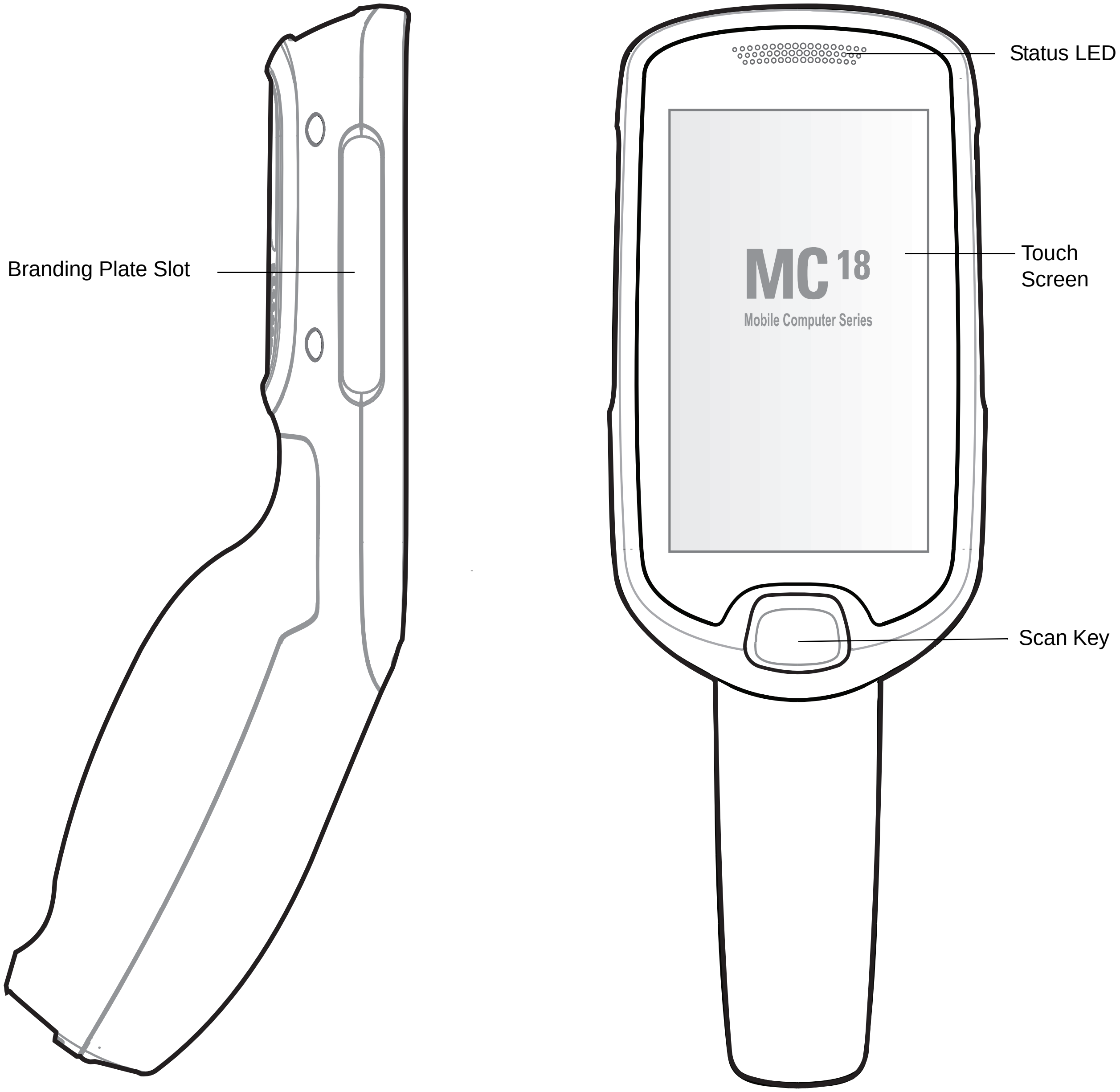


Figure 1-1 *Front View*

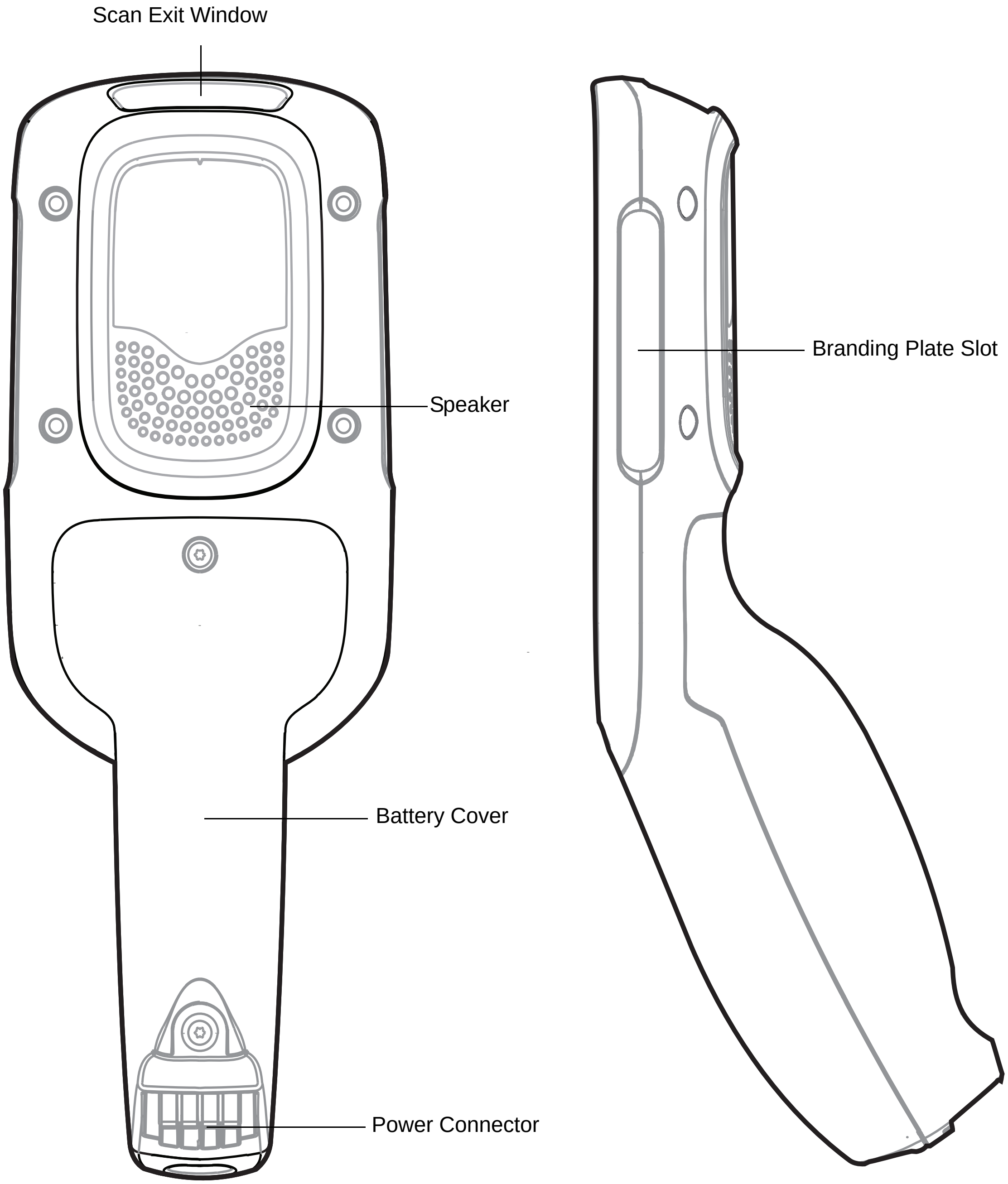


Figure 1-2 *Back View*

Accessories

Table 1-1 *Accessories*

Accessory	Part Number	Description
MC18 Lithium Ion Battery	BTRY-MC18-27MAG-01	MC18 Lithium Ion Battery.
	BTRY-MC18-27MAG-10	MC18 Lithium Ion Battery (QTY-10).
High Density (HD) Three Slot Cradle (Locking).	CRD-MC18-3SLCKH-01	The cradle is used for docking up to three MC18 units in HD installation configuration. The cradle slots are equipped with a mechanism that locks the MC18 units inside the slots. The Three Slot Cradle requires power supply unit (PWRS-14000-241R), DC line cord and country specific AC line cord (sold separately).
High Density (HD) Three Slot Cradle (Non-Locking)	CRD-MC18-3SLOTH-01	The cradle is used for docking up to three MC18 units in HD installation configuration. Requires power supply unit (PWRS-14000-241R), DC line cord and country specific AC line cord (sold separately).
Super High Density (SHD) Three Slot Cradle (Locking)	CRD-MC18-3SLCKS-01	The cradle is used for docking up to three MC18 units in SHD installation configuration. The cradle slots are equipped with a mechanism that locks the MC18 units inside the slots. Requires power supply unit (PWRS-14000-241R), DC line cord and country specific AC line cord (sold separately).
Single Slot Cradle	CRD-MC18-1SLOT-01	The cradle is used for docking a single MC18. Requires power supply unit (PWRS-14000-241R), DC line cord and country specific AC line cord (sold separately).
Release Key	KT-MC18-CKEY-20	Tool used to mechanically unlock the MC18 from the Three Slot Cradle and the Single Slot Cradle (QTY-20).
MC18 Terminal Reboot Tool	KT-MC18-REBOOT-05	Tool used to perform cold boot of the MC18 (QTY-5).
Cradle Cover Removal Tool	KT-MC18-CTOOL-01	Tool used for removing the Three Slot Cradle cover.
Deployment Kit	KT-MC18-CSTKIT-01	Includes: • 20-pack of Release Key (KT-MC18-CKEY-20) • 5-pack of Terminal Reboot Tool KT-MC18-REBOOT-05) • One Three Slot Cradle Front Panel Removal Tool (KT-MC18-CTOOL-01)

Table 1-1 *Accessories (Continued)*

Accessory	Part Number	Description
Single Slot Cradle Release Key	PSS-3KY01-00R	Key used to mechanically unlock the MC18 from a Single Slot Cradle (QTY-20).
Cart Holder Mounting Kit	PSS-3SH01-00R	Kit for mounting the MC18 on a shopping cart.
Programming Cable	CBL-MC18-USB1-01	USB communication cable for connecting the MC18 to a host computer.
Interconnection Cable	25-66431-01R	An extension cable (12.6 Inch / 32 centimeter) for connecting the Three Slot Cradle to DC “Y” charging cable that is connected to power supply unit (PWRS-14000-241R).
Cradle Interconnection Extension Cable	CBL-MC18-EXINT1-01	An Interconnection extension cable (12.6 Inch / 32 centimeter) for connecting Three Slot Cradle.
Charging Cable	CBL-MC18-Y2MET-01	DC “Y” charging cable (19.5 Inch / 49.5 centimeter) for connecting cradles to power supply unit (PWRS-14000-241R).
DC Charging Cable	25-66420-01R	DC charging cable (19.5 Inch / 49.5 centimeter) used to connect a power supply unit (PWRS-14000-241R) to one Single Slot Cradle.
DC “Y” Charging Cable Long	25-67592-01R	DC “Y” charging cable (39.7 Inch / 1 meter). Connects a power supply unit (PWRS-14000-241R) to two separate Three Slot Cradles.
DC “Y” Charging Cable Short	25-66210-01R	DC “Y” charging cable (19.5 Inch / 1 meter). Connects a power supply unit (PWRS-14000-241R) to two separate Three Slot Cradles.
Power Supply Unit	PWRS-14000-241R	100-240VAC, 12VDC, 9A. Requires country specific AC line cord and DC cable (sold separately).
AC Line Cord	23844-00-00R	AC Line Cord, 7.5 feet long, grounded, three wire for power supplies. Associated Country: United States
AC Line Cord	50-16000-221R	AC Line Cord, 1.8 meter, meter grounded, three wire, USA NEMA 5-15P. Associated Country: United States
AC Line Cord	50-16000-671R	AC Line Cord, 1.8 meter, grounded, three wire, CIE 23-16 plug. Associated Country: Italy.
AC Line Cord	50-16000-217R	AC Line Cord, 1.9 meter, grounded, three wire, AS 3112 plug. Associated Countries: Australia, New Guinea
AC Line Cord	50-16000-218R	AC Line Cord, 1.8 meter, grounded, three wire, NEMA 1-15P plug. Associated Country: Japan.

Table 1-1 *Accessories (Continued)*

Accessory	Part Number	Description
AC Line Cord	50-16000-219R	AC Line Cord, 1.8 meter, grounded three wire, BS1363 plug. Associated countries: Hong Kong, Iraq, Malaysia, Singapore, United Kingdom.
AC Line Cord	50-16000-220R	AC Line Cord, 1.8 meter, grounded three wire CEE 7/7plug. Associated countries: Europe, Abu Dhabi, Bolivia, Dubai, Egypt, Iran, Russia, Vietnam.
AC Line Cord	50-16000-257R	AC Line Cord, 1.8 meter, grounded three wire, IEC 60320 C13 plug. Associated Country: China.
AC Line Cord	50-16000-669R	1.9 meter grounded three wire, BS 546 Plug. Associated country: India.
AC Line Cord	50-16000-672R	1.9 meter grounded three wire, S132 Plug. Associated country: Israel.
AC Line Cord	50-16000-678R	36 inch grounded three wire. Associated country: United States

Status LED

The Status LED indicates imaging and charging status. *Table 1-2* describes the Status LED indications.

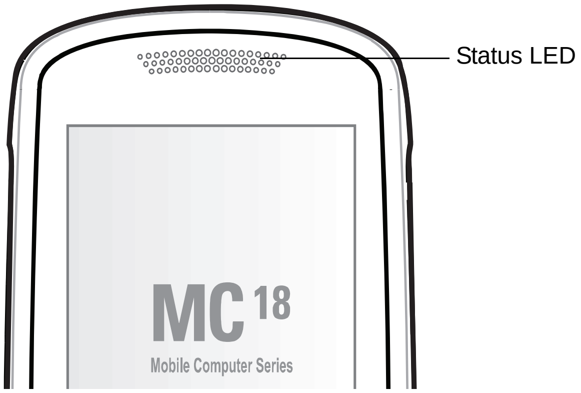


Figure 1-3 *MC18 Status LED*

Table 1-2 *Status LED Indications*

LED State	Indication
Imaging	
Off	Normal operation or MC18 is turned off.
Red	Imaging in progress (Scan key is pressed).
Single Green blink	Successful decode.
Charging (MC18 docked in cradle)	
Off	Power not applied to cradle. MC18 not inserted properly. Charging LED feature disabled. See *Charging the Battery on page 1-10*.
Blinking green	Charging.
Solid green	Charging complete.
Blinking red	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).

Scan Key

The Scan key operates the imager when a scanning application is active. When the MC18 is turned off, pressing the Scan key to power on the MC18.

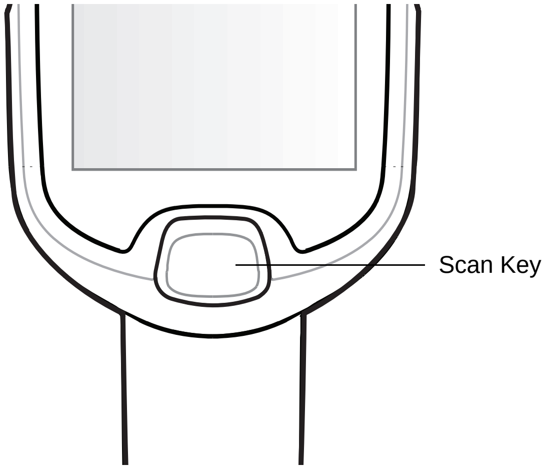


Figure 1-4 *Scan Key*

Getting Started

To start using the MC18 for the first time:

- Install the battery
- Charge the battery.

Installing the Battery

To install the battery:

1. Remove tape securing battery cover to handle.
2. Lift the battery cover from the handle.
3. Guide and press the battery cable connector into the female connector inside the battery compartment. The connector is designed to only fit one way.
4. Place the battery inside the battery compartment.
5. Place the battery cover onto the handle.
6. Remove the two Torx screws from the provided plastic bag, inside the shipping box.
7. Secure the battery cover with the two Torx screws using a T8 Torx drive. Torque the screws to 3.6 Kgf-cm (3.1 in-lb).

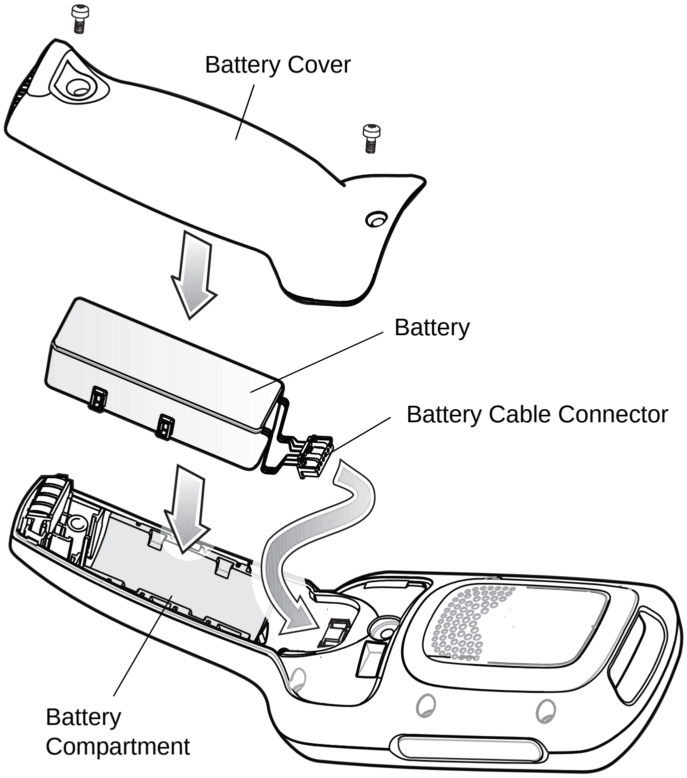


Figure 1-5 *Installing the Battery*

Removing the Battery

To remove the battery:

1. Touch and hold the soft power button ⏻ until the menu appears.

2. Touch **Power off**.

3. Touch **OK**.

CAUTION The MC18 must be off before removing the battery. Failing to turn off the MC18 before removing the battery may damage the data stored on flash memory or corrupt the operating system files.

4. Use T8 Torx drive to remove the two screws that secure the battery cover.

5. Lift the battery cover from the handle.

6. Inside the battery compartment, press down the plastic tab of the Battery cable connector and slide it out of the female connector.

7. Remove the battery from the battery compartment.

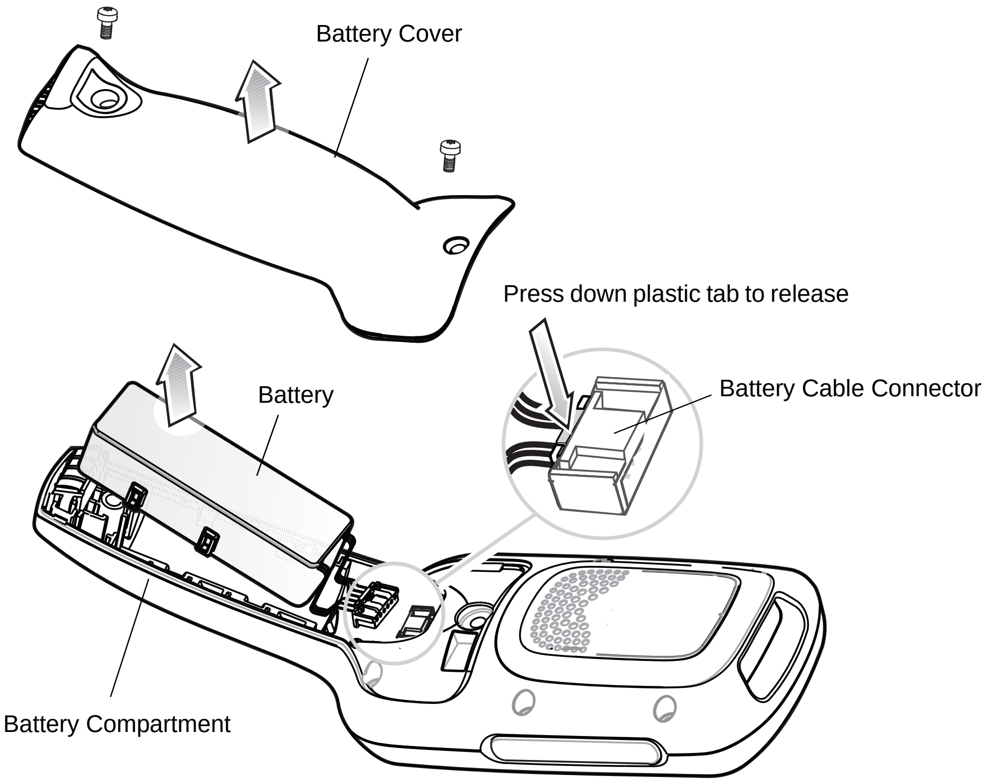


Figure 1-6 *Removing the Battery*

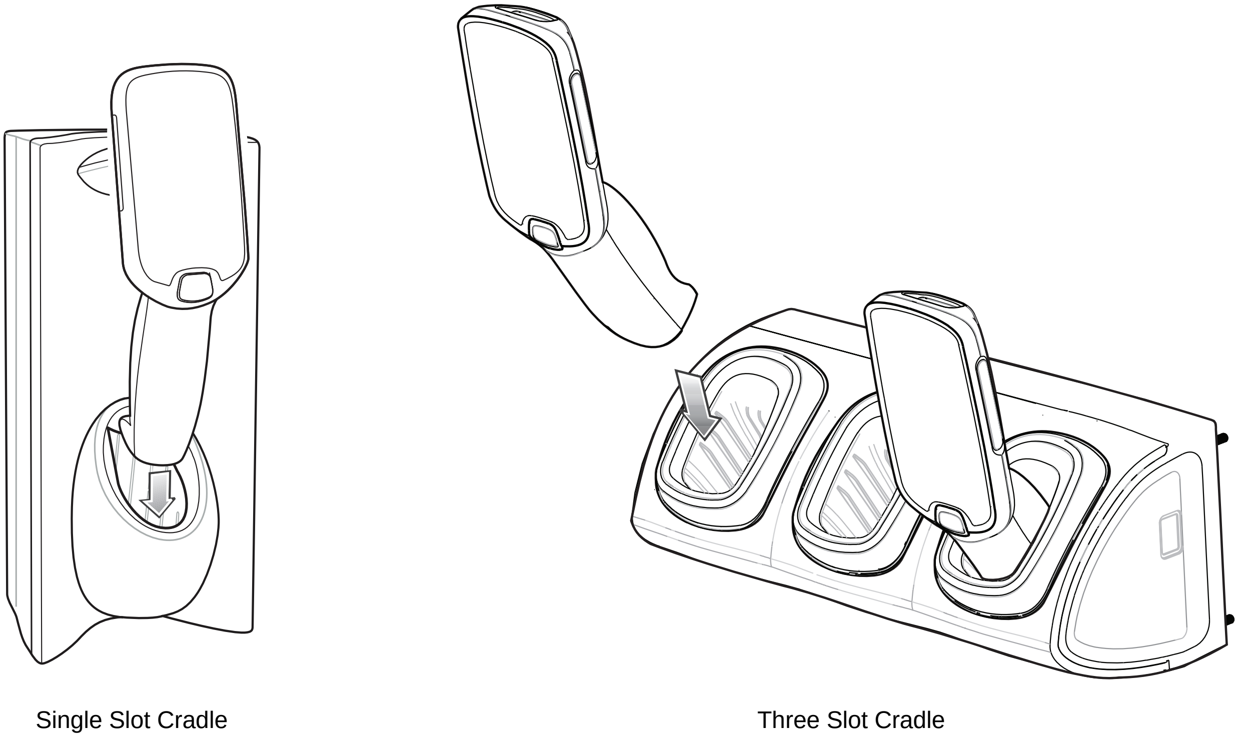
Charging the Battery

CAUTION Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 12-1*.

Before using the MC18 for the first time, charge the battery. The battery fully charges in approximately four hours.

To charge the battery:

1. Ensure the cradle is connected to the appropriate power source. See *Chapter 6, Cradle Installation* for more information.
2. Dock the MC18 in a cradle. The MC18 starts to charge automatically.



Single Slot Cradle

Three Slot Cradle

Figure 1-7 *Docking MC18 into Cradle*

By default the Charging LED indication is disabled. The user can enable the Charging LED indication. Touch ⚙ > **Charging indicator**. Touch **Enable Charging indicator** checkbox.

Table 1-3 *Charging Status LED Indications*

LED State	Indication
Off	Power not applied to cradle. MC18 not inserted properly. Charging LED feature disabled.
Blinking green	Charging.
Solid green	Charging complete.
Blinking red	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).

Starting the MC18

The MC18 starts automatically as soon as power is applied; either with a charged battery installed or when inserted into the cradle.

If charged battery is installed and the MC18 is turned off, press the Scan key to turn on.

When the MC18 is powered on for the first time, it initializes its system. The splash screen appears for a short period of time.

Figure 1-8 *Splash Screen*

The splash screen is followed by the boot animation screen and then the **Home Screen**.

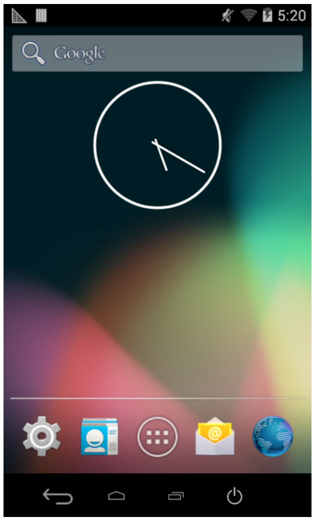


Figure 1-9 *Home Screen*

Powering On

To power on the MC18, press and release the Scan key.

Manual Release of MC18 from Cradles

The MC18 cradles contain a locking mechanism that locks the MC18 inside the cradle when docked. The MC18 releases from the cradle when a software command is received from the system. If the MC18 fails to un-lock during normal operation, use a release key to un-lock the MC18.

Software Release

To remove the MC18 from the cradle:

1. Touch and hold the soft power button ⏻ until the menu appears.
2. Touch **Cradle unlock**. The cradle unlocks the MC18.
3. Remove the MC18 from the cradle.

Manual Release of MC18 from the Single Slot Cradle

✓ ***NOTE*** The MC18 also can be unlocked from the cradle by software command using the Cradle Utility (see *Cradle Utility on page 4-15*).

To release a locked MC18 from a Single Slot Cradle:

1. Insert the release key into the slot located at the bottom side of the cradle.
2. While pressing the release key all the way into the slot, remove the MC18 from the cradle.

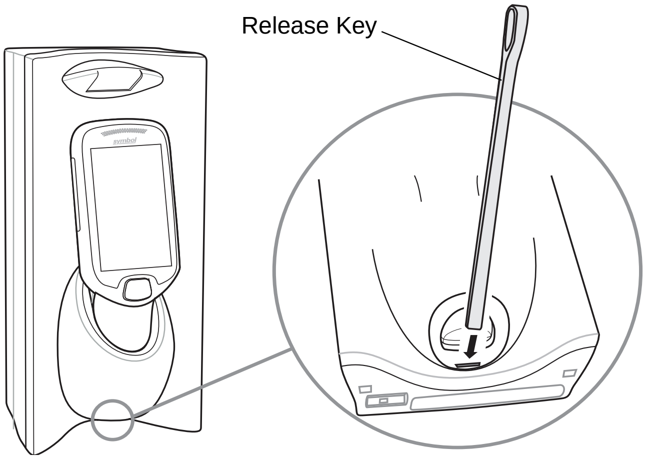


Figure 1-10 *Manual Release of MC18 from a Single Slot Cradle*

Manual Release of MC18 from the Three Slot Cradle

✓ ***NOTE*** The cradle includes models that do not have a locking mechanism. To identify the model of cradle, refer to *Table 1-1 on page 1-4*.

✓ ***NOTE*** The MC18 also can be released by software command using the Cradle Utility application (see *Cradle Utility on page 4-15*) or customer developed application using Zebra Android EMDK.

To release a locked MC18 from a Three Slot Cradle:

1. Insert the release key straight into the slot, to a point where the bend stops.
2. Hold the release key pressed inside the slot and remove the MC18 from the slot.

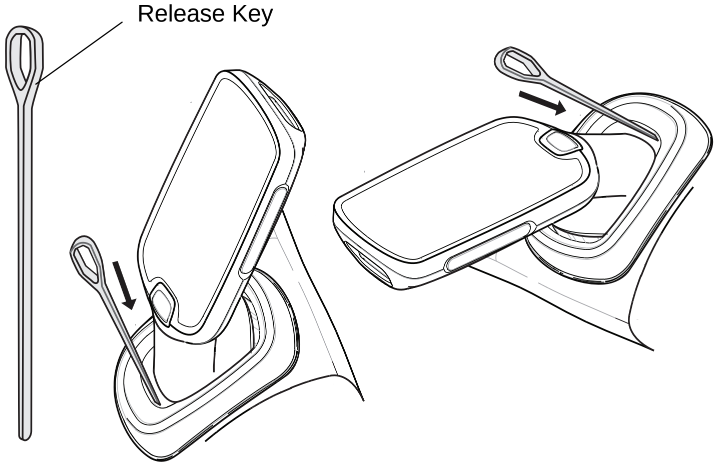


Figure 1-11 *Manual Release of MC18 from a Three Slot Cradle*

Battery Management

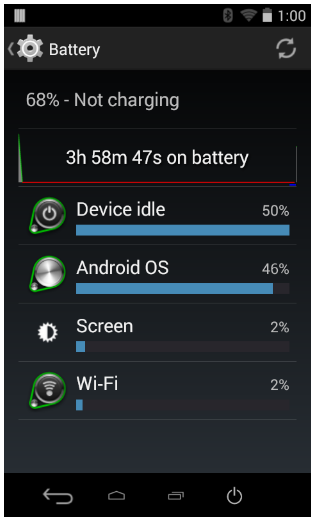
To check the charge status of the main battery, on the Home screen touch ⚙ > ⓘ **About device** > **Status**.

Battery status indicates that the battery is discharging (not charging) and **Battery level** lists the battery charge (as a percentage of fully charged).

Monitor Battery Usage

The Battery screen lists which applications consume the most battery power. Also use it to turn off applications that were downloaded if they are consuming too much power.

Touch ⚙ > **Battery**.



68% - Not charging

3h 58m 47s on battery

Device idle	50%
Android OS	46%
Screen	2%
Wi-Fi	2%

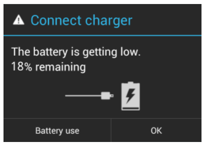
Figure 1-12 *Battery Screen*

The Battery screen lists the applications using the battery. The discharge graph at the top of the screen shows the rate of the battery discharge since last charged (short periods of time when connected to a charger are shown as thin green lines at the bottom of the chart), and how long it has been running on battery power.

Touch an application in the Battery screen to display details about its power consumption. Different applications display different information. Some applications include buttons that open screens with settings to adjust power use.

Low Battery Notification

When the battery charge level drops below 15%, the MC18 displays a notice to connect the MC18 to power. Place the MC18 into a cradle to charge the battery.



Connect charger

The battery is getting low.
18% remaining

Figure 1-13 *Low Battery Notification*

When the battery charge drops below 10%, the MC18 displays a notice to connect the MC18 to power. The user must charge the battery using one of the charging accessories.

When the battery charge drops below 5%, the MC18 turns off.

Place the MC18 into a cradle to charge the battery.

Battery Optimization

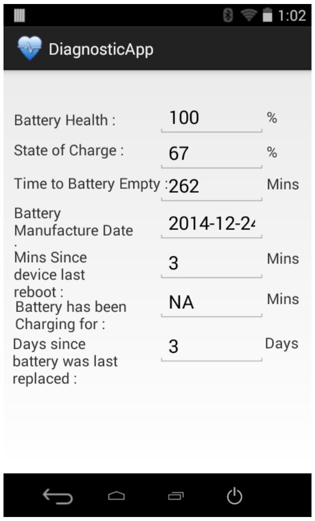
Observe the following battery saving tips:

- Set the screen to turn off after a short period of non-use. See *Setting Screen Timeout Setting on page 1-17*.
- Reduce screen brightness. See *Setting the Screen Brightness on page 1-17*.
- Turn off all wireless radios when not in use.
- Turn off automatic syncing for Email, Calendar, Contacts and other applications.
- Use the Power Control widget to check and control the status of radios, the screen brightness, and syncing.
- Minimize use of applications that keep the MC18 from suspending, for example, music and video applications.

Battery Diagnostics

The Diagnostic App displays battery status information. This information can also be retrieved programmatically using the Zebra Android EMDK.

To view the results of the diagnostics test touch ⊞ > ♥.



DiagnosticApp

Battery Health : 100 %

State of Charge : 67 %

Time to Battery Empty : 262 Mins

Battery Manufacture Date : 2014-12-2

Mins Since device last reboot : 3 Mins

Battery has been Charging for : NA Mins

Days since battery was last replaced : 3 Days

Figure 1-14 *Diagnostic App Screen*

- **Battery Health** - Indicates the health of the battery.
- **State of Charge** - Indicates the current charge level of the battery.
- **Time to Battery Empty** - Indicates the amount of time (in minutes) before the device goes into critical suspend mode.The device goes to suspend depending on the display timeout setting. However, the device goes to critical suspend when the battery charge level is at 5%.
- **Battery Manufacture Date** - Displays the battery manufacturer date (YYYY-MM-DD).
- **Minutes Since device last reboot** - Indicates how long ago (in minutes) the device was rebooted.
- **Battery has been charging for** - Indicates the amount of time (in minutes) that the device has been charging during the current charge cycle.
- **Days since battery was last replaced** - Indicates the number since the battery was replaced in the device.

Turning Off the Radios

To turn off all the radios:

NOTE Alternately, you can place the device into **Airplane mode** using the **Quick Settings** option.

1. Press the soft power button ⏻ until the menu appears.
2. Touch **Airplane mode**. The airplane icon ✈ appears in the Status bar indicating that all the radios are off.

Setting the Date and Time

The date and time is automatically synchronized using a NITZ server when the MC18 is connected to a cellular network. The user is only required to set the time zone or set the date and time when not connected to a cellular network.

1. Touch ⚙.
2. Touch 🕓 **Date & time**.

3. Touch **Automatic date & time** to disable automatic date and time synchronization.
4. Touch **Set date**.
5. Move the sliders up and down to select the month, date and year.
6. Touch **Done**.
7. Touch **Set time**.
8. Move the sliders up and down to select the hour, minutes and part of the day.
9. Touch **Done**.
10. Touch **Select time zone**.
11. Select the current time zone from the list.
12. Touch ⌂.

Display Setting

Use Display settings to change the screen brightness, set sleep time and change font size.

Setting the Screen Brightness

To set the screen brightness:

1. Touch ⚙.
2. Touch ◐ **Display**.
3. Touch **Brightness**.

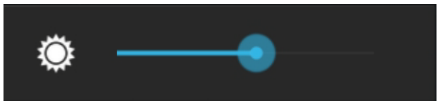


Figure 1-15 *Brightness Dialog Box*

4. In the Brightness dialog box, use the slider to set a brightness level.
5. Touch ⌂.

Setting Screen Timeout Setting

To set the screen sleep time:

1. On the Home screen, touch ⚙.
2. Touch ◐ **Display**.
3. Touch **Sleep**.
4. Select one of the sleep values.
   - **15 seconds**

- **30 seconds**
- **1 minute**
- **2 minutes**
- **5 minutes**
- **10 minutes**
- **30 minutes**
- **Never** (default).

5. Touch ⌂.

Setting Font Size

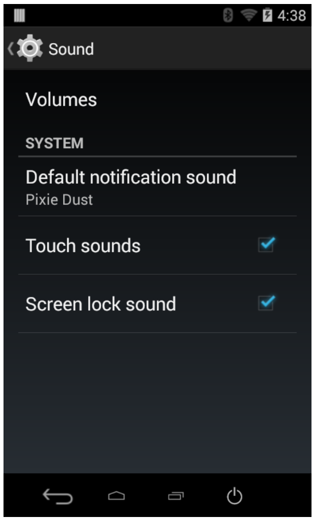
To set the size of the font is system applications:

1. Touch ⚙.
2. Touch ◐ **Display**.
3. Touch **Font size**.
4. Select one of the font size values.
   - **Small**
   - **Normal** (default)
   - **Large**
   - **Huge**.
5. Touch ⌂.

General Sound Setting

Use the Sounds settings to configure media and alarm volumes. On the Home screen, touch ⚙ > 🔊 **Sounds**.

Alternately, touch the Status bar and drag down to open the Notification panel. Touch ▦ > ⚙ > 🔊 **Sounds**.



4:38

Sound

Volumes

SYSTEM

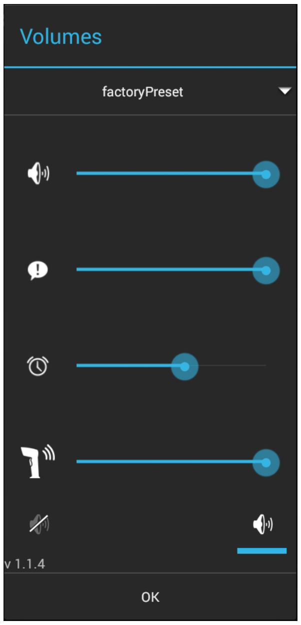
Default notification sound
Pixie Dust

Touch sounds ☑

Screen lock sound ☑

Figure 1-16 *Sounds Screen*

- **Volumes** – Use to change the volume of media, ringtones, notifications and alarms.



Volumes

factoryPreset

v 1.1.4

OK

Figure 1-17 *Volumes Dialog Box*

- 🔊 - Controls the music and media volume.
- ❗ - Controls the system notification volume.
- ⏰ - Controls the alarm clock volume.
- - Controls the scan good decode beep volume.
- Bottom row icons:
  - 🔇 - Places the system notification in silent mode.
  - 🔊 - Places the system notification in sound mode.

- **System**
  - **Default notification sound** - Touch to select a sound to play for all system notifications.
  - **Touch sounds** - Check to play a sound when making screen selections (default – enabled).
  - **Screen lock sounds**- Check to play a sound when locking and unlocking the screen (default – disabled).

Resetting the MC18

There are four reset functions:

- Soft reset
- Hard reset
- Enterprise reset
- Factory reset.

Performing a Soft Reset

Perform a soft reset if applications stop responding.

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

Performing a Hard Reset

⚠ ***CAUTION*** Perform a hard reset only if the MC18 stops responding.

When in a Cradle

To perform a hard reset when the MC18 is docked inside the cradle:

✓ ***NOTE*** Ensure power is applied to the cradle.

1. Press and hold the Scan key for 10 seconds until the display powers off.
2. Release of the Scan key.
3. Briefly press and release the Scan key, the MC18 reboots.

When Out of the Cradle

To perform a hard reset when the MC18 is out of the cradle:

1. Insert the terminal reboot tool into the MC18 power connector.

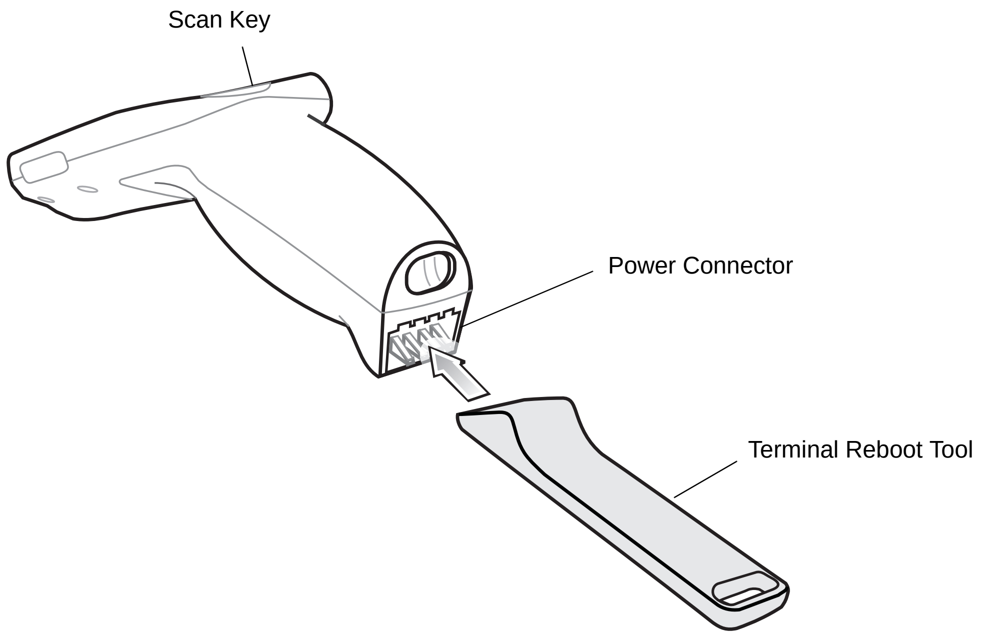


Figure 1-18 *Terminal Reboot Tool*

2. Press and hold the Scan key for 10 seconds until the display powers off.
3. Release of the Scan key.
4. Remove the terminal reboot tool.

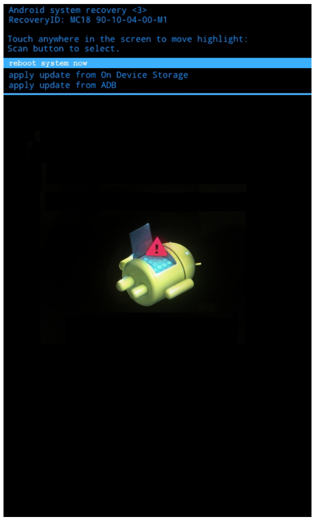
   Briefly press and release the Scan key, the MC18 reboots.

Performing an Enterprise Reset

An Enterprise Reset erases all data in the /cache and /data partitions and clears all device settings, except those in the /enterprise partition.

Before performing an Enterprise Reset, copy all applications and the key remap configuration file that you want to persist after the reset into the /enterprise/usr/persist folder.

1. Download the Enterprise Reset file from the Support Central web site.
2. Copy the 18N0KXXAE0000001.zip file to the root of the Internal Storage. See *Chapter 7, USB Communication*.
3. Remove the Programming cable from the device.
4. Press and hold the soft power button ⏻ until the menu appears.
5. Touch **Power Off**.
6. Touch **OK**.
7. Press and hold the Scan key.
8. When the System Recovery screen appears, release the button.



```
Android system recovery <3>
RecoveryID: MC18 90-10-04-00-M1

Touch anywhere in the screen to move highlight:
Scan button to select.
reboot system now
apply update from On Device Storage
apply update from ADB
```

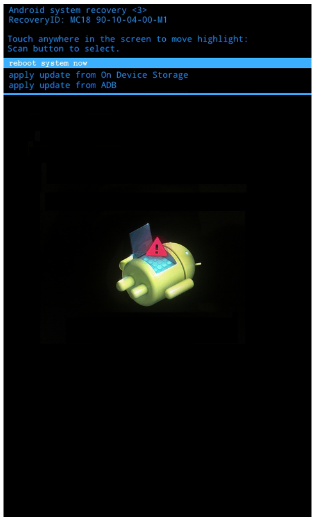
Figure 1-19 *System Recovery Screen*

9. Tap the display until **apply update from On Device Storage** is highlighted.
10. Press the Scan key.
11. Tap the display until 18N0KXXAE0000001.zip file is highlighted.
12. Press the Scan key. The Enterprise Reset occurs and then the device resets.

Performing a Factory Reset

A Factory Reset erases all data in the /cache, /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 MC18 System Update on page 138 for more information.

1. Download the Enterprise Reset file from the Support Central web site.
2. Copy the 18N0KXXFR0000001.zip file to the root of On Device Storage or the root of Internal Storage. See *Chapter 7, USB Communication*.
3. Remove the Programming cable from the device.
4. Press and hold the soft power button ⏻ until the menu appears.
5. Touch **Power Off**.
6. Touch **OK**.
7. Press and hold the Scan key.
8. When the System Recovery screen appears, release the button.



```
Android system recovery <3>
RecoveryID: MC18 90-10-04-00-M1

Touch anywhere in the screen to move highlight:
Scan button to select.

reboot system now
apply update from On Device Storage
apply update from ADB
```

Figure 1-20 *System Recovery Screen*

9. **Tap the display until apply update from On Device Storage** is highlighted.
10. Press the Scan key.
11. Tap the display until the 18N0KXXFR0000001.zip file is highlighted.
12. Press the Scan key. The Factory Reset occurs and then the device resets.

CHAPTER 2 USING THE MC18

Introduction

This chapter describes the screens, status and notification icons, and controls on the MC18, and provides basic instructions for using the MC18.

Home Screen

The Home screen displays when the MC18 turns on. Depending upon the configuration, the Home screen might appear different. Contact your system administrator for more information.

After a suspend or screen time-out, the Home screen displays with the lock sliders. Slide to the right toward to unlock the screen. For screen locking information see *Un-Locking the Screen on page 2-11*.

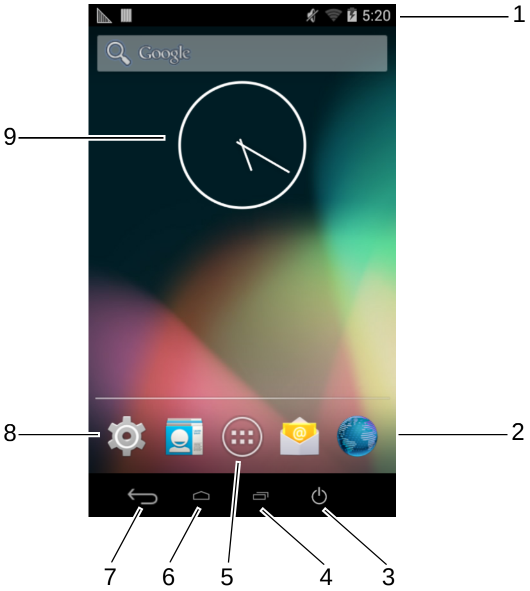


Figure 2-1 *Home Screen*

NOTE The Home screen icons can be configured by the user and may look different than shown.

The Home screen consists of the following:

Table 2-1 *Home Screen Items*

Item	Description
1 — Status Bar	Displays the time, status icons (right side), and notification icons (left side). For more information see *Status Icons on page 2-2* and *Managing Notifications on page 2-4*.
2 — Browser Icon	Opens the Browser application.
3 — Power Icon	Places the MC18 in suspend mode when touched and opens menu when touched and held.
4 — Menu Icon	Displays running applications.
5 — All Apps Icon	Opens the APPS window.
6 — Home Icon	Displays the Home screen.
7 — Back Icon	Displays the previous screen.
8 — Settings Icon	Opens the Settings window.
9 — Shortcut Icons	Opens applications installed on the MC18. See *Application Shortcuts and Widgets on page 2-5* for more information.
10 — Widgets	Launches stand-alone applications that run on the Home screen. See *Application Shortcuts and Widgets on page 2-5* for more information.

The Home screen provides four additional screens for placement of widgets and shortcuts. Swipe the screen left or right to view the additional screens.

Status Bar

The Status bar displays the time, notification icons (left side) and status icons (right side).

If there are more notifications than can fit in the Status bar, displays indicating that more notifications exist. Open the Notifications panel to view all notifications and status.

Status Icons

Table 2-2 *Status Icons*

Icon	Description
⏰	Indicates that the Alarm is active.
🔇	Indicates that the ringer is silenced.
🔋	Indicates that the battery is fully charged.

Table 2-2 *Status Icons*

Icon	Description
🔋	Indicates that the battery is partially drained.
🪫	Indicates that the battery charge is low.
❗	Indicates that the battery charge is very low.
⚡	Indicates that the battery is charging.
✈	Indicates that the Airplane Mode is active. All radios are turned off.
ᛒ	Indicates that Bluetooth is on.
📶	Connected to a Wi-Fi network.
▽	No Wi-Fi signal.

Notification Icons

Table 2-3 *Notification Icons*

Icon	Description
+	Indicates that more notifications are available for viewing.
🔄	Indicates that data is syncing.
1	Indicates an upcoming event.
?	Indicates that an open Wi-Fi network is available.
◉	Indicates that a song is playing.
!	Indicates that a problem with sign-in or sync has occurred.
↑	Indicates that the MC18 is uploading data.
↓	Indicates that the MC18 is downloading data when animated and download is complete when static.
ψ	Indicates that the MC18 is connected via USB cable.
🔑	Indicates that the MC18 is connected to or disconnected from virtual private network (VPN).

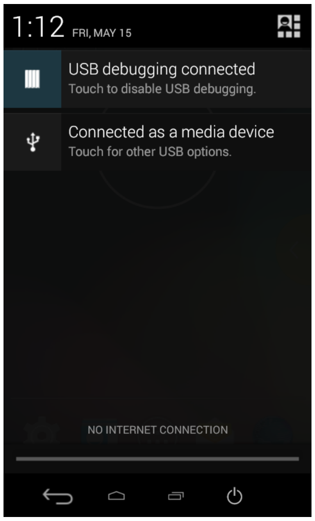
Table 2-3 *Notification Icons*

Icon	Description
⚙	Preparing Internal Storage.
||||	Indicates that USB debugging is enabled on the MC18.
👥	Indicates that the MultiUser feature is enabled. Appears only when MultiUser Administrator application is installed.
✓	Indicates that a new user is logging in. Appears only when MultiUser Administrator application is installed.
Rx	Indicates that the RxLogger application is running and capturing data.

Managing Notifications

Notification icons report the arrival of new messages, calendar events, and alarms, as well as ongoing events. When a notification occurs, an icon appears in the Status bar with a brief description. See *Notification Icons on page 2-3* for a list of possible notification icons and their description. Open the Notifications panel to view a list of all the notifications.

To open the Notification panel, drag the Status bar down from the top of the screen.


1:12 FRI, MAY 15

USB debugging connected
Touch to disable USB debugging.

Connected as a media device
Touch for other USB options.

NO INTERNET CONNECTION

Figure 2-2 *Notification Panel*

To respond to a notification, open the Notifications Panel and then touch a notification. The Notifications Panel closes and the subsequent activity is dependent on the notification.

To clear all notifications, open the Notifications Panel and then touch ☰. All event-based notifications are removed.

Ongoing notifications remain in the list.

To close the Notification Panel, drag the bottom of the Notifications Panel to the top of the screen or press.

Application Shortcuts and Widgets

Application shortcuts placed on the Home screen allow quick and easy access to applications. Widgets are self-contained applications placed on the Home screen to access frequently used features.

Adding an Application or Widget to the Home Screen

1. Go to the desired Home screen.
2. Touch ⊞.
3. Swipe right, if necessary, to find the application icon or widget.
4. Touch and hold the icon or widget until the Home screen appears.
5. Position the icon on the screen and then release.

Moving Items on the Home Screen

1. Touch and hold the item until it floats on the screen.
2. Drag the item to a new location. Pause at the edge of the screen to drag the item onto an adjacent Home screen.
3. Lift finger to place the item on the Home screen.

Removing an App or Widget from the Home Screen

1. Go to the desired Home screen.
2. Touch and hold the application shortcut or widget icon until it floats on the screen.
3. Drag the icon to ✕ Remove on the top of the screen and then release.

Folders

Use Folders to organize similar applications together. Tap the folder to open and display items in the folder.

Creating a Folder

To create a folder, there must be at least two app icons on the Home screen.

1. Go to the desired Home screen.
2. Touch and hold on one application icon.
3. Drag the icon and stack on top of another icon.
4. Lift and release.

Naming Folders

1. Touch the folder.

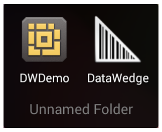


Figure 2-3 *Open Folder*

2. Touch the title area and enter a folder name using the keyboard.
3. Touch **Done**.
4. Touch anywhere on the Home screen to close the folder. The folder name appears under the folder.

Figure 2-4 *Renamed Folder*

Removing a Folder

1. Touch and hold the folder icon until it enlarges.
2. Drag the icon to ✕ Remove and release.

Home Screen Wallpaper

NOTE Use of Live Wallpaper may reduce battery life.

Changing the Home Screen Wallpaper

NOTE Use of Live Wallpaper may reduce battery life.

1. Touch and hold the desktop until the menu appears.
2. From the **Choose wallpaper from** menu, touch **Gallery**, **Live wallpapers** or **Wallpapers**.
   - **Gallery** - Select to use an image stored on the device.
   - **Live wallpapers** - Select to use an animated wallpaper image.
   - **Wallpapers** - Select to use a wallpaper image.
3. Touch **Save** or **Set wallpaper**.

Using the Touchscreen

Use the multi-tap sensitive screen to operate the device.

- **Tap** - Tap to:
  - select items on the screen
  - type letters and symbols using the on-screen keyboard
  - press on-screen buttons.

- **Tap and Hold** - Tap and hold:
  - an item on the Home screen to move it to a new location or to the trash.
  - an item in Apps to create a shortcut on the Home screen.
  - the Home screen to open a menu for customizing the Home screen.
  - an empty area on the Home screen until the menu appears.
- **Drag** - Tap and hold an item for a moment and then move finger on the screen until reaching the new position.
- **Swipe** - Move finger up and down or left and right on the screen to:
  - unlock the screen
  - view additional Home screens
  - view additional application icons in the Launcher window
  - view more information on an application's screen.
- **Double-tap** - Tap twice on a web page, map, or other screen to zoom in and out.
- **Pinch** - In some applications, zoom in and out by placing two fingers on the screen and pinching them together (to zoom out) or spreading them apart (to zoom in).

Using the On-screen Keyboard

Use the on-screen keyboard to enter text in a text field. To configure the keyboard settings, touch and hold , (comma) > ⚙ and then select **Android keyboard settings**.

Editing Text

Edit entered text and use menu commands to cut, copy, and paste text within or across applications. Some applications do not support editing some or all of the text they display; others may offer their own way to select text.

Entering Numbers, Symbols and Special Characters

To enter numbers and symbols:

- Touch and hold one of the top-row keys until a menu appears then select a number. Keys with alternate characters display an ellipsis (...) below the character.
- Touch and hold the Shift key with one finger, touch one or more capital letters or symbols to enter them, and then lift both fingers to return to the lowercase keyboard.
- Touch ?123 to switch to the numbers and symbols keyboard.
- Touch the =\< key on the numbers and symbols keyboard to view additional symbols.

To enter special characters, touch and hold a number or symbol key to open a menu of additional symbols.

- A larger version of the key displays briefly over the keyboard.
- Keys with alternate characters display an ellipsis (...) below the character.

Applications

The APPS screen displays icons for all installed applications. The table below lists the applications installed on the MC18. Refer to the MC18 Integrator Guide for information on installing and uninstalling application.

Table 2-4

Icon	Description
	App Gallery - Provides links to utilities and demonstration applications that can be installed on the MC18.
	Browser - Use to access the Internet or intranet.
	Calculator - Provides the basic and scientific arithmetic functions.
	Calendar - Use to manage events and appointments.
	Clock - Use to schedule alarms for appointments or as a wake-up.
	Cradle Utility - Use to control cradle functionality.
	DataWedge - Enables data capture using the imager.
	Diagnostic App - Provides information about battery health.
	Downloads - Lists all downloads files.
	DWDemo - Provides a way to demonstrate the data capture features using the imager. See *DataWedge Demonstration on page 4-10* for more information.
	elemez - Use to provide diagnostic information. See *Elemez on page 4-12* for more information.
	Email - Use to send and receive email.
	File Browser - Organize and manage files on the MC18. See *File Browser on page 4-1* for more information.
	Gallery - Use to view photos stored on the device. For more information, see *Gallery on page 4-3* for more information.

Table 2-4

Icon	Description
	MLog Manager - Use to capture log files for diagnostics. See *MLog Manager on page 4-11* for more information.
	Mobi Control Stage – Opens the **Mobi Control Stage** application to stage the device.
MSP	**MSP Agent** - Enables management of the MC18 from an MSP server. Requires the purchase of an appropriate MSP client license per device to suit the level of management functionality required.
●	**Music** - Play music stored on the device.
	People - Use to manage contact information. *People on page 4-2* for more information.
MSP	**Rapid Deployment**- Allows the MC18 to stage a device for initial use by initiating the deployment of settings, firmware and software. Requires the purchase of an MSP client license per device.
Rx	**RxLogger** - Use to diagnose device and application issues. See the *MC18 Integrator Guide* for more information.
🔍	**Search** - Use the Google search engine to search the Internet and the MC18.
⚙	**Settings** - Use to configure the MC18.
	StageNow - Allows the MC18 to stage a device for initial use by initiating the deployment of settings, firmware and software.
	AppLock Administrator - Use to configure the Application Lock feature. This icon appears after the optional application is installed.
	MultiUser Administrator - Use to configure the MultiUser feature. This icon appears after the optional application is installed.
	Secure Storage Administrator - Use to configure the Secure Storage feature. This icon appears after the optional application is installed.

Accessing Applications

All applications installed on the device are accessed using the **APPS** window.

1. On the Home screen, touch ⊞.

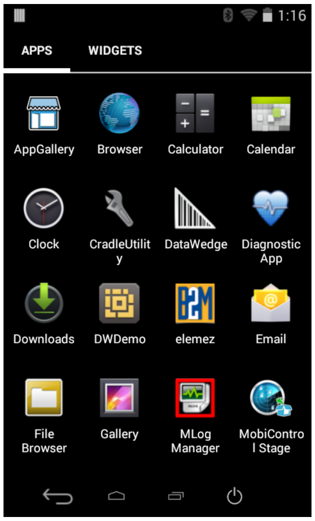


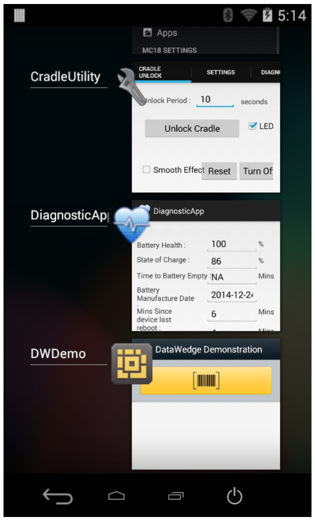
Figure 2-5 *APPS Window*

2. Slide the **APPS** window left or right to view more application icons. Touch an icon to open the application.

✓ ***NOTE*** See *Application Shortcuts and Widgets on page 2-5* for information on creating a shortcut on the Home screen.

Switching Between Recent Applications

1. Touch and hold ▭. A window appears on the screen with icons of recently used applications.



nlock Period : 10 seconds

☑ LED

□ Smooth Effect

Battery Health : 100 %

State of Charge : 86 %

Time to Battery Empty : NA Mins

Battery Manufacture Date 2014-12-2

Mins Since device last reboot : 6 Mins

Figure 2-6 *Recently Used Applications*

2. Slide the window up and down to view all recently used applications.

3. Swipe left or right to remove application from the list and force close the application.

4. Touch an icon to open it or touch ↩ to return to the current screen.

Un-Locking the Screen

Use the Lock screen to protect access to data on the MC18. Some email account require locking the screen. See *Chapter 11, Settings* for information on setting up the locking feature. The Locking feature functions differently in Single User mode or Multiple User mode.

Single User Mode

When locked, a 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 🔒 to the right toward 🔓 to unlock the screen.

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.

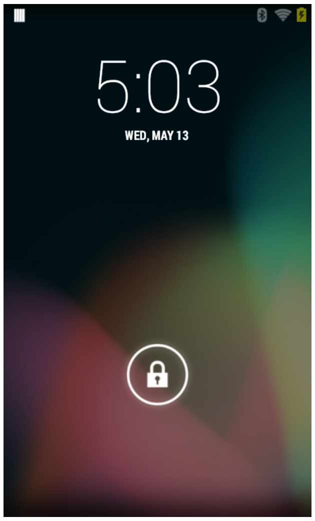


Figure 2-7 *Lock Screen*

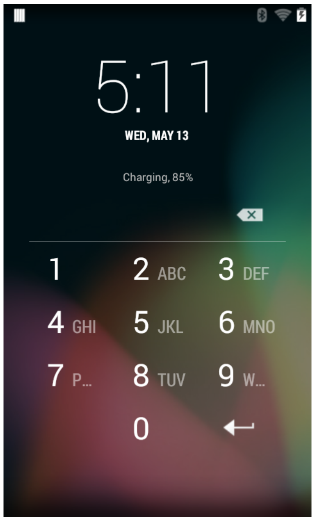


Figure 2-8 *PIN Screen*

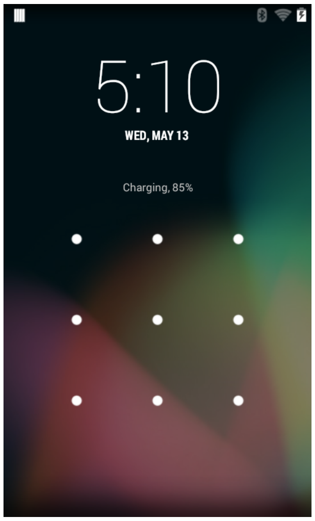


Figure 2-9 *Pattern Screen*

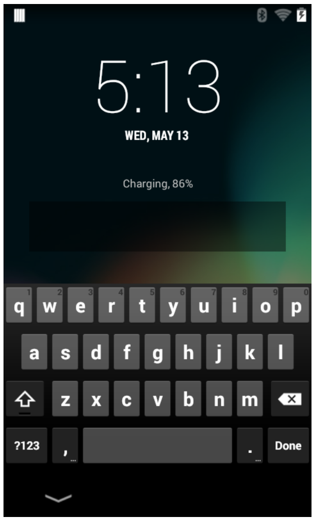


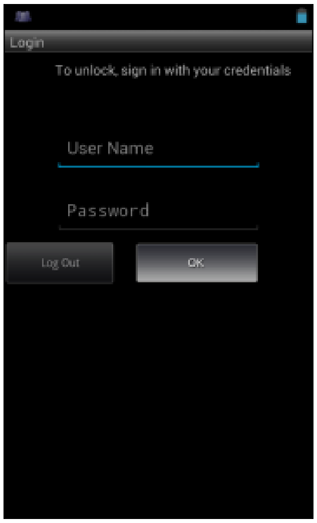
Figure 2-10 *Password Screen*

MultiUser Mode

With MultiUser login, multiple users can log on to the device with each user having access to various applications and features. When enabled, the Login screen appears after powering on, resetting or after the device wakes from suspend mode.

MultiUser Login

1. In the **Login** text field, enter the username.


Login

To unlock, sign in with your credentials

Figure 2-11 *Multiple User Log In Screen*

2. In the **Password** text field, enter the password.
3. Touch **OK**. After a resume from suspend, the user must enter the password.

MultiUser Logout

1. Drag the Status Bar down from the top of the screen.
2. Touch **MultiUser is active**.
3. Touch **Logout**.
4. The **Login** screen appears.

Suspend Mode

The MC18 goes into suspend mode when the user presses the Power button or after a period of inactivity (set in the Display settings window).

To wake the MC18 from Suspend mode, press the Power button.Alternately, press the Scan or Programmable button to wake the device.

The Lock screen displays. Slide 🔒 to the right toward 🔓 to unlock the screen. If the Pattern screen unlock feature is enabled, the Pattern screen appears instead of the Lock screen. See *Un-Locking the Screen on page 2-11*.

✓ ***NOTE*** If the user enters the PIN, password or pattern incorrectly five times, they must wait 30 seconds before trying again.

If the user forgets the PIN, password or pattern contact the system administrator.

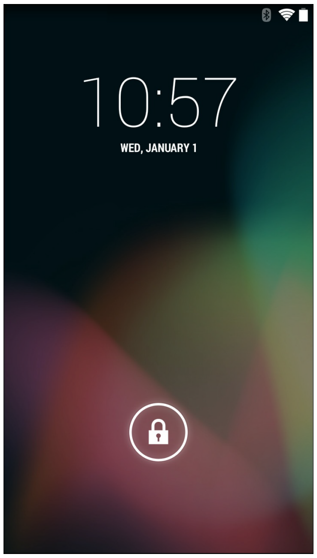


Figure 2-12 *Lock Screen*

CHAPTER 3 WIRELESS

Wireless Local Area Networks

Wireless local area networks (WLANs) allow the MC18 to communicate wirelessly inside a building. Before using the MC18 on a WLAN, the facility must be set up with the required hardware to run the WLAN (sometimes known as infrastructure). The infrastructure and the MC18 must both be properly configured to enable this communication.

Refer to the documentation provided with the infrastructure (access points (APs), access ports, switches, Radius servers, etc.) for instructions on how to set up the infrastructure.

Once the infrastructure is set up to enforce the chosen WLAN security scheme, use the **Wireless & networks** settings configure the MC18 to match the security scheme.

The MC18 supports the following WLAN security options:

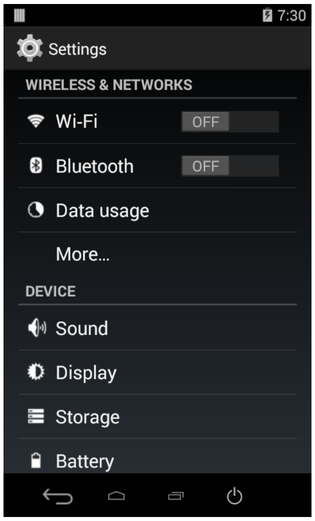
- Open
- Wireless Equivalent Privacy (WEP).
- Wi-Fi Protected Access (WPA/WPA2) Personal (PSK).
- Extensible Authentication Protocol (EAP).
  - Protected Extensible Authentication Protocol (PEAP) - with MSCHAPV2 and GTC authentication.
  - Transport Layer Security (TLS)
  - TTLS - with Password Authentication Protocol (PAP), MSCHAP and MSCHAPv2 authentication.
  - LEAP
  - EAP-FAST - with MSCHAPV2 and GTC authentication.

The **Status** bar displays icons that indicate Wi-Fi network availability and Wi-Fi status. See *Status Bar on page 2-2* for more information.

✓ ***NOTE*** Turn off Wi-Fi when not using it, to extend the life of the battery.

Scan and Connect to a Wi-Fi Network

1. Touch ⚙.



7:30

Settings

WIRELESS & NETWORKS

Wi-Fi OFF

Bluetooth OFF

Data usage

More...

DEVICE

Sound

Display

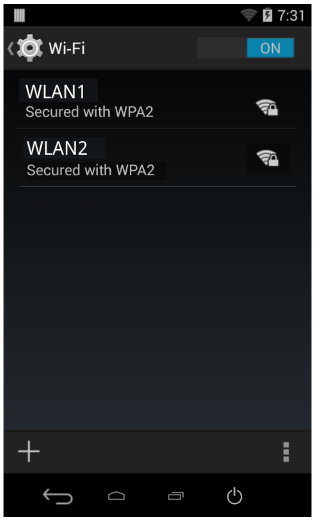
Storage

Battery

Figure 3-1 *Settings Screen*

2. Slide the **Wi-Fi** switch to the **ON** position.

3. Touch 📶 **Wi-Fi**. The MC18 searches for WLANs in the area and lists them.



7:31

Wi-Fi ON

WLAN1
Secured with WPA2

WLAN2
Secured with WPA2

Figure 3-2 *Wi-Fi Screen*

4. Scroll through the list and select the desired WLAN network.

5. For open networks, touch profile once or press and hold and then select **Connect to network** or for secure networks enter the required password or other credentials then touch **Connect**. See the system administrator for more information.

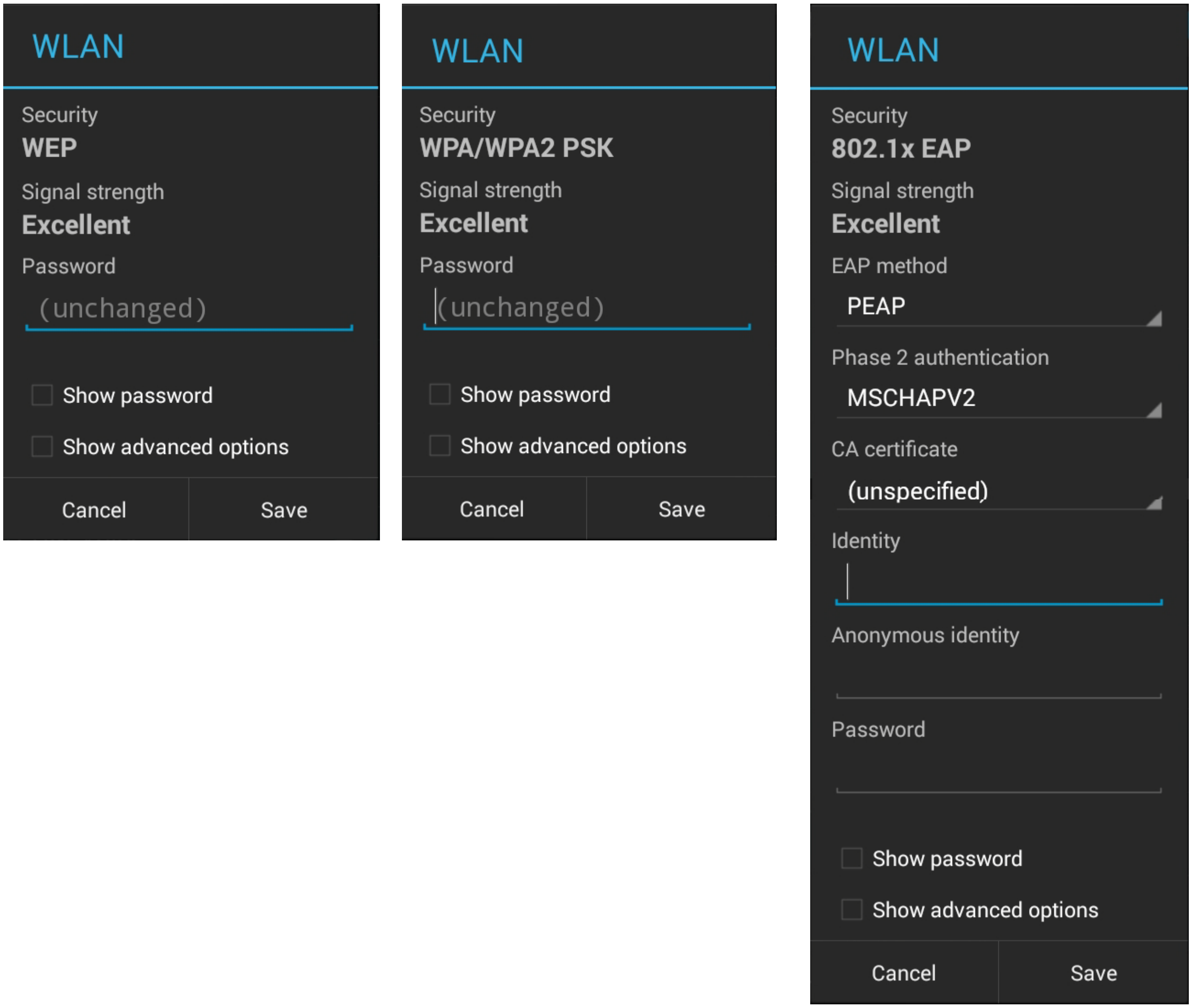
6. The MC18 obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the MC18 with a fixed internet protocol (IP) address, See *Configuring the Device to Use a Static IP Address on page 3-6*.

7. In the Wi-Fi setting field, **Connected** appears indicating that the MC18 is connected to the WLAN.

Configuring a Wi-Fi Network

To set up a Wi-Fi network:

1. Touch ⚙.
2. Touch 📶 **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.



WLAN

Security
WEP

Signal strength
Excellent

Password
(unchanged)

□ Show password

□ Show advanced options

Cancel | Save

WLAN

Security
WPA/WPA2 PSK

Signal strength
Excellent

Password
(unchanged)

□ Show password

□ Show advanced options

Cancel | Save

WLAN

Security
802.1x EAP

Signal strength
Excellent

EAP method
PEAP

Phase 2 authentication
MSCHAPV2

CA certificate
(unspecified)

Identity

Anonymous identity

Password

□ Show password

□ Show advanced options

Cancel | Save

Figure 3-3 *WLAN 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**, **TTLS**, **LEAP** or **FAST**.
- 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 on page 3-5* for setting connection to a proxy server and see *Configuring the Device to Use a Static IP Address on page 3-6* 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 to add a Wi-Fi network when out of range.

1. Touch ⚙.
2. Touch 📶 **Wi-Fi**.
3. Slide the Wi-Fi switch to the **On** position.
4. Touch **+** in the bottom left corner of the screen.
5. In the **Network SSID** text box, enter the name of the Wi-Fi network.
6. In the **Security** drop-down list, select the type of security. Options:
   - 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**, **TTLS**, **LEAP** or **FAST**.
   - 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 then given identity.

By default, the network Proxy is set to **None** and the IP settings is set to **DHCP**. See *Configuring for a Proxy Server on page 3-5* for setting connection to a proxy server and see *Configuring the Device to Use a Static IP Address on page 3-6* for setting the device to use a static IP address.

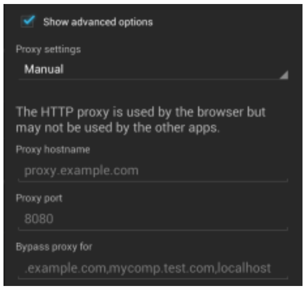
1. Touch **Connect**.
2. Touch ⌂.

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, requesting 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, and proxy configuration is an essential part of doing that. 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.

1. In the **Wi-Fi** list, touch a network.
2. Touch **Show advanced options** checkbox.
3. Touch **Proxy settings** and select **Manual**.



☑ Show advanced options

Proxy settings

Manual

The HTTP proxy is used by the browser but may not be used by the other apps.

Proxy hostname

proxy.example.com

Proxy port

8080

Bypass proxy for

example.com,mycomp.test.com,localhost

Figure 3-4 *Proxy Settings*

4. In the **Proxy hostname** text box, enter the address of the proxy server.
5. In the **Proxy port** text box, enter the port number for the proxy server.

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

6. 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.

7. Touch **Connect**.

8. Touch ⌂.

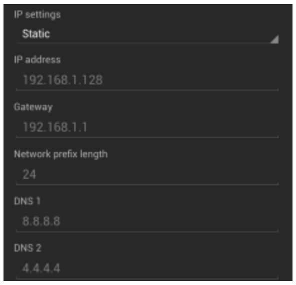
Configuring the Device to Use a Static IP Address

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. In the **Wi-Fi** list, touch a network.

2. Touch **Show advanced options** checkbox.

3. Touch **IP settings** and select **Static**.



IP settings
Static

IP address
192.168.1.128

Gateway
192.168.1.1

Network prefix length
24

DNS 1
8.8.8.8

DNS 2
4.4.4.4

Figure 3-5 *Static IP Settings*

4. In the **IP address** text box, enter an IP address for the device.

5. If required, in the **Gateway** text box, enter a gateway address for the device.

6. If required, in the **Network prefix length** text box, enter a the prefix length.

7. If required, in the **DNS 1** text box, enter a Domain Name System (DNS) address.

8. If required, in the **DNS 2** text box, enter a DNS address.

9. Touch **Connect**.

10. Touch ⌂.

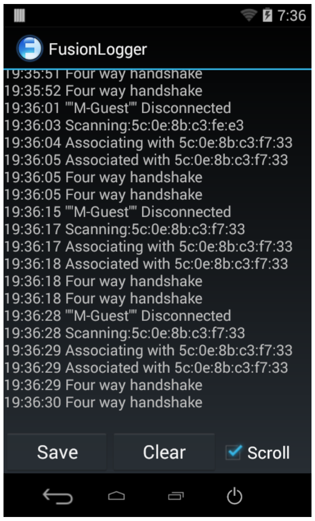
Advanced Wi-Fi Settings

✓ ***NOTE*** Advanced Wi-Fi settings are for the device not for a specific wireless network.

Use the **Advanced** settings to configure additional Wi-Fi settings. From the **Wi-Fi** screen, touch ⋮ > **Advanced** to view the advanced settings.

- **General**
  - **Network notification** - When enabled, notifies the user when an open network is available.
  - **Keep Wi-Fi on during sleep** - Opens a menu to set whether and when the Wi-Fi radio turns off.
    - **Always On** - The radio stays on when the device enters suspend mode.
    - **Only when plugged in** - The radio stays on while the device is connected to external power.

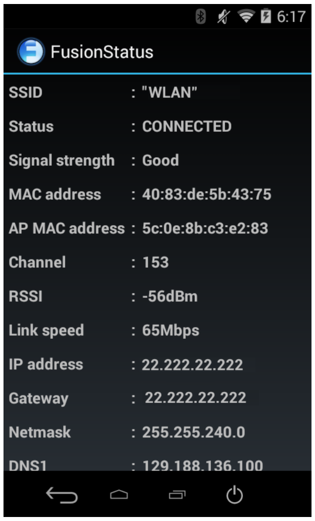
    - **Never On** - The radio turns off when the device enters suspend mode (default).
  - **Install Certificates** – Touch to install certificates.
  - **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **Regulatory**
  - **Country selection** - Displays the acquired country code if **Auto** is selected else displays the selected country code. Default: Auto.
  - **Region code** - Displays the configured region code for the device.
- Band and Channel Selection
  - **Wi-Fi frequency band** - Use to select the frequency band. Options: **Auto** (default), **5 GHz only** or **2.4 GHz only**.
  - **Available channels (2.4 GHz)** - Use to select specific channels. Touch to display the **Available channels** menu. Select specific channels. Touch **OK**.
  - **Available channels (5 GHz)** - Use to select specific channels. Touch to display the **Available channels** menu. Select specific channels. Touch **OK**.
- **Logging**
  - **Advanced Logging** – Touch to enable advanced logging.
  - **Wireless logs** - Use to capture Wi-Fi log files.
    - **Fusion Logger** - Touch to open the **Fusion Logger** application. This application maintains a history of high level WLAN events which helps to understand the status of connectivity.



```
19:35:51 Four way handshake
19:35:52 Four way handshake
19:36:01 ""M-Guest"" Disconnected
19:36:03 Scanning:5c:0e:8b:c3:fe:e3
19:36:04 Associating with 5c:0e:8b:c3:f7:33
19:36:05 Associated with 5c:0e:8b:c3:f7:33
19:36:05 Four way handshake
19:36:05 Four way handshake
19:36:15 ""M-Guest"" Disconnected
19:36:17 Scanning:5c:0e:8b:c3:f7:33
19:36:17 Associating with 5c:0e:8b:c3:f7:33
19:36:18 Associated with 5c:0e:8b:c3:f7:33
19:36:18 Four way handshake
19:36:18 Four way handshake
19:36:28 ""M-Guest"" Disconnected
19:36:28 Scanning:5c:0e:8b:c3:f7:33
19:36:29 Associating with 5c:0e:8b:c3:f7:33
19:36:29 Associated with 5c:0e:8b:c3:f7:33
19:36:29 Four way handshake
19:36:30 Four way handshake
```

Figure 3-6 *Fusion Logger Screen*

    - **Fusion Status** - Touch to display live status of WLAN state. Also provides information of device and connected profile.



FusionStatus

SSID	: "WLAN"
Status	: CONNECTED
Signal strength	: Good
MAC address	: 40:83:de:5b:43:75
AP MAC address	: 5c:0e:8b:c3:e2:83
Channel	: 153
RSSI	: -56dBm
Link speed	: 65Mbps
IP address	: 22.222.22.222
Gateway	: 22.222.22.222
Netmask	: 255.255.240.0
DNS1	: 129.188.136.100

Figure 3-7 *Fusion Status Screen*

- About
  - **Version** - Displays the current Fusion information.

Remove a Wi-Fi Network

To remove a remembered or connected network:

1. Touch ⚙.
2. Touch 📶 **Wi-Fi**.
3. In the **Wi-Fi networks** list, touch and hold the name of the network.
4. In the menu, touch **Forget network**.
5. Touch ⌂.

Wi-Fi Advanced Features

Some additional Wi-Fi settings cannot be accessed from the User Interface. They can be configured by using Wi-Fi (CSP). Refer to EMDK documentation for the details on the Wi-Fi settings configuration using the Wi-Fi CSP.

- **Auto Time Config** - Using this feature, the device can sync up its time with Zebra WLAN infrastructure. This feature works only when the device is connected to Zebra WLAN infrastructure and the feature is enabled on the WLAN infrastructure side. Default: disabled.
- **PMKID Caching** - Allows the device to skip 802.1x authentication during roaming if it had previously connected to that AP with a full 802.1x authentication. Default: disabled. Note: disable OKC when enabling PMKID Caching.
- **Opportunistic Key Caching** - Use this feature to skip 802.1x authentication during roaming. The device will go for full 802.1x authentication for the first time it connects to the network. For subsequent roaming, the device skips 802.1x authentication. Default: enabled.

- **Cisco Centralized Key Management** - Allows the device to skip 802.1x and key-handshake phases during roaming. This feature is available only when the device is connected to a Cisco infrastructure that supports Cisco Centralized Key Management (CCKM). Default: enabled.
- **Fast Transition** - Fast Transition (FT) is the fast roaming standard, 802.11r. With this feature, the device can skip 802.1x and key-handshake phases during roam. Default: enabled.
- **Fast Transition Resource Information Container** - Allows the device to request TSPEC as part of reassociation frame exchange. This helps to avoid sending a separate resource request after roaming is completed. Default: disabled.
- **Power Save** - The device can be configured to work in different power save modes:
  - **i. Active** - Keeps the WLAN radio always in active mode (i.e. power save mode disabled).
  - **ii. Power save using WMM-PS** - This is the default power save mode. Device uses WMM-PS power save method if the AP is configured to use this. If the AP is not supporting WMM-PS, the device will use PS-Poll power save method.
  - **iii. Power save using PS-Poll** - In this method, the device will use PS-Poll frames to retrieve buffered frames from the AP.
  - **iv. Null Data Power Save** - In Null Data Power Save (NDP), the device will stay awake for 100 ms after the last frame is sent or received. The device will send a Null Data packet with power management bit cleared to retrieve buffered frames from the AP.
- **FIPS** - The device supports FIPS 140-2 Level 1. In this mode, the device will not support TKIP and WEP encryption modes. When Wi-Fi is enabled, the stack will run predefined tests to make sure that the encryption engine is working correctly and the firmware and firmware loader modules are correct.
- **802.11k** - Using 802.11k, the device can discover neighbor APs and adds support for different types of radio resource measurements. Default: enabled.
- **Band Preference** - The device can be configured to prefer one band over another. By default, device prefers 5 GHz frequency band over 2.4 GHz.
- **Subnet Roaming** - When the device roams between different sub networks, if it detects that it is roaming to a different subnet, the device will request a fresh IP address. Default: disabled.

Zebra Mobility Extensions

Zebra Mobility Extensions make use 802.11 specifications and Zebra proprietary extensions to achieve the highest level of performance, efficiency and reliability. The MC18 adds support for the following Zebra Mobility Extensions.

- Coverage Hole Detection - The MC18 includes enhancements to the IEEE 802.11k standard. These improvements will report gaps in signal coverage to the Zebra wireless LAN infrastructure. Network administrators can detect and mitigate coverage gaps present in the network for greater reliability. Default: enabled.
- • Aggregated Fast Transition - Aggregated FT improves on IEEE 802.11r, Over-the-DS fast roaming. In conjunction with Zebra wireless LAN infrastructure, the MC18 will achieve more reliable and consistent fast roaming. Default: enabled.
- • Scan Assist - The MC18 monitors neighbor access points and retrieves roaming related information from the Zebra wireless LAN infrastructure without doing scans. Using this Scan Assist feature, the MC18 improves roaming. Default: enabled.

Bluetooth

Bluetooth-equipped devices can communicate without wires, using frequency-hopping spread spectrum (FHSS) radio frequency (RF) to transmit and receive data in the 2.4 GHz Industry Scientific and Medical (ISM) band (802.15.1). Bluetooth wireless technology is specifically designed for short-range (10 meters (32.8 feet)) communication and low power consumption.

Devices with Bluetooth capabilities can exchange information (e.g., files, appointments, and tasks) with other Bluetooth enabled devices such as printers, access points, and other mobile devices.

Adaptive Frequency Hopping

Adaptive Frequency Hopping (AFH) is a method of avoiding fixed frequency interferers, and can be used with Bluetooth voice. All devices in the piconet (Bluetooth network) must be AFH-capable in order for AFH to work. There is no AFH when connecting and discovering devices. Avoid making Bluetooth connections and discoveries during critical 802.11b communications. AFH for Bluetooth consists of four main sections:

- **Channel Classification** - A method of detecting an interference on a channel-by-channel basis, or pre-defined channel mask.
- **Link Management** - Coordinates and distributes the AFH information to the rest of the Bluetooth network.
- **Hop Sequence Modification** - Avoids interference by selectively reducing the number of hopping channels.
- **Channel Maintenance** - A method for periodically re-evaluating the channels.

When AFH is enabled, the Bluetooth radio “hops around” (instead of through) the 802.11b high-rate channels. AFH coexistence allows Enterprise devices to operate in any infrastructure.

The Bluetooth radio in this device operates as a Class 2 device power class. The maximum output power is 2.5 mW and the expected range is 10 meters (32.8 ft.). A definition of ranges based on power class is difficult to obtain due to power and device differences, and whether one measures open space or closed office space.

✓ ***NOTE*** It is not recommended to perform Bluetooth wireless technology inquiry when high rate 802.11b operation is required.

Security

The current Bluetooth specification defines security at the link level. Application-level security is not specified. This allows application developers to define security mechanisms tailored to their specific need. Link-level security occurs between devices, not users, while application-level security can be implemented on a per-user basis. The Bluetooth specification defines security algorithms and procedures required to authenticate devices, and if needed, encrypt the data flowing on the link between the devices. Device authentication is a mandatory feature of Bluetooth while link encryption is optional.

Pairing of Bluetooth devices is accomplished by creating an initialization key used to authenticate the devices and create a link key for them. Entering a common personal identification number (PIN) in the devices being paired generates the initialization key. The PIN is never sent over the air. By default, the Bluetooth stack responds with no key when a key is requested (it is up to user to respond to the key request event). Authentication of Bluetooth devices is based-upon a challenge-response transaction. Bluetooth allows for a PIN or passkey used to create other 128-bit keys used for security and encryption. The encryption key is derived from the link key used to authenticate the pairing devices. Also worthy of note is the limited range and fast frequency hopping of the Bluetooth radios that makes long-distance eavesdropping difficult.

Recommendations are:

- Perform pairing in a secure environment
- Keep PIN codes private and do not store the PIN codes in the device
- Implement application-level security.

Bluetooth Profiles

The device supports the following Bluetooth services:

- **Service Discovery Protocol (SDP)** - Handles the search for known and specific services as well as general services.
- **Serial Port Profile (SPP)** - Allows use of RFCOMM protocol to emulate serial cable connection between two Bluetooth peer devices. For example, connecting the device to a printer.
- **Generic Access Profile (GAP)** - Controls connections in Bluetooth. Makes device visible and determines how two devices communicate.

Bluetooth Power States

The Bluetooth radio is off by default.

- **Suspend** - When the MC18 goes into suspend mode, the Bluetooth radio stays on.
- **Airplane Mode** - When the MC18 is placed in Airplane Mode, the Bluetooth radio turns off. When Airplane mode is disabled, the Bluetooth radio returns to the prior state. When in Airplane Mode, the Bluetooth radio can be turned back on if desired.

Bluetooth Radio Power

Turn off the Bluetooth radio to save power or if entering an area with radio restrictions (e.g., an airplane). When the radio is off, other Bluetooth devices cannot see or connect to the device. Turn on the Bluetooth radio to exchange information with other Bluetooth devices (within range). Communicate only with Bluetooth radios in close proximity.

✓ ***NOTE*** To achieve the best battery life turn off radios when not in use.

Enabling Bluetooth

1. Touch ⚙.
2. Slide the Bluetooth switch to the **ON** position. ᛒ also appears in the Status bar.
3. Touch ⌂.

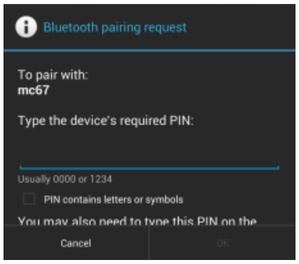
Disabling Bluetooth

1. Touch ⚙.
2. Slide the Bluetooth switch to the **OFF** position.
3. Touch ⌂.

Discovering Bluetooth Device(s)

The MC18 can receive information from discovered devices without pairing. However, once paired, the MC18 and a paired device exchange information automatically when the Bluetooth radio is on. To find Bluetooth devices in the area:

1. Ensure that Bluetooth is enabled on both devices.
2. Ensure that the Bluetooth device to discover is in discoverable mode.
3. Ensure that the two devices are within 10 meters (32.8 feet) of one another.
4. Touch .
5. Touch **Bluetooth**.
6. Touch **SCAN FOR DEVICES**. The MC18 begins searching for discoverable Bluetooth devices in the area and displays them under **AVAILABLE DEVICES**.
7. Scroll through the list and select a device. The **Bluetooth pairing request** dialog box appears.



Bluetooth pairing request

To pair with:
mc67

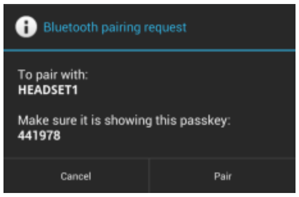
Type the device's required PIN:

Usually 0000 or 1234

□ PIN contains letters or symbols

You may also need to type this PIN on the

Figure 3-8 *Bluetooth Pairing - Enter PIN*



Bluetooth pairing request

To pair with:
HEADSET1

Make sure it is showing this passkey:
441978

Figure 3-9 *Bluetooth Pairing - Smart Pairing*

8. Enter a PIN in the text box and touch **OK**. Enter the same PIN on the other device.
9. For Simple Pairing, touch **Pair** on both devices.
10. The Bluetooth device is added to the **Bluetooth devices** list and a trusted (“paired”) connection is established.

Changing the Bluetooth Name

By default, the MC18 has a generic Bluetooth name that is visible to other devices when connected.

1. Touch .
2. Touch **Bluetooth**.
3. If Bluetooth is not on, slide the switch to the **ON** position.

4. Touch ⋮ .
5. Touch **Rename device**.
6. Enter a name and touch **Done**.
7. Touch ⌂.

Connecting to a Bluetooth Device

Once paired, connect to a Bluetooth device.

1. Touch ⚙.
2. Touch ᛒ **Bluetooth**.
3. If Bluetooth is not on, slide the switch to the **ON** position.
4. In the **PAIRED DEVICES** list, touch and hold on a unconnected Bluetooth device until a menu appears.
5. Touch **Connect**. When connected, the device is displayed as connected in the list.

Selecting Profiles on the Bluetooth Device

Some Bluetooth devices have multiple profiles. To select a profile:

1. Touch ⚙.
2. Touch ᛒ **Bluetooth**.
3. In the **PAIRED DEVICES** list, touch ☰ next to the device name.
4. Under **PROFILES**, check or uncheck a profile to allow the device to use that profile.
5. Touch ⌂.

Unpairing a Bluetooth Device

To unpair a Bluetooth device and erase all pairing information:

1. Touch ⚙.
2. Touch ᛒ **Bluetooth**.
3. In the **PAIRED DEVICES** list, touch ☰ next to the device name.
4. Touch **Unpair**.
5. Touch ⌂.

CHAPTER 4 APPLICATIONS

Introduction

This chapter describes the applications installed on the device.

File Browser

Use the **File Browser** application to view and mange files on the device.

To open **File Browser**, touch ⊞ > 📁.

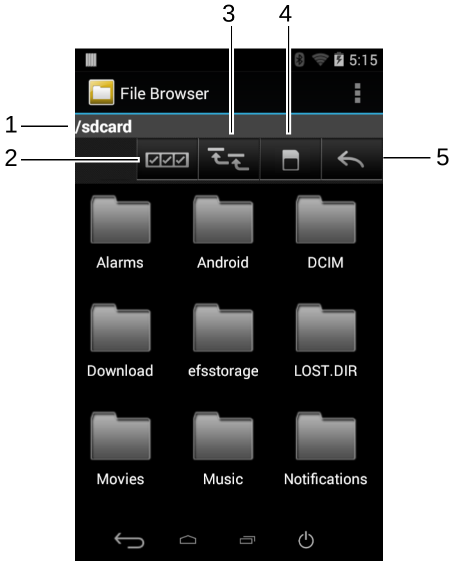


Figure 4-1 *File Browser Screen*

The address bar (1) indicates the current folder path. Touch the current folder path to manually enter a path and folder name.

Use ☑☑☑ (2) to select multiple files/folder.

Use ⇆ (3) to view the internal storage root folder.

Use ▯ (4) to view the Internal Storage root folder.

Use ↩ (5) to view the previous folder or to exit the application.

Touch and hold an item to perform an operation on that item. Select one of the options from the **File Operations** menu:

- **Information** - View detailed information about the file or folder.
- **Move** - Move the file or folder to a new location.
- **Copy** - Copy the select file.
- **Delete** - Delete the selected file.
- **Rename** - Rename the select file.
- **Open as** - Open the selected file as a specific file type.
- **Share** - Share the file with other devices.

Touch ⋮ to open additional functionality:

- Touch ⋮ > **New Folder** to create a new folder in the current folder.
- Touch ⋮ > **Search** to search for a file or folder.
- Touch ⋮ > **Sort** to sort the list by name, by type, by size or by date.
- Touch ⋮ > **Refresh** to re-display the contents of the current folder.
- Touch ⋮ > **List View** to change the folder view from tile to list format.
- Touch ⋮ > **Change Size** to change the size of the icons: Large, Normal or Small.
- Touch ⋮ > **About File Browser** to view the application version information.

People

Use the **People** application to manage contacts.

From a Home or Apps screen, touch 👤. People opens to the main list of contacts. View contacts in three ways at the top of the screen: Groups, All contacts, and Favorites. Touch the tabs to change how to view the contacts. Swipe up or down to scroll through the lists.

Adding People

1. In the People application, touch 👤+.
2. If there are more than one account with contacts, touch the one to use.
3. Type the contact’s name and other information. Touch a field to start typing, and swipe down to view all categories.
4. To add more than one entry for a category – for example, to add a work address after typing a personal address – touch **Add new** for that field. To open a menu with preset labels, such as Home or Work for an email address, touch the label to the right of the item of contact information. Or, to create your own label, touch **Custom** in the menu.

5. Touch **Done**.

Editing People

1. In the People application, touch 👤 tab.
2. Touch a person to edit.
3. Touch ⋮ .
4. Touch **Edit**.
5. Edit the contact information.
6. Touch **Done**.

Deleting People

1. In the People application, touch 👤 tab.
2. Touch a person to edit.
3. Touch ⋮ .
4. Touch **Delete**.
5. Touch **OK** to confirm.

Gallery

✓ ***NOTE*** The device supports the following image formats: jpeg, gif, png and bmp.

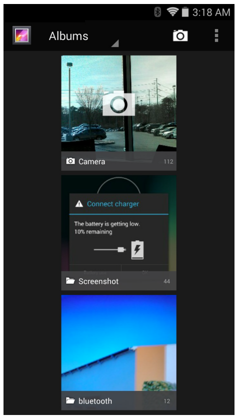
The device supports the following video formats: H.263, H.264 and MPEG4 Simple Profile.

Use Gallery to:

- view photos
- play videos
- perform basic editing of photos
- set photos as wallpaper
- set photos as a contact photo
- share photos and videos.

To open the Gallery application, touch ⊞ > 🖼.

Gallery presents all photos and videos stored in memory.



The battery is getting low.
10% remaining

Figure 4-2 *Gallery — Albums*

- Touch an album to open it and view its contents. The photos and videos in the album are displayed in chronological order.
- Touch a photo or video in an album to view it.
- Touch 🖼 icon (top left corner) to return to the main **Gallery** screen.
- Touch ↩ to return to the main **Gallery** screen.

Working with Albums

Albums are groups of images and videos in folders. Touch an album to open it. The photos and videos are listed in a chronologically ordered grid. The name of the album displays at the top of the screen.

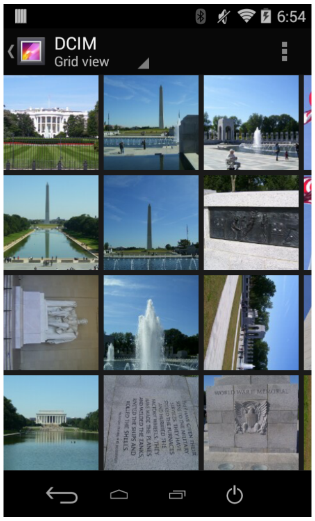


Figure 4-3 *Photos Inside an Album*

Swipe left or right to scroll images across the screen.

Share an Album

1. Touch ⊞ > 🖼.

2. Touch and hold an album until it highlights.
3. Touch other albums as required.
4. Touch ⋖ . The Share menu opens. Touch the application to use to share the selected albums.
5. Follow the instructions within the selected application.

Get Album Information

1. Touch ⊞ > 🖼.
2. Touch and hold an album until it highlights.
3. Touch ⋮ .
4. Touch **Details**.

Deleting an Album

To delete an album and its contents:

1. Touch ⊞ > 🖼.
2. Touch and hold an album until it highlights.
3. Check other albums to delete. Ensure that other albums are selected.
4. Touch 🗑.
5. In the **Delete selected item?** menu, touch **OK** to delete the album.

Working with Photos

Use Gallery to view photos and edit and share photos.

Viewing and Browsing Photos

To view a photo:

1. Touch ⊞ > 🖼.
2. Touch an album to open it.
3. Touch a photo.

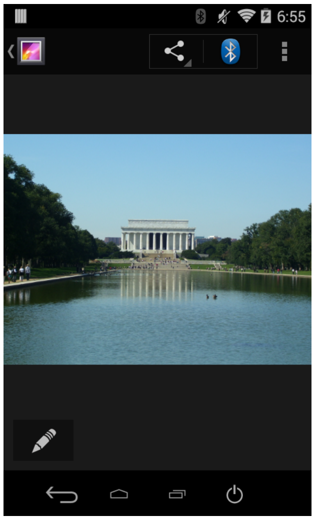


Figure 4-4 *Photo Example*

4. Swipe left or right to view the next or previous photo in the album.
5. Touch the photo to view the controls.
6. Double-tap the screen to zoom in or pinch two fingers together or spread them apart to zoom in or out.
7. Drag the photo to view parts that are not in view.

Cropping a Photo

1. In Gallery, touch a photo to view the controls.
2. Touch ⋮ .
3. Touch **Crop**. The white cropping tool appears.
4. Use the cropping tool to select the portion of the photo to crop.
   - Drag from the inside of the cropping tool to move it.
   - Drag an edge of the cropping tool to resize it to any proportion.
   - Drag a corner of the cropping tool to resize it with fixed proportions.

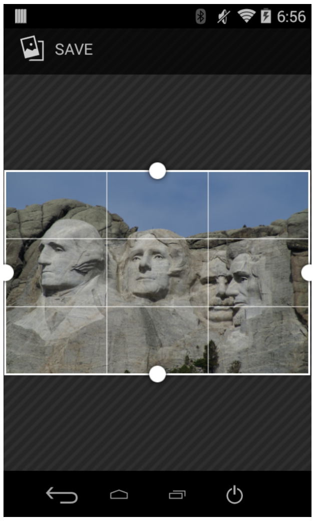


Figure 4-5 *Cropping Tool*

5. Touch **SAVE** to save a copy of the cropped photo. The original version is retained.

Setting a Photo as a Contact Icon

1. Touch ⊞ > 🖼.
2. Touch an album to open it.
3. Touch the photo to open it.
4. Touch ⋮ .
5. Touch **Set picture as**.
6. Touch **Contact photo**.
7. In the People application, touch a contact.
8. Touch the white box and crop the photo accordingly.
9. Touch **OK**.

Share a Photo

1. Touch ⊞ > 🖼.
2. Touch an album to open it.
3. Touch a photo to open it.
4. Touch ⋖ .
5. Touch the application to use to share the selected photo. The application selected opens with the photo attached to a new message.

Deleting a Photo

1. Touch ⊞ > 🖼.

2. Touch an album to open it.
3. Touch a photo to open it.
4. Touch 🗑.
5. Touch ⋮ .
6. Touch **Delete**.
7. Touch **OK** to delete the photo.

Working with Videos

Use Gallery to view videos and share videos.

Watching Videos

1. Touch ⊞ > 🖼.
2. Touch an album to open it.
3. Touch a video.

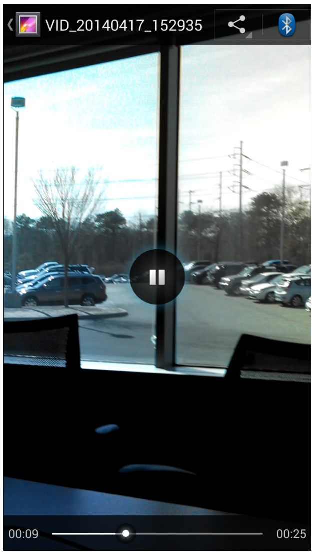


Figure 4-6 *Video Example*

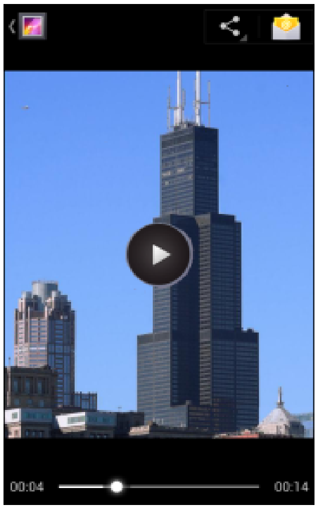


Figure 4-7

4. Touch ▶. The video begins to play.

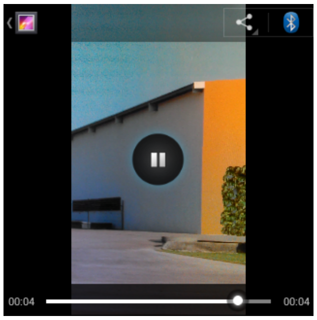


Figure 4-8 *Video Example*

5. Touch the screen to view the playback controls.

Sharing a Video

1. Touch ⊞ > 🖼.
2. Touch an album to open it.
3. Touch a video to open it.
4. Touch ⋖ . The Share menu appears.
5. Touch the application to use to share the selected video. The application selected opens with the video attached to a new message.

Deleting a Video

1. Touch ⊞ > 🖼.
2. Touch an album to open it.
3. Touch a video to open it.

4. Touch 🗑.
5. Touch ⋮ .
6. Touch **Delete**.
7. Touch **OK**.

DataWedge Demonstration

Use DataWedge Demonstration to demonstrate data capture functionality.

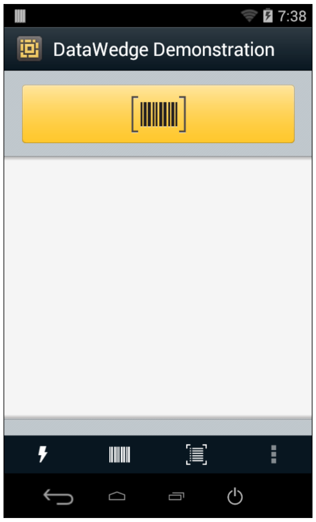


Figure 4-9 *DataWedge Demonstration Window*

Table 4-1 *DataWedge Demonstration Icons*

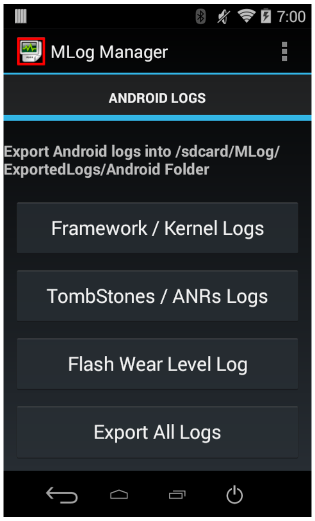
Icon	Description
⚡	Not applicable.
▥	Indicates that the data capture function is through the imager.
⛶ / ▤	Toggles between normal scan mode and picklist mode when capturing bar code data.
⋮	Opens a menu to view the application information or to set the application DataWedge profile.

✓ ***NOTE*** See *Chapter 9, DataWedge* for information on DataWedge configuration.

Either press the Scan key or touch the yellow scan button in the application to enable data capture. The captured data appears in the text field below the yellow button.

MLog Manager

Use **MLog Manager** to capture log files for diagnostics. See the *MC18 Integrator Guide* for detailed information on configuring the application.



Export Android logs into /sdcard/MLog/ExportedLogs/Android Folder

Figure 4-10 *MLog Manager*

RxLogger

RxLogger is a comprehensive diagnostic tool that provides application and system metrics. It allows for custom plug-ins to be created and work seamlessly with this tool. RxLogger is used to diagnose device and application issues. Its information tracking includes the following: 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 logs and files generated are saved onto flash storage on the device (internal or external).

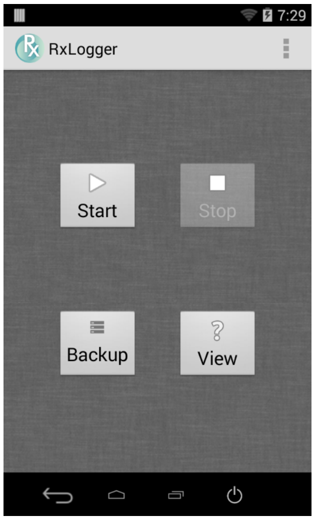


Figure 4-11 *RxLogger*

RxLogger Configuration

RxLogger is built with an extensible plug-in architecture and comes packaged with a number of plugins already built-in. The included plug-ins are described below. Touch ⋮ > **Settings** to open the configuration screen.

Configuration File

RxLogger configuration can be set using an XML file. The *config.xml* configuration file is located on the **Enterprise storage** in the **`RxLogger\config`** folder. Copy the file from the device to a host computer using a USB connection. Edit the configuration file and the 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

1. Touch ⊞ > ℞.
2. Touch **Start**.
3. Touch ⌂.

Disabling Logging

1. Touch ⊞ > ℞.
2. Touch **Stop**.
3. Touch ⌂.

Extracting Log Files

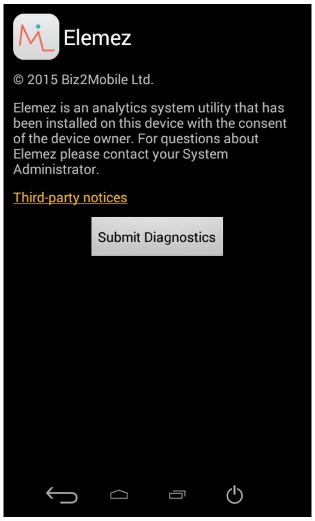
1. Connect the device to a host computer using an USB connection.
2. Using a file explorer, navigate to the **On Device Storage** in the **`/RxLogger`** folder.
3. Copy the file from the device to the host computer.
4. Disconnect the device from the host computer.

Elemez

✓ ***NOTE*** Elemez collects specific device information in the background and sends this information to us to help improve product functionality. This feature can be disabled.

See Disabling Elemez Data Collection. Ensure that the date, time and time zone are set correctly prior to using Elemez.

Use **Elemez** to provide diagnostics information to us. Touch **Submit Diagnostics** button to send the data.



Elemez

© 2015 Biz2Mobile Ltd.

Elemez is an analytics system utility that has been installed on this device with the consent of the device owner. For questions about Elemez please contact your System Administrator.

Figure 4-12 *Elemez Application*

Disabling Elemez Data Collection

The user can disable the Elemez application from collection specific data in the background and sending it to Zebra Technologies.

1. From the Home screen, touch ⚙ > **Apps**.
2. Swipe left or right until the **ALL** tab displays.
3. Scroll through the list and touch **Elemez**.
4. In the **App info** screen, touch **Uninstall updates**.
5. In the **Uninstall updates** dialog box, touch **OK**.
6. Touch **OK**.
7. After uninstall is complete, touch **OK**.
8. In the **All** tab, scroll through the list and touch **Elemez**.
9. Touch **Disable**.
10. In the **Disable built-in app?** dialog box, touch **OK**.
11. Touch ⌂.

Enabling Elemez Data Collection

The user can re-enable the Elemez application for collection specific data in the background and sending it to Zebra Technologies.

1. From the Home screen, touch ⚙.
2. Touch **Manage Apps**.
3. Swipe left or right until the **ALL** tab displays.

4. Scroll through the list and touch **Elemez**.
5. In the **App info** screen, touch **Enable**.
6. Touch ⌂.
7. Touch ⠿.
8. Touch 📈.
9. Touch **Enable Elemez**.

Cradle Utility

Use the **Cradle Utility** to:

- control of the cradle
- Set up the cradle
- Perform cradle diagnostics
- View cradle information.

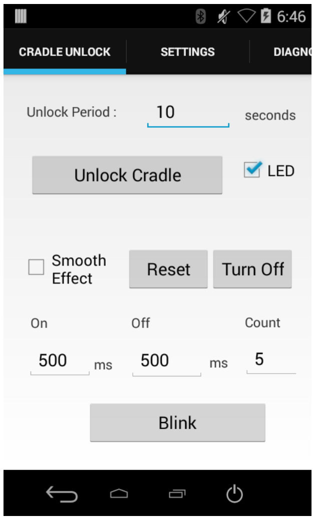
To use the Cradle Utility:

1. Dock the MC18 inside the cradle.
2. Touch ⊞ > 🔧 .

NOTE The cradle ID and location information and charge settings are retained across firmware upgrades.

Controlling the Cradle

1. Tap the **CRADLE UNLOCK** tab to set the cradle unlock information.



Unlock Period : 10 seconds

☑ LED

□ Smooth Effect

On 500 ms

Off 500 ms

Count 5

Figure 4-13 *Cradle Utility - Cradle Unlock Tab*

- **Unlock Period**: The duration in seconds for which the MC18 remains in unlocked state (if not removed from the cradle). For example; if unlock period is set to 15 and unlock signal is received, the MC18 will unlock and lock back after 15 seconds (if its not removed by user).
- **Unlock Cradle**: Press **Unlock Cradle** to manually unlock the MC18 from the cradle.
- **LED**: Check the LED box to enable the cradle LED indication.
- **Smooth Effect**: Check the Smooth Effect box to enable smooth blinking of the LEDs.
- LED Setting > **On**: The duration (in ms) that the cradle LED is remains turned on or blinks during unlock.
- LED Setting > **Off**: The duration (in ms) that the cradle LED is remains turned off or blinks during unlock.
- LED Setting > **Count**: The number of times the cradle LED blinks when user presses the blink button.

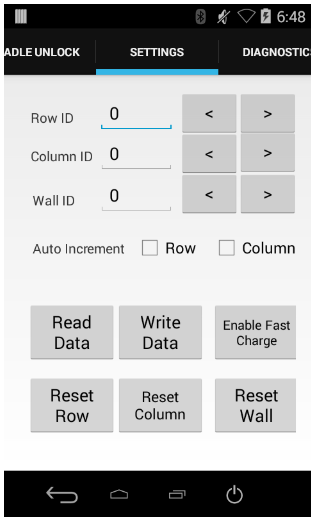
- **Blink**: Tap to test the cradle LED operation.

Setting the Cradle

Setting the cradle charging rate: Depending on the cradle installation configuration, the store technician can configure each individual cradle slot to enable/disable fast charge. Each cradle can be configured to charge its docked terminal at 1Ah (normal charging mode - default setting) or 1.5Ah (fast charging mode).

✓ ***NOTE*** The cradle charging rate is retained across firmware upgrades.

1. Tap the **Settings** tab to set the cradle information.



Row ID 0

Column ID 0

Wall ID 0

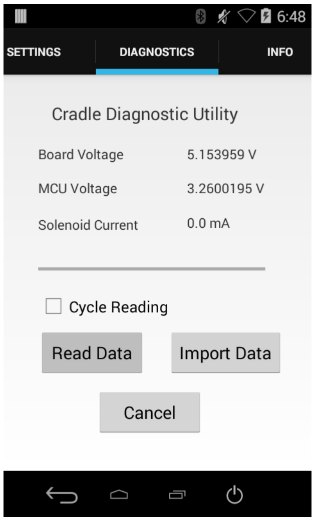
Auto Increment □ Row □ Column

Figure 4-14 *Cradle Utility - Setting Tab*

- **Row ID**: The cradle row number in the dispenser wall.
- **Column ID**: The cradle column number in the dispenser wall.
- **Wall ID**: The number of dispenser wall where the cradle is positioned.
- **Read Data**: Retrieve setting data from the cradle memory and display on the screen.
- **Write Data**: Tap this button to program the row/col/wall information onto the cradle. Note that each slot on the Three Slot Cradle needs to be programmed separately.
- **Enable Fast Charge**: Enable the cradle to charge the MC18 at a current of 1.5A (default setting is 1A)
- **Reset Row**: Tap to update the **Row ID** the text field to “0” on the application.
- **Reset Column**: Tap to update the **Column ID** the text field to “0” on the application.
- **Reset Wall**: Tap to update the **Wall ID** the text field to “0” on the application.

Performing Cradle Diagnostics

1. Touch **Diagnostic** tab to perform the cradle diagnostics:



Cradle Diagnostic Utility

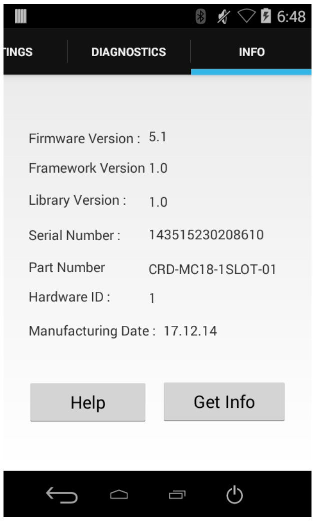
Board Voltage	5.153959 V
MCU Voltage	3.2600195 V
Solenoid Current	0.0 mA

Figure 4-15 *Cradle Utility - Diagnostic Tab*

- **Cycle Reading**: Check the **Cycle Reading** box to perform continues diagnostics and display the cradle status information. During diagnostics, a progress bar is shown of the screen.
- **Read Data**: Tap to start performing diagnostics.
- **Import Data**: Tap to save the recorded results of the diagnostics on a file.

Viewing Cradle Information

1. Touch **Info** tab.



Firmware Version :	5.1
Framework Version	1.0
Library Version :	1.0
Serial Number :	143515230208610
Part Number	CRD-MC18-1SLOT-01
Hardware ID :	1
Manufacturing Date :	17.12.14

Figure 4-16 *Cradle Utility - Info Tab*

2. Touch **Get Info** to read the cradle information.

CHAPTER 5 DATA CAPTURE

Introduction

The MC18 imager allows collection of data by scanning bar codes.

The imager has the following features:

- Reads a variety of bar code symbologies, including the most popular linear, postal, and 2-D code types (see *Appendix A, Technical Specifications*).
- Contains advanced intuitive aiming light for easy point-and-shoot operation.

Scanning Considerations

Typically, scanning is a simple matter of aim, scan/decode and a few quick trial efforts master it. However, two important considerations can be used to optimize any scanning performance:

- Range

  Any scanning device decodes well over a particular working range — minimum and maximum distances from the bar code. This range varies according to bar code density and scanning device optics.

  Scanning within range brings quick and constant decodes; scanning too close or too far away prevents decodes. Move the MC18 closer and further away to find the right working range for the bar codes being scanned. However, the situation is complicated by the availability of various integrated scanning modules. The best way to specify the appropriate working range per bar code density is through a chart called a decode zone for each scan module. A decode zone simply plots working range as a function of minimum element widths of bar code symbols.

- Angle

  Don’t scan at too sharp an angle; the scanner needs to collect scattered reflections from the scan to make a successful decode. Practice quickly shows what tolerances to work within.

✓ ***NOTE*** Contact the Global Customer Support if chronic scanning difficulties develop. Decoding of properly printed bar codes should be quick and effortless.

Scanning Bar Codes

1. Open any application that can receive text.
2. Aim the scan exit window at the bar code.
3. Press the Scan key - the status LED illuminates red.
   Ensure the red aiming dot is at the center of the bar code. Upon successful decode, the Status LED changes from red to green and audible beep sounds if bar code was decoded successfully.

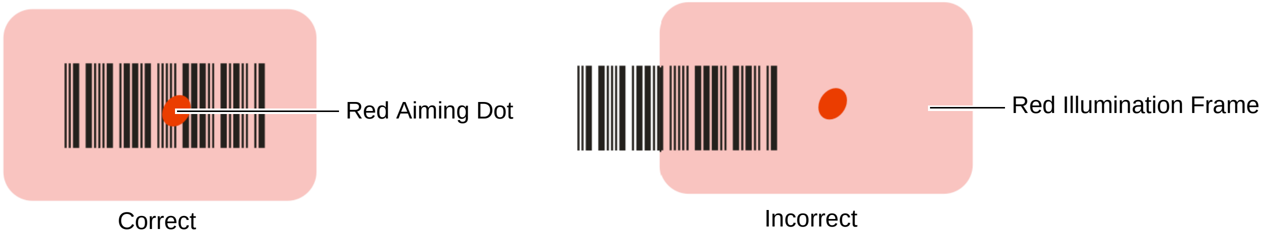


Figure 5-1 *Imager Illumination Frame*

4. Release the Scan key. The bar code data displays on the screen.

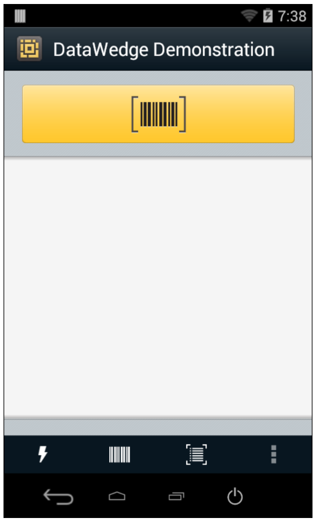


Figure 5-2 *DataWedge Demo Screen*

Scanning Tips

Optimal scanning distance varies with bar code density and scanner optics.

- Hold the scanner farther away for larger symbols.
- Move the scanner closer for symbols with bars that are close together.

✓ ***NOTE*** Scanning procedures depend on the application and MC18 configuration. An application may use different scanning procedures from the one listed above.

DataWedge

DataWedge is a utility that adds advanced bar code scanning capability to any application without writing code. It runs in the background and handles the interface to built-in bar code scanners. The captured bar code data is converted to keystrokes and sent to the target application as if it was typed on the keypad.

Enabling DataWedge

To enable the DataWedge Application:

1. Touch ⊞ > ◣ > ⋮ .
2. Touch **Settings**.
3. Touch the **DataWedge enabled** checkbox. A blue checkmark appears in the checkbox indicating that DataWedge is enabled.
4. Touch ⌂.

Disable DataWedge

To disable DataWedge:

1. Touch ⊞ > ◣ > ⋮ .
2. Touch **Settings**.
3. Touch the **DataWedge enabled** checkbox. The blue checkmark disappears from the checkbox indicating that DataWedge is disabled.
4. Touch ⌂.

CHAPTER 6 CRADLE INSTALLATION

Introduction

A typical Personal Shopper system is comprised of a family of hardware devices interconnected through a WLAN radio backbone to the retail establishment's server(s). The hardware devices are the MC18 mobile computers, single-slot or Three Slot Cradles, power supplies and cables. A *dispenser* typically refers to a piece of furniture which has mounted to it the cradles, their power supplies, and cables.

Customers (retail establishments) design their own dispensers to meet their particular floor space and display requirements. The information in this chapter should help a customer to design a dispenser and to understand the installation requirements.

✓ ***IMPORTANT*** The MC18 cradles are NOT compatible with MC17 cradles and the MC17 cradles are NOT compatible with MC18 cradles.

Installation of the Single Slot Cradle

Installation of the Single Slot Cradle include the following mounting steps:

- Select the charging mode (see *Charging Modes on page 6-1*)
- Mount the Single Slot Cradles on a dispenser wall (see *Mounting the Single Slot Cradle on a Dispenser Wall on page 6-2*)
- Connect the wires to the cables (see *Wiring on page 6-5*)
- Set the cradle(s) (see *Controlling the Cradle on page 4-4*)

Charging Modes

Single Slot Cradles can be installed in the following charging modes:

- Standard charging
- Fast charging

There are some general charging considerations that must be taken into account when designing a dispenser and ordering hardware elements of a system:

Standard Charging Mode

- In standard charging mode, no more than 12 cradles can be powered off of one power supply unit (p/n PWRS-14000-241R) using “Y” power cable 25-67592-01R.
- In standard charging mode, the current draw by each docked MC18 can reach a maximum of 1A.

Fast Charging Mode

- In fast charging mode, no more than six cradles can be powered off of one power supply unit (p/n PWRS-14000-241R) using power cable 25-66420-01R.
- In fast charging mode, the current draw by each docked MC18 can reach a maximum of 1.5A.

Mounting the Single Slot Cradle on a Dispenser Wall

The cradle contains two mounting holes in the back housing so that it can be hanged on screws fixed to a supporting furniture. In addition, it comes with plugs and a variety of cable routing outlets. *Figure 6-3* provides the necessary information about the location and dimensions of the mounting holes of the cradle.

To mount the Single Slot Cradle:

1. Loosen two captive screws securing the front cover to the base.

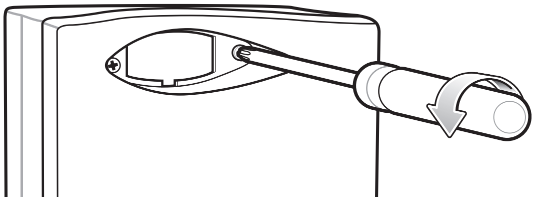


Figure 6-1 *Remove Screws*

2. Pull front cover away from base and then lift out of the base.

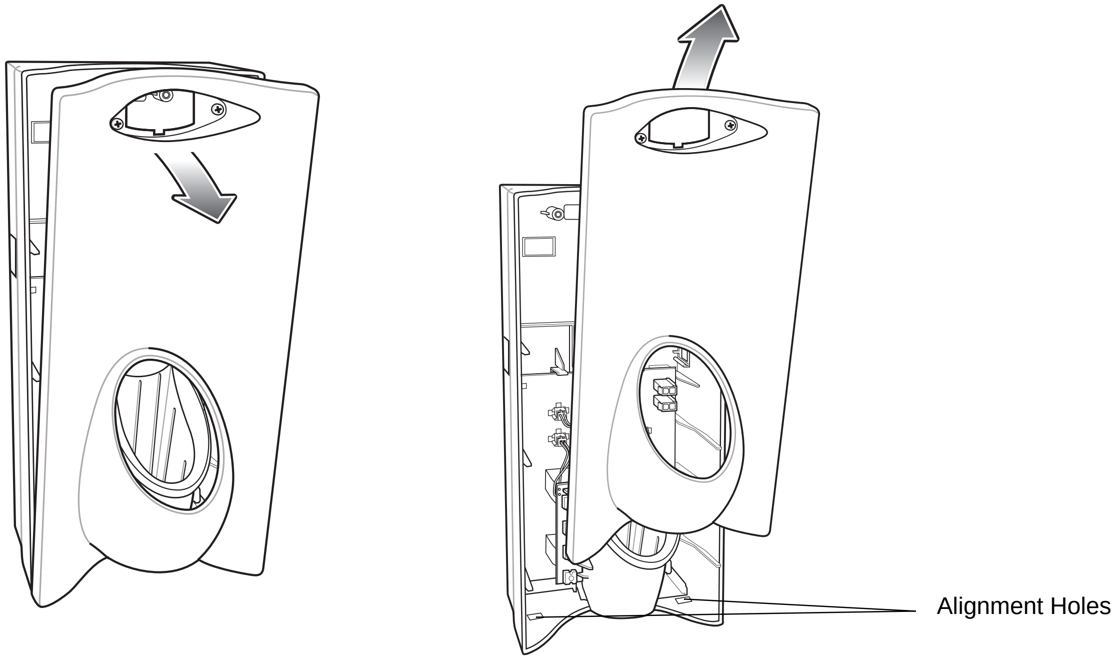


Figure 6-2 *Cover Removal*

3. Use two screws to hang the cradle on a wall.

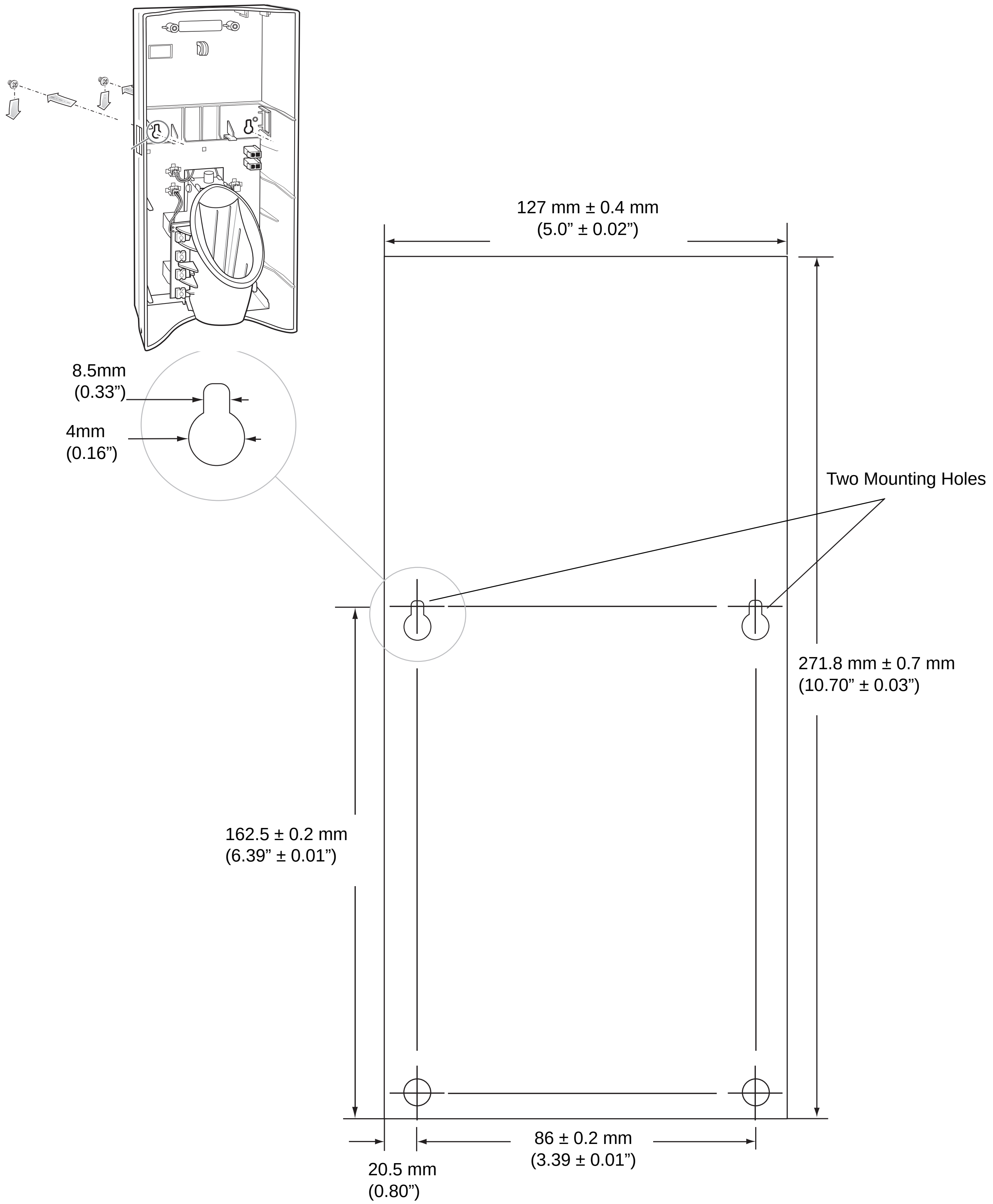


Figure 6-3 *Hanging the Cradle on a Wall - Mounting Template*

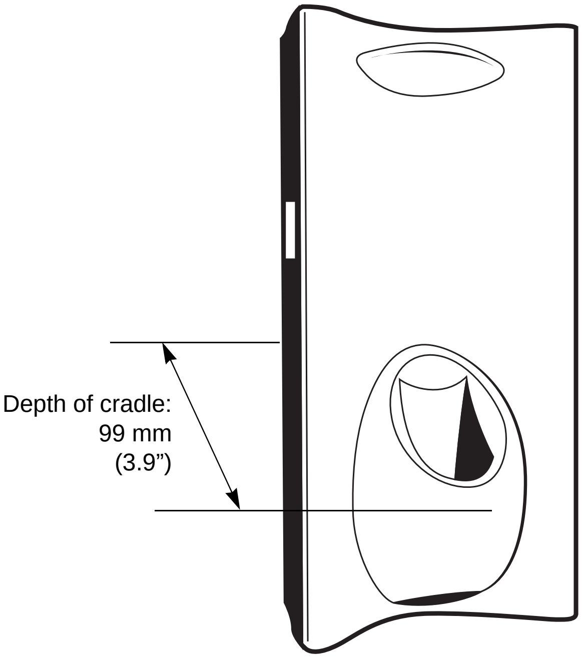


Figure 6-4 *Overall Depth of Cradle*

Wiring

✓ ***NOTE*** During installation ensure all interconnect cables are fully enclosed within the power supply or cradle enclosure.

1. Install power supply, including AC line cord and power cable, into Decorative Housing.

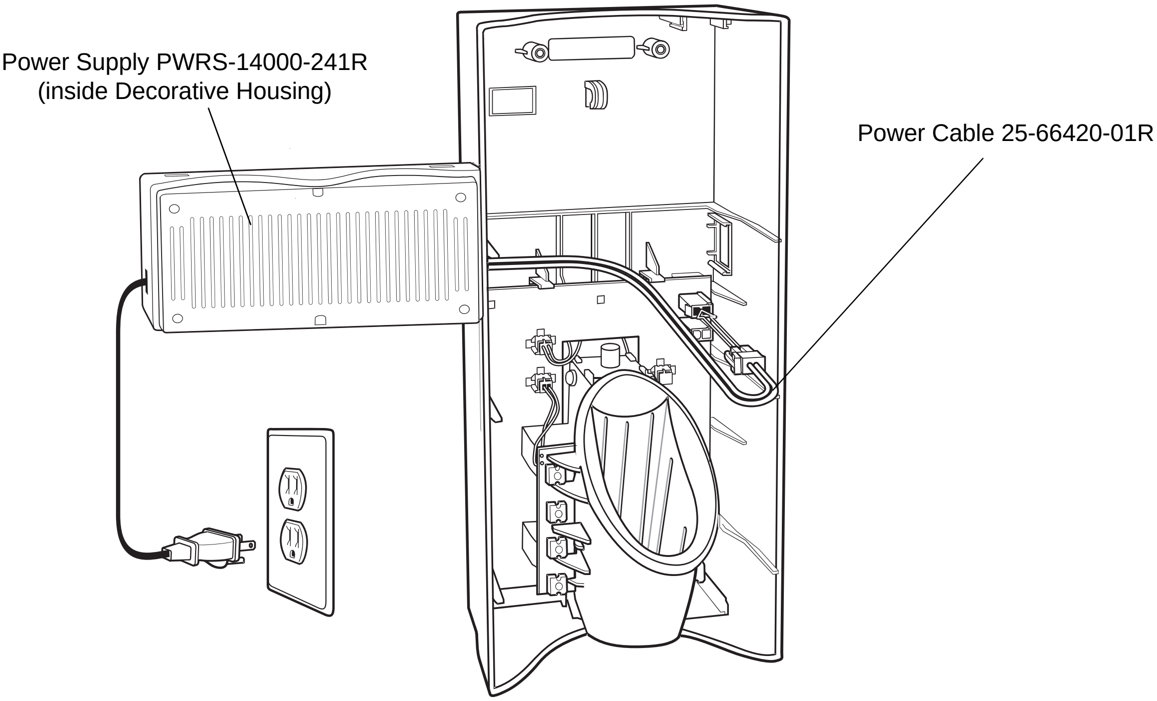


Figure 6-5 *Connecting Power Supply*

2. Insert power cable through a cable outlet of cradle back housing.
3. Plug connector into power connector on printed circuit board.
4. If more than one cradle is being installed, connect the interconnect cable from the first cradle to the second cradle.

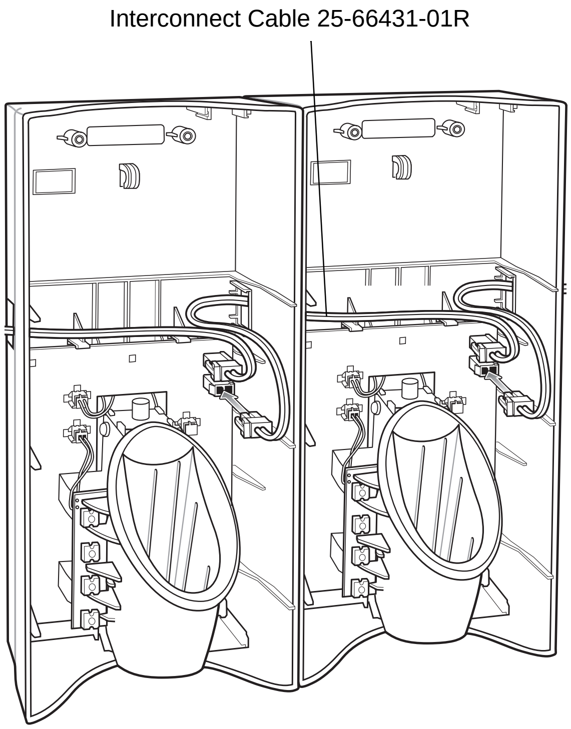


Figure 6-6 *Daisy-Chaining Cradles*

5. Use plugs to cover un-used cable outlets.

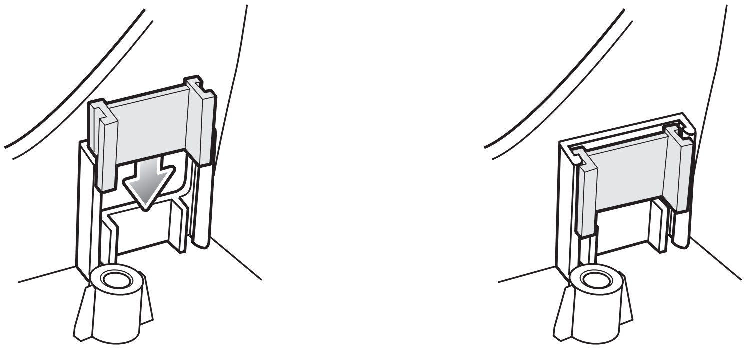


Figure 6-7 *Cable Hole Plug Installation*

Assembly

1. Replace cover.
2. Secure cover with screws.

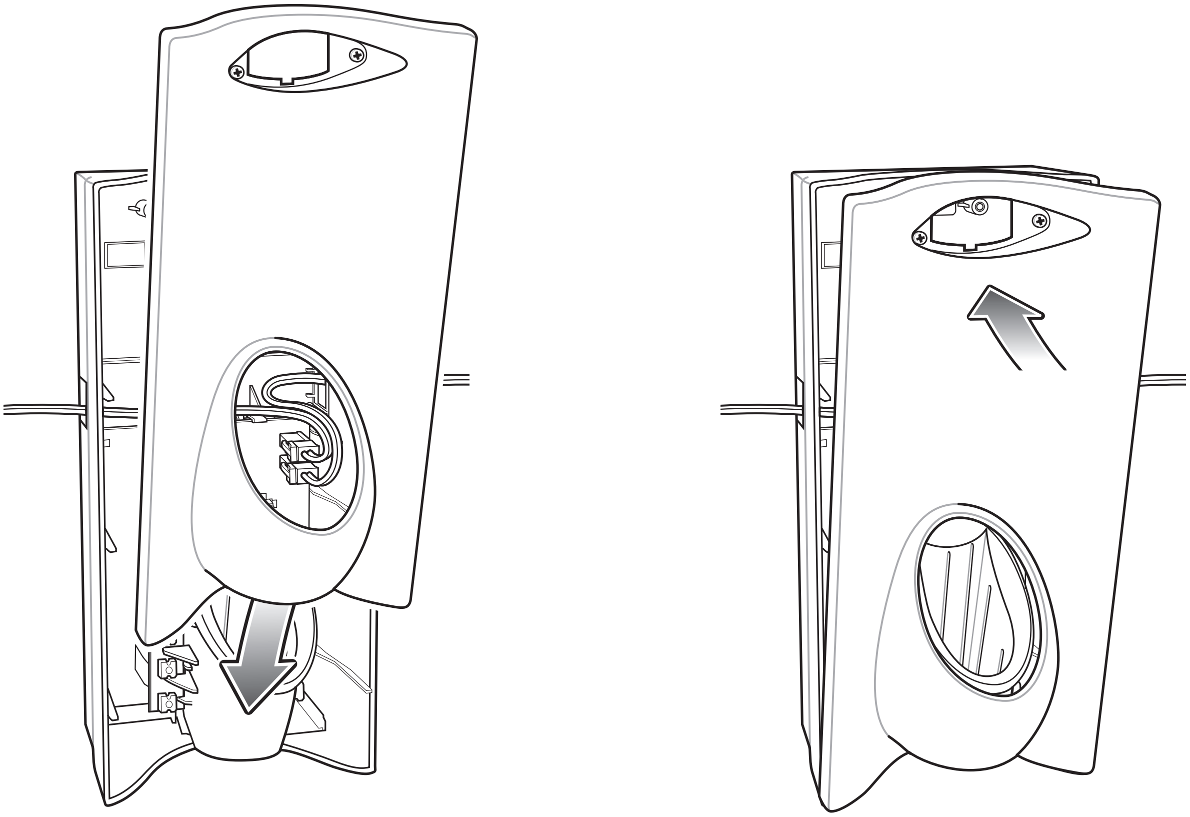


Figure 6-8 *Replace Cover*

✓ ***NOTE*** Do not install the target cover until you are sure that you do not need to remove the front cover again.

3. Insert bar code target cover.

4. Push target cover into front cover until it snaps into place.

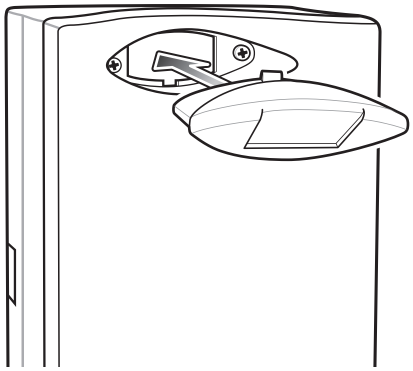


Figure 6-9 *Replace Target Bar Code Cover*

System Cabling

There are some general limitations that must be taken into account when designing a dispenser and ordering hardware elements of a Personal Shopper system:

- No more than six cradles can be powered off each leg of the "Y" power cable.

- A power supply cable runs from the power supply to one or two cradles.
- Cradle interconnection cables run between each successive cradle in the chain.
- The power supply is air cooled, and as such expects some circulation of fresh air around it. Do not enclose it in a small airtight location.
- Power supplies must be mounted in their natural, landscape orientation. They contain fans and their vents must allow for the free flow of air.
- Power supplies should be mounted either above or below dispensers and entrance heads. Mounting of power supplies to the right or left is not preferred.
- When laying out your furniture and cabling plan, routing should be as direct as possible. Routing should follow vertical and horizontal runs through the modules. A set of labels, numbered 1 to 12, is part of each power supply unit. These labels are to be used to track the number of loads on a particular supply. Each label is designed to be attached to the cradle interconnection cable when a cradle is added to the daisy chain. When all labels are used, the supply is fully loaded.

Figure 6-10 shows how the maximum number of cradles can be cabled to a power supply using power cable 25-66420-01R.

Figure 6-11 shows how the maximum number of cradles can be cabled to a power supply using the “Y” power cable 25-67592-01R. Note that there are only six cradles per leg of the power supply cable, and only 12 cradles in total.

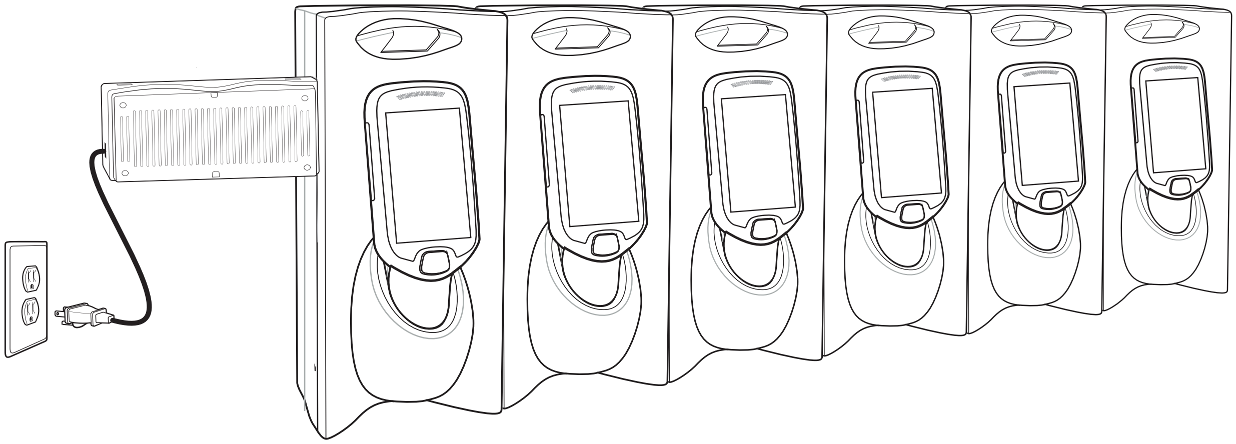


Figure 6-10 *Maximum Number of Charge Cradles per Power Supply*

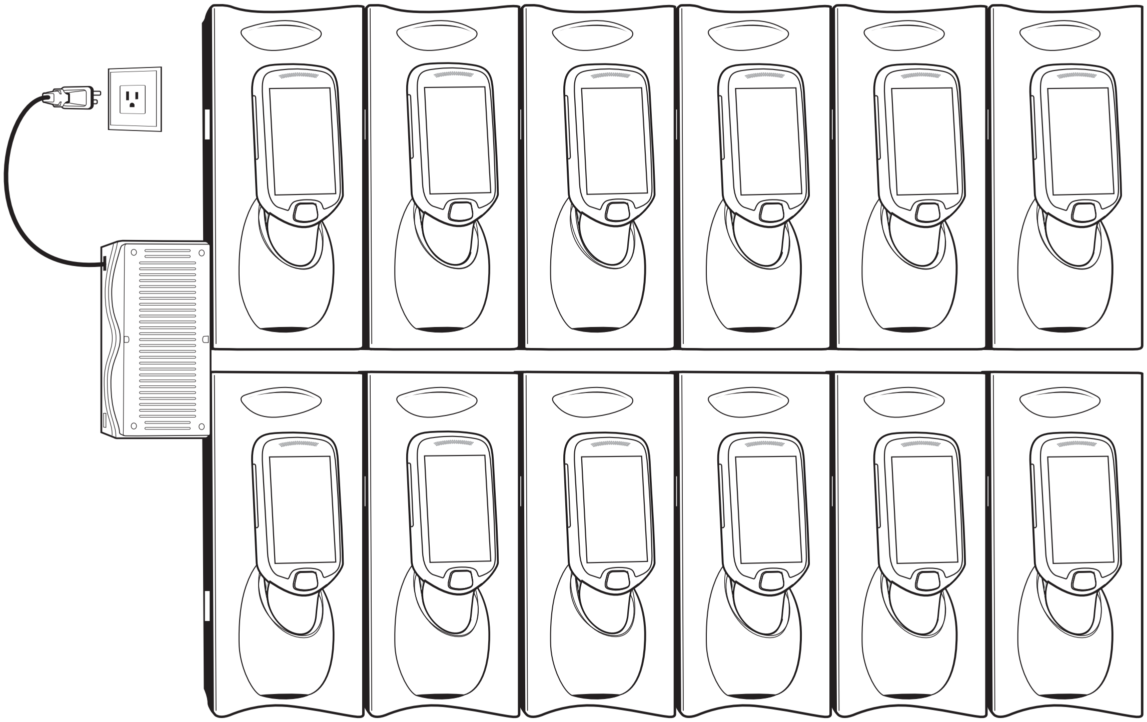


Figure 6-11 *Maximum Number of Charge Cradles per Power Supply with “Y” Power Cable*

Installation of the Three Slot Cradle

Installation of the Three Slot Cradle include the following mounting steps:

- Select the mounting configuration (see *Mounting Configurations on page 6-11*)
- Select the charging mode (see *Charging Modes on page 6-13*)
- Mount the Three Slot Cradles on a dispenser wall (see *Mounting the Three Slot Cradle on a Dispenser Wall on page 6-16*)
- Mount the power supply unit (see *Mounting the Power Supply Unit on page 6-21*)
- Set the cradle(s) (see *Controlling the Cradle on page 4-4*)

Mounting Configurations

Three slot cradles can be installed in the following mounting configurations:

- High Density (HD) configuration - Using HD cradles
- Super High Density (SHD) configuration - Using SHD cradles
- Desktop configuration - Using stand alone cradle(s) on a flat surface

High Density Configuration

The cradle can be installed in high density configuration so that the display of the MC18 devices are facing the user. In this configuration, cradles are installed with a vertical gap of 35mm between each other.

✓ ***NOTE*** In high density configuration, the MC18 units have a 10-degree forward-facing tilt that should be taken in consideration, especially if furniture is planned to be placed in front of the dispenser wall.

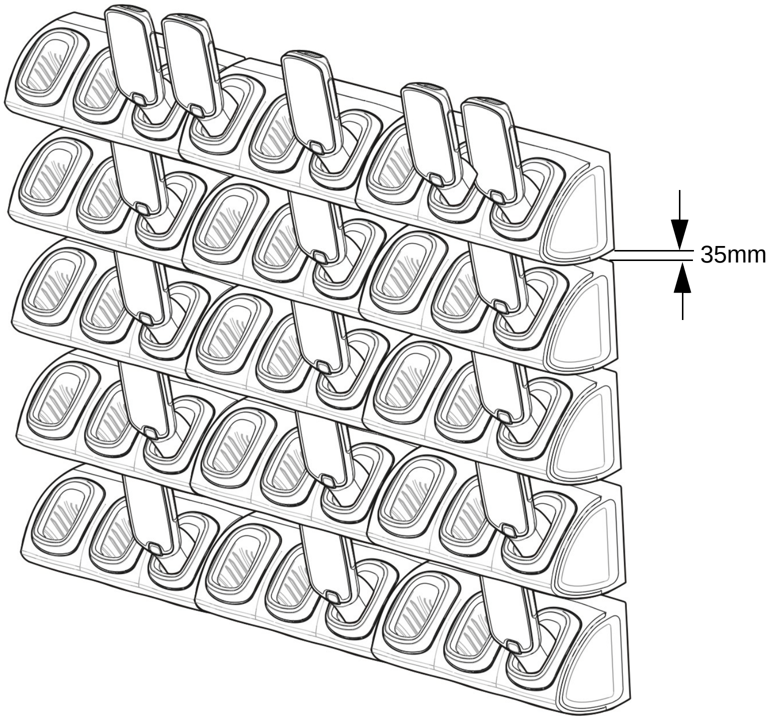


Figure 6-12 Installation in High Density Configuration

The installation of the dispenser wall can be designed so that it tilts slightly backward in the following angles:

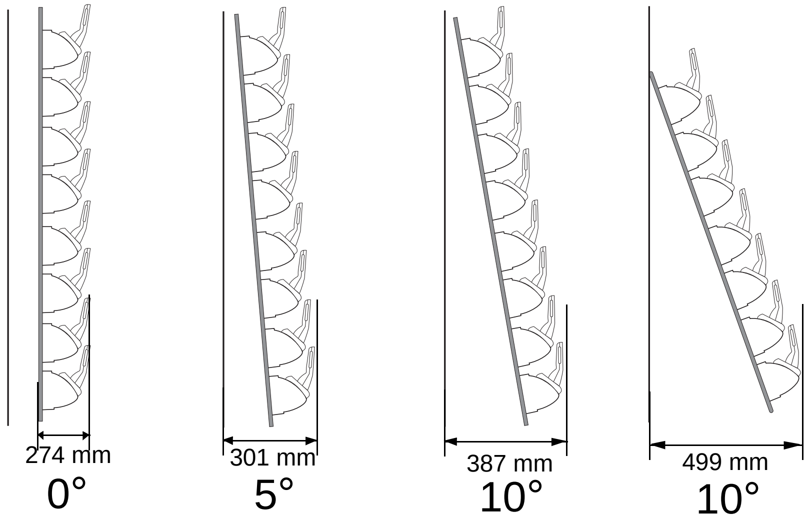


Figure 6-13 *Dispenser Wall Angles*

Super High Density Configuration

The cradle can be installed in super high density configuration so that the display of the MC18 devices are facing up. In such configuration, cradles are installed with a vertical gap of 7mm from each other to allow more cradles per square meter.

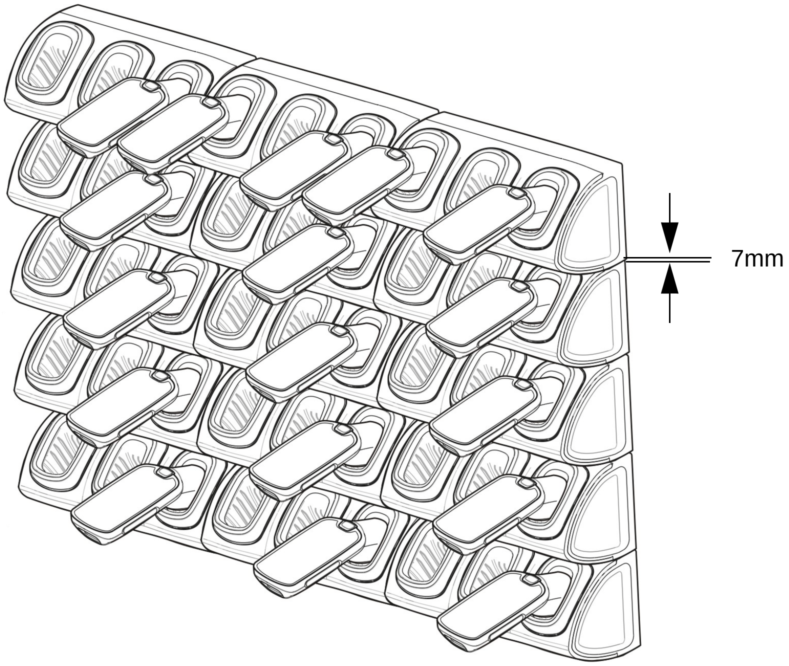


Figure 6-14 *Installation in Super High Density Configuration*

Desktop Configuration

In desktop configuration, the cradle can be placed on a flat tabletop or shelf at checkout or back room locations.

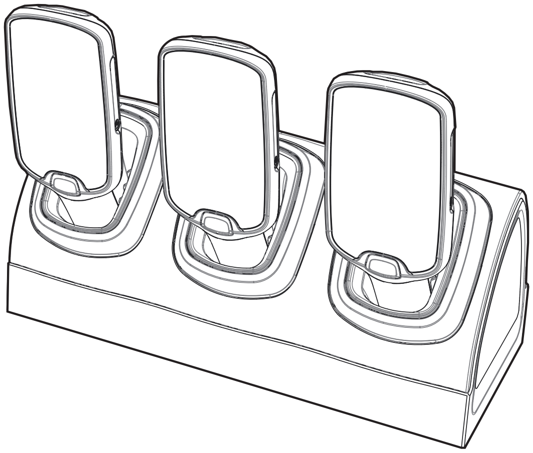


Figure 6-15 *Installation in Desktop Configuration*

Charging Modes

Three Slot Cradles can be installed in the following charging modes:

- Standard charging
- Fast charging

There are some general charging considerations that must be taken into account when designing a dispenser and ordering hardware elements of a system:

Standard Charging Mode

- In standard charging mode, no more than four cradles can be powered off of one power supply unit (p/n PWRS-14000-241R) using “Y” power cable (p/n 25-67592-01R or p/n 25-66210-01R), power extension cables (p/n CBL-MC18-EXINT1-01) and interconnect cables (p/n 25-66431-01R).
- In standard charging mode, the current draw by each docked MC18 can reach a maximum of 1A.
- Cable routing should be as direct as possible. Routing should follow vertical and horizontal runs through the modules.

Figure 6-16 shows how the four cradles can be cabled to a power supply unit in standard charging mode.

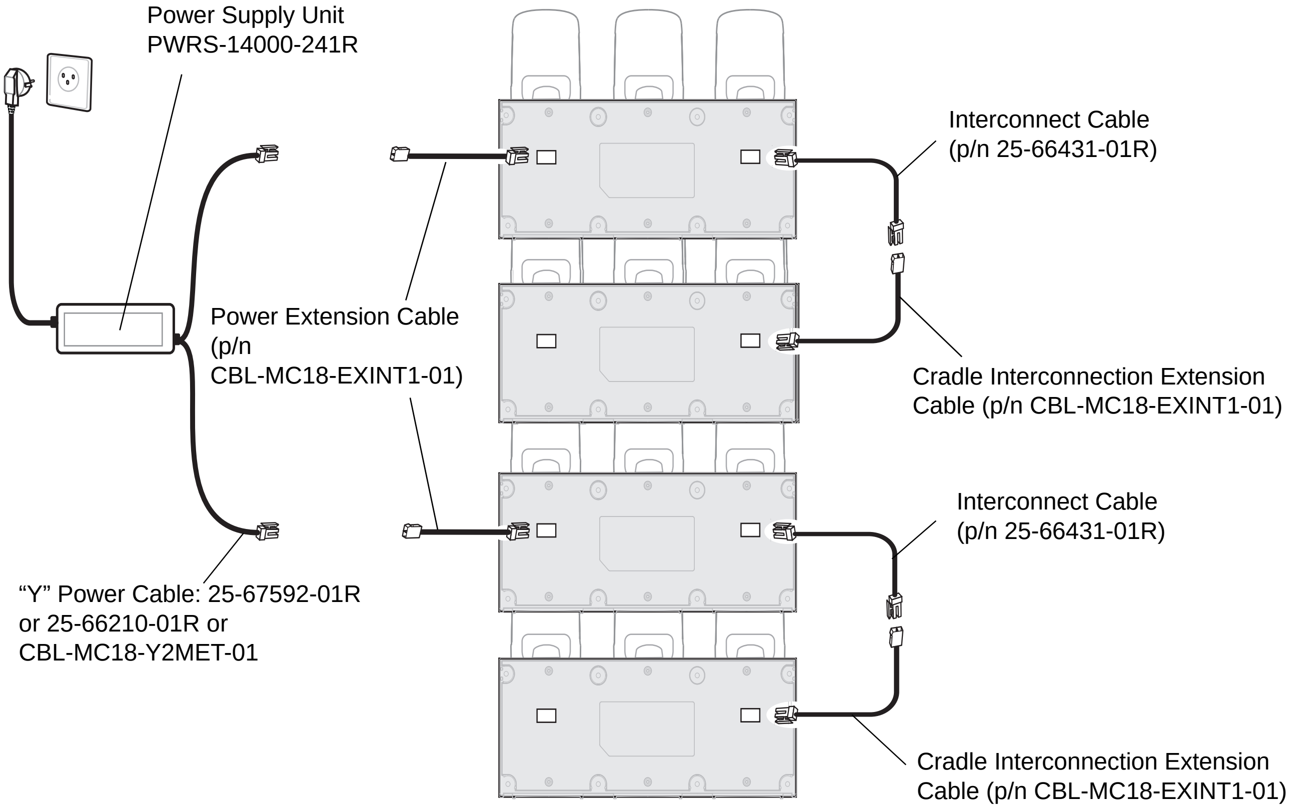


Figure 6-16 *Standard Charging Mode - Cable Connections*

Fast Charging Mode

- In fast charging mode, no more than three cradles can be powered off of one power supply unit (p/n PWRS-14000-241R) using “Y” power cable (p/n 25-67592-01R or p/n 25-66210-01R or CBL-MC18-Y2MET-01), Interconnect cables (p/n 25-66431-01R) and cradle interconnection extension cables (p/n CBL-MC18-EXINT1-01).
- In fast charging mode, the current draw by each docked MC18 can reach a maximum of 1.5A.
- Cable routing should be as direct as possible. Routing should follow vertical and horizontal runs through the modules.

Figure 6-17 shows how the three cradles can be cabled to a power supply unit in fast charging mode.

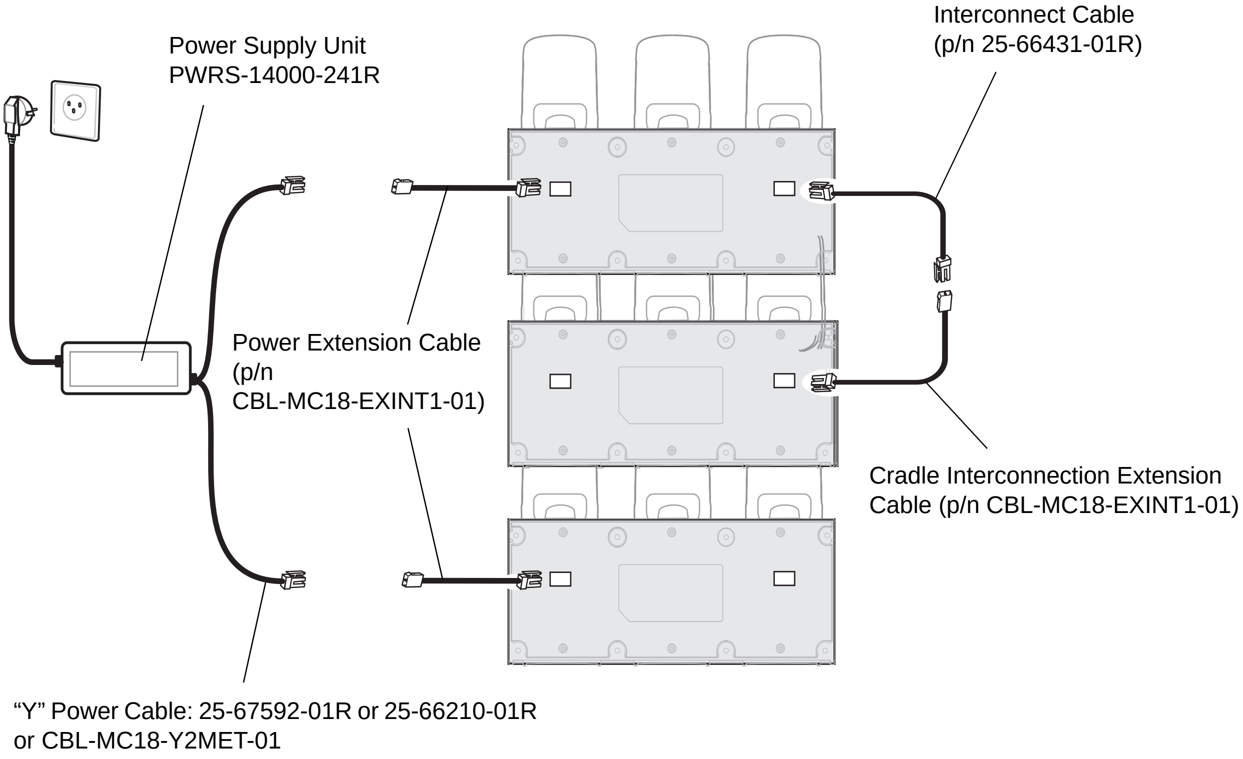


Figure 6-17 *Fast Charging Mode Cable Connections*

Mounting the Three Slot Cradle on a Dispenser Wall

The cradle can be bolted to a dispenser wall or any supporting furniture using eight mounting holes. The back cover of the cradle has two access holes for routing power cables to \ from a power supply unit or adjacent cradle. *Figure 6-18* provides a mounting template for cradle installation.

Perform this procedure to mount the cradle on a dispenser wall:

✓ ***CAUTION*** DO NOT connect more than four cradles when is standard charging mode or three cradles when in fast charging mode to a single power supply unit.
DO NOT connect the power supply unit to a power outlet until all installation steps are completed.

✓ ***NOTE*** The following procedure is an example installation of Three Slot Cradles in fast charging mode - high density configuration.

1. Use the wall mount template to plan and mark the screw locations on the dispenser wall.

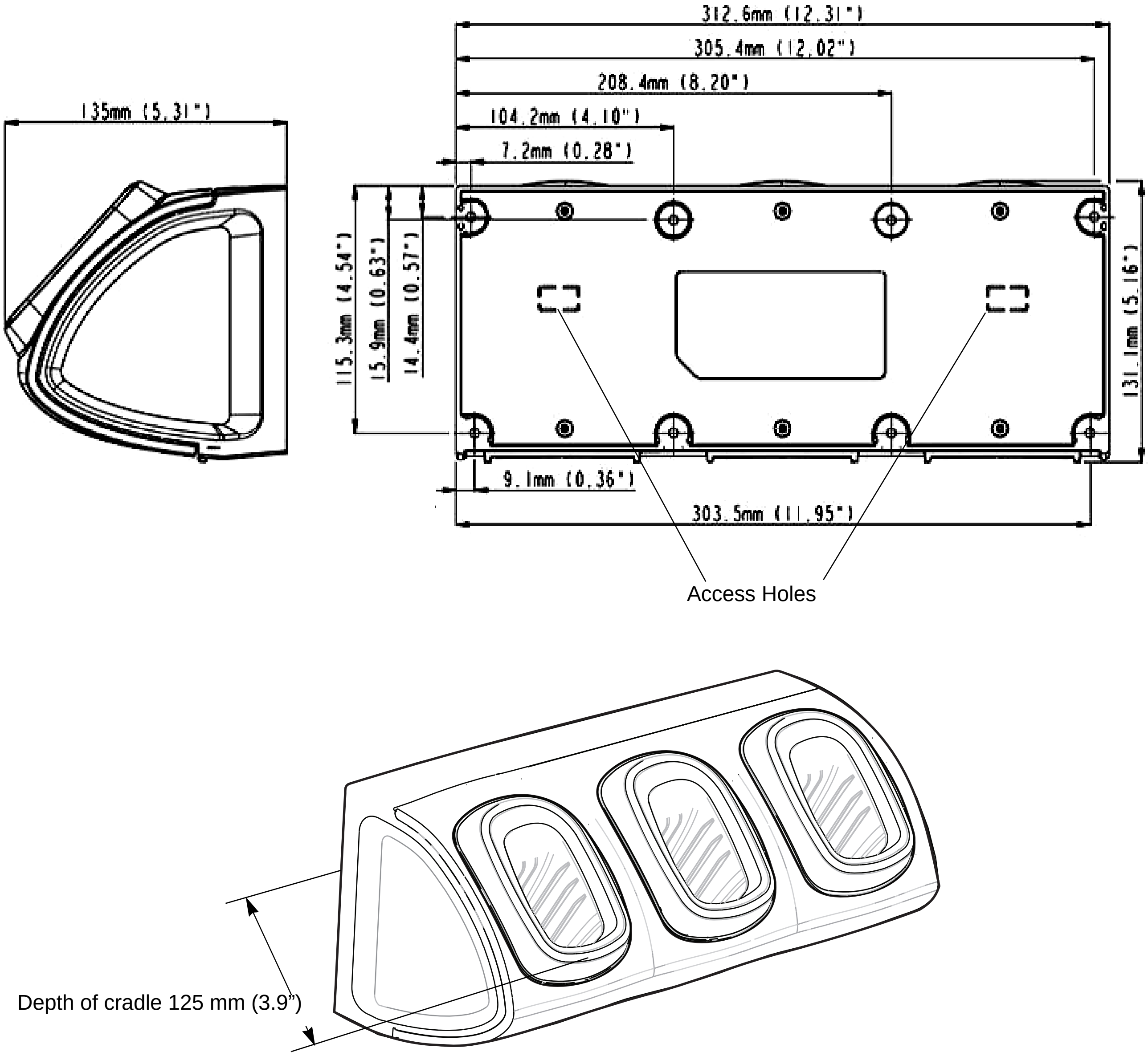


Figure 6-18 *Three Slot Cradle - Mounting Template and Overall Depth*

2. In all cradles, plug the power extension cable (p/n CBL-MC18-EXINT1-01) to free the connector on left slot.

3. Plug interconnect cable (p/n 25-66431-01R) to free connector on right slot.

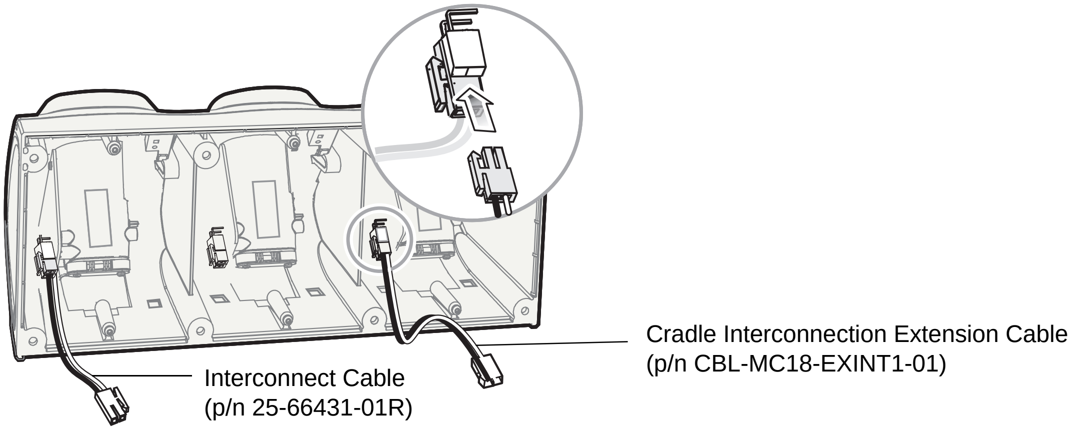


Figure 6-19 *Three Slot Cradle - Cable Connections*

4. On all the back covers, knock-out the stamped access hole(s).

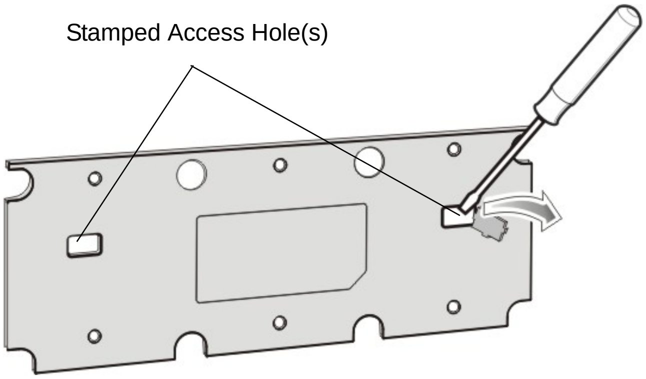


Figure 6-20 *Three Slot Cradle - Stamped Access Hole(s)*

5. Route interconnect cables through access holes in back covers.

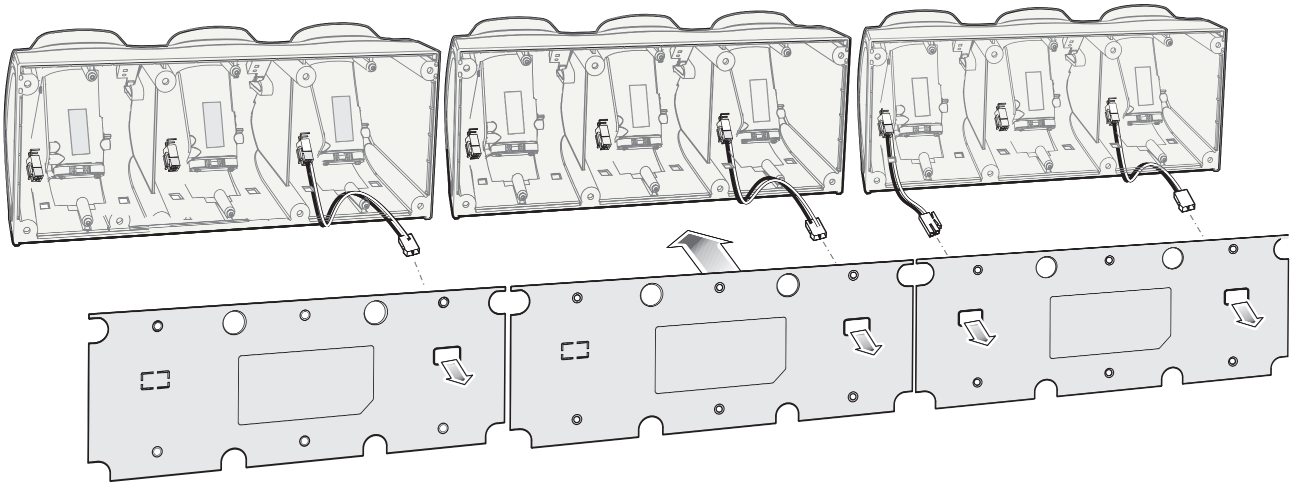


Figure 6-21 *Three Slot Cradle - Back Cover Cable Routes*

6. Secure the back cover of each cradle using six T10 Torx screws (supplied). Torque screws to 6 Kgf-cm (5.2 in-lb).

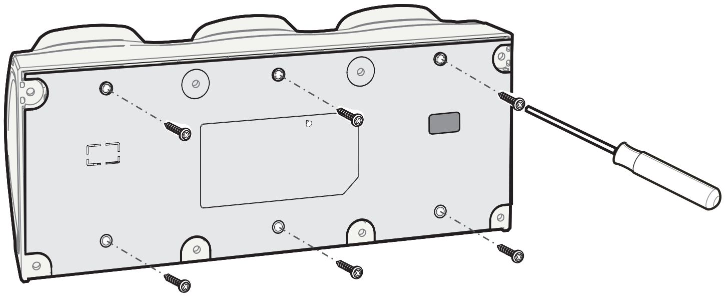


Figure 6-22 *Three Slot Cradle - Securing the Back Cover*

7. Insert the front cover removal tool into two slots, lever upwards and pull to remove front cover from cradle.

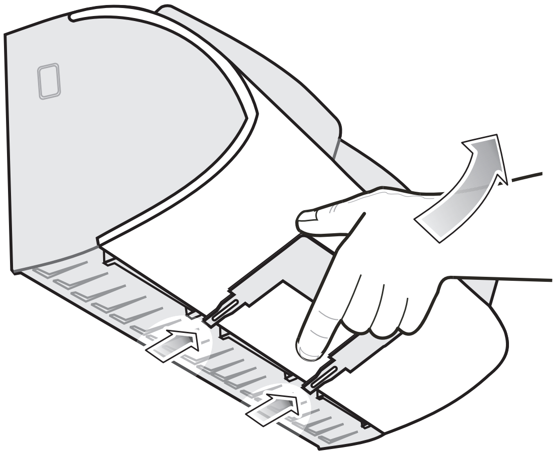


Figure 6-23 *Three Slot Cradle - Removing Front Cover*

8. Position the cradle on the dispenser wall and route all interconnect cables through the access holes in the dispenser wall.

9. Fasten the cradle to the wall using eight screws (not supplied). Make sure to use additional wall mounting hardware, as needed, for safe mounting, according to the wall type.

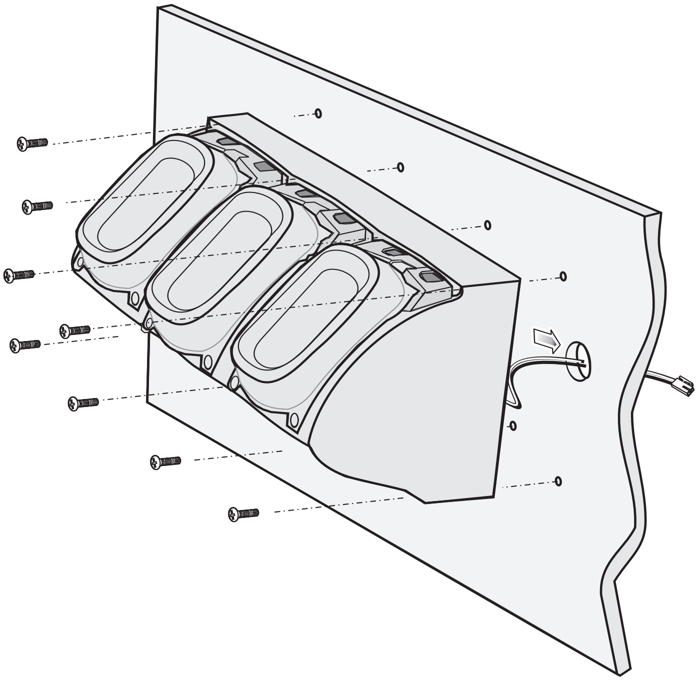


Figure 6-24 *Three Slot Cradle - Fastening the Cradle to a Wall*

10. Insert tabs on upper side of front cover into slots on cradle and rotate cover down until it snaps into place.

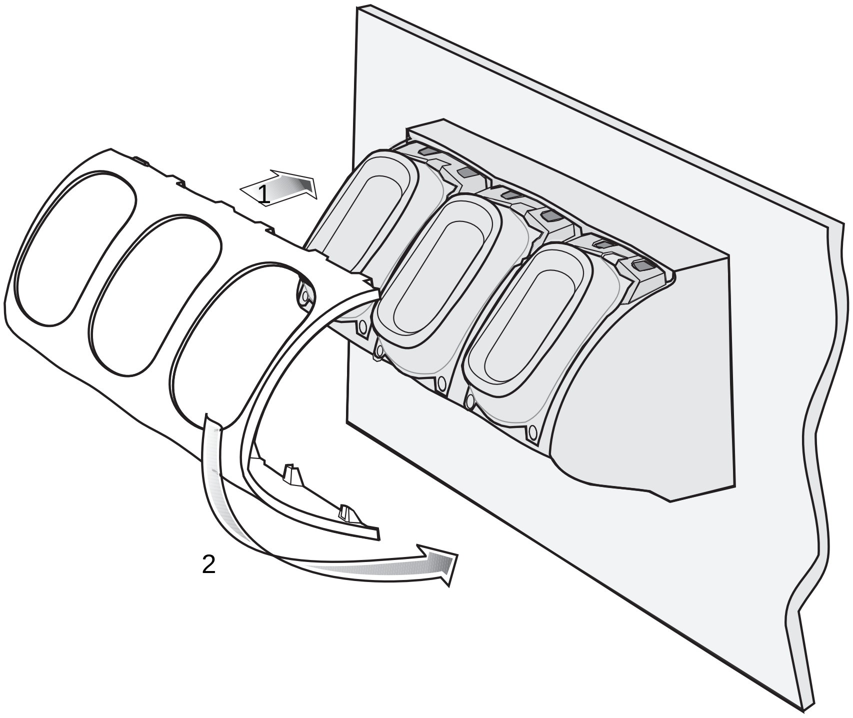


Figure 6-25 *Three Slot Cradle - Connecting the Front Cover*

11. Plug Power Extension Cable (p/n CBL-MC18-EXINT1-01) to interconnect cable (p/n 25-66431-01R).
12. Plug “Y” cable (25-67592-01R) to Interconnect cables (p/n 25-66431-01R).
13. Plug “Y” cable (25-67592-01R) to power supply unit.

14. Secure power supply unit (p/n PWRS-14000-241R) to the back of the dispenser wall.

15. Connect the power cord to the power supply unit and to a 110/220 VAC outlet.

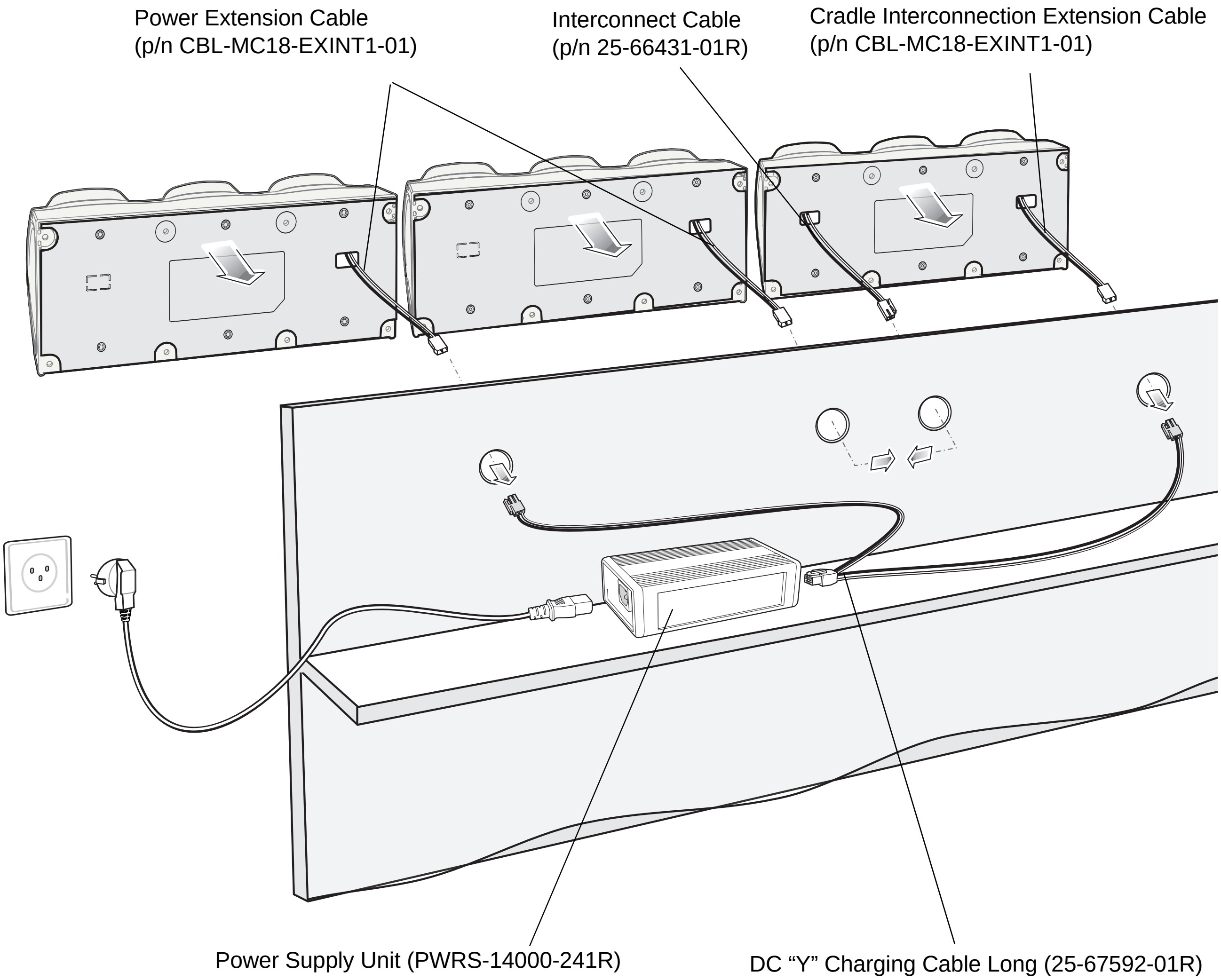

Power Extension Cable
(p/n CBL-MC18-EXINT1-01)
Interconnect Cable
(p/n 25-66431-01R)
Cradle Interconnection Extension Cable
(p/n CBL-MC18-EXINT1-01)
Power Supply Unit (PWRS-14000-241R)
DC "Y" Charging Cable Long (25-67592-01R)

Figure 6-26 *Three Slot Cradle - Connection to Power Supply Unit*

16. Place the socket onto the cradle and secure the four screws.

17. Place the socket cover onto the cradle and secure the two screws.

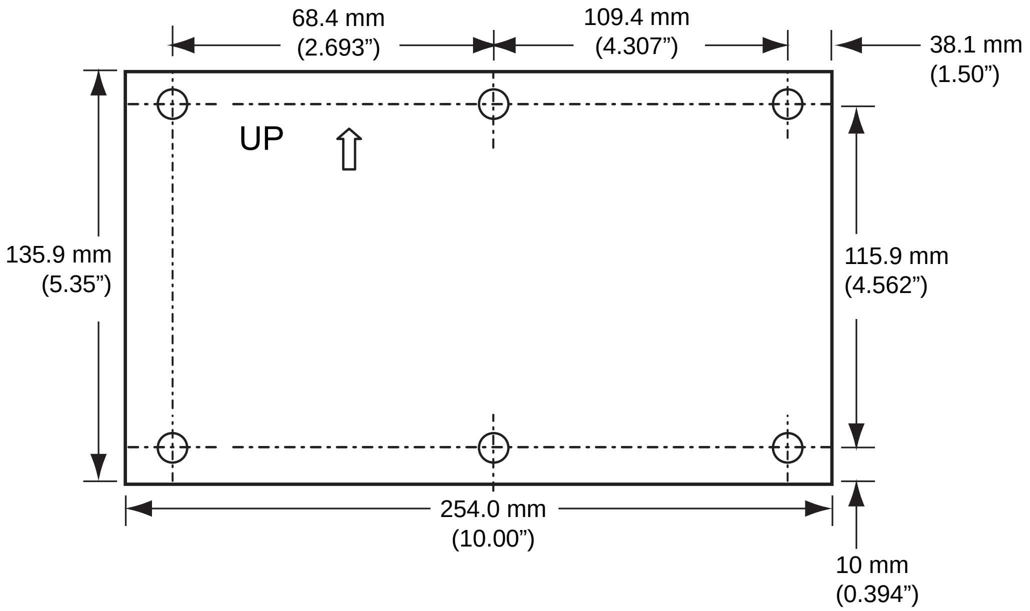
Mounting the Power Supply Unit

✓ ***IMPORTANT*** The power supply unit is air cooled and requires circulation of free air around it. Do not enclose it in a small airtight enclosure other than plastic housing, p/n PSS-3PS04-00R.

The power supply can be housed in an optional plastic housing, p/n PSS-3PS04-00R, to match the cradles and hide bare power supplies and cables. This section provides the information required to mount the plastic housing.

To install the power supply unit inside the plastic housing:

1. Use the mounting template of the power supply housing to plan and mark the screw locations on the dispenser wall.



(View from Inside Housing)
The depth of the fully-assembled power supply decorative housing is 81.23 mm (3.198”).

Figure 6-27 *Power Supply Housing Mounting Template*

2. Feed cables through access holes in bottom housing.
3. Plug connectors into power supply.
4. Place power supply into bottom housing.
5. Place two mounting brackets over power supply and secure each mounting bracket with two screws.

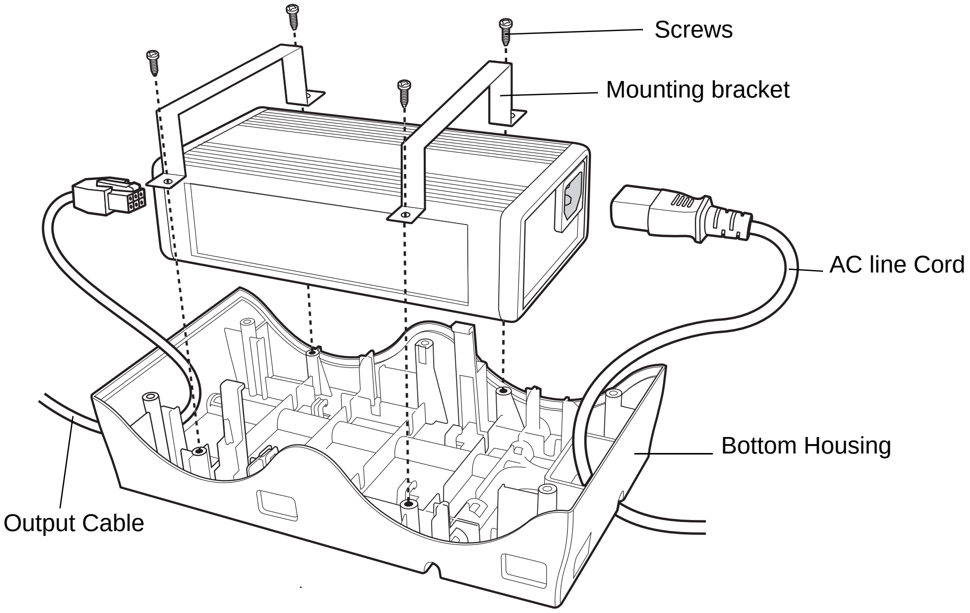


Figure 6-28 *Power Supply Assembly*

6. Align top housing over bottom housing and secure using six screws.

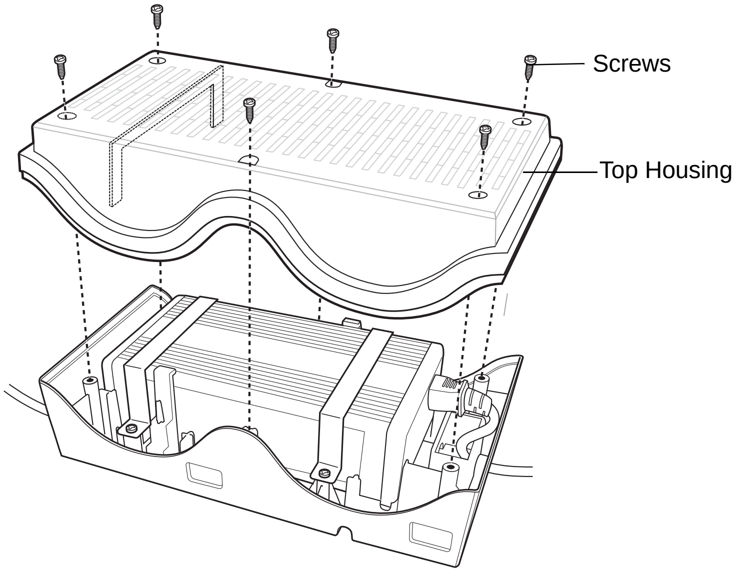


Figure 6-29 *Top Housing Installation*

CHAPTER 7 USB COMMUNICATION

This chapter provides information for transferring files between the device and a host computer.

Connecting to a Host Computer via USB

Connect the MC18 to a host computer using the Programming cable to transfer files between the MC18 and the host computer.

⚠ ***CAUTION*** When connecting the MC18 to a host computer, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Connecting to the MC18 as a Media Device

✓ ***NOTE*** Using Media Device, you can copy files to the internal memory.

1. Connect the Programming cable to the MC18 and then to the host computer.

   Connected as a media device appears on the Status bar.

2. On the host computer, open a file explorer application.
3. Locate the **MC18N0** as a portable device.
4. Open the **On Device Storage** folder.
5. Copy or delete files as required.

Disconnect from the Host Computer

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

1. On the host computer, unmount the device.
2. Remove the Programming cable from the device.

CHAPTER 8 ADMINISTRATOR UTILITIES

Zebra provide a suite of utilities that allow an administrator to manage the following features:

- Multi-user Login - The Multi-user Login feature allows an administrator to set up the device to be used by multiple users. The users have access to specific applications and features depending upon the user settings.
- Application Lock - The Application Lock feature allows an administrator to restrict application access for specific applications by user or groups of users. The permitted applications are managed using groups of user accounts from Multi-user Login feature.
- Secure Storage - Secure Storage Administrator application allows installation and deletion of encrypted keys and creation, mounting, un-mounting and deletion of the encrypted file systems.

The following applications help the administrator configure these features.

- On-device applications - reside on the device.
  - MultiUser Administrator
  - AppLock Administrator
  - Secure Storage Administrator.
- Host computer application - reside on a host computer.
  - Enterprise Administrator.

Required Software

These tools are available on the Support Central web site at Support Central. Download the required files from the Support Central web site and follow the installation instruction provided.

On-device Application Installation

See *Application Installation on page 10-3* for instruction on installing applications onto the device.

Multi-user/AppLock Configuration

To use the Multi-user Login and Application Lock features, the administrator must create user and group account information using the Enterprise Administrator application.

✓ ***NOTE*** The administrator can also create the account information manually. See *Manual File Configuration on page 8-11* for more information.

Enterprise Administrator Application

NOTE Net Compact Framework 4 or later is required to run the Enterprise Administrator. To download, go to www.microsoft.com.

Use the Enterprise Administrator application to setup user and group accounts and create the required (Password, Group and White List) files for using the Multi-user and Application Lock features.

On the host computer launch the Enterprise Administrator application.

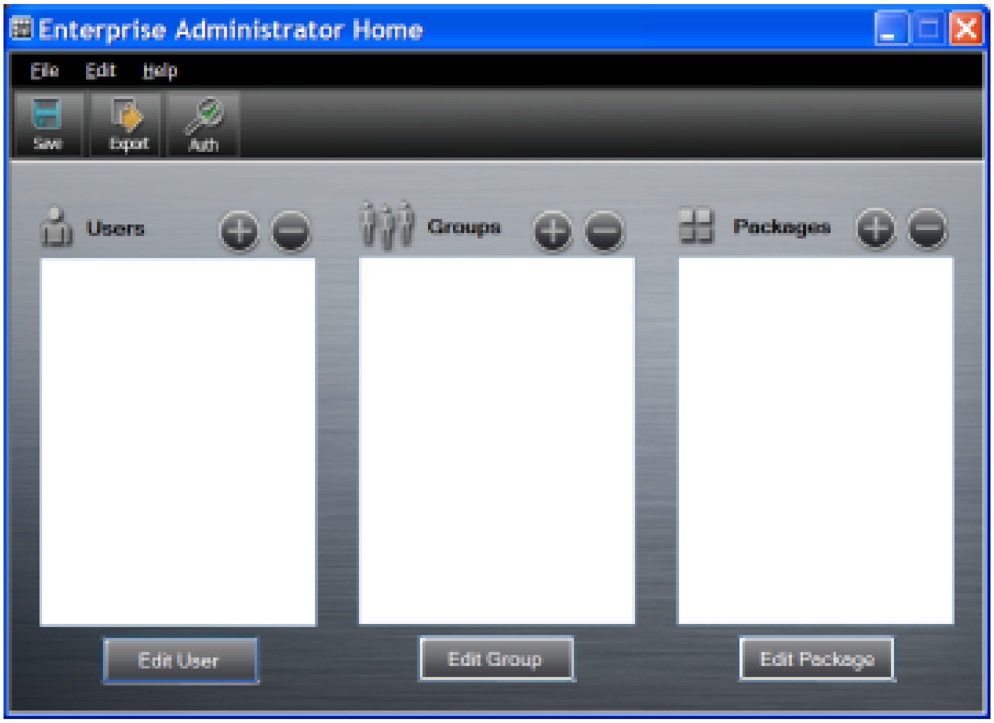


Figure 8-1 *Enterprise Administrator Window*

Creating Users

Each person that uses the device has to have a user name and password. To create a user:

1. Click **+** above the **Users** list box.

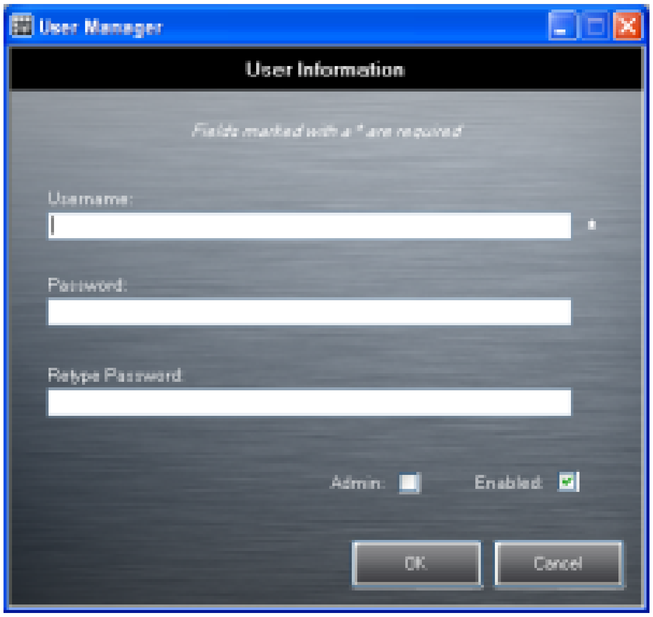


Figure 8-2 *User Manager Window*

2. In the **Username** text box, enter a user name. The text is case sensitive and required.
3. In the **Password** text box, enter a password for the user. The text is case sensitive and required.
4. In the **Retype Password** text box, re-enter the user password.
5. Select the **Admin** checkbox to set the user to have administrator rights.
6. Select the **Enabled** checkbox to enable the user.
7. Click **OK**.
8. Repeat steps 1 through 7 for each additional user.

Adding Packages

NOTE All system applications that are on the default image are available to all users.

Create a list of installed applications (packages) on the device that are available for use by all the users.

1. Click **+** next to **Packages**.

NOTE To get a list of all the applications (packages) on the device see *Determining Applications Installed on the Device on page 8-14*.

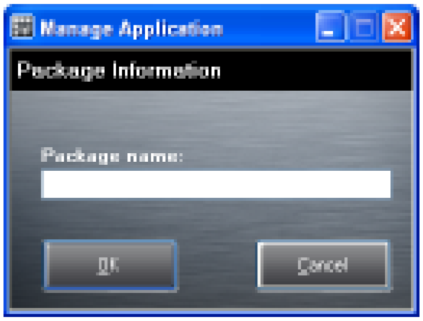


Figure 8-3 *Package Information Window*

2. In the **Package name** text box, enter the name of an application.
3. Click **OK**.
4. Repeat steps 1 through 3 for each additional package.

Creating Groups

Create groups of users that have access to specific applications.

1. Click **+** above the **Groups** list. The **Group Manager** window appears with a list of users and packages.

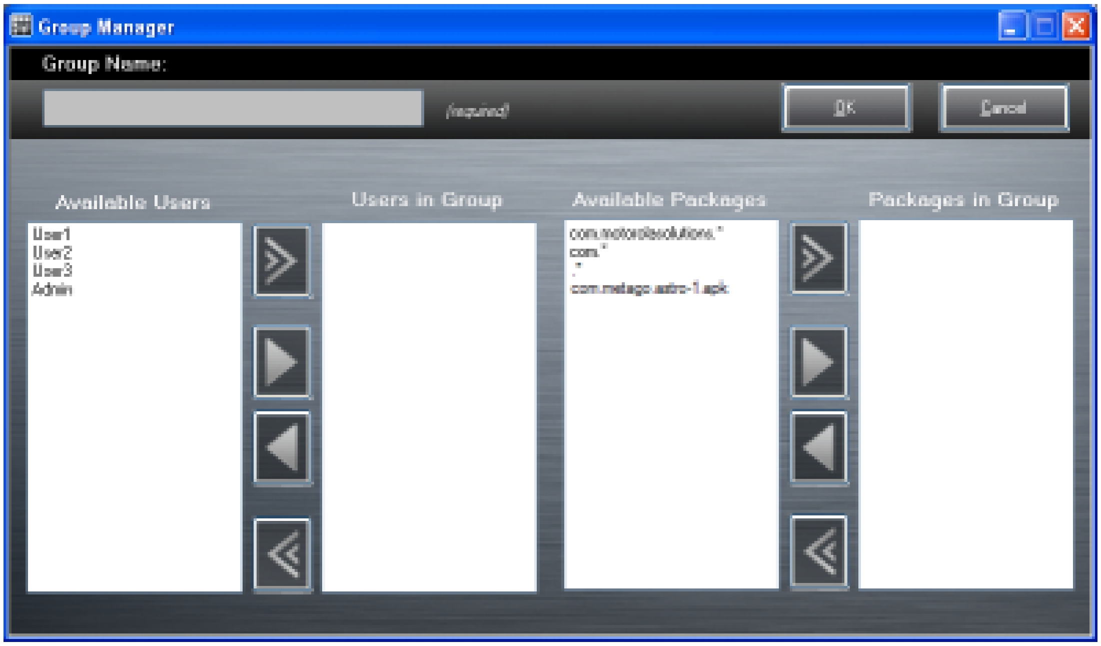


Figure 8-4 *Group Manager Window*

2. In the **Group name** text box, enter a name for the group. This field is required.
3. Select a user in the **Available Users** list box and then click the **Add** button to add the user to the **Users in Group** list box or click the **Add All** button to add all the users in the **Available Users** list box to the **Users in Group** list box.
4. Select a package in the **Available Packages** list box and then click the **Add** button to add the package to the **Packages in Group** list box or click the **Add All** button to add all the packages in the **Available Packages** list box to the **Packages in Group** list box.

5. Click **OK**.
6. Click **Save**.

Creating Remote Authentication

Use the Remote Authentication feature to set a remote server for authentication.

1. Click the **Auth** button. The **Authentication** window appears.

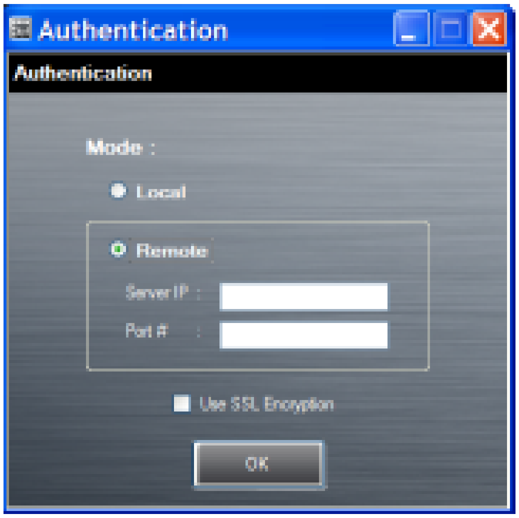


Figure 8-5 *Authentication Window*

2. Select the **Remote** radio button.
3. In the **Server IP** text box, enter the address of the remote server.
4. In the **Port** text box, enter the port number of the remote server.
5. Select the **use SSL Encryption** check box if SSL encryption is required.
6. Click **OK**.

Save Data

At any time, the administrator can save the current data. The application creates two files in the **`<user>\_APP_DATA`** folder: *database* and *passwd*.

Exporting File

In order to use the features on the device, export the required files and then copy them to the device. The following files are created by the Enterprise Administrator application:

- Password File - Filename: *passwd*. Lists the user names, encrypted passwords, administrator and enable flags.
- Group File - Filename: *groups*. Lists each group and users associated to each group.
- White List Files - Filename: the filenames are the names of the group created in the Group file. Lists the user installed applications that the group is allowed to access.
- Remote Server - Filename: *server*. Lists the remote server IP address and port number.

1. Click **Export**.
2. In the Browse For Folder window, select a folder and then click **OK**.
3. Click **OK**.
4. Click **File > Export > Server Information**.

   The server file is saved in the **`<user>\_APP_DATA`** folder.
5. Copy all the files to the root of the On-device Storage. See *Chapter 7, USB Communication* for information on copying files to the device.

Importing User List

1. Click **File** > **Import** > **User List**.
2. Navigate to the location when the *passwd* file is stored.
3. Select the *passwd* file.
4. Click **Open**.

   The user information is populated into the **Users** list.

Importing Group List

1. Click **File** > **Import** > **Group List**.
2. Navigate to the location when the *group* file is stored.
3. Select the *group* file.
4. Click **Open**.

   The group and package information is populated into the **Groups** and **Packages** list.

Importing Package List

To import a package list (see *Package List File on page 8-14* for instructions for creating a Package List file):

1. Click **File** > **Import** > **Package List**.
2. Navigate to the location when the package file is stored.
3. Select the package text file.
4. Click **Open**.

   The package information is populated into the **Packages** list.

Editing a User

1. Select a user in the **Users** list.
2. Click **Edit User**.
3. Make changes and then click **OK**.

Deleting a User

1. Select a user in the **Users** list.
2. Click **-**. The user name is removed from the list.

Editing a Group

1. Select a user in the **Groups** list.
2. Click **Edit Group**.
3. Make changes and then click **OK**.

Deleting a Group

1. Select a group in the **Groups** list.
2. Click **-**.
3. Click **Yes**. The group name is removed from the list.

Editing a Package

1. Select a package in the **Packages** list.
2. Click **Edit Package**.
3. Make changes and then click **OK**.

Deleting a Package

1. Select a package in the **Packages** list.
2. Click **-**. The package name is removed from the list.

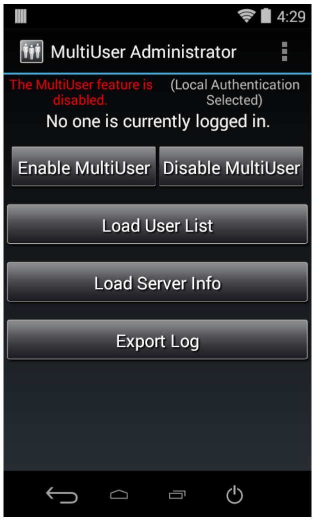
MultiUser Administrator

Use the **MultiUser Administrator** application to allow an administrator to enable, disable and configure the Multiuser Login feature.

Importing a Password

When the **MultiUser Administrator** is used for the first time, the password file must be imported.

1. Touch ⊞ > ⊞.



The MultiUser feature is disabled.

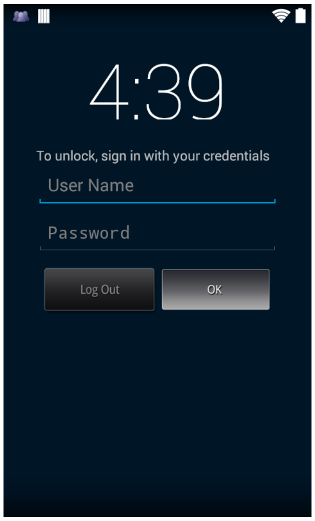
(Local Authentication Selected)

No one is currently logged in.

Figure 8-6 *MultiUser Administrator Screen*

2. Touch **Load User List**. The application reads the data from the *passwd* file and configures the Multi-user Login feature.

3. Touch **Enable Multiuser** to enable the feature.



4:39

To unlock, sign in with your credentials

Figure 8-7 *MultiUser Login Screen*

4. In the **Login** text box, enter the username.

5. In the **Password** text box, enter the password.
6. Touch **OK**.

Disabling the Multi-user Feature

NOTE To disable the Multi-user Login feature, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

1. Touch ⊞ > 👥.
2. Touch **Disable MultiUser**.

   The Multi-user feature is disabled immediately.

Enabling Remote Authentication

CAUTION When Remote Authentication is enable, the device searches for the remote server during the login procedure. If the remote server is not available or the address is incorrect, the user would not be able to login and an Enterprise reset is required to access the device.

1. Touch ⊞ > 👥.
2. Touch **Load Server Info**. The application reads the data from the *server* file and configures the Multi-user Login feature.
3. Touch ⋮ .
4. Touch **Enable Remote Authentication**.

   The device accesses the remote server and then Login screen appears.

Disabling Remote Authentication

CAUTION When Remote Authentication is enable, the device searches for the remote server during the login procedure. If the remote server is not available or the address is incorrect, the user would not be able to login and an Enterprise reset is required to access the device.

1. Touch ⊞ > 👥.
2. Touch ⋮ .
3. Touch **Disable Remote Authentication**.

   The remote authentication feature is disabled immediately. The device suspends. When resumed, the login screen appears.

Enabling Data Separation

NOTE To enable Data Separation, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Data Separation feature allows each user of the device to have separate isolated data area for installed application. To enable data separation:

1. Touch ⠿ > 👥.
2. Touch ⋮ .
3. Touch **Enable Data Separation**. The current user is logged out to prepare the data space for each user as they log in.

Disabling Data Separation

✓ ***NOTE*** To disable Data Separation, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

1. Touch ⠿.
2. Touch 👥.
3. Touch ⋮ .
4. Touch **Disable Data Separation**. The current user is logged out to restore the system to common data space for all users.

Delete User Data

✓ ***NOTE*** To delete user data, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

1. Touch ⠿ > 👥.
2. Touch ⋮ .
3. Touch **Delete Individual User Data**. A dialog box displays with all of the users that currently have data associated with their log in.
4. Select each user to delete or **Select All** to delete all user data.
5. Touch **Delete** to delete the data.

Capturing a Log File

1. Touch ⠿ > 👥.

✓ ***NOTE*** To capture a log file, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

2. Touch **Export Log** to copy the log file to the On-device Storage. The log file can be captured when the multi-user feature is in either the enabled or disabled mode.
3. The log file and a backup log file are named **`multiuser.log`** and **`multiuser.log.bak`**, respectively.

AppLock Administrator

The Application Lock feature allows the system administrator to restrict application access for specific applications by user or groups of users. The permitted applications are managed using groups of user accounts from Multi-user feature.

The permitted application names are built into an application White List that is used to know which applications are managed by the system.

The Application Lock feature does not prevent execution of native code or plug-ins and it does not prevent applications from accessing public classes within non-permitted applications. The AppLock Administrator application takes advantage of the Application Lock feature allowing an administrator to enable, disable and install White Lists and Groups files.

NOTE To use the AppLock Administrator application, the user must have administrator rights. A message displays at the bottom of the screen notifying the user.

Enabling Application Lock

1. Touch ⠿ > ▦.
2. Touch **Enable Application Lock**.

Disabling Application Lock

1. Touch ⠿ > ▦.
2. Touch **Disable Application Lock**.

Manual File Configuration

Groups File

A Groups file is a text file that provides a list of groups and assigns users to each group.

The text file contains one line for each group. Each line is formatted as follows:

```
<groupname>:<user1>,<user2>,...<usern>
```

where:

`<groupname>` = the name for a group. This is also the name of the White List file for this group. This field uses any alphanumeric character.

`<user1>` through `<userN>` = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 8-8* for more information.

NOTE If the same user is assigned to multiple groups, then that user's White List will be a logical union of the White Lists for all of the groups that user is assigned.

A line starting with the # character is considered a comment and is ignored.

Examples:

- AdminGroup:alpha
  - The Group name is AdminGroup and assigns user alpha to the group.
- ManagersGroup:beta,gamma
  - The Group name is ManagerGroup and assigns users beta and gamma to the group.

White List File

A White List file is a text file that provides a list of allowed packages from that group. The text file contains one line for each allowed package for that user group. Each line is format as follows:

```
<package1name>
.
.
.
<packageNname>
```

where:

- `<package1Name>` = the package name allowed for this group. Wild cards are allowed for this field.

Example:

Refer to the example of the Groups file above. A White List file of the name AdminGroup could have the following lines:

```
com.companyname.application
com.symbol.*
```

where:

com.companyname.application = the specific application with the package name **com.companyname.application** will be permitted for this group.

com.symbol.*= any application that has a package name that starts with **com.symbol** will be permitted for this group.

✓ ***NOTE*** The wildcard “.*” is allowed and indicates that this group is permitted to run any package.

A default White List for use when the MultiUser feature is disabled takes the same form as above but in named default.

To assure that administrative users have access to all device functionality, the White List for the administrative users group should use the wildcard.

At a minimum, the White List for the administrative users group should contain *com.symbol.fusion* to allow administrative users the ability to configure Wi-Fi advanced settings.

Package List File

A Package List file is a text file that lists package names that can be imported into the Packages list. The file makes it easier to enter package name into the application. The text file contains one line for each package name.

Example:

```
com.symbol.example1
com.symbol.example2
com.symbol.example3
com.symbol.example4
```

Groups File

A Groups file is a text file that provides a list of groups and assigns users to each group.

The text file contains one line for each group. Each line is formatted as follows:

`<groupname>:<user1>`,**`<user2>`**,...**`<usern>`**

where:

`<groupname>` = the name for a group. This is also the name of the White List file for this group. This field uses any alphanumeric character.

`<user1>` through **`<userN>`** = the name of the user assigned to this group. The user name is the same as that defined for the MultiUser feature. See *MultiUser Administrator on page 8-8* for more information.

✓ ***NOTE*** If the same user is assigned to multiple groups, then that user’s White List will be a logical union of the White Lists for all of the groups that user is assigned.

A line starting with the # character is considered a comment and is ignored.

Examples:

- AdminGroup:alpha
  - The Group name is AdminGroup and assigns user alpha to the group.
- ManagersGroup:beta,gamma
  - The Group name is ManagerGroup and assigns users beta and gamma to the group.

White List File

A White List file is a text file that provides a list of allowed packages from that group. The text file contains one line for each allowed package for that user group. Each line is format as follows:

```
<package1name>
.
.
.
<packageNname>
```

where:

- **`<package1Name>`** = the package name allowed for this group. Wild cards are allowed for this field.

Example:

Refer to the example of the Groups file above. A White List file of the name AdminGroup could have the following lines:

```
com.companyname.application
com.symbol.*
```

where:

`com.companyname.application` = the specific application with the package name

`com.companyname.application` will be permitted for this group.

`com.symbol.*`= any application that has a package name that starts with

`com.symbol` will be permitted for this group.

NOTE The wildcard “.*” is allowed and indicates that this group is permitted to run any package.

A default White List for use when the MultiUser feature is disabled takes the same form as above but in named default.

To assure that administrative users have access to all device functionality, the White List for the administrative users group should use the wildcard.

At a minimum, the White List for the administrative users group should contain *com.symbol.fusion* to allow administrative users the ability to configure Wi-Fi advanced settings.

Determining Applications Installed on the Device

To determine the names of applications installed on the device for use with the Enterprise Administrator application:

1. Connect the device to the host computer.

NOTE See *Development Tools on page 10-2* for information on installing the USB driver for use with adb.

2. On the host computer, open a command prompt (or a terminal in Ubuntu) and run the following:

   `adb devices`. This returns the device id.

   ```
   adb shell
   $pm list packages -f > sdcard/pkglist.txt
   $exit
   ```

3. A pkglist.txt file is created in the root of the On-device Storage. The file lists all the .apk files installed with their package names.

Package List File

A Package List file is a text file that lists package names that can be imported into the Packages list. The file makes it easier to enter package name into the application. The text file contains one line for each package name.

Example:

```
com.symbol.example1
com.symbol.example2
com.symbol.example3
com.symbol.example4
```

Secure Storage

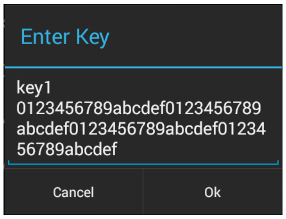
Secure Storage Administrator application allows:

- installation and deletion of encrypted keys
- creation, mounting, un-mounting and deletion of the encrypted file systems.

Installing a Key

To install a key:

1. Touch ⊚.
2. Touch ⊞.
3. Touch **Install Key**.
4. Touch **Manual**.
5. Touch **OK**.



Enter Key

key1
0123456789abcdef0123456789
abcdef0123456789abcdef01234
56789abcdef

Figure 8-8 *Enter Key Dialog Box*

6. In the **Enter key** text box, enter the key name followed by the key value obtained in step 1, using the following format:

   <Key Name> <Key value in Hex String>

   Example: key2 1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef

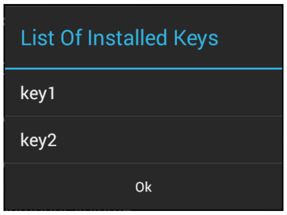
   The key value must be a 64 hexadecimal character string.

7. Touch **OK**. The key is imported into the device. The message **successfully installed the key** appears on the screen.

Viewing Key List

To view a key list:

1. Touch **Key List**.



List Of Installed Keys

key1

key2

Figure 8-9 *List of Keys*

2. Touch **OK**.

Deleting a Key

To delete a key:

1. Touch **Revoke Key**.
2. Touch the key to deleted.
3. Touch **OK**.

✓ ***NOTE*** If a key is deleted then all the volumes created using that key are un-mounted. The same key is required to re-mount the volume.

Volumes

Creates an encrypted file system (volume) on the device. The user must have Administrative privileges to create a volume.

Creating Volume Using EFS File

1. Create an efs file. See *Creating an EFS File on page 8-18* for instruction on creating the efs file.
2. Copy the keyfile and efsfile files to root of Internal Storage. *Chapter 7, USB Communication*.
3. Touch **Create Volume**.
4. Touch **Import**.
5. Touch **OK**. The message **Successfully Created the Volume** appears briefly.

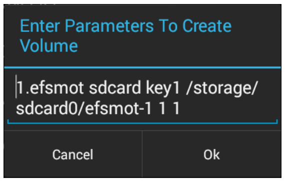
Creating a Volume Manually

1. Touch **Create Volume**.
2. Touch **Manual**.
3. Touch **OK**.
4. In the **Enter Parameters To Create Volume** text box, enter the parameters in the follow format:

   <Volume Name> <Volume Storage Type> Key Name> <Mount Path> <Auto Mount> <Volume size>

   where:

   - <Volume Name> = name of the volume.
   - <Volume Storage Type> = storage location. Options: internal or sdcrad.
   - <Key Name> = name of the key to use when creating the volume.
   - <Mount Path> = path where the volume will be located.
   - <Auto Mount> = Options: 1 = yes, 0 = no.
   - <Volume size> = size of the volume in Megabytes.


Enter Parameters To Create Volume

1.efsmot sdcard key1 /storage/sdcard0/efsmot-1 1 1

Figure 8-10 *Enter Parameter To Create Volume Dialog Box*

5. Touch **OK**. The message **Successfully Created the Volume** appears briefly. If the size of the volume is very large, a progress bar displays.

Mounting a Volume

1. Touch **Mount Volume**.
2. Touch **sdcard** or **internal**.
3. Touch **OK**.
4. Select a volume.
5. Touch **OK**.

Listing Volumes

1. Touch **Volume List**.
2. Touch **sdcard** to list volumes on the On-device Storage or **internal** to list volumes on internal storage.
3. Touch **OK**. The **List of EFS Volumes** dialog box appears with all the volumes of the selected storage location.
4. Touch **OK**.

Unmounting a Volume

1. Touch **Unmount Volume**.
2. Touch **sdcard** to list the mounted volumes on the On-device Storage or **internal** to list the mounted volumes on internal storage.
3. Touch **OK**.
4. Select the volume to un-mount.
5. Touch **OK**.

Deleting a Volume

1. If the encrypted volume is mounted, unmount it.
2. Touch **Delete Volume**.
3. Touch **sdcard** to list the unmounted volumes on the On-device Storage or **internal** to list the unmounted volumes on internal storage.
4. Select the volume to delete.
5. Touch **OK**.

Creating an EFS File

When creating an encrypted volume, the parameter information can be imported from a file instead of entering manually.

1. On a host computer, create a text file.
2. In the text file enter the following:

   <Volume Name> <Volume Storage Type> <Key Name> <Mount Path> <Auto Mount> <Volume size>

where:

<Volume Name> = name of the volume

<Volume Storage Type> = storage location. Options: internal or sdcard.

<Key Name> = name of the key to use when creating the volume.

<Mount Path> = path where the volume will be located.

<Auto Mount> = Options: 1 = yes, 0 = no.

<Volume size> = size of the volume in Megabytes.

Example:

MyVolume sdcard key1 /mnt/sdcard/efsfolder 1 1

1. Save the text file as *efsfile*.

Off-line Extraction Tool

The Secure Storage feature allows for the usage of an encrypted file system. The off-line extraction tool allows encrypted file systems to be used on an Ubuntu version number 10.04LTS desktop. The off-line extraction tool is a shell script used to create, mount and unmount an encrypted file system used with the Secure Storage feature.

Connect the device to the host computer.

Usage

On a Ubuntu desktop, at a terminal prompt, type: `offline_extraction.sh`.

The following Main Menu appears:

```
[ Offline-extraction tool ]
1) Create an image
2) Mount an existing EFS image
3) Unmount final mount location, device mapper and loop device
4) Quit
Please, choose one from the list and press ENTER:
```

Creating an Image

1. From the Main Menu, select item **1**. The following appears:

   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>

   Please enter encryption key (64-bytes hex value):

   Please enter the EFS image size (in MB): <volume size in MB>

Please enter EFS image filesystem type (e.g. ext4, vfat...): ext4

DONE - OK

2. The utility first prompts for the name of the volume to create. Any ASCII string that meets standard Linux file naming rules is valid. Enter the image name and then press **Enter**.
3. The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.
4. The utility then prompts for the image size. Enter the size of the volume in MB. A number must be entered without the units. It is understood that MB. A value of 2000, is 2 GB. Note that 4 GB is the largest volume that is supported on the device.
5. The utility lastly prompts for the filesystem type. Enter ext4 and then press **Enter**.

   The utility then creates the volume in the current working directory.

   The utility then finishes the creation process and then prompts to whether the volume should be mounted.

   Press [1] if you want to mount or press [2] if you want to exit
6. Press **1** will prompt for the mount point. For example, /mnt is prompted. Press **Enter** to mount the encrypted volume at the selected point. After mounting, an option to return to the Main Menu or Exit is provided.

   Press **2** to exit the utility without mounting.
7. If the volume is mounted on the desktop, then that volume can be provisioned with files for deployment.
8. Unmounted volumes can then be copied to the device and subsequently mounted using the Secure Storage Administrator by providing the encryption key used.

Mounting an Image

1. From the Main Menu, select item **2**. The following appears:

   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>

   Please enter encryption key (64-bytes hex value):

   Please enter mount path (e.g. /mnt): <existing mount point>

   DONE - OK
2. Enter the name of the volume and then press **Enter**.
3. The utility then prompts for the encryption key. This is a 64 byte hexadecimal value. Enter a string of 64 hexadecimal digits and then press **Enter**.
4. Enter the mount point where to connect the volume into the file system and then press **Enter**. The example of /mnt is provided.

Unmounting an Image

1. From the Main Menu, select item **3**. The following appears:

   Please enter EFS file name (e.g. /tmp/1.efsmot): <volume name>

DONE - OK

2. Enter the name of the volume to unmount.
3. Press **Enter**.

CHAPTER 9 DATAWEDGE

DataWedge Configuration

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

Scanning can be performed using the imager.

Using the Imager

To capture bar code data:

1. Ensure that an application is open on the MC18 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 key. The red aiming dot turns on to assist in aiming. Ensure that the aiming dot is over the bar code. The Data Capture LED lights red to indicate that data capture is in process.
4. The Data Capture LED lights green, a beep sounds and theMC18 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 visible and hidden 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** - disables scanning when the Launcher is in foreground.
  - **DWDemo** - provides support for the DWDemo application.
- Hidden profiles (not shown to the device):
  - **RD Client** - provides support for MSP.
  - **MSP Agent** - provides support for MSP.
  - **MspUserAttribute** - provides support for MSP.
  - **Camera** - disables scanning when the default camera application is in foreground.
  - **RhoElements** - disables scanning when RhoElements is in foreground.

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 bar code 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 bar code scanner contained in, or attached to the device. **DataWedge** contains base plug-ins for these input devices.

- **Bar Code Scanner Input Plug-in** – The Bar Code Scanner Input Plug-in is responsible for reading data from the integrated bar code scanner and supports different types of bar code readers including laser, imager and internal camera. Raw data read from the bar code scanner can be processed or formatted using Process Plug-ins as required. **DataWedge** has built-in feedback functionality for the bar code 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.

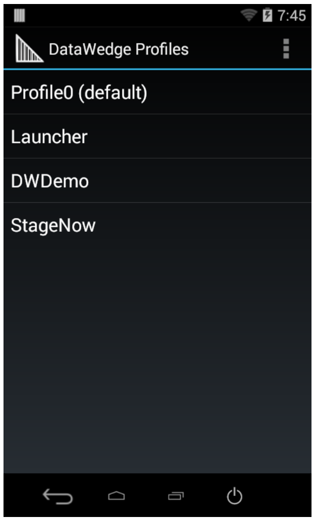
- **Keystroke Output Plug-in** – The Keystroke Output Plug-in collects and sends data received from the Input Plug-in to the foreground applications by emulating keystrokes.
- **Intent Output Plug-in** – The Intent Output Plug-in collects and sends data received from the Input Plug-ins to foreground 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, touch ⊞ > **DataWedge**. By default, three profiles appear:

- Profile0
- Launcher
- DWDemo.

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



DataWedge Profiles

Profile0 (default)

Launcher

DWDemo

StageNow

Figure 9-1 *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.

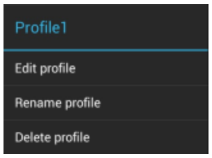


Figure 9-2 *Profile Context Menu*

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.

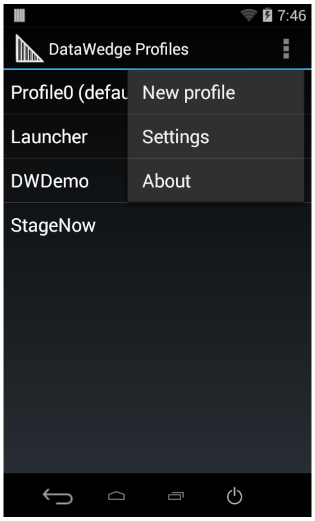


Figure 9-3 *DataWedge Options Menu*

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

Disabling DataWedge

1. 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

1. 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).

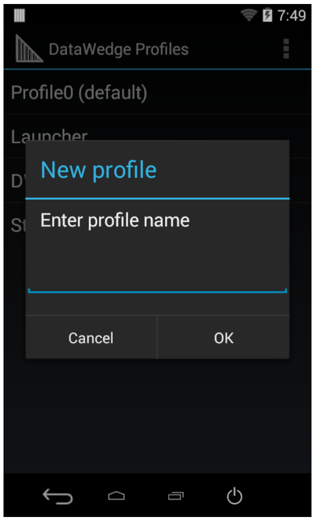


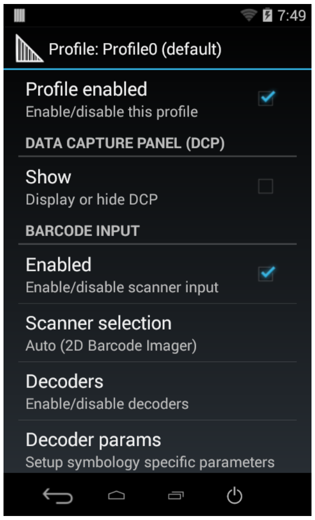
Figure 9-4 *New Profile Name Dialog Box*

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.



Profile: Profile0 (default)

Profile enabled ☑
Enable/disable this profile

DATA CAPTURE PANEL (DCP)

Show ☐
Display or hide DCP

BARCODE INPUT

Enabled ☑
Enable/disable scanner input

Scanner selection
Auto (2D Barcode Imager)

Decoders
Enable/disable decoders

Decoder params
Setup symbology specific parameters

Figure 9-5 *Profile Configuration Screen*

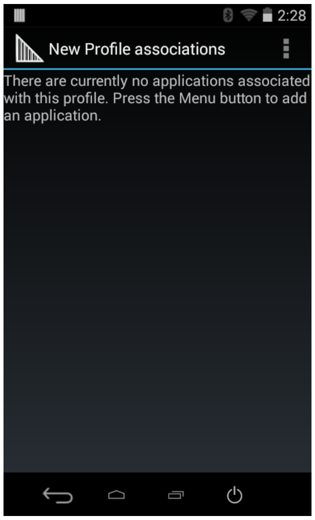
The configuration screen lists the following sections:

- Profile enabled
- Applications
- Data Capture panel (DCP)
- Barcode 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.



There are currently no applications associated with this profile. Press the Menu button to add an application.

Figure 9-6 *Associated Apps Screen*

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

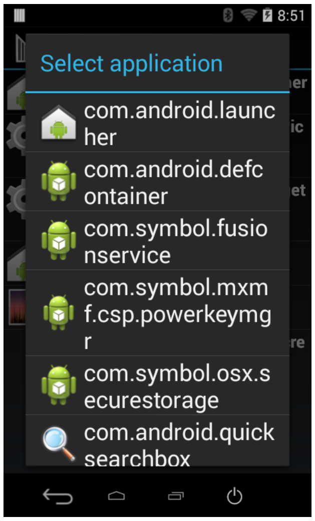


Figure 9-7 *Select Application Menu*

4. In the **Select application** screen, select the desired application from the list.

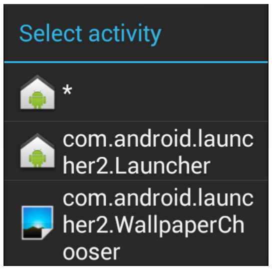
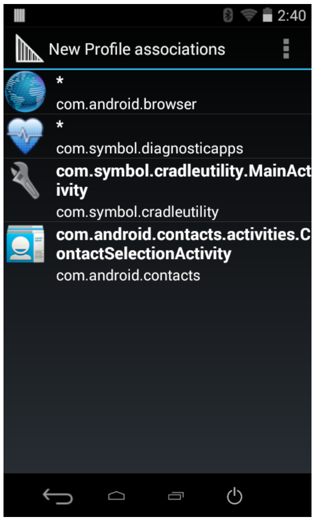

Select activity
*
com.android.launcher2.Launcher
com.android.launcher2.WallpaperChooser

Figure 9-8 *Select Activity Menu*

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 ↩.



2:40

New Profile associations

*
com.android.browser

*
com.symbol.diagnosticapps

com.symbol.cradleutility.MainActivity
com.symbol.cradleutility

com.android.contacts.activities.ContactSelectionActivity
com.android.contacts

Figure 9-9 *Selected Application/Activity*

Data Capture Panel

The Data Capture panel (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.

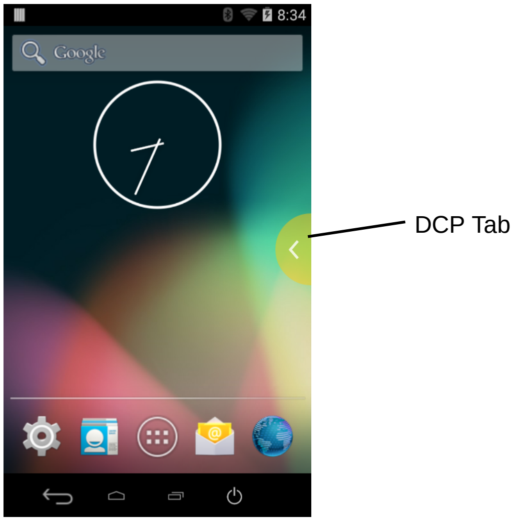


Figure 9-10 *Minimized Data Capture Panel*

Drag the DCP tab horizontally to maximized overlay. Drag the DCP tab vertically to reposition the tab.

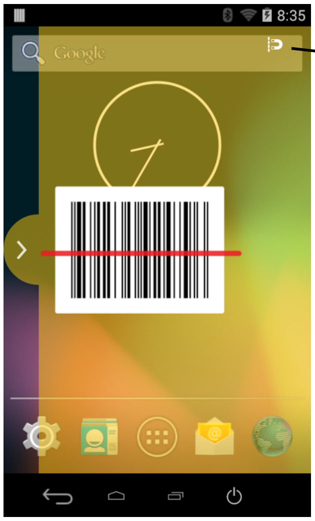
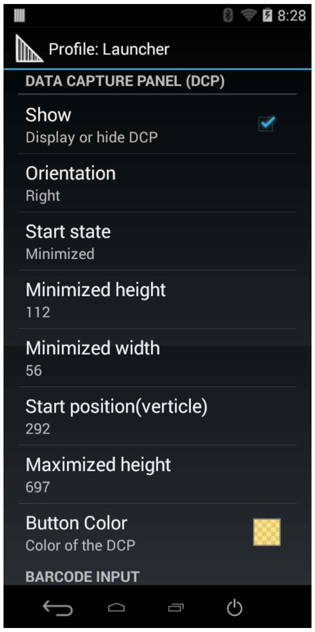


Figure 9-11 *Maximized DCP*

Touch the Magnet icon to change the orientation of the overlay to opposite side of the screen.

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.


8:28

Profile: Launcher

DATA CAPTURE PANEL (DCP)

Show
Display or hide DCP ☑

Orientation
Right

Start state
Minimized

Minimized height
112

Minimized width
56

Start position(verticle)
292

Maximized height
697

Button Color
Color of the DCP

BARCODE INPUT

Figure 9-12 *Data Capture Panel Settings*

- **Orientation** - Indicates whether the DCP displays on the right hand or left hand side of the screen. Options: **Left** (default) or **Right**.
- **Start state** - Indicates whether the DCP should be started in maximized or minimized state. Options: **Minimized** (default) or **Maximized**.
- **Minimized height** - Indicates the height of the DCP when in the minimized state (default - 112).
- **Minimized width** - Indicates the width of the DCP when in the minimized state (default - 56).

- **Start position (vertical)** - Indicates the distance from top of the device screen to the DCP (default - 292).
- **Maximized height** - Indicates the height of DCP when in maximized state (default - 697).
- **Button Color** - Use to change the color and transparency of the DCP overlap. Touch to open the color picker window.

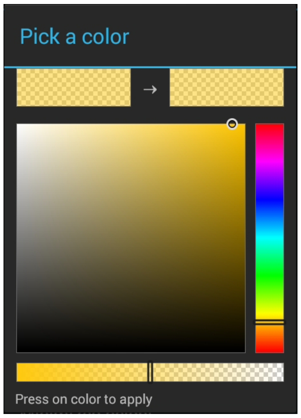


Figure 9-13 *Color Picker*

✓ ***NOTE*** The DCP overlay does not appear if the scanner is disabled in the profile even though the show option is set.

Bar Code Input

Use the **Bar Code Input** options to configure the Bar Code 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 bar code data capture when the profile is active.

- **Auto** - The software automatically selects the 2D Imager.
- **2D Imager** - Scanning is performed using the 2D Imager.

Decoders

Configures which bar code 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.

Touch ↩ to return to the previous screen.

UPC-A*	UPC-E0*	EAN-13*
EAN-8*	Code 128*	Code 39*
Interleaved 2 of 5	GS1 DataBar*	GS1 DataBar Limited
GS1 DataBar Expanded*	Datamatrix*	QR Code*
PDF417*	Composite AB	Composite C
MicroQR	Aztec*	Maxicode*
MicroPDF	US Postnet	US Planet
UK Postal	Japanese Postal	Australian Postal
Canadian Postal	Dutch Postal	US4state
US4state FICS	Codabar*	MSI
Code 93	Trioptic 39	Discrete 2 of 5
Chinese 2 of 5	Korean 3 of 5	Code 11
TLC 39	MAIL MARK	HAN XIN
Matrix 2 of 5	UPC-E1	

Decoder Params

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

- **UPCA**
  - **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).
  - **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.
- **UPCE0**
  - **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).
  - **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 Sys Char** - Transmit System Character only.
    - **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA).

        - **Preamble None** - Transmit no preamble (default).
    - **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).

- **Code128**
    - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 9-16* for more information.
    - **Length2**- Use to set decode lengths (default - 55). See *Decode Lengths on page 9-16* for more information.
    - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
    - **Enable Plain Code 128** - Flag to enable other 128 sub types (besides GS1-128 and ISBT-128).
    - **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).
    - **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.
    - **Check ISBT Table** - The ISBT specification includes a table that lists several types of ISBT bar codes 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).
    - **Security Level** - The scanner offers four levels of decode security for Code 128 bar codes. Select increasing levels of security for decreasing levels of bar code 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” bar codes.
        - **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 bar codes. 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 bar codes.
    - **Code128 Reduced Quiet Zone** - Enables decoding of margin-less Code 128 bar codes.
    - **Ignore Code128 FCN4** - When enabled, and a Code 128 bar code 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.

- **Code39**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 9-16* for more information.
  - **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 9-16* for more information.
  - **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).
  - **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).
  - **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),
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
  - **Convert Code39 To Code32** - Code 32 is a variant of Code 39 used by the Italian pharmaceutical industry. Scan the appropriate bar code below to enable or disable converting Code 39 to Code 32 (default - disabled).
  - **Report Code32 Prefix** - Scan the appropriate bar code to enable or disable adding the prefix character “A” to all Code 32 bar codes (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” bar codes.
    - **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 bar codes. 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 bar codes.
  - **Code39 Reduced Quiet Zone** - Enables decoding of margin-less Code 39 bar codes.
- **Interleaved 2 of 5**
  - **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 9-16* for more information.
  - **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **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.
  - **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).
  - **Convert ITF-14 To EAN13** - Convert 14-character Interleaved 2 of 5 bar codes to EAN-13, and transmit as EAN-13. The Interleaved 2 of 5 bar code 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 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).
  - **I2of5 Reduced Quiet Zone** - Enables decoding of margin-less I2of5 bar codes.
- **GS1 DataBar Limited**
  - **GS1 Limited Security Level** -
    - **Security Level 0** - This setting allows the scanner to operate in its most aggressive state, while providing sufficient security in decoding most “in-spec” bar codes.
    - **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 bar codes. 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 bar codes.
- **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).
- **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).
- **Codabar**
  - **Length1** - Use to set decode lengths (default - 6). See *Decode Lengths on page 9-16* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **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).
  - **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).
- **MSI**
  - **Length 1** - Use to set decode lengths (default - 4). See *Decode Lengths on page 9-16* for more information.
  - **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **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.
  - **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).

- **Code93**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 9-16* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - disabled).
- **Discrete 2 of 5**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 9-16* for more information.
  - **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code 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 on page 9-16* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code twice before accepting data. A check in the checkbox indicates that redundancy is enabled (default - enabled).
  - **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 bar code.
    - **No Check Digit** - Do not verify check digit.
    - **1 Check Digit** - Bar code contains one check digit (default).
    - **2 Check Digits** - Bar code contains two check digits.
  - **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).
- **HAN XIN**
  - **HAN XIN Inverse**
    - **Disable** - Disables decoding of HAN XIN inverse bar codes (default).
    - **Enable** - Enables decoding of HAN XIN inverse bar codes.
    - **Auto** - Decodes both HAN XIN regular and inverse bar codes.

- **Matrix 2 of 5**
  - **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 9-16* for more information.
  - **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 9-16* for more information.
  - **Redundancy** - Sets the reader to read the bar code 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).
- **UPCE1**
  - **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).
  - **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 Sys Char** - Transmit System Character only.
    - **Preamble Country and Sys Char** - Transmit System Character and Country Code (“0” for USA).
    - **Preamble None** - Transmit no preamble (default).
  - **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).

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.

- **Security Level** - The scanner offers four levels of decode security for UPC/EAN bar codes. Select higher security levels for lower quality bar codes. 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 bar codes (default).
  - **Level 1** - As bar code quality levels diminish, certain characters become prone to misdecodes before others (i.e., 1, 2, 7, 8). If the scanner is misdecoding poorly printed bar codes, and the misdecodes are limited to these characters, select this security level.
  - **Level 2** - If the scanner is misdecoding poorly printed bar codes, 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 bar codes. 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 bar codes.
- **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 bar code 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 bar code 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 bar code 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 bar code not starting with 378 or 379. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code 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 bar code not starting with 978 or 979. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code 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 bar code 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 bar code is returned.
  - **Supplemental 977** - Enables (auto-discriminate) supplemental for UPC/EAN codes starting with 977. Disables reading of supplementals for another UPC/EAN bar code not starting with 977. Tries to scan the supplemental if it is present. If the supplemental scanning failed, then the main bar code is returned.

- **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).
- **Bookland** - Enable Bookland decoding. A check in the checkbox indicates that the option is enabled.
- **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.
- **Coupon Repost Mode** - Traditional coupon symbols are composed of two bar code: UPC/EAN and Code 128. A new coupon symbol is composed of a single Data Expanded bar code. 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 bar codes: 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.
- **Ean Zero Extended** – 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.
- **Convert DataBar To UPC EAN** - If this is set it converts DataBar bar codes 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.
- **UPC Reduced Quiet Zone** - Enables decoding of margin-less UPC bar codes.

Reader Params

Allows the configuration of parameters specific to the selected bar code reader.

- **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 -15000).
- **Linear Security Level** - Sets the number of times a bar code is read to confirm an accurate decode.
  - **Security Short or Codabar** - Two times read redundancy if short bar code or Codabar.
  - **Security All Twice** - Two times read redundancy for all bar codes (default).
  - **Security Long and Short -** Two times read redundancy for long bar codes, three times for short bar codes.
  - **Security All Thrice** - Three times read redundancy for all bar codes.

- **Picklist** - Allows the imager to decode only the bar code that is directly under the cross-hair/reticle (+) part of the pattern. This feature is useful in applications where multiple bar codes may appear in the field of view during a decode session and only one of them is targeted for decode.
  - **Disable** – Disables Picklist mode. Any bar code within the field of view can be decoded (default).
  - **Hardware Picklist** – Enables Picklist mode so that only the bar code under the projected reticle can be decoded.
  - **Software Picklist** - Enables Picklist mode so that only the bar code in the center of the image is decoded.
- **AIM Type**
  - **Trigger** - The device decodes a bar code on each Scan button press. (default).
  - **Continuous Read** - The device continuously decodes bar codes as long as the Scan button is held down and the previous bar code decoding is complete. This mode is useful when the user wants to perform rapid scanning.
- **Same Symbol Timeout** - Use to prevent the device from decoding the same bar code within a specific time interval (applicable only when Aim Type is set to **Continuous Read**). The user can perform rapid scanning and prevents the user from decoding the same bar code twice. Set this value to an appropriate interval (in milliseconds). A value of 0 indicates no interval is required between two successive reads (default - 500).
- **Different Symbol Timeout** - Use to prevent the device from decoding another bar code within a specific interval (applicable only when aim type is set to **Continuous Read**). The user may want to prevent decoding too quickly and set an interval that the user can aim before scanning the next bar code. A value of 0 indicates no interval is required between two successive reads (default - 500).
- **Illumination mode** - Turns camera illumination on and off. This option is only available when camera is selected in the Barcode input Scanner selection option.
  - **On** - Illumination is on.
  - **Off** - Illumination is off (default).
- **LCD Mode** - Enables or disables LCD mode. LCD mode enhances the ability of the imager to read bar codes from LCD displays such as cellphones.
  - **Disable** - Disables the LCD mode (default).
  - **Enable** - Enables LCD mode.
- **Hardware Engine Low Power Timeout -**
- **Inverse 1D Mode** - This parameter allows the user to select decoding on inverse 1D bar codes.
  - **Disable** - Disables decoding of inverse 1D bar codes (default).
  - **Enable** - Enables decoding of only inverse 1D bar codes.
  - **Auto** - Allows decoding of both twice positive and inverse 1D bar codes.
- **1D Quiet Zone Level** - Sets the effort the decoder performs to decode margin-less bar codes. Applies to any symbology with margin-less bar code decode enabled parameter. Since higher margin-less levels will increase the mis-decode risk and decoding time, we strongly recommend the user only enable the symbologies which needs to choose higher margin-less level, and leave all other symbologies at low default level 1.
- **Poor Quality Decode Effort** - Enable poor quality bar code decoding enhancement feature.

Scan Params

Allows the configuration of Code ID and decode feedback options.

- **Code ID Type** - A Code ID character identifies the code type of a scanned bar code. 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** - A standards based three character prefix.
  - **Code ID Type Symbol** - A Symbol defined single character prefix.

✓ ***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.

- **Volume Type** - Set the good decode beep to a system or other sound. This allows for independent control of the good beep volume.
  - **Ringer and Notifications** - Set the good decode beep to the ringer and notifications sound.(default)
  - **Music and media** - Set the good decode beep to the music and media sound
  - **Alarms** - Set the good decode beep to the alarm sound
- **Decode Audio Feedback** - Select an audio tone to sound upon a good decode.
- **Decode Haptic Feedback** - Enable the device to vibrate upon a good decode (default - enabled).
- **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.)
- **Decoding LED Notification** - Enable the device to light the red Data Capture LED when data capture is in progress. (default - disabled).

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 bar code 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 bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Line feed** - Line feed character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
  - **Carriage return** - Carriage return character code in a bar code is processed. When DataWedge detects this character code in a bar code, move the focus to the next field.
- **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 on page 9-26* 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, http://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
- **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 on page 9-26* 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.category.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 bar code.
- String DATA_STRING_TAG = “com.symbol.emdk.datawedge.data_string”;
  - String contains the output data as a String. In the case of concatenated bar codes, the decode data is concatenated and sent out as a single string.
- String DECODE_DATA_TAG = “com.symbol.emdk.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 bar code symbologies that support concatenation e.g. Codabar, Code128, MicroPDF, etc., the decoded data is stored in multiple byte arrays (one byte array per bar code). 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: http://www.zebra.com/support.

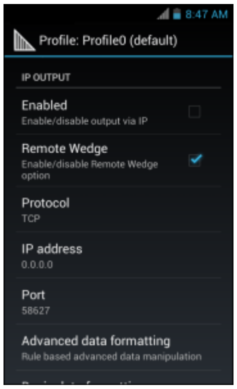
IP Output allows DataWedge to send captured data to a host computer via a network connection. Captured data can be sent over an IP network to a specified IP address and port using either TCP or UDP transport protocols.

- **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).
- **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 on page 9-26* 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**.



8:47 AM

Profile: Profile0 (default)

IP OUTPUT

Enabled ☐
Enable/disable output via IP

Remote Wedge ☑
Enable/disable Remote Wedge option

Protocol
TCP

IP address
0.0.0.0

Port
58627

Advanced data formatting
Rule based advanced data manipulation

Figure 9-14 *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:

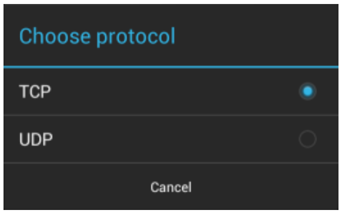
1. In **IP Output**, touch **Enabled**.

   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).

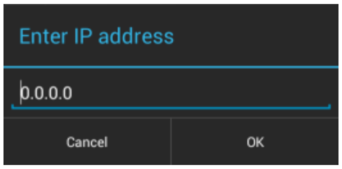


TCP ●

UDP ○

Figure 9-15 *Protocol Selection*

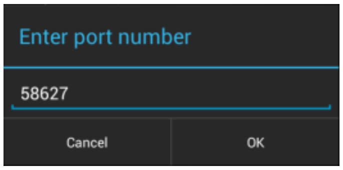
5. Touch **IP Address**.
6. In the **Enter IP Address** dialog box, enter the IP address of host computer to send data to.



0.0.0.0

Figure 9-16 *IP Address Entry*

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



58627

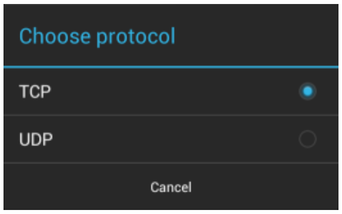
Figure 9-17 *Port Number Entry*

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



Choose protocol

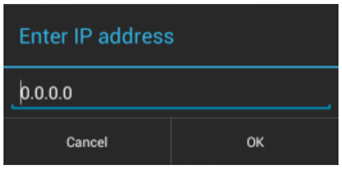
TCP ●

UDP ○

Figure 9-18 *Protocol Selection*

6. Touch **IP Address**.

7. In the **Enter IP address** dialog box, enter the IP address of host computer to send data to.



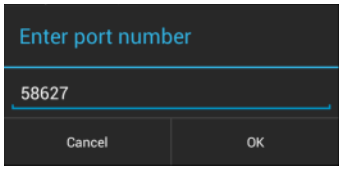
Enter IP address

0.0.0.0

Figure 9-19 *IP Address Entry*

8. Touch **Port**.

9. In the **Enter port number** dialog box, enter the port number that the host computer application is listening on.



Enter port number

58627

Figure 9-20 *Port Number Entry*

10. 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

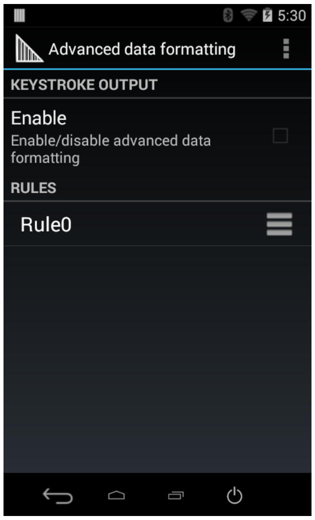
The ADF plug-in applies rules (actions to be performed based on defined criteria) to the data received via an input plug-in before sending it to the output plug-in.

- 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. Touch ⊞ > .
2. Touch a DataWedge profile.
3. In **Keystroke Output**, touch **Advanced data formatting**.



5:30

Advanced data formatting ⋮

KEYSTROKE OUTPUT

Enable
Enable/disable advanced data formatting □

RULES

Rule0

Figure 9-21 *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 **Done**.
6. Touch **OK**.

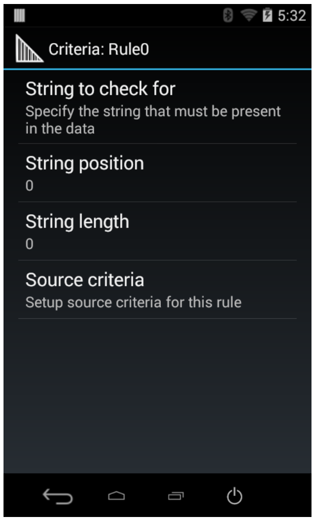
Deleting a Rule

1. Touch and hold on a rule until the context menu appears.
2. Touch **Delete** 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.

Defining Criteria

1. Touch **Criteria**.



Criteria: Rule0

String to check for
Specify the string that must be present in the data

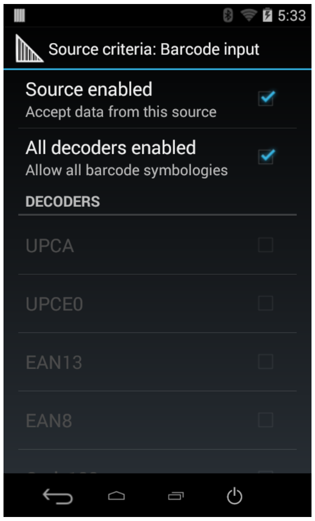
String position
0

String length
0

Source criteria
Setup source criteria for this rule

Figure 9-22 *Criteria Screen*

2. Touch **String to check for** option to specify the string that must be present in the data.
3. In the **Enter the string to check for** dialog box, enter the string.
4. Touch **OK**.
5. Touch **String position** option to specify the position of the string specified in the **String to check for** option. The ADF rule is only applied if the specific string in **String to check** for is found at the specified **String position** location (zero for the start of the string).
6. Touch the **+** or **-** to change the value.
7. Touch **OK**.
8. Touch **String length option** to specify a length for the received data. The ADF rule only applies to the bar code data with that specified length.
9. Touch the **+** or **-** to change the value.
10. Touch **OK**.
11. Touch **Source criteria** option to associate an input device to an ADF rule. The ADF rule only applies to data received from associated input devices.
12. Touch **Barcode input**.
13. Touch the **Source enabled** checkbox to accept data from this source.



5:33

Source criteria: Barcode input

Source enabled ☑
Accept data from this source

All decoders enabled ☑
Allow all barcode symbologies

DECODERS

UPCA □

UPCE0 □

EAN13 □

EAN8 □

Figure 9-23 *Barcode Input Screen*

14. For **Barcode inputs**, touch the **All decoders enabled** checkbox to select all bar code symbologies. Deselect the **All decoders enabled** checkbox to individually select the symbologies.

15. Touch ↩ until the **Rule** screen appears.

16. If required, repeat steps to create another rule.

17. Touch ↩ until the Rule screen appears.

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 *Table 9-1 on page 9-30* 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** 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 9-1 *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 9-1 *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 bar code with the following criteria:

- Code 39 bar code.
- 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. Touch ⊞.
2. Touch **DataWedge**.
3. Touch **Profile0**.
4. Under **Keystroke Output**, touch **Advanced data formatting**.
5. Touch **Enable**.
6. Touch **Rule0**.
7. Touch **Criteria**.

8. Touch **String to check for**.
9. In the **Enter the string to check for** text box, enter `129` and then touch **OK**.
10. Touch **String position**.
11. Change the value to `0`.
12. Touch **OK**.
13. Touch **String length**.
14. Change value to `12`.
15. Touch **OK**.
16. Touch **Source criteria**.
17. Touch **Barcode input**.
18. Touch **All decoders enabled** to disable all decoders.
19. Touch **Code 39**.
20. Touch ↩ three times.
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. Touch ↩ three times.
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 ↩ three times.
38. Touch ⋮ .
39. Touch **New action**.

40. Select **Send char**.

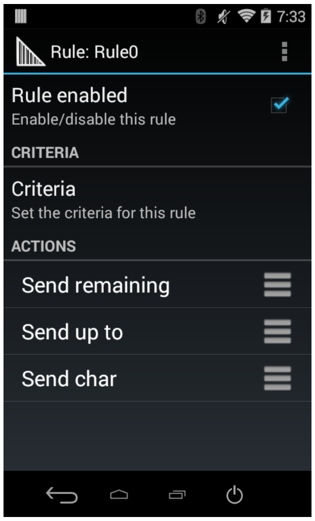
41. Touch **Send char** rule.

42. Touch **Character code**.

43. In the **Enter character code** text box, enter 32.

44. Touch **OK**.

45. Touch ↩.



7:33

Rule: Rule0

Rule enabled ☑
Enable/disable this rule

CRITERIA

Criteria
Set the criteria for this rule

ACTIONS

Send remaining

Send up to

Send char

Figure 9-24 *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 bar code.

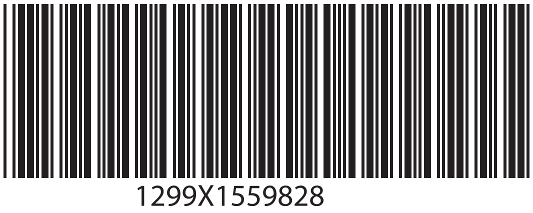


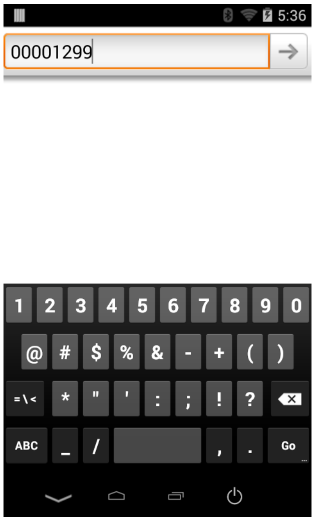
Figure 9-25 *Sample Bar Code*

48. Press and hold the scan key.

    The red laser aiming pattern turns on to assist in aiming. Ensure that the bar code 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 bar code was decoded successfully.The LED lights green and a beep sounds, by default, to indicate the bar code was decoded successfully. The formatted data 000129X<space>appears in the text field.

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



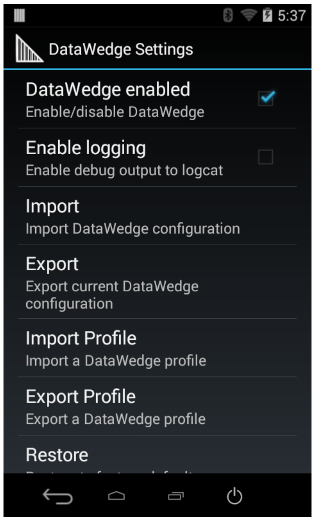
5:36

00001299

Figure 9-26 *Formatted Data*

DataWedge Settings

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



5:37

DataWedge Settings

DataWedge enabled ☑
Enable/disable DataWedge

Enable logging □
Enable debug output to logcat

Import
Import DataWedge configuration

Export
Export current DataWedge configuration

Import Profile
Import a DataWedge profile

Export Profile
Export a DataWedge profile

Restore

Figure 9-27 *DataWedge Settings Window*

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

Importing a Configuration File

1. Copy the configuration file to the On Device Storage **`/Android/data/com.symbol.datawedge`** folder.
2. Touch ⊞ > ▥ .
3. Touch ⋮ .
4. Touch **Settings**.
5. Touch **Import**.
6. Touch filename to import.
7. Touch **Import**. The configuration file (*datawedge.db*) is imported and replaces the current configuration.

Exporting a Configuration File

1. Touch ⊞ > ▥ .
2. Touch ⋮ .
3. Touch **Settings**.
4. Touch **Export**.
5. In the **Export to** dialog box, select the location to save the file.
6. 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`** folder.
2. Touch ⊞ > ▥ .
3. Touch ⋮ .
4. Touch **Settings**.
5. Touch **Import Profile**.
6. Touch the profile file to import.
7. 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 ⋮ .
3. Touch **Settings**.
4. Touch **Export Profile**.

5. Touch the profile to export.
6. Touch **Export**.

   The profile file (*dwprofile_x.db*, where x = name of the profile) is saved to the root of the MC18 On-device Storage.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

1. Touch ⠿ > ◢.
2. Touch ⋮ .
3. Touch **Settings**.
4. Touch **Restore**.
5. 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 MSP. DataWedge monitors the */enterprise/device/settings/datawedge/autoimport* folder for the DataWedge configuration file (*datawedge.db*) or a profile file (*dwprofile_x.db*). When DataWedge launches it checks the folder. 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.

While DataWedge is running it receives a notification from the system that a file has been placed into the */enterprise/device/settings/datawedge/autoimport* folder. When this occurs, DataWedge imports this new configuration or profile, replacing the existing one and delete the file. 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.

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.

Soft Scan Feature

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.

The structure of the broadcast intent that resolves to the soft scan is:

action: “com.symbol.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”

extras: This is a String name/value pair that contains trigger state details.

name: “com.symbol.emdk.datawedge.api.EXTRA_PARAMETER”

value: “START_SCANNING” or “STOP_SCANNING” or “TOGGLE_SCANNING”

Sample

```
Intent sendIntent = new Intent();

sendIntent.setAction(“com.symbol.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”);

sendIntent.putExtra(“com.symbol.emdk.datawedge.api.EXTRA_PARAMETER”, “TOGGLE_SCANNING”);

sendBroadcast(sendIntent);
```

CHAPTER 10 APPLICATION DEPLOYMENT

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

1. Copy the certificate from the host computer to the root of the On-device Storage. See *Chapter 7, USB Communication* for information about connecting the device to a host computer and copying files.
2. Touch ⚙.
3. Touch 🔒 **Security**.
4. Touch **Install from On-device Storage**.
5. Navigate to the location of the certificate file.
6. Touch the filename of the certificate to install. Only the names of certificates not already installed display.

7. If prompted, enter the certificate’s password and touch **OK**.
8. Enter a name for the certificate and touch **OK**. If a password has not been set for the credential storage, enter a password for it twice and then touch **OK**.

   The certificate can now be used when connecting to a secure network. For security, the certificate is deleted from the On-device Storage.

Development Tools

Android development tools are available at http://developer.android.com.

To start developing applications for the device, download the development SDK and the Eclipse IDE. 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 VM (a non-Java virtual machine). Once the Java code is compiled cleanly, the developer tools make sure the application is packaged properly, including the AndroidManifest.xml file.

The development SDK is distributed as a ZIP file that unpacks to a directory on the host computer hard drive. The SDK includes:

- android.jar
  - Java archive file containing all of the development SDK classes necessary to build an application.
- documention.html and docs directory
  - The SDK documentation is provided locally and on the Web. It's largely in the form of JavaDocs, making it easy to navigate the many packages in the SDK. The documentation also includes a high-level Development Guide and links to the broader community.
- Samples directory
  - The samples subdirectory contains full source code for a variety of applications, including ApiDemo, which exercises many APIs. The sample application is a great place to explore when starting application development.
- Tools directory
  - Contains all of the command-line tools to build applications. The most commonly employed and useful tool is the adb utility.
- usb_driver
  - Directory containing the necessary drivers to connect the development environment to an enabled device. These files are only required for developers using the Windows platform.

Open the Developer options screen to set development related settings.

On the Home screen, touch ⚙ > { } **Developer options**. Slide the switch to the **ON** position to enable developer options.

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 http://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 http://www.zebra.com/support. Download the ADB and USB Driver Setup package. Following the instructions with the package to install the ADB and USB drivers for Windows and Linux.

Application Installation

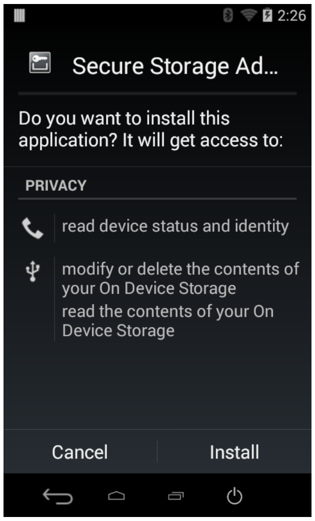
After an application is developed, install the application onto the device using one of the following methods:

- USB connection, see *Installing Applications Using the USB Connection on page 10-3*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 10-4*.
- 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 its On-device Storage, 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 *Chapter 7, USB Communication*.
2. On the host computer, copy the application *.apk* file from the host computer to the device.
3. Disconnect the device from the host computer. See *Chapter 7, USB Communication*.
4. On the device, touch ⊞.
5. Touch 📁 to view files on the On-device Storage or Internal Storage.
6. Locate the application *.apk* file.
7. Touch the application file to begin the installation process.
8. To confirm installation and accept what the application affects, touch **Install** otherwise touch **Cancel**.



2:26

Secure Storage Ad...

Do you want to install this application? It will get access to:

PRIVACY

read device status and identity

modify or delete the contents of your On Device Storage
read the contents of your On Device Storage

Cancel Install

Figure 10-1 *Accept Installation Screen*

9. Touch **Open** to open the application or **Close** 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 On-device Storage, 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 on page 10-2*.

1. Connect the device to a host computer using USB. See *Chapter 7, USB Communication*.
2. Touch ⚙.
3. Touch { } **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:
8. adb install <application>
9. where: <application> = the path and filename of the apk file.
10. Disconnect the device from the host computer. See *Chapter 7, USB Communication*.

Uninstalling an Application

To uninstall an application:

1. Touch ⚙.
2. Touch **Apps**.
3. Swipe left or right until the **Downloaded** screen displays.

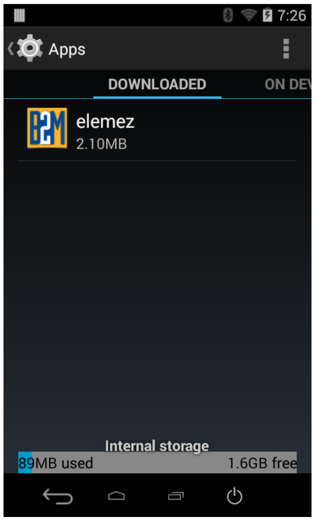


Figure 10-2 *Downloaded Screen*

4. Touch the application to uninstall.

5. Touch **Uninstall**.

6. Touch **OK** to confirm.

System Update

System Update packages can contain either partial or complete updates for the operating system. We distribute the System Update packages on the Support Central web site.

1. Download the system update package:

   a. Go to the Support Central web site, http://www.zebra.com/support.

   b. Download the appropriate System Update package to a host computer.

2. Copy the 18N0KXXRU0000001.zip file to the root directory of On Device Storage. See *Chapter 7, USB Communication* for more information.

3. Remove the Programming cable from the device.

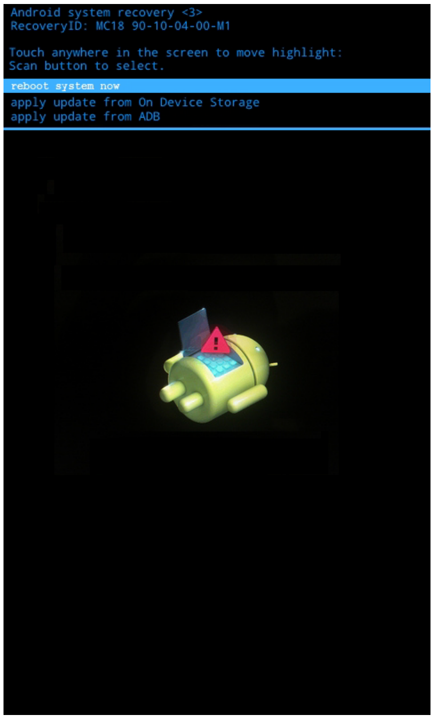
4. Press and hold the soft power button ⏻ until the menu appears.

5. Touch **Power Off**.

6. Touch **OK**.

7. Press and hold the Scan key.

8. When the System Recovery screen appears, release the button.



```
Android system recovery <3>
RecoveryID: MC18 90-10-04-00-M1

Touch anywhere in the screen to move highlight:
Scan button to select.
reboot system now
apply update from On Device Storage
apply update from ADB
```

Figure 10-3 *System Recovery Screen*

9. Tap the display until **apply update from On Device Storage** is highlighted.
10. Press the Scan key.
11. Tap the display until the 18N0KXXRU0000001.zip file is highlighted.
12. Press the Scan key. The System Update installs and then the MC18 resets.

Storage

The device contains four types of file storage:

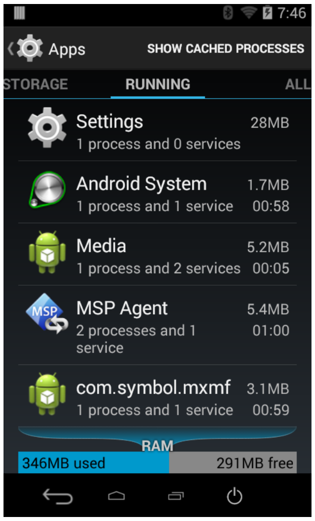
- Random Access Memory (RAM)
- On-device Storage
- Internal storage
- Enterprise folder.

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.

To view the amount of free and used memory, touch ⚙ > **Apps**. Swipe the screen until the **Running** screen appears.



Settings 28MB
1 process and 0 services

Android System 1.7MB
1 process and 1 service 00:58

Media 5.2MB
1 process and 2 services 00:05

MSP Agent 5.4MB
2 processes and 1 service 01:00

com.symbol.mxmf 3.1MB
1 process and 1 service 00:59

RAM
346MB used 291MB free

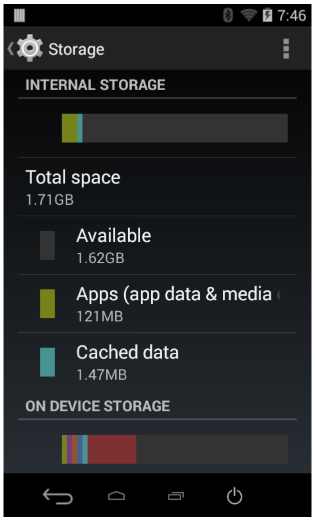
Figure 10-4 *Running Screen*

The bar at the bottom of the screen displays the amount of used and free RAM.

Internal Storage

The MC18 has internal storage. The internal storage content can be viewed and files copied to and from when the MC18 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, touch ⚙ > ☰ **Storage**.



INTERNAL STORAGE

Total space
1.71GB

Available
1.62GB

Apps (app data & media
121MB

Cached data
1.47MB

ON DEVICE STORAGE

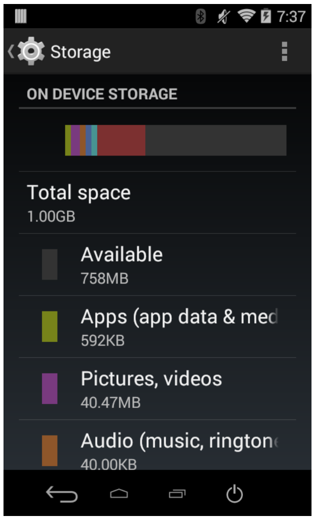
Figure 10-5 *Internal Storage Screen*

- Internal Storage
  - **Total space** - Displays the total amount of space on internal storage (approximately 1.0 GB).
  - **Available** - Displays the available space on internal storage.
  - **Apps** - Displays the available space used for applications and media content on internal storage.
  - **Cached data** - Displays the amount of cached data on internal storage.

On Device Storage

The MC18 has On Device Storage. The On Device Storage content can be viewed and files copied to and from when the MC18 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 On Device Storage, touch ⚙ > ☰ **Storage**.



7:37

Storage

ON DEVICE STORAGE

Total space
1.00GB

Available
758MB

Apps (app data & med
592KB

Pictures, videos
40.47MB

Audio (music, rington
40.00KB

Figure 10-6 *On Device Storage Screen*

- On Device Storage
  - **Total space** - Displays the total amount of space on On Device Storage (approximately 1.0 GB).
  - **Available** - Displays the available space on On Device Storage.
  - **Apps** - Displays the available space used for applications and media content on On Device Storage.
  - **Pictures, videos** - Displays the amount of photos and videos on On Device Storage.
  - **Audio** - Displays the amount of audio files on On Device Storage.
  - **Downloads** - Displays the amount of downloaded data on On Device Storage.
  - **Cached data** - Displays the amount of cached data on On Device Storage.
  - **Misc.** - Displays the amount of miscellaneous files on On Device Storage.

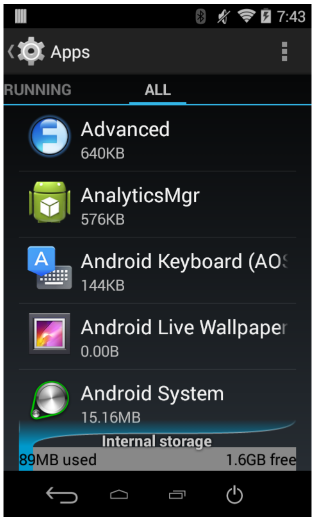
Enterprise Folder

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.

Application Management

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

From the Home screen touch ⚙ > **Apps**.



Advanced
640KB

AnalyticsMgr
576KB

Android Keyboard (AO
144KB

Android Live Wallpaper
0.00B

Android System
15.16MB

Internal storage
89MB used 1.6GB free

Figure 10-7 *Apps Screen*

The **Apps** screen has four tabs, with lists of applications and their components in each. At the bottom of each tab is a graph of the memory used by the items in the list and amount of free memory.

Touch an application, process, or service in a list to open a screen with details about it and, depending on the item, to change its settings, stop it or uninstall it

- Slide the screen to the **Downloaded** tab to view the applications downloaded to the device.
- Slide the screen to the **On Device Storage** tab to view the applications installed on On-device Storage. A check mark indicates that the application is installed on On-device Storage. Unchecked items are installed in internal storage and can be moved to On-device Storage.
- Touch the **Running** tab to view the applications and their processes and services that are running or cached
- Slide the screen to the **All** tab to view all the applications installed on the device, including factory installed applications and downloaded applications.

When on the **Downloaded**, **All**, or **On Device Storage** tab, press ⋮ > **Sort by size** to switch the order of the list.

Viewing Application Details

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

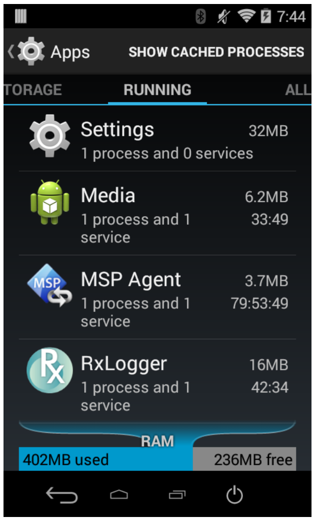
- Touch **Force stop** to stop an application.
- Touch **Uninstall** to remove the application and all of its data and settings from the device. See *Uninstalling an Application on page 10-4* for information about uninstalling applications.
- Touch **Clear data** to delete an application’s settings and associated data.
- Touch **Move to USB storage** or **Move to On Device Storage** to change where some applications are stored.
- Cache If the application stores data in a temporary area, lists how much information is stored, and includes a button for clearing it.
- **Launch by default** clears If you have configured an application to launch certain file types by default, you can clear that setting here.

- **Permissions** lists the areas on the device that the application has access to.

Stopping an Application

To monitor how much RAM running applications and cached processes are using and if necessary, stop them.

1. Touch ⚙ > **Apps**.
2. Swipe the screen to display the **Running** tab.
3. Touch **Show cached processes** or **Show running services** to switch back and forth. The **Running** tab lists the applications, processes, and services that are currently running or that have cached processes and how much RAM they are using.



Settings 32MB
1 process and 0 services

Media 6.2MB
1 process and 1 service 33:49

MSP Agent 3.7MB
1 process and 1 service 79:53:49

RxLogger 16MB
1 process and 1 service 42:34

RAM
402MB used
236MB free

Figure 10-8 *Running Applications*

4. The graph at the bottom of the screen displays the total RAM in use and the amount free. Touch an application, process, or service.

✓ ***NOTE*** Stopping an application or operating system processes and services disables one or more dependent functions on the device. The device may need to be reset to restore full functionality.

5. Touch **Stop**.

Changing Application Location

Some applications are designed to be stored on On-device Storage, rather than in internal storage. Others are designed so you can change where they are stored. You may find it helpful to move large applications off of your internal storage, to make more room for other applications that don’t offer the option. Many large applications are designed this way for exactly this reason.

1. Touch ⚙ > **Apps**.
2. Swipe the screen to display the **On Device Storage** tab.

The tab lists the applications that must be or can be stored on On-device Storage. Each application lists the amount of storage it uses on internal storage (even when not stored there, all applications use at least a small amount of internal storage).

Applications that are stored on On-device Storage card are checked.

The graph at the bottom shows the amount of memory used and free of On-device Storage: the total includes files and other data, not just the applications in the list.

3. Touch an application in the list.
4. The Storage section of the application’s details screen shows details about the memory used by the application. If the application can be moved, the Move button is active.
5. Touch **Move to On-device Storage** to move the bulk of the application from the device’s internal storage to the On-device Storage.
6. Touch **Move to device** to move the application back to the device’s internal storage.

Managing Downloads

Files and applications downloaded using the Browser or Email are stored on On–device Storage in the Download directory. Use the Downloads application to view, open, or delete downloaded items.

1. Touch ⊞ > ⬇.
2. Touch an item to open it.
3. Touch headings for earlier downloads to view them.
4. Check items to delete; then touch 🗑. The item is deleted from storage.
5. Touch **Sort by size** or **Sort by time** to switch back and forth.

   When an application is opened, the other applications being used do not stop. The operating system and applications work together to ensure that applications not being used do not consume resources unnecessarily, stopping and starting them as needed. For this reason, there’s no need to stop applications unless it is not functioning properly.

CHAPTER 11 SETTINGS

Screen Unlock Settings

Use the **Security settings** to set preferences for locking the screen. Touch ⚙ > 🔒 **Security**.

NOTE Options vary depending upon the application's policy, for example, 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.
  - **Slide** - Slide the lock icon to unlock the screen.
  - **Pattern** - Draw a pattern to unlock screen. See *Set Screen Unlock Using Pattern on page 11-3* for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See *Set Screen Unlock Using PIN on page 11-1* for more information.
  - **Password** - Enter a password to unlock screen. See *Set Screen Unlock Using Password on page 11-2* 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.

Single 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 up to unlock the screen.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.

Set Screen Unlock Using PIN

1. Touch ⚙.

2. Touch 🔒 **Security**.
3. Touch **Screen lock**.
4. Touch **PIN**.
5. Touch in the text field.
6. Enter a PIN (between 4 and 16 characters) then touch **Next**.
7. Re-enter PIN and then touch **Next**.
8. Touch ⌂. The next time the device goes into suspend mode a PIN is required upon waking.

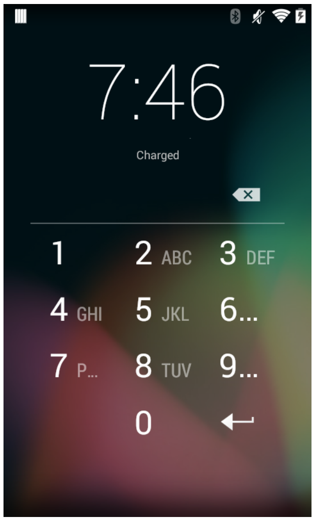


Figure 11-1 *PIN Screen*

Set Screen Unlock Using Password

1. Touch ⚙.
2. Touch 🔒 **Security**.
3. Touch **Screen lock**.
4. Touch **Password**.
5. Touch in the text field.
6. Enter a password (between 4 and 16 characters) then touch **Next**.
7. Re-enter the password and then touch **Next**.
8. Touch ⌂. The next time the device goes into suspend mode a PIN is required upon waking.

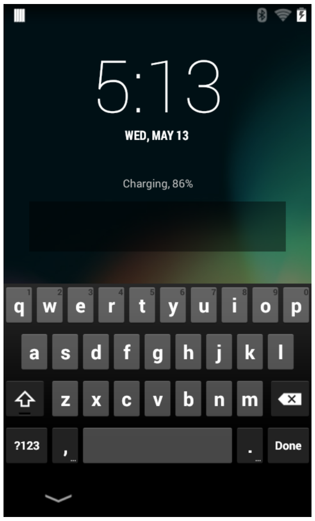


Figure 11-2 *Password Screen*

Set Screen Unlock Using Pattern

1. Touch ⚙.
2. Touch 🔒 **Security**.
3. Touch **Screen lock**.
4. Touch **Pattern**.
5. Watch pattern example and then touch **Next**.
6. Draw a pattern connecting at least four dots.

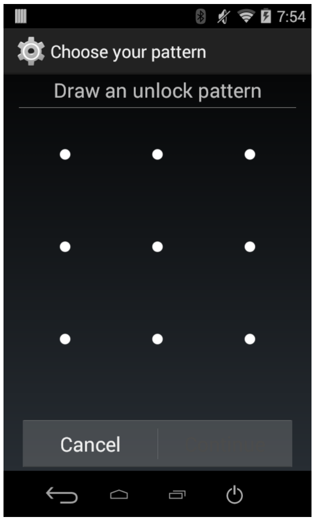


Figure 11-3 *Choose Your Pattern Screen*

7. Touch **Continue**.
8. Re-draw the pattern.
9. Touch **Confirm**.

10. On the **Security** screen, touch **Make pattern visible** to show pattern when you draw the pattern.

11. Touch **Vibrate on touch** to enable vibration when drawing the pattern.

12. Touch ⌂.

    The next time the device goes into suspend mode a Pattern is required upon waking.

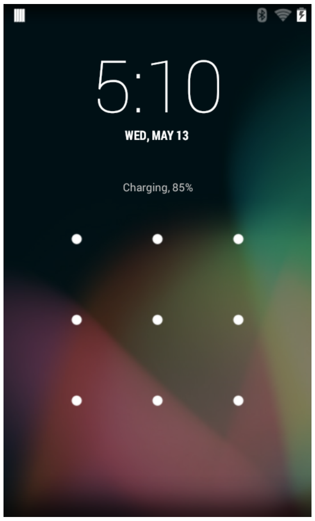


Figure 11-4 *Pattern Screen*

Multiple User Mode

For Multi-user Mode configuration, see *Chapter 8, Administrator Utilities*.

Passwords

To set the device to briefly show password characters as the user types, set this option. Touch ⊞ > ⚙ > 🔒 **Security**. Touch **Make passwords visible**. A check in the checkbox indicates that the option is enabled.

Language Usage

Use the Language & input settings to change the language that display for the text and including words added to its dictionary.

Changing the Language Setting

1. Touch **Language**.

2. In the **Language** screen, select a language from the list of available languages.

   The operating system text changes to the selected language.

Adding Words to the Dictionary

1. In the **Language & input** screen, touch **Personal dictionary**.

2. Touch **+** to add a new word or phrase to the dictionary.

3. In the **Phrase** text box, enter the word or phrase.
4. In the **Shortcut** text box, enter a shortcut for the word or phrase.
5. In the **Language** drop-down list, select the language that this word or phase is stored.
6. Touch **Add to dictionary** in the top left corner of the screen to add the new word.

Keyboard Settings

Use the **Language & input** settings for configuring the on-screen keyboards. The device contains the following keyboard settings:

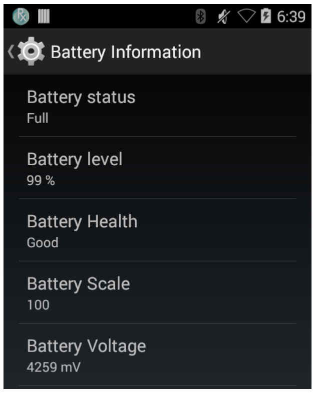
- Android Keyboard
- Japanese IME
- Chinese keyboard.

About Device

Use **About device** settings to view information about the MC18. Touch ⚙ > **About device**.

- **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 MC18 has been running since being turned on.
- **SW components** - Lists filenames and versions for various software on the MC18.
- **Legal information** - Opens a screen to view legal information about the software included on the MC18.
- **Battery Management** - Displays information about the battery.
- **Battery information** - Displays information about the battery.
- **Hardware config** - Lists part number for various hardware on the MC18.
- **Legal information** - Opens a screen to view legal information about the software included on the MC18.
- **Model number** - Displays the devices model number.
- **Android version** - Displays the operating system version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

Battery Information



Battery status
Full

Battery level
99 %

Battery Health
Good

Battery Scale
100

Battery Voltage
4259 mV

Figure 11-5 *Battery information Screen*

- **Battery status** - Indicates current battery state; **Unknown**, **Charging**, **Discharging**, **Not changing**, **Full** or **Error**.
- **Battery level** - Indicates the current battery level in percentage.
- **Battery Health** - Indicates the health of the battery; **Good**, **Dead**, **Overheat**, **Over voltage**, **Unknown**, **Unspecified failure**, **Cold**, **Over current** or **CommFailure**.
- **Battery Scale** - Indicates maximum battery level.
- **Battery Voltage** - Indicates the current battery voltage in millivolts.
- **Battery Temperature** - Indicates the current battery temperature in degrees Celsius.
- **Battery Technology** - Indicates the type of battery.
- **Battery Part Number** - Indicates the part number of the battery.
- **Battery Serial Number** - Indicates the serial number of the battery.
- **Battery Manufacture Date** - Indicates the date (month, day, year) that the battery was manufactured.
- **Battery Rated Capacity** - Indicates the rated capacity (in mAh) of the battery.
- **Battery Decommission** - Indicates the decommission status of the battery. 0 - less than decommission threshold, 1 - greater than or equal to the decommission threshold, 2 - unknown state.
- **Base Cumulative Charge** - Indicates the cumulative charge (in mAh) using non Zebra charging equipment.
- **Battery Preset Capacity** - Indicates the maximum amount of charge (in mAh) that can be pulled from the battery under the present discharge conditions if the battery is fully charged.
- **Battery Health Percentage** - Indicates the maximum amount of charge (in percentage) that could be pulled from the battery under the present discharge conditions if the battery is fully charged.
- **Battery Present Charge** - Indicates the amount of usable charge (in mAh) remaining in the battery under current discharge conditions.
- **Battery Time to Empty** - Indicates the amount of time (in minutes) until the battery is discharged.
- **Battery Time to Full** - Indicates the amount of time (in minutes) until the battery is at full charge.
- **Battery Total Cumulative Charge** - Indicates the cumulative charge (in mAh) using any charging equipment.

- **Battery Seconds Since Last Use -** Indicates the number of seconds that have passed since the battery was placed in a device and charger for the first time.

CHAPTER 12 MAINTENANCE AND TROUBLESHOOTING

Introduction

This chapter includes instructions on cleaning and storing the MC18, battery maintenance and provides troubleshooting solutions for potential problems during MC18 operations.

Maintaining the MC18

For trouble-free service, observe the following tips when using the MC18:

- Protect the MC18 from temperature extremes.
- Do not store or use the MC18 in any location that is extremely dusty, damp, or wet.
- Use a soft lens cloth to clean the scan exit window of the MC18. If the surface of the MC18 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution. Do not use bleach or ammonia.
- Take care not to scratch the screen of the MC18.
- The display of the MC18 contains glass. Take care not to drop the MC18 or subject it to strong impact.

Battery Safety Guidelines

- The area in which the MC18 units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non-commercial environment.
- Do not use incompatible batteries and chargers. If you have any questions about the compatibility of a battery or a charger, contact Zebra Support. See *Service Information on page xiii* for contact information.
- Do not crush, puncture, or place a high degree of pressure on the battery.
- Follow battery usage, storage, and charging guidelines found in the MC18 Quick Reference Guide.
- Improper battery use may result in a fire, explosion, or other hazard.

- To charge the mobile device battery, the battery and charger temperatures must be between +32°F and +104°F (0°C and +40°C)
- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- Do not short circuit a battery or allow metallic or conductive objects to contact the battery terminals.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Do not leave or store the equipment in or near areas that might get very hot, such as in a parked vehicle or near a radiator or other heat source. Do not place battery into a microwave oven or dryer.
- Battery usage by children should be supervised.
- Please follow local regulations to promptly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- Seek medical advice immediately if a battery has been swallowed.
- In the event of a battery leak, do not allow the liquid to come in contact with the skin or eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- If you suspect damage to your equipment or battery, call Customer Support to arrange for inspection. See *Service Information on page xiii* for contact information.

Long Term Storage

When storing the MC18 for a long period of time, it is recommended to remove the battery.

When returning the MC18 to everyday operation, install a fully charged battery.

Cleaning

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 Symbol Technologies 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.**

Materials Required

- Alcohol wipes
- Lens tissue
- Cotton tipped applicators

- Isopropyl alcohol
- Can of compressed air with a tube.

Cleaning the MC18

Housing

Using the alcohol wipes, wipe the housing including the Scan key.

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 dried the display with a soft, non-abrasive cloth to prevent streaking.

Scan Exit Window

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

Power Connector

1. Remove the main battery from MC18. See *Removing the Battery on page 1-9*.
2. Install the battery cover.
3. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.
4. Repeat at least three times.
5. Use the cotton tipped applicator dipped in alcohol to remove any grease and dirt near the connector area.
6. Use a dry cotton tipped applicator and repeat steps 3 through 6.
7. Spray compressed air on the connector area by pointing the tube/nozzle about ½ inch away from the surface.

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

8. Inspect the area for any grease or dirt, repeat if required.

Cleaning Cradle Connectors

Use this procedure to clean the connectors on a cradle:

1. Remove power 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 let any cotton residue on the connector.
4. All sides of the connector should also be rubbed with the cotton tipped applicator.

5. Spray compressed air in the connector area by pointing the tube/nozzle about ½ inch away from the surface.

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

6. Ensure that there is no lint left by the cotton tipped applicator, remove lint if found.
7. If grease and other dirt can be found on other areas of the cradle, use 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.

Cleaning Frequency

The cleaning frequency is up to the customer’s discretion due to the varied environments in which the MC18 units are used. They may be cleaned as frequently as required. However when used in dirty environments it may be advisable to periodically clean the scanner exit window to ensure optimum scanning performance.

Troubleshooting

MC18

Table 12-1 *Troubleshooting the MC18*

Problem	Cause	Solution
MC18 does not turn on.	Battery not charged.	Charge or replace the battery in the MC18.
	Battery not installed properly.	Ensure battery is installed properly. See *Installing the Battery on page 1-8*.
	System crash.	Perform a soft reset. If the MC18 still does not turn on, perform a hard reset. See *Resetting the MC18 on page 1-21*.
Battery did not charge.	Battery failed.	Replace battery. If the MC18 still does not operate, try a soft reset, then a hard reset. See *Resetting the MC18 on page 1-21*.
	MC18 removed from cradle before charging completed.	Insert the MC18 into the cradle and begin charging. The battery fully charges in approximately four hours.
	Ambient temperature of the cradle is too warm or too cold.	The ambient temperature must be between 0 °C and 40 °C (32 °F and 104 °F).
During data communication, no data was transmitted, or transmitted data was incomplete.	MC18 unplugged from host computer during communication.	Reconnect the programming cable to the host computer and re-transmit.
	Communication software was incorrectly installed or configured.	See system administrator.
MC18 turns itself off.	MC18 is inactive.	The MC18 turns off after a period of inactivity. If the MC18 is running on battery power, this period can be set to 15 seconds, 30 seconds, 1 minute, 2 minutes, 5 minutes, 10 minutes, or 30 minutes. Change the setting if you need a longer delay before the automatic shutoff feature activates.
	Battery is depleted.	Place the MC18 in the cradle to re-charge the battery.
	Battery is not inserted properly.	Insert the battery properly (see *Installing the Battery on page 1-8*).
	The MC18's battery is low and it powers down to protect memory content.	Place the MC18 in the cradle to re-charge the battery.

Table 12-1 *Troubleshooting the MC18 (Continued)*

Problem	Cause	Solution
A message appears stating that the MC18 memory is full.	Too many files stored on the MC18.	Delete unused memos and records. You can save these records on the host computer.
	Too many applications installed on the MC18.	If you have installed additional applications on the MC18, remove them to recover memory. See *Uninstalling an Application on page 10-4*.
The MC18 does not accept scan input.	Scanning application is not loaded.	Verify that the MC18 is loaded with a scanning application. See the System Administrator.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between imager exit window and bar code is incorrect.	Move the MC18 closer or further from the bar code to the proper scanning range.
	MC18 is not programmed for the bar code.	Verify that the MC18 can read the type of bar code being scanned (See *Technical Specifications*). Ensure that the bar code parameters are set properly for the bar code being scanned.
	MC18 is not programmed to generate a beep.	Verify that a beep on a good decode is used. See *Bar Code Input on page 9-10* for more information.
	Battery is low.	If the scanner is still not reading symbols, contact the distributor or service.
During USB data communications, no data was transmitted, or transmitted data was incomplete.	Incorrect cable connection.	See *Connecting the MC18 to a Host Computer on page 4-2*.
	Communications software is not installed or configured properly.	Perform setup as described in *Chapter 6, Cradle Installation*.
		Ensure that a sync program is installed on the host computer.
Cannot sync with Host Computer	Host computer not configured properly.	Ensure that sync program on the host computer is set to allow USB connections. See Chapter 4, Sync with Host Computer for more information.

Cradles

Table 12-2 *Troubleshooting the Cradles*

Symptom	Possible Cause	Solution
MC18 battery is not charging.	MC18 was removed from cradle or cradle was unplugged from AC power.	Ensure cradle is receiving power. Ensure MC18 is seated correctly. Confirm main battery is charging. The battery fully charges in approximately four hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery (see *Installing the Battery on page 1-8*).
	The MC18 is not fully seated in the cradle.	Remove and re-insert the MC18 into the cradle, ensuring it is firmly seated.
	Ambient temperature of the cradle is too warm or too cold.	Move the cradle to an area where the ambient temperature is between 0 °C and 40 °C (32 °F and 104 °F).
When the MC18 is placed in the cradle, the cradle LED does not blink.	Cradle is not powered.	Ensure cradle is receiving power.
	Cradle firmware is corrupted.	Contact system administrator.
	The MC18 is not operational.	Contact system administrator.
	Cradle - MC18 communication error.	Contact system administrator.
Cradle LED blinks red.	The cradle is issued an unlock command and it fails to unlock.	Contact system administrator.
	Cradle is overheating due to continuous lock/unlock or other cradle faults.	Contact system administrator.

APPENDIX A TECHNICAL SPECIFICATIONS

Technical Specifications

The following tables summarize the MC18’s intended operating environment and general technical hardware specifications.

Table A-1 *Technical Specifications*

Item	Description
Physical and Environmental Characteristics	
Dimensions (H x L x W)	2.34 in. x 8.37 in. x 2.93 in. (5.94 cm x 21.25 cm x 7.44 cm)
Weight	297 g (10.47 oz) with battery
Keys	Single Scan key
Display	Color LCD, 4",480x800 WVGA resolution, 16 bits/pixel RGB, 450 Nits LED backlight, capacitive touch screen
Speaker	2W speaker
Main Battery	PowerPrecision+ rechargeable 3.7 VDC Lithium Ion battery Typical Capacity: 2,725 mAh. Minimum Capacity: 2,625 mAh.
Performance Characteristics	
CPU	TI OMAP4430, Dual Core, 1 GHz
Operating System	Android -based ASOP 4.4.4
Memory	Flash - 4GB, RAM - 1GB
Application Development	Zebra Android EMDK.
Data Capture Method	Imager (SE4710) with red LED Illumination and LED dot aim pattern. Imaging rate: 30 Frames per second, 1280p x 800p

Table A-1 *Technical Specifications (Continued)*

Item	Description
User Environment	
Operating Temperature	0° C to 40° C (32° F to 104° F)
Storage Temperature	-20° C to 60° C (-4° F to 140° F)
Battery Charging Temperature	0° C to +40° C (32° F to 104° F) ambient temperature range.
Humidity	40° C (RH 10% - 95%) Non-condensing
Flammability	UL94V1
Drop Specification	4 ft.(1.2 m) to vinyl tile over concrete, over product temperature range. 4 ft.(1.2 m) to concrete, at room temperature of 23° C (73.4° F).
Sealing	Liquid penetration per "A4T Casual Spill Test Spec" document number 71-98611-01. Applies ONLY with battery installed.
ESD	± 20k VDC air discharge ± 10k VDC contact discharge
Wireless LAN Data Communications	
Radio	IEEE ® 802.11a/b/g/n/d/h/i/k/r
Data Rates	5GHz: 802.11a/n - up to 72.2 Mbps; 2.4GHz: 802.11b/g/n - up to 72.2 Mbps
Operating Channels	Channels 36 - 165 (5180 - 5825 MHz) Channels 1 - 13 (2412 - 2472 MHz) Actual operating channels/frequencies 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, PE APv1-EAP-GTC, EAP-FAST (MSCHAPv2 and EAP-GTC) and LEAP

Multimedia	Wi-Fi Multimedia™ (WMM)
Certifications	WFA (802.11n, WMM, WMM-PS), Cisco CCXv4
Fast Roam	PMKID Caching, Opportunistic Key Caching (OKC), Cisco CCKM, 802.11r, Zebra Aggregated FT
Wireless PAN Data Communications	
Bluetooth	V4.0 with Low Energy

Table A-1 *Technical Specifications (Continued)*

Item	Description
USB	USB 2.0 Client for service and maintenance
Imager Decode Capability	
	The SE4710 2D supports barcode symbologies listed below (The specific engine configuration is identified / readable in the system configuration). • Code 39: Trioptic Code 39 UPC/EAN: UPCA (+ add-on), UPCE (+ add-on), UPCE1, EAN-8, EAN-13 (+ add-on), JAN-8 (Note: This is supported but not handled separately from EAN8 or EAN 13), JAN-13 (+ add-on), SBN / Bookland (+ISBN 13), ISSN, Coupon Codes including GS1 Databar Expanded Format. • Code 128: ISBT-128, UCC/EAN 128, GS1-128 (Note this is the new name for EANUCC-128) • Code 93 • MSI • Codabar: ABC, Ames • 2 of 5: Interleaved 2 of 5 / ITF, Discrete 2 of 5, IATA, Chinese 2 of 5, Code 11, Matrix 2 of 5 • Korean 3 of 5 • RSS/GS1 data bar: GS1-DataBar (Previously known as RSS), GS1-DataBar Limited, GS1-DataBar Expanded (Including stacked) 2D symbologies • PDF-417: Macro PDF, Macro Micro PDF, Composite, Composite C, Composite AB • Data Matrix: GS1-Datamatrix • QR code: Micro QR, GS1-QR code • Aztec • Maxicode • Han Xin (Chinese Sensible Code) • Postal codes: Linked Aztec, US Planet, US Postnet, US Intelligent Mail, Royal Mail 4 State, USPS 4CB/OneCode/Intelligent Mail, UPU FICS Postal, UK Postal, Japan Postal, Australian Postal, Canada Post, Netherlands KIX Code • Signature capture

Three Slot Cradle

Table A-2 *Cradle Specifications*

Item	Description
Operating Temperature	0° C to +40° C (32° F to 104° F)
Storage Temperature	-20° C to 60° C (-4° F to 140° F)
Battery Charging Temperature	0° C to +40° C (32° F to 104° F) ambient temperature
Humidity	10% to 95% non-condensing
Size (H x L x W)	129 mm x 134 mm x 310 mm (5 in x 5.2 in x 12.2 in)
Weight	1550 g (54.67 oz)
Power Supply	12.0 VDC,9.0 A
Electrostatic Discharge (ESD)	±20 kV air discharge, ± 10 kV contact discharge

Single-Slot Cradle

Table A-3 *Cradle Specifications*

Item	Description
Operating Temperature	0° C to +40° C (32° F to 104° F)
Storage Temperature	-20° C to 60° C (-4° F to 140° F)
Battery Charging Temperature	0° C to +40° C (32° F to 104° F) ambient temperature
Humidity	10% to 95% non-condensing
Size (L x W x H)	98 mm x 127 mm x 272 mm (4 in. x 5 in. x 10.7 in.)
Weight	620 g (21.87 oz)
Power Supply	12.0 VDC,9.0 A
Electrostatic Discharge (ESD)	±20 kV air discharge, ± 10 kV contact discharge

MC18 Interface Connector Pin-Outs

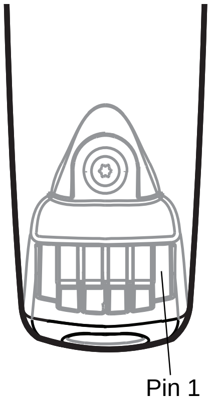


Figure A-1 *Power Connector Pin-Outs*

Table A-4 *Power Connector Pin-Outs*

PIN	Signal Name	Function
1	+5V	Input power
2	TX	Transmit Output to Cradle
3	RX	Receive Input from Cradle
4	GND	Ground

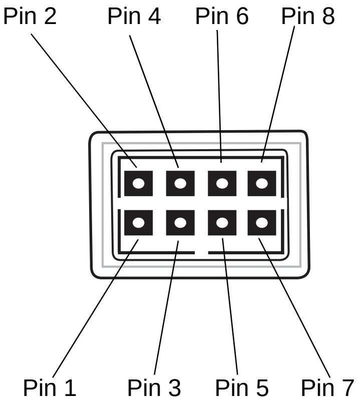


Figure A-2 *Sync Connector Pin-Outs*

Table A-5 *Sync Connector Pin-Outs*

PIN Number	Signal Name	Function
1	USB_PWR	+5 VDC
2	USBA0_OTG_DP	USB DATA +
3	Reserved	Not Used
4	USBA0_OTG_DM	USB DATA -

Table A-5 *Sync Connector Pin-Outs (Continued)*

PIN Number	Signal Name	Function
5	Sys_Boot5	Not Used
6	GND	Forces system to cold boot from USB
7	UART4_TXD	Debug Transmit Output
8	UART4_RXD	Debug Receive Input

Cable Specifications

Power Supply Cable, Y-type

Table A-6 *Wire Run List & Specifications*

Wire Color	AWG	Connector 1 Molex 39-01-2060 housing; 4x, 39-00-0211 contacts	Connector 2 Molex 39-01-2025 housing; 2x, 39-00-0211 contacts	Connector 3 Molex 39-01-2025 housing; 2x, 39-00-0211 contacts	Function
Red	16	1	1		(+) term
Black	16	6	2		(-) term
Red	16	2		1	(+) term
Black	16	5		2	(-) term

The 16 AWG wire should have the following specifications: UL1007, 300 Volt, PVC, -40° C to 80° C operating temperature.

Cradle Interconnection Cable

Table A-7 *Wire Run List & Specifications*

Wire Color	AWG	Connector 1 Molex 39-01-2025 housing; 2x, 39-00-0211 contacts	Connector 2 Molex 39-01-2025 housing; 2x, 39-00-0211 contacts	Function
Red	16	1	1	(+) term
Black	16	2	2	(-) term

The 16 AWG wire should have the following specifications: UL1007, 300 Volt, PVC, -40° C to 80° C operating temperature.

INDEX

ZEBRA

Zebra Technologies Corporation

3 Overlook Point

Lincolnshire, IL 60069 U.S.A.

http://www.zebra.com

Zebra and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

© 2015 ZIH Corp and/or its affiliates. All rights reserved.

MN002177A01 Revision A - July 2015