ET1 Enterprise Tablet
INTEGRATOR GUIDE

Copyrights

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your contact for further information.

Trademarks

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	08/30/2013	Initial release.
-02 Rev A	02/10/2015	Zebra rebranding.

Contents

About This Guide

This guide provides information on using the ET1 Enterprise Tablet and accessories.

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

Documentation Set

The documentation set for the ET1 provides information for specific user needs, and includes:

- *ET1 Enterprise Tablet Quick Start Guide* - describes how to set up the ET1 and basic operating instructions.
- *ET1 Enterprise Tablet User Guide* - describes how to use the ET1.
- *ET1 Enterprise Tablet Integrator Guide* - describes how to configure the ET1 and accessories.

Configurations

This guide covers the following configurations:

Configuration	Radios	Display	Memory	Data Capture Options	Operating System
ET1N0	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR	7.0” WSVGA Color	1 GB RAM / 4 GB Flash / 4 GB microSD card	camera, Scanning Module, Scanning/MSR Module, optional CS3070	Android-based, Android Open-Source Project 4.1.1
ET1N2	WLAN: 802.11a/b/g/n WPAN: Bluetooth v2.1 with EDR WWAN: HSDPA / CDMA	7.0” WSVGA Color	1 GB RAM / 4 GB Flash / 4 GB microSD card	camera, Scanning Module, Scanning/MSR Module, optional CS3070	Android-based, Android Open-Source Project 4.1.1

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:

- *Getting Started on page 17* provides information on getting the ET1 up and running for the first time.
- *Accessories on page 29* describes the available accessories and how to use them with the ET1.
- *USB Communication on page 51* describes how to connect the ET1 to a host computer using USB.
- *DataWedge Configuration on page 53* describes how to use and configure the DataWedge application.
- *WLAN Configuration on page 87* describes the how to configure the ET1 to connect with a wireless LAN network.
- *WWAN Configuration on page 95* describes the how to configure the ET1 to connect with a wireless WAN network.
- *Administrator Utilities on page 101* provides information for using the suite of administrative tools for configuring the ET1.
- *Settings on page 121* provides the settings for configuring the ET1.
- *Application Deployment on page 131* provides information for developing and managing applications.
- *Maintenance and Troubleshooting on page 145* includes instructions on cleaning and storing the ET1, and provides troubleshooting solutions for potential problems during ET1 operation.
- *Technical Specifications on page 153* provides the technical specifications for the ET1.
- *Keypad Remap Strings on page 165* provides a list of remap strings used when remapping keys.

Notational Conventions

The following conventions are used in this document:

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

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set. These icons and their associated meanings are described below.

⚠ **Warning:** The word WARNING with the associated safety icon implies information that, if disregarded, could result in death or serious injury, or serious product damage.

Caution: The word CAUTION with the associated safety icon implies information that, if disregarded, may result in minor or moderate injury, or serious product damage.

Note: NOTE contains information more important than the surrounding text, such as exceptions or preconditions. They also refer the reader elsewhere for additional information, remind the reader how to complete an action (when it is not part of the current procedure, for instance), or tell the reader where something is located on the screen. There is no warning level associated with a note.

Related Documents

- *ET1 Enterprise Tablet Quick Start Guide*, p/n MN000021A01-xx
- *ET1 Enterprise Tablet Regulatory Guide*, p/n 72-148509-xx
- *ET1 Enterprise Tablet Integrator Guide*, p/n MN000022A01-xx
- *Symbol CS3000 Series Scanner Product Reference Guide*, p/n 72E-136088-xx
- *MSP Client Software Guide*, p/n 72E-128805-xx
- *MSP 4.2 Release Notes*, p/n 72E-100160-xx.

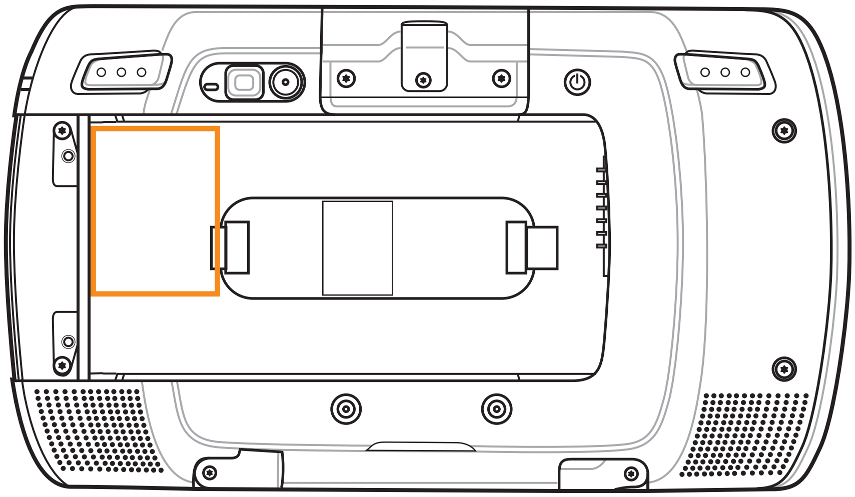
For the latest version of this guide and all guides, go to: *http://www.zebra.com/support*

Service Information

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

When contacting Zebra Customer Support Center, have the following information available:

- Serial number of the unit (found on the manufacturing label)
- Model number or product name (found on the manufacturing label)
- Software type and version number



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

If the Zebra Customer Support Center cannot solve the problem, you may need to return the equipment for servicing. The Support Center provides the 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 product from a Zebra business partner, contact that business partner for support.

Chapter 1

Getting Started

This chapter provides the features of the ET1 and explains how to set it up for the first time.

Unpacking

Carefully remove all protective material from the ET1 and save the shipping container for later storage and shipping.

Verify the following items are in the box:

- ET1 Enterprise Tablet with 4 GB micro secure digital (SD) card installed
- Lithium-ion battery
- Quick Start Guide
- Regulatory Guide.

Inspect the equipment for damage. If any equipment is missing or damaged, contact the Zebra Customer Support Center immediately. See *Service Information on page 15* for contact information.

Setup

To start using the ET1 for the first time:

- Install SIM card in an ET1N2 with GSM (optional).
- Install the battery.
- Charge the ET1.
- Power on the ET1.
- Activate the ET1N2 on a mobile data network (optional).

Installing the SIM Card

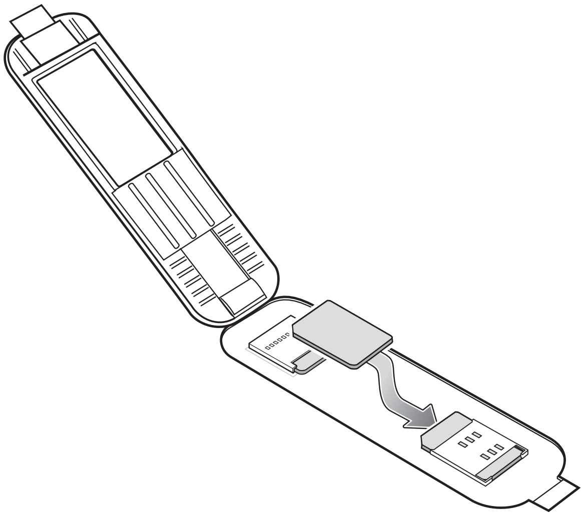
Note: ET1N2 only.

The ET1N2 requires an activated SIM card. Obtain the card from a service provider.

Procedure:

1 Lift the access door.

Figure 1: Installing SIM Card



2 Insert SIM card into the SIM holder with the contacts facing down and the cut edge facing away from the holder.

3 Close the access door.

Installing the Battery

Note: Ensure that the correct battery is used with the ET1. On the ET1N0 use either the 4620 mAh battery, p/n 82-149690-xx or the 5640 mAh battery, p/n 82-158261-xx. On the ET1N2 use only the 5640 mAh battery, p/n 82-158261-xx.

To install the battery:

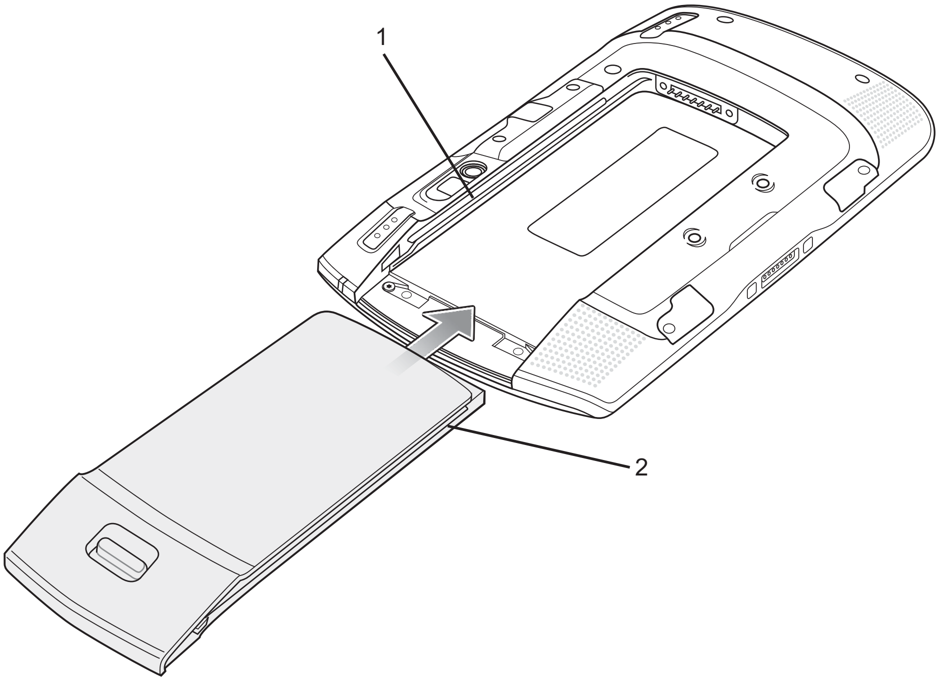
Procedure:

1 Align the tracks on the side of the battery with the rails in the battery compartment.

2 Push the battery in until the battery release latch snaps into place.

3 If the battery is charged, press and hold the Power button for two seconds until the splash screen appears.

Figure 2: Inserting the Battery



1 Rails
2 Battery Tracks

Charging the Battery

Caution: Ensure that you follow the guidelines for battery safety described in *Battery Safety Guidelines on page 145*.

Charging the Main Battery

Before using the ET1 for the first time, charge the main battery until the Battery Charge light emitting diode (LED) turns solid green (see *Table 1: Battery Charge LED Status on page 20* for charge status indications). To charge the ET1, use a cable or a cradle with the appropriate power supply. For information about the accessories available for the ET1, see *Accessories on page 29*.

The ET1 is equipped with a memory backup battery that automatically charges from the fully-charged main battery. When using the ET1 for the first time, the backup battery requires approximately 40 hours to fully charge. This is also true any time the backup battery is discharged, which occurs when the main battery is removed for several hours. The backup battery retains random access memory (RAM) data in memory for at least 15 minutes (at room temperature) when the ET1's main battery is removed, when Battery swap feature is used. When the ET1 reaches a very low battery state, the combination of main battery and backup battery retains RAM data in memory for at least 36 hours.

For cable and cradle setup and charging procedures see *Accessories on page 29*.

- USB/Charge Cable
- Single-slot USB Docking Cradle
- Four-slot Charge Only Docking Cradle.

To charge the main battery:

1 Connect the charging accessory to the appropriate power source. See *Accessories on page 29* for more information.

2 Insert the ET1 into a cradle or attach to a cable. The ET1 begins charging. The Battery Charge LEDs blink yellow while charging, then turns solid green when fully charged. See *Table 1: Battery Charge LED Status on page 20* for charging indications.

The battery charges in less than six hours.

Table 1: Battery Charge LED Status

Status	Indications
Off	ET1 is not inserted correctly in the cradle. ET1 is not connected to a power source. Charger or cradle is not powered.
Slow Blinking Yellow (3 blinks every 2 seconds)	ET1 is charging.
Solid Green	Charging complete.
Fast Blinking Yellow (2 blinks/ second)	Charging error, e.g.: • Temperature is too low or too high. • Charging has gone on too long without completion (typically eight hours).
Flashes Yellow three times when Power button pressed	Critical battery state. Battery too low to boot device.
Fast Blinking Yellow (when Power button pressed)	Battery over-temperature condition. Device shuts down. Battery will not charge until temperature returns to normal operating value.

Charging Temperature

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Note that charging is intelligently controlled by the ET1. To accomplish this, for small periods of time, the ET1 or accessory alternately enables and disables battery charging to keep the battery at acceptable temperatures. The ET1 or accessory indicates when charging is disabled due to abnormal temperatures via its LED. See *Table 1: Battery Charge LED Status on page 20*.

Charging Spare Batteries

See *Accessories on page 29* for information on using accessories to charge spare batteries.

Powering On the ET1

Press the Power button until the Battery Charge LED flashes three times. The splash screen displays for about a minute as the ET1 initializes its flash file system. Note that these windows also appear upon reset.

Powering Off the ET1

Press and hold the Power button until a menu appears. Touch **Power off** and then **OK**.

WAN Activation

Note: ET1N2 only.

In order to use the WAN radio for data communication, the ET1N2 must be activated on the service provider's network. By default, the ET1N2 is configured for a GSM network. To activate on a CDMA network, manual configuration is required.

Refer to the *ET1 Enterprise Tablet Integrator Guide* for detailed WAN configuration information.

GSM Activation

When the ET1N2 turns on it automatically configures for the network. If the SIM card requires a PIN, the PIN screen appears. Enter the PIN and touch **OK**.

CDMA Activation

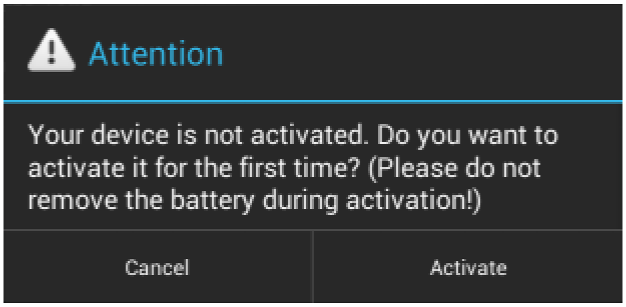
Prior to using the ET1N2 on a CDMA network, the ET1 must be registered with the service provider. Contact the service provider to set up an account and provide the MEID number (located under the battery).

By default, the ET1N2 is configured for a GSM network. To activate on a CDMA network:

Procedure:

1 Touch ⚙.
2 Touch **More...**.
3 Touch **Mobile networks**.
4 Touch **Technology preferences**.
5 Touch **Network mode**.
6 In the **Network mode** menu, select either **Sprint** or **Verizon**. The ET1 switches the modem firmware and the Activation Dialog box appears.

Figure 3: Activation Screen



Attention

Your device is not activated. Do you want to activate it for the first time? (Please do not remove the battery during activation!)

7 Touch **Activate**. The ET1N2 begins the activation process. If the activation is unsuccessful, contact the service provider.

Replacing the Battery

Caution:

Do not remove the microSD card while in Battery Swap mode.

Ensure that the Battery Swap mode procedures are followed, otherwise the backup battery will deplete quickly and on the ET1N2, SIM card data corruption might occur.

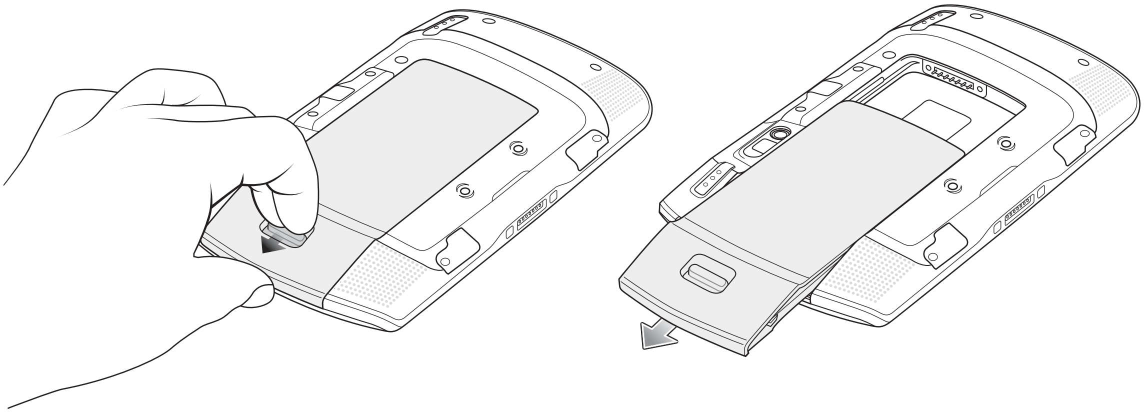
To replace the battery:

Procedure:

1 Press the Power button until the menu displays.
2 Touch **Battery Swap**. The Scan LED lights red.
3 Wait until the Scan LED turns off.
4 Press thumb against the side of the ET1 and battery. Using the index and middle fingers, move the battery release latch toward thumb.

5 Pull the battery out of the battery compartment.

Figure 4: Removing the Battery



6 Align the tracks on the side of the replacement battery with the rails in the battery compartment.

7 Push the battery in until the battery release latch snaps into place.

8 Press the Power button to turn on the ET1.

Replacing the microSD Card

Caution:

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

Changing the microSD card can change the functionality of the ET1.

To replace the microSD card:

Procedure:

1 Press the Power button until the menu displays.

2 Touch **Power off**.

3 Touch **OK**.

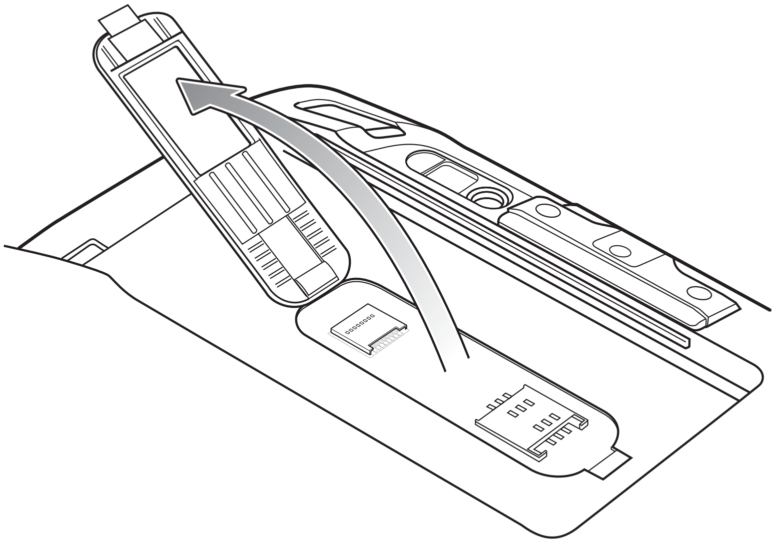
4 Wait for the ET1 to power off completely.

5 Press thumb against the side of the ET1 and battery. Using the index and middle fingers, move the battery release latch toward thumb.

6 Pull the battery out of the battery compartment.

7 Lift the access door.

Figure 5: Lift Access Door

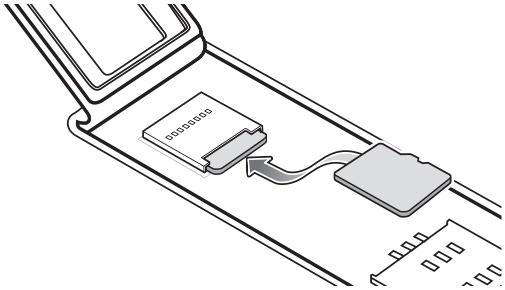


8 Remove the microSD card from the card holder.

9 Align the replacement microSD card with the card holder. Ensure that the contacts on the card are facing down and toward the card holder.

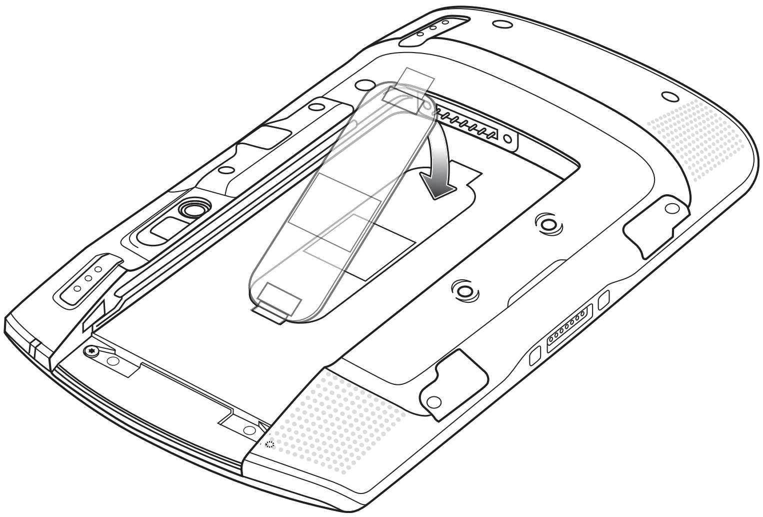
10 Insert the microSD card into the card holder.

Figure 6: Insert microSD Card



11 Close the access door.

Figure 7: Close Access Door



12 Align the tracks on the side of the replacement battery with the rails in the battery compartment.

13 Push the battery in until the battery release latch snaps into place.

14 Press the Power button to turn on the ET1.

Resetting the Device

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.

Procedure:

1 Press and hold the Power button until the menu appears.

2 Touch **Reset**.

3 The device shuts down and then reboots.

4 The device reboots.

Performing a Hard Reset

⚠ **Caution:** Performing a hard reset with a SIM card installed in the ET1N2 may cause damage or data corruption to the SIM card.

Perform a hard reset if the ET1 stops responding. To perform a hard reset:

Procedure:

1 Simultaneously press the Power, Left Scan/Action and Right Scan/Action buttons.

2 The ET1 shuts down and then reboots.

Performing an Enterprise Reset

An Enterprise Reset erases all data in the /cache and /data partitions and clears all ET1 settings, except those in the /enterprise partition.

Procedure:

1 Download the Enterprise Reset file from Zebra Support Central web site.

2 Copy the `ET1NxGenER0000002.zip` file to the root directory of the microSD card. See *USB Communication on page 51*.

3 Press and hold the Power button until the **Device options** menu appears.

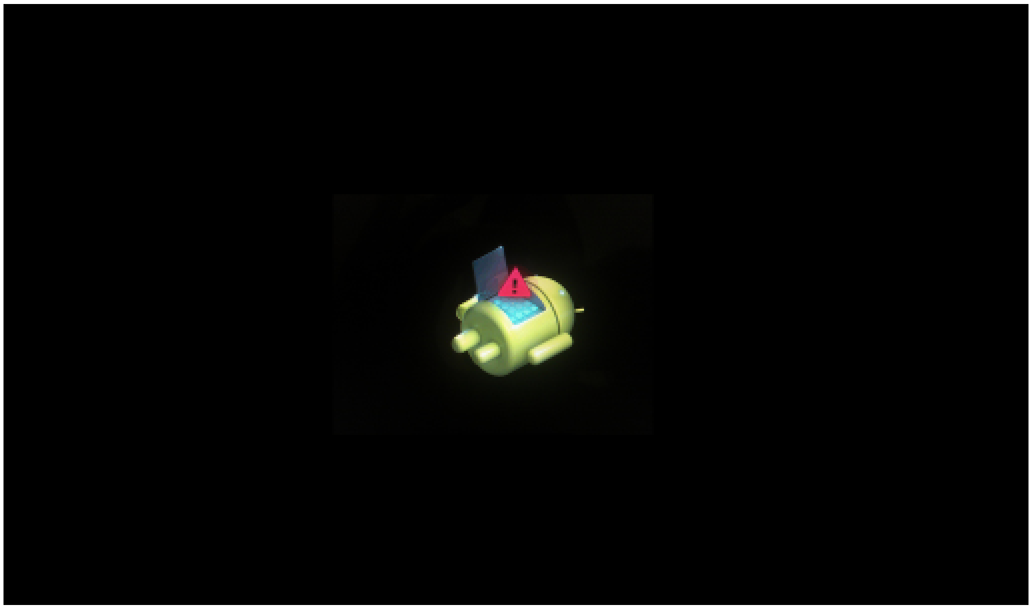
4 Touch **Reset**.

5 Touch **OK**. The ET1 resets.

6 Press and hold the Right Scan/Action button.

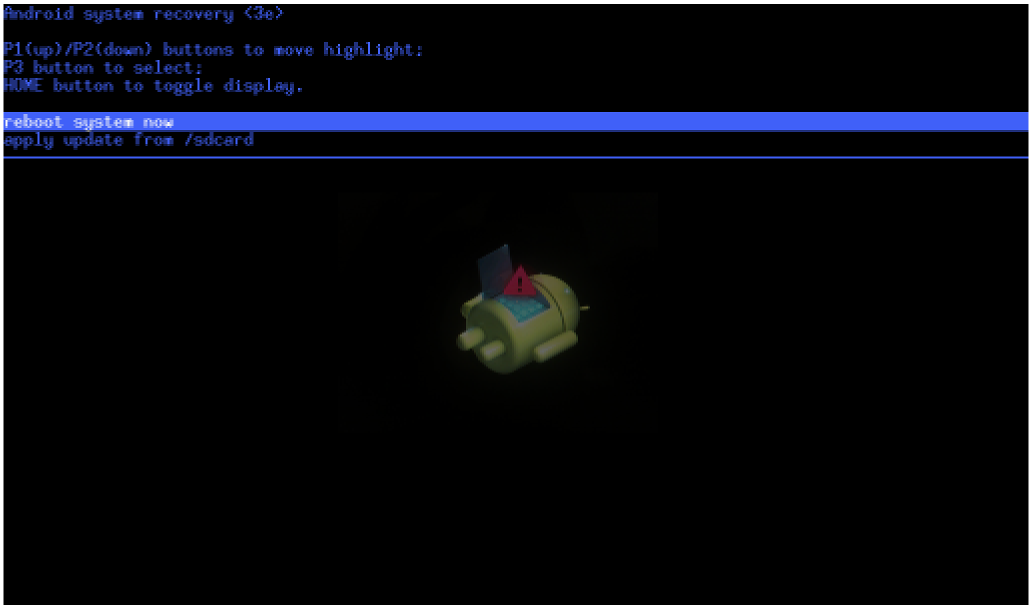
7 When the Recovery Mode screen appears release the Right Scan/Action button.

Figure 8: Recovery Mode Screen



8 Touch ⌂. The System Recovery screen appears.

Figure 9: System Recovery Screen



```
Android system recovery <3e>

P1(up)/P2(down) buttons to move highlight:
P3 button to select:
HOME button to toggle display.

reboot system now
apply update from /sdcard
```

9 Touch **P1** or **P2** to navigate to the **Apply update from /sdcard** option.

10 Touch **P3**.

11 Touch **P1** or **P2** to navigate to the `ET1NxGenER0000002.zip` file.

12 Touch **P3**. The Enterprise Reset occurs and then the ET1 resets.

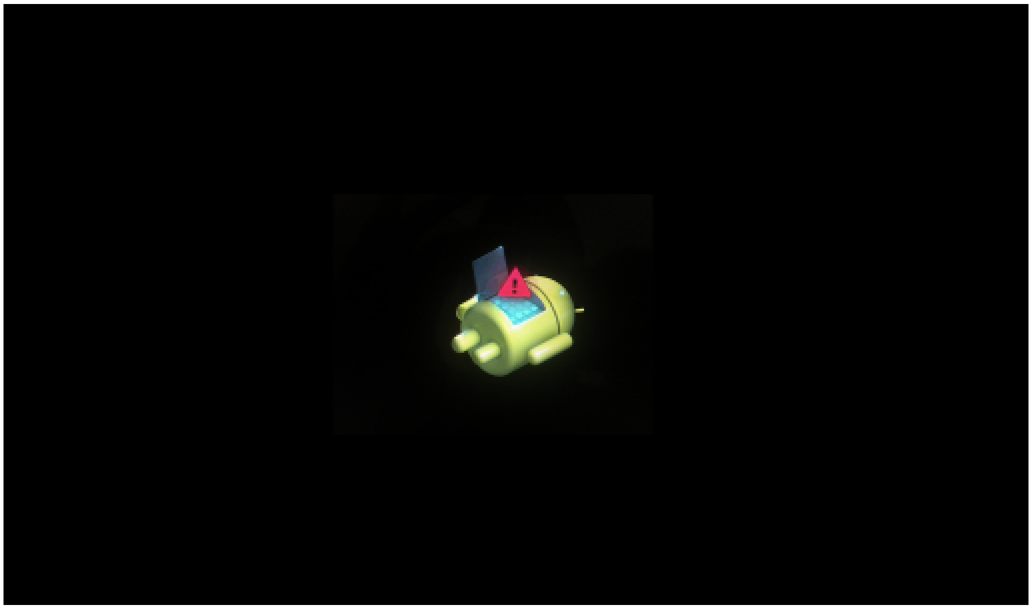
Performing a Factory Reset

A Factory Reset erases all data in the /cache, /data and /enterprise partitions in internal storage and clears all ET1 device settings. A Factory Reset returns the ET1 to the last installed operating system image. To revert to a previous operating system version, re-install that operating system image. See *Updating the System on page 135* for more information.

Procedure:

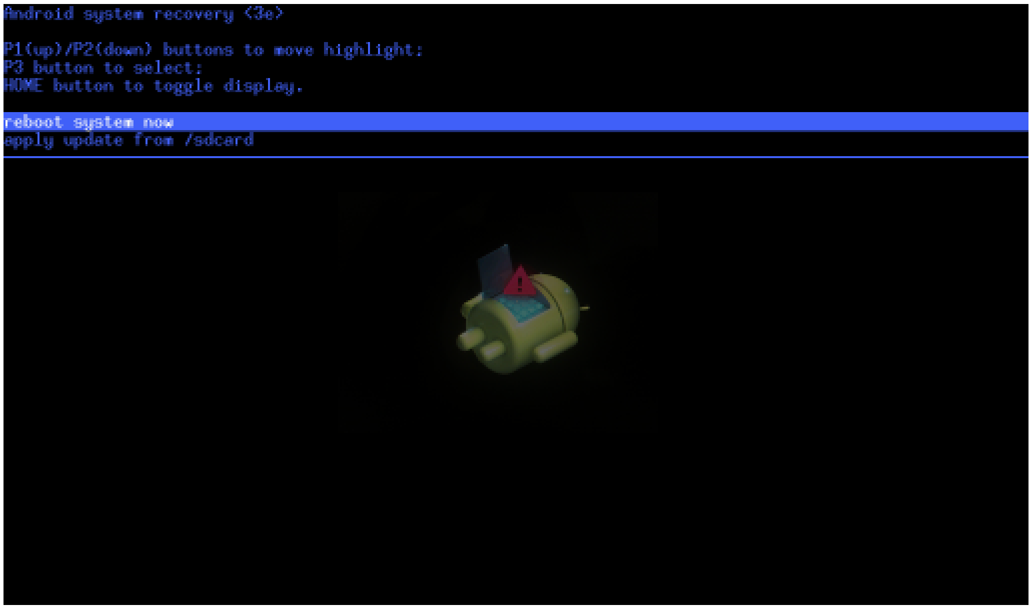
1. Download the Enterprise Reset file from Zebra Support Central web site.
2. Copy the `ET1NxGenFR0000002.zip` file to the root directory of the microSD card. See *USB Communication on page 51*.
3. Press and hold the Power button until the **Device options** menu appears.
4. Touch **Reset**.
5. Touch **OK**. The ET1 resets.
6. Press and hold the Right Scan/Action button.
7. When the Recovery Mode screen appears release the Right Scan/Action button.

Figure 10: Recovery Mode Screen



8. Touch ⌂.

Figure 11: System Recovery Screen



```
Android system recovery <3e>

P1(up)/P2(down) buttons to move highlight:
P3 button to select:
HOME button to toggle display.

reboot system now
apply update from /sdcard
```

9 Touch **P1** or **P2** to navigate to the **Apply update from /sdcard** option.

10 Touch **P3**.

11 Touch **P1** or **P2** to navigate to the `ET1NxGenFR0000002.zip` file.

12 Touch **P3**. The Factory Reset occurs and then the ET1 resets.

Wake-up Settings

The wake-up conditions define what actions wake up the ET1 after it has gone into suspend mode. The ET1 can go into suspend mode by either pressing the Power button or automatically by a time-out settings. *Table 2: Wake-up Default Settings on page 27* list the default wake up conditions.

Table 2: Wake-up Default Settings

Condition for Wake-up	Power Button	Automatic Time-out
AC power is applied.	No	Yes
ET1 is inserted into a cradle.	Yes	Yes
ET1 is removed from a cradle.	No	No
ET1 is connected to a USB device.	No	Yes
ET1 is disconnected from a USB device.	No	Yes
Scan/Action button is pressed.	Yes	Yes
The screen is touched.	No	No
Bluetooth communication	Yes	Yes

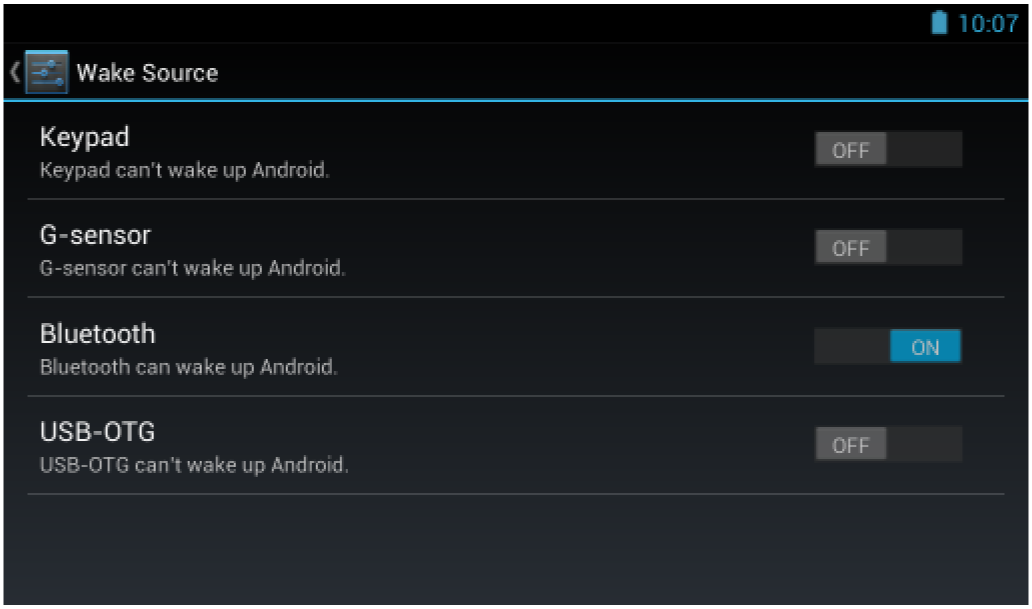
Setting the Wake Up Sources

To set the user configurable wake conditions:

Procedure:

1. Touch ☰.
2. Touch **Wake Source**.

Figure 12: Wake Source Screen



Keypad
Keypad can't wake up Android.
OFF

G-sensor
G-sensor can't wake up Android.
OFF

Bluetooth
Bluetooth can wake up Android.
ON

USB-OTG
USB-OTG can't wake up Android.
OFF

3. Slide the switch to turn on or off the wake up condition.
4. Touch ⌂.

Chapter 2

Accessories

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

ET1 Accessories

Table 3: ET1 Accessories on page 29 lists the accessories available for the ET1.

Table 3: ET1 Accessories

Accessory	Part Number	Description
Cradles		
Single-slot USB Docking Cradle	DC1000-1000U	Charges the ET1 main battery and a spare battery. Synchronizes the ET1 with a host computer through a USB connection.
Four-slot Charge Only Docking Cradle	DC1000-4000C	Charges up to four ET1 devices.
Chargers		
Four-slot Spare Battery Charger	SAC1000-4000C	Charges up to four ET1 battery packs.
Power Supply	PWRS-14000-148C	Provides power to the Single-slot USB Docking cradle or the USB/Charge cable. 12 VDC, 4.16 A.
Power Supply	PWRS-14000-241R	Provides power to the Four-slot Charge Only Docking cradle or the Four-slot Battery Charger. 12 VDC, 9 A.
Cables		
USB Charge Cable	25-153149-01R	Provides power to the ET1 and USB communication with a host computer.
DC Charge Cable	50-16002-029R	Connects one power supply to the one Four-slot Charge Only Docking Cradle or the Four-slot Battery Charger.
2-way Charge Cable	25-153150-01R	Connects one power supply to one Four-slot Charge Only Docking Cradle and one Four-slot Battery Charger or two Four-slot Battery Chargers.
US AC Line Cord (3-wire)	23844-00-00R	Provides power to the power supplies.
International AC line Cord	-	Provides power to the power supplies. Purchase separately.

Table continued…

Accessory	Part Number	Description
Miscellaneous		
Spare 4620 mAh lithium-ion battery	BTRY-ET01EAB0E BTRY-ET01EAB0E-10	Replacement 4620 mAh battery for ET1N0. Replacement 4620 mAh battery for ET1N0 (10-pack)
Spare 5640 mAh lithium-ion battery	BTRY-ET01EAB0H BTRY-ET01EAB0H-10	Replacement 5640 mAh battery for ET1N0 and ET1N2. Replacement 5640 mAh battery for ET1N0 and ET1N2 (10-pack).
Handstrap	SG-ET0123245-01R	Adjustable and 360-degree rotatable handstrap that mounts on the back of the ET1 and provides a secure option for holding the device.
Scanning Module	SCANMOD-ET1	Provides 2D bar code scanning.
Scanning/MSR Module	MSRSCAN-ET1	Provides 2D bar code scanning and magnetic stripe card reading.
Protective Rubber Bezel	KT-161552-01R	Add additional protection for the ET1.
Mobile Payment Module	MPM-100	Adds mobile point of sale capable of Chip and PIN, and MSR transactions to the ET1.

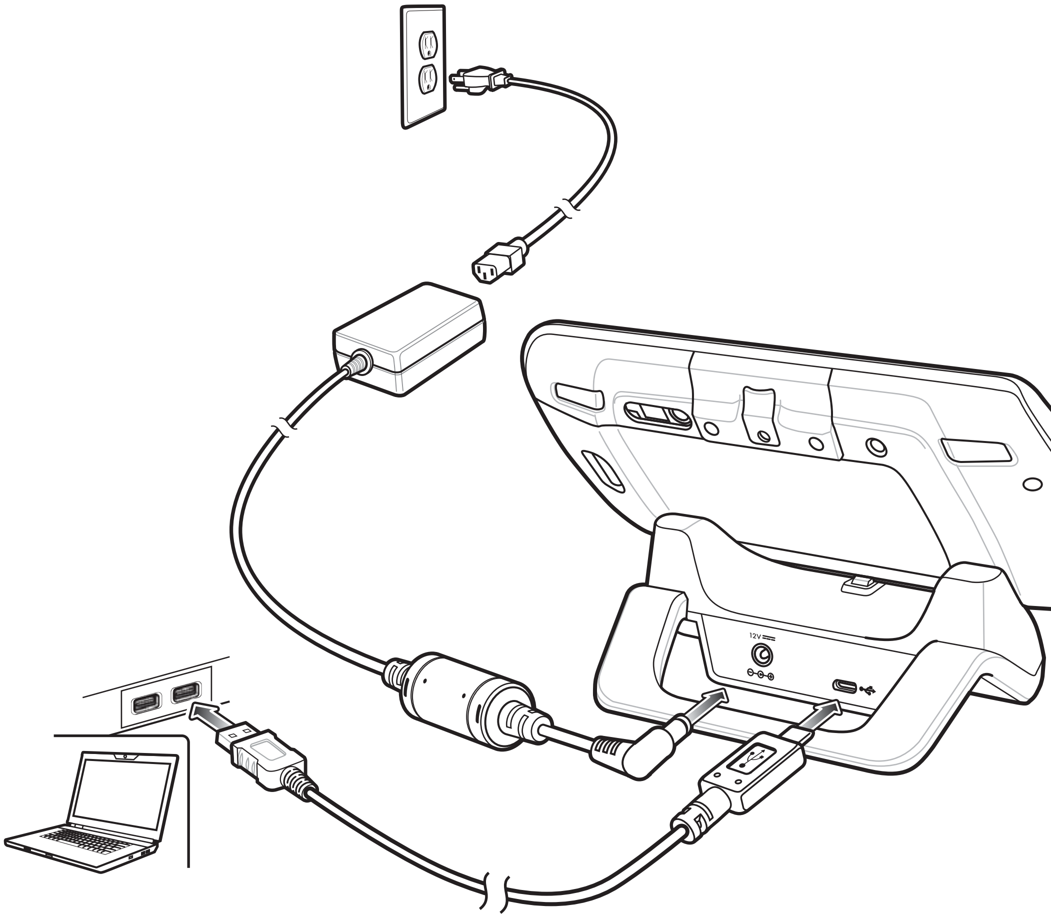
Single-Slot USB Docking Cradle

The Single-slot USB Docking cradle:

- Provides 12 VDC power for operating the ET1.
- Synchronizes information between the ET1 and a host computer. See the *ET1 Enterprise Tablet Integrator Guide* for information on setting up a connection to a host computer.
- Charges the battery.

Setup

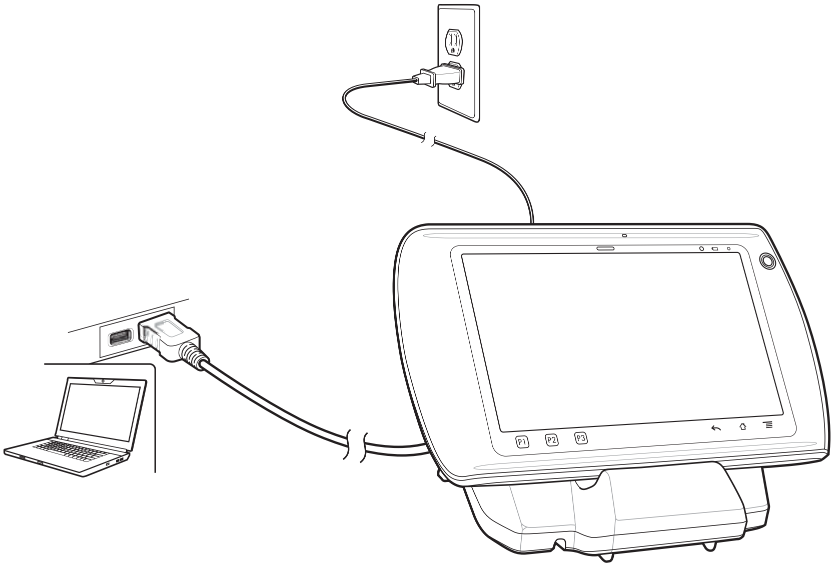
Figure 13: Single-Slot USB Docking Cradle Setup



Charging the ET1 Battery

Connect the cradle to power, then insert the ET1 into the slot to begin charging.

Figure 14: ET1 in Single-Slot USB Docking Cradle



The ET1 Battery Charge light emitting diode (LED) indicates the status of the battery charging in the ET1. See *Table 1: Battery Charge LED Status on page 20* for charging status indications. The battery fully charges in approximately six hours.

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the ET1. To accomplish this charging, for small periods of time, the ET1 or accessory alternately enables and disables the battery charging to keep the battery at acceptable temperatures. The ET1 indicates when charging is disabled due to abnormal temperatures via Battery Charge LED. See *Table 1: Battery Charge LED Status on page 20*.

Communication

When the ET1 is connected to a host computer using the Single-slot USB Docking cradle, the ET1 appears as a **Portable Device** on the host computer. Refer to the *ET1 Enterprise Tablet Integrator Guide* for more information.

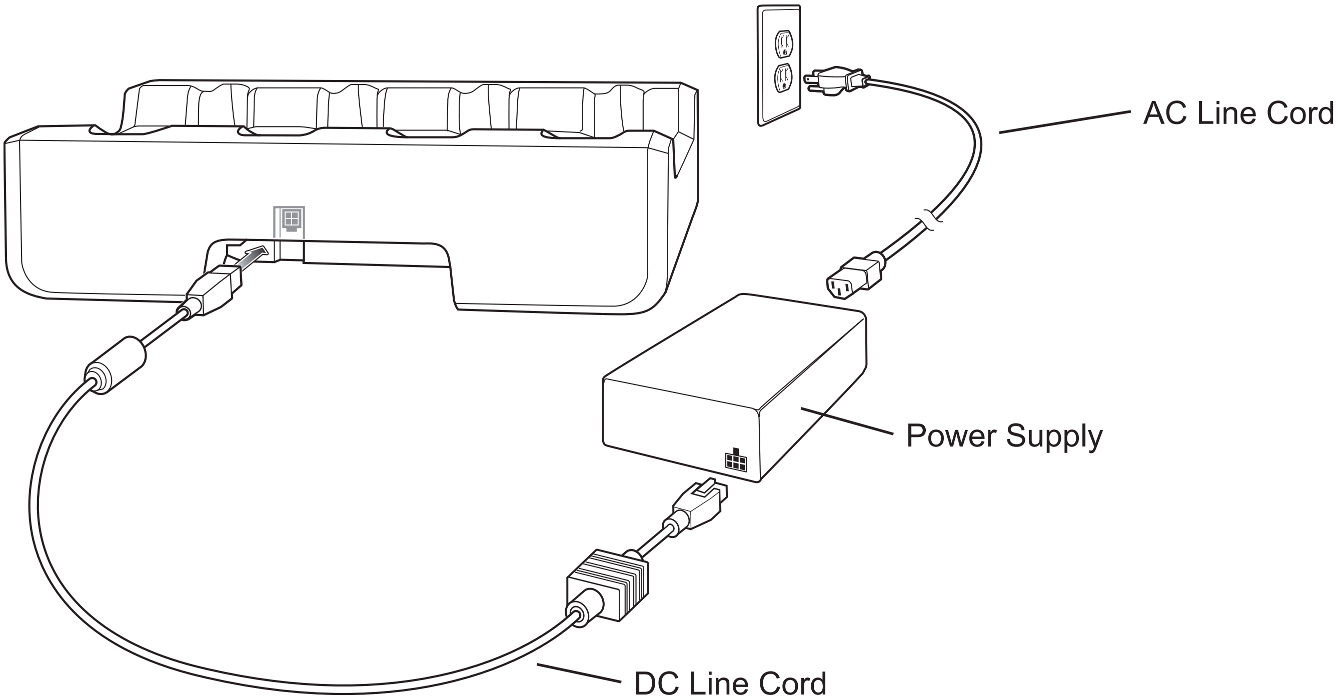
Four-Slot Charge Only Docking Cradle

The Four-slot Charge Only Docking cradle:

- Provides 12 VDC power for operating the ET1.
- Simultaneously charges up to four ET1 devices.

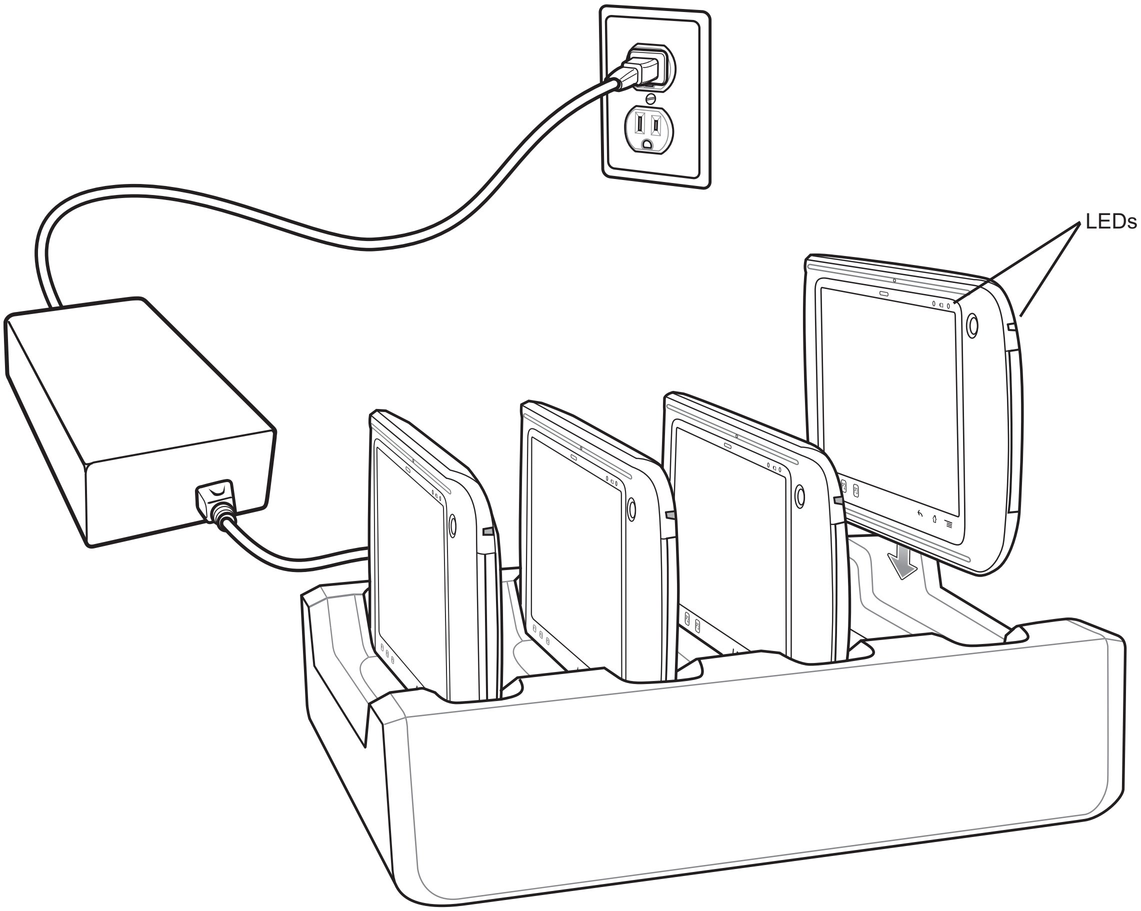
Setup

Figure 15: Setup



Charging

Figure 16: ET1 Battery Charging



Insert an ET1 into a slot to begin charging.

The ET1's Battery Charge LED shows the status of the battery charging in the ET1. See *Table 1: Battery Charge LED Status on page 20* for charging status indications. The battery fully charges in approximately six hours.

Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the ET1. To accomplish this, for small periods of time, the ET1 or accessory alternately enables and disables battery charging to keep the battery at acceptable temperatures. The ET1 indicates when charging is disabled due to abnormal temperatures via the Battery Charge LED. See *Table 1: Battery Charge LED Status on page 20*.

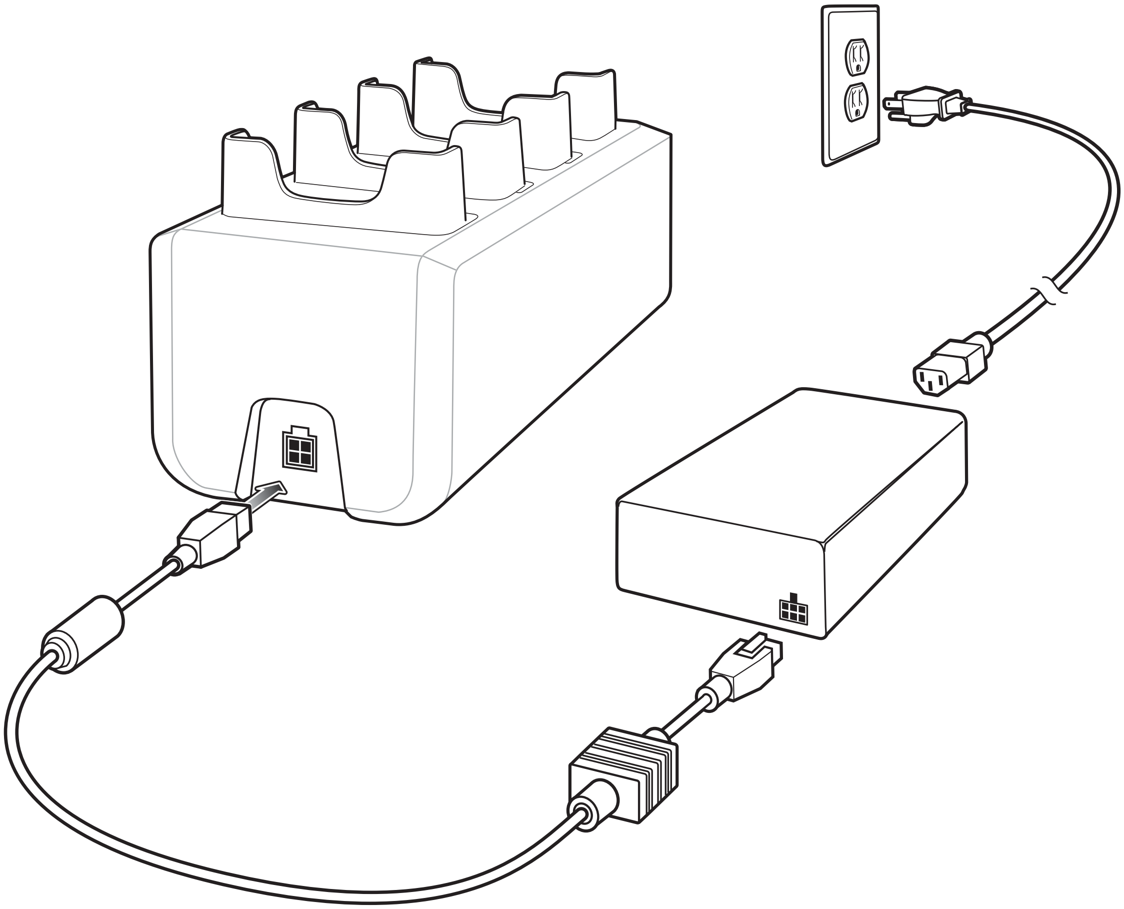
Four-Slot Battery Charger

The Four-slot Battery Charger:

- Provides 12 VDC power for charging the batteries.
- Simultaneously charges up to four ET1 batteries.

Setup

Figure 17: Four–Slot Battery Charger Setup

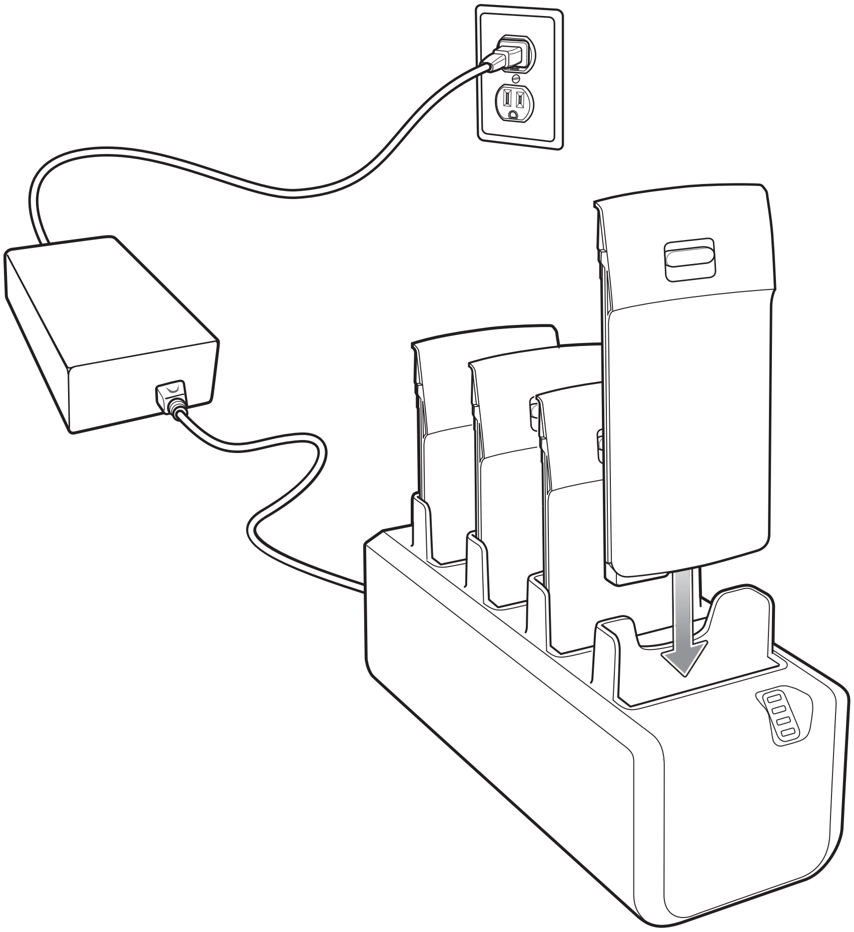


Charging the Batteries

Insert the spare battery into a spare battery charging well.

A Charge LED is provided for each battery charging well. See *Table 4: Battery LED Charging Indicators on page 35* for charging status indications. The 4620 mAh battery fully charges in approximately six hours.

Figure 18: ET1 Battery Charging



Charge batteries in temperatures from 0 °C to 40 °C (32 °F to 104 °F). Charging is intelligently controlled by the charger in order to ensure safe operation and optimize long-term battery life. To accomplish this, for small periods of time, the charger alternately enables and disables battery charging to keep the battery at acceptable temperatures. The charger indicates when charging is disabled due to abnormal temperatures via the Charge LED. See *Table 4: Battery LED Charging Indicators on page 35*.

Table 4: Battery LED Charging Indicators

LED	Indication
Off	No battery in slot. Battery is not charging. Battery is not inserted correctly in the charger. Charger is not powered.
Slow Blinking Amber	Battery is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Charging error.

2–Way Charge Cable

Caution:

Do not connect two Four-slot Charge Only cradles to one 2–way Charge Cable.

The 2–way Charge cable provides 12 VDC power to:

- one Four-slot Charge Only Docking cradle and one Four-slot Spare battery Charger.
- two Four-slot Spare battery Chargers.

Figure 19: 2–way Charge Cable — Cradle/Charger

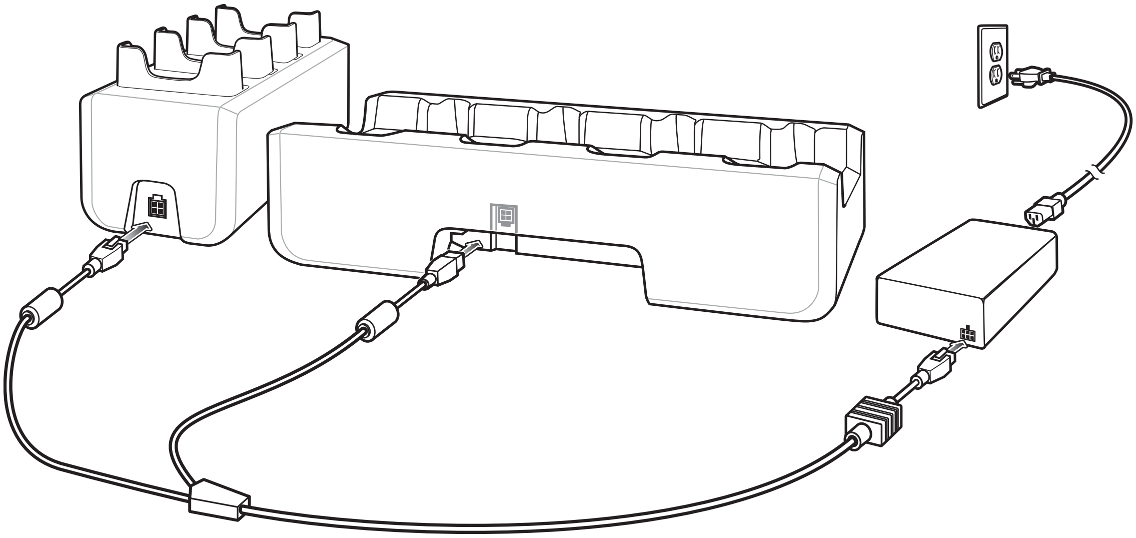
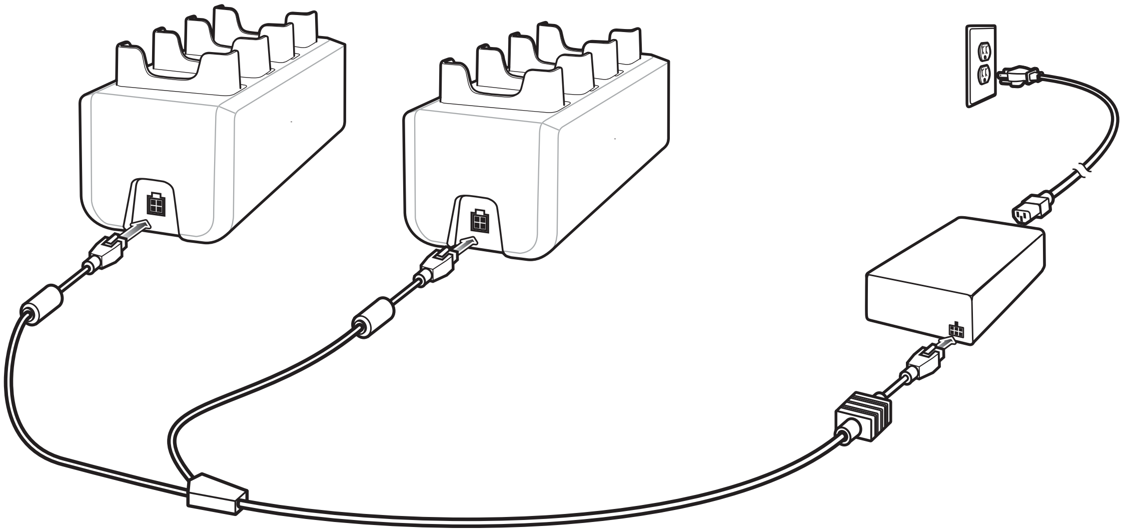


Figure 20: 2–way Charge Cable — Two Chargers



Handstrap

The handstrap provides a secure option for holding the ET1. It is adjustable and rotates 360°.

To install the handstrap:

Procedure:

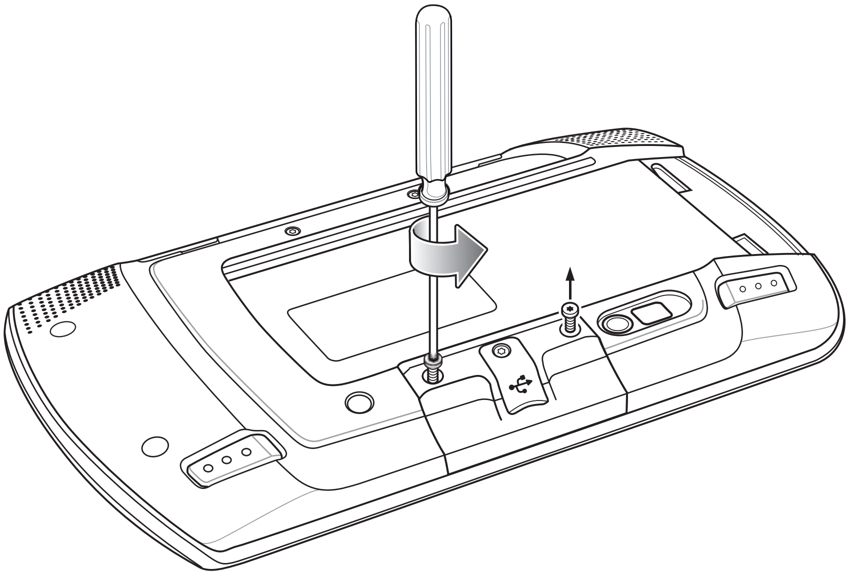
1 Press the Power button until the **Device options** menu appears.

2 Touch **Power off**.

3 Remove the battery.

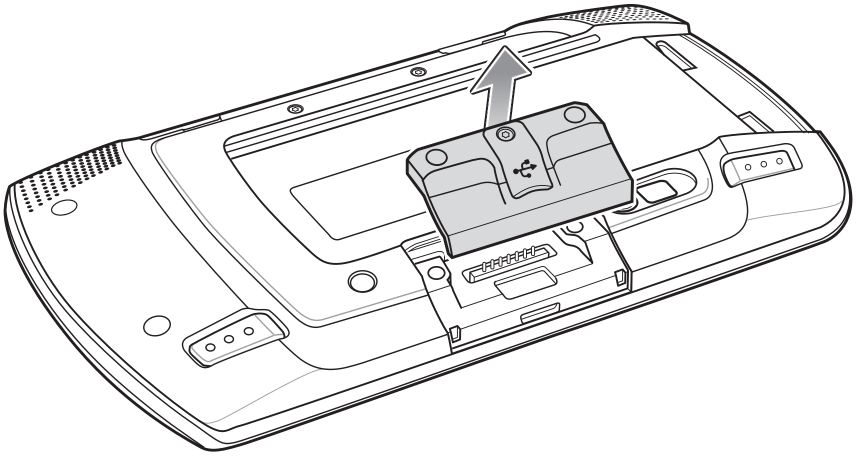
4 Using a Torx® T8 screwdriver, remove the two screws securing the expansion module.

Figure 21: Remove Expansion Module Screws



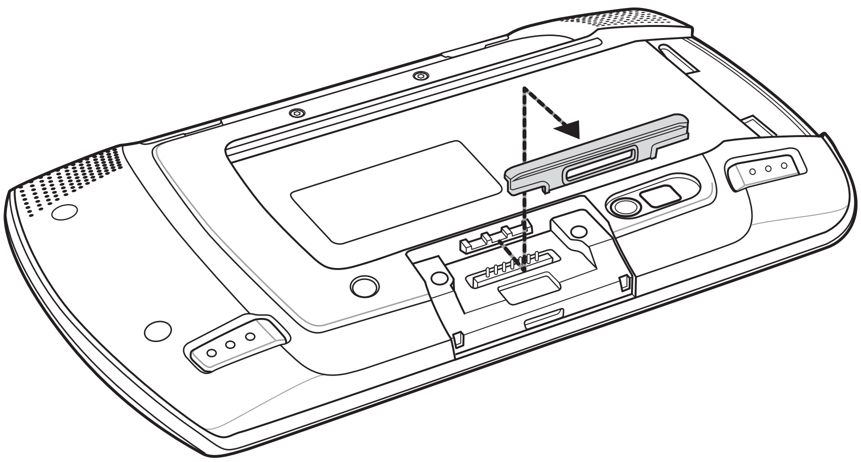
5 Remove the expansion module.

Figure 22: Remove Expansion Module



6 Remove the filler plate.

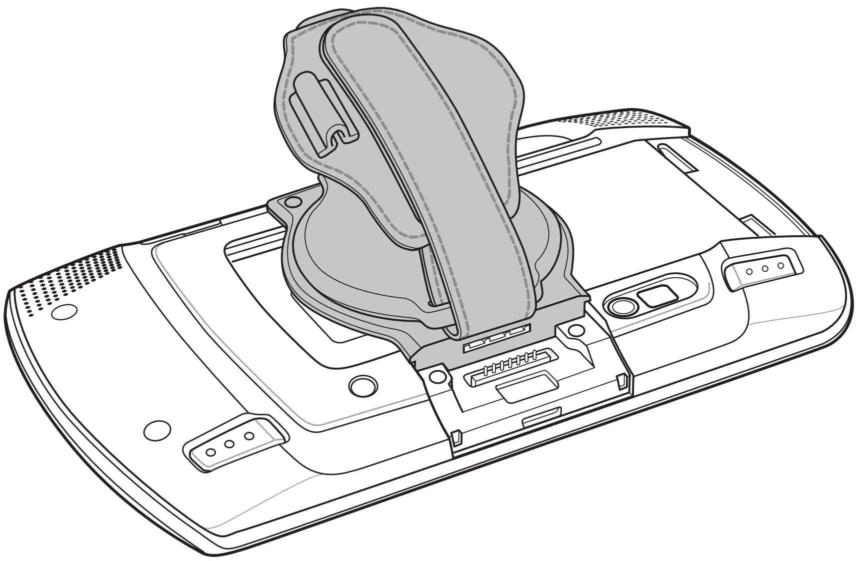
Figure 23: Remove Filler Plate



7 Align the rectangle opening on the handstrap with the tab in the module mounting area.

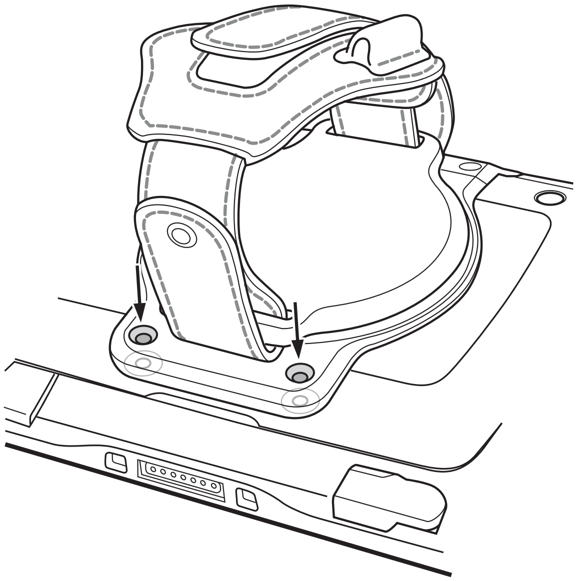
8 Place the handstrap onto the back of the ET1.

Figure 24: Align Handstrap



9 Align the two screw holes on the handstrap with the screw holes on the back of the ET1.

Figure 25: Align Screw Holes

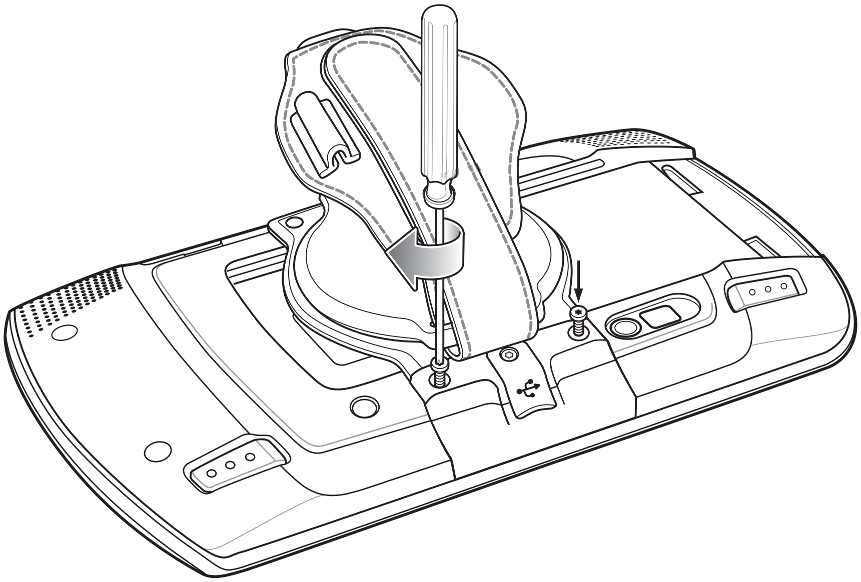


10 Using a Torx T8 screwdriver, secure the bottom of the handstrap to the ET1 using the two screws provided with the handstrap.

11 Replace the expansion module into the mounting area. Do not replace the filler plate.

12 Using a Torx T8 screwdriver, secure the expansion module to the ET1 using the two screws.

Figure 26: Secure Expansion Module



13 Install the battery.

CS3070 Bluetooth Scanner

The Human Interface Device (HID) Emulation Bluetooth profile is a lightweight wrapper of the HID protocol defined for USB. Data transmitted from the Bluetooth scanner appears as keyboard entries on the ET1.

Note:

Wedge data appears within whichever application has input focus.

Pairing the CS3070 with the ET1 requires entering a pairing PIN on both the CS3070 and the ET1. To enter the PIN on the CS3070, use the Numeric Bar Codes. See *CS3070 Numeric Bar Codes for PIN Entry on page 41*. For the ET1, use the keyboard to enter the PIN.

Refer to the *CS3000 Series Scanner Product Reference Guide* for detailed information for configuring the CS3070.

Pairing with the CS3070

Procedure:

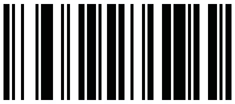
1 Press the CS3070 scan button (+) to wake the scanner.

2 Press and hold the Bluetooth button (round button) for five seconds. The scanner beeps and the Bluetooth button starts blinking quickly to indicate that the scanner is discoverable by the host.

Note:

HID is the default profile for the CS3070. If this was changed, scan for bar code below.

Figure 27: Bluetooth Keyboard Emulation (HID) Bar Code



3 Touch ⊞.

4 On the ET1, touch ⚙.

5 Touch ᛒ **Bluetooth**.

6 Slide the switch to the **ON** position.

7 The CS3070 appears in the **Available Devices** list, indicated by its model name and serial number.

8 Select the CS3070 from the list.
A dialog box displays the PIN to enter on the CS3070.

9 With the CS3070, scan the PIN using the Numeric Bar Codes. See *CS3070 Numeric Bar Codes for PIN Entry on page 41* and then scan **Enter**. The scanner beeps to indicate it has paired with the device, and the device displays **Connected** below the CS3070 device name.

Verifying the Bluetooth Connection

Procedure:

1 Tap in any text input field.

2 Scan a bar code. The bar code contents appear in the text entry field.

Unpairing the CS3070

Unpair devices when they are no longer used with the ET1.

Procedure:

1 On the ET1, touch ⚙.

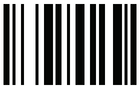
2 Touch ᛒ **Bluetooth**.

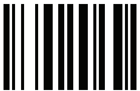
3 Touch ☰ next to CS3070.

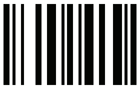
4 Touch **Unpair**.

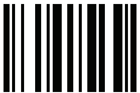
CS3070 Numeric Bar Codes for PIN Entry

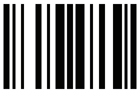
Use the following bar codes for pin entry for Bluetooth connection.

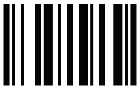

0

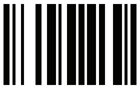

1

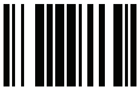

2

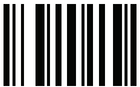

3

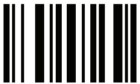

4

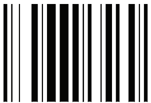

5


6


7


8


9


Enter

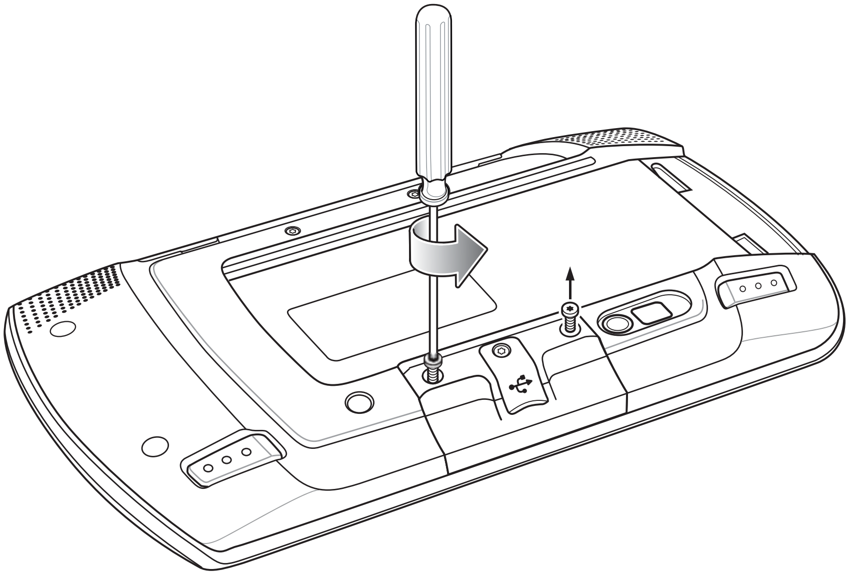
Installing an Expansion Module

To install the Scan Module or Scan/MSR Module:

Procedure:

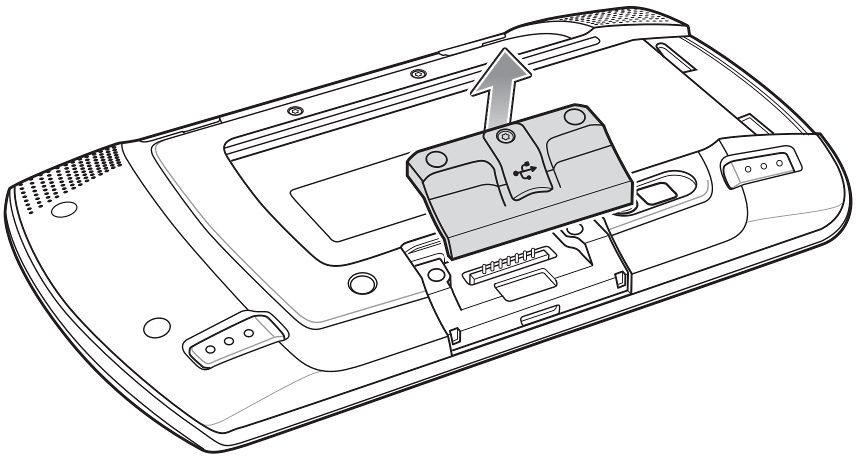
1. Power off the ET1.
2. Remove the battery.
3. If the handstrap is installed, rotate the handstrap to access the expansion module screws.
4. Remove the two screws using a T8 Torx screwdriver.

Figure 28: Remove Screws Securing Module



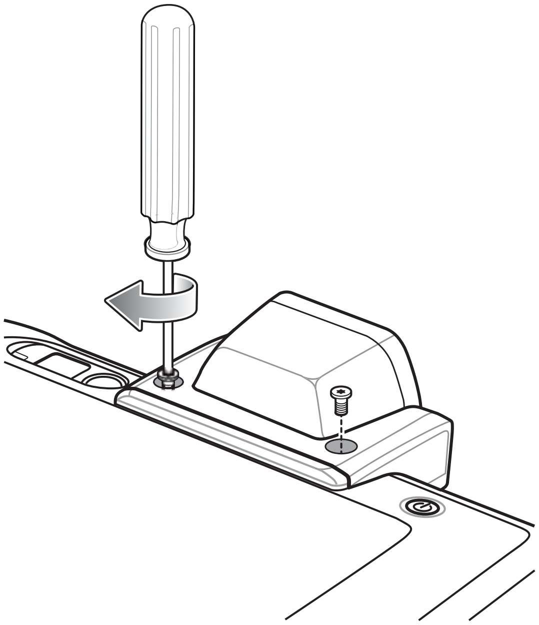
5. Remove the existing module.
6. Install the new module.

Figure 29: Remove Expansion Module



7. Secure the two screws using a T8 Torx screwdriver.

Figure 30: Secure Module



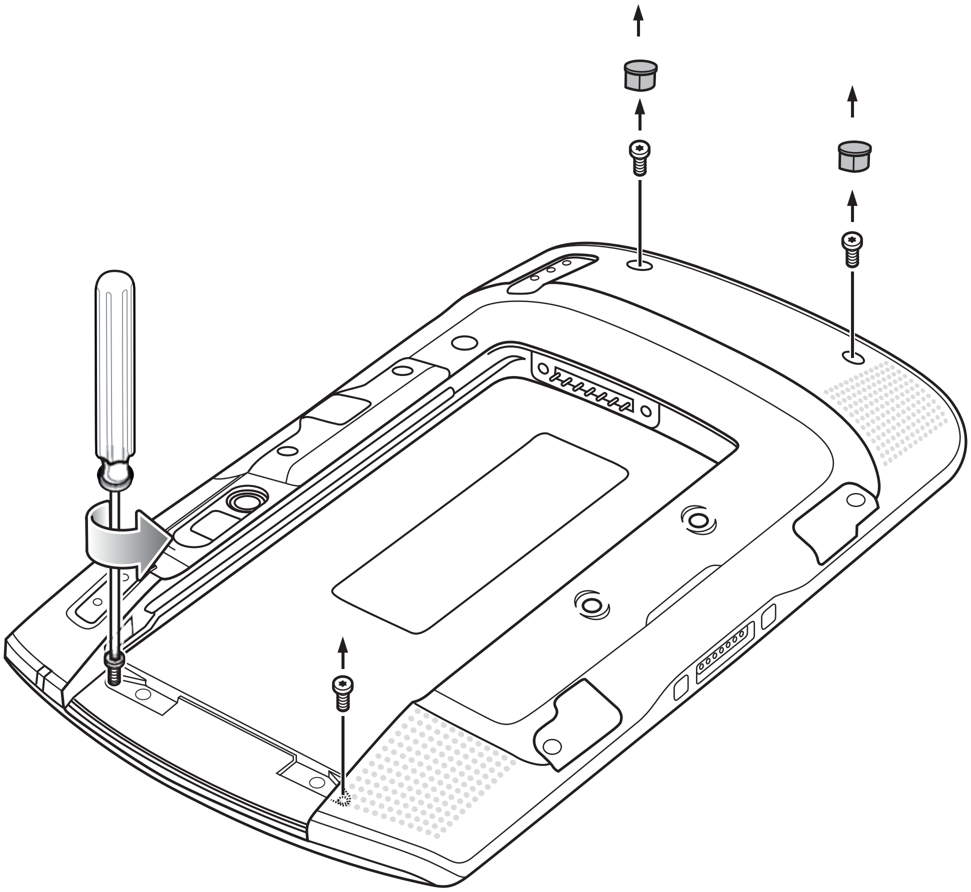
8 Replace the battery.

Replacing the Bezel

Procedure:

1 Press the Power button until the Device options menu appears.
2 Touch Power off.
3 Remove the battery.
4 Place the ET1 face down on a table.
5 Remove two plugs covering the screws.
6 Using a Torx T6 screwdriver, remove four Torx screws.

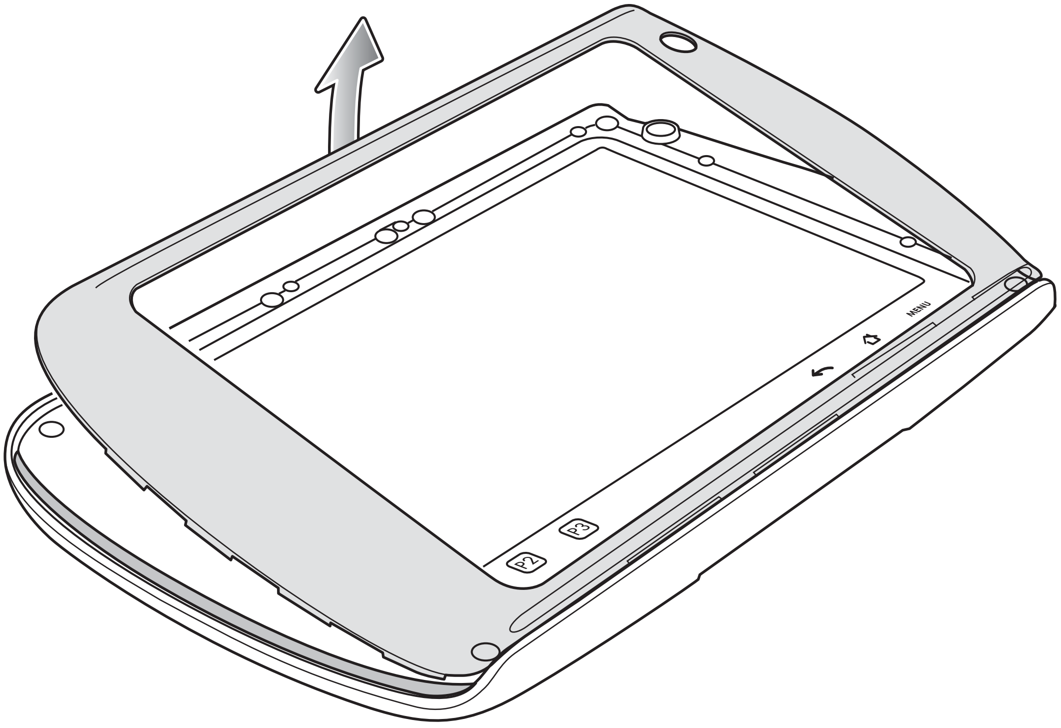
Figure 31: Remove Screws



7 Using tool, pry bezel from top of ET1.

8 Lift the bezel from ET1.

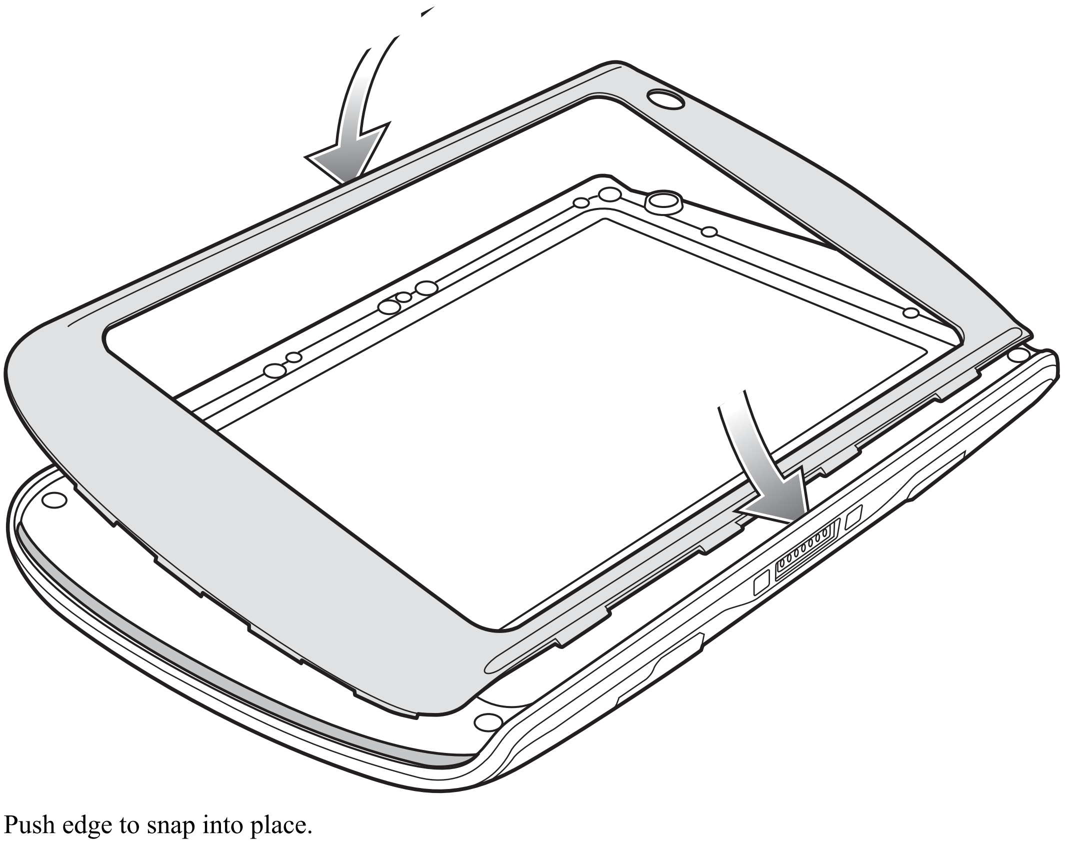
Figure 32: Lift Bezel



9 Align new bezel.

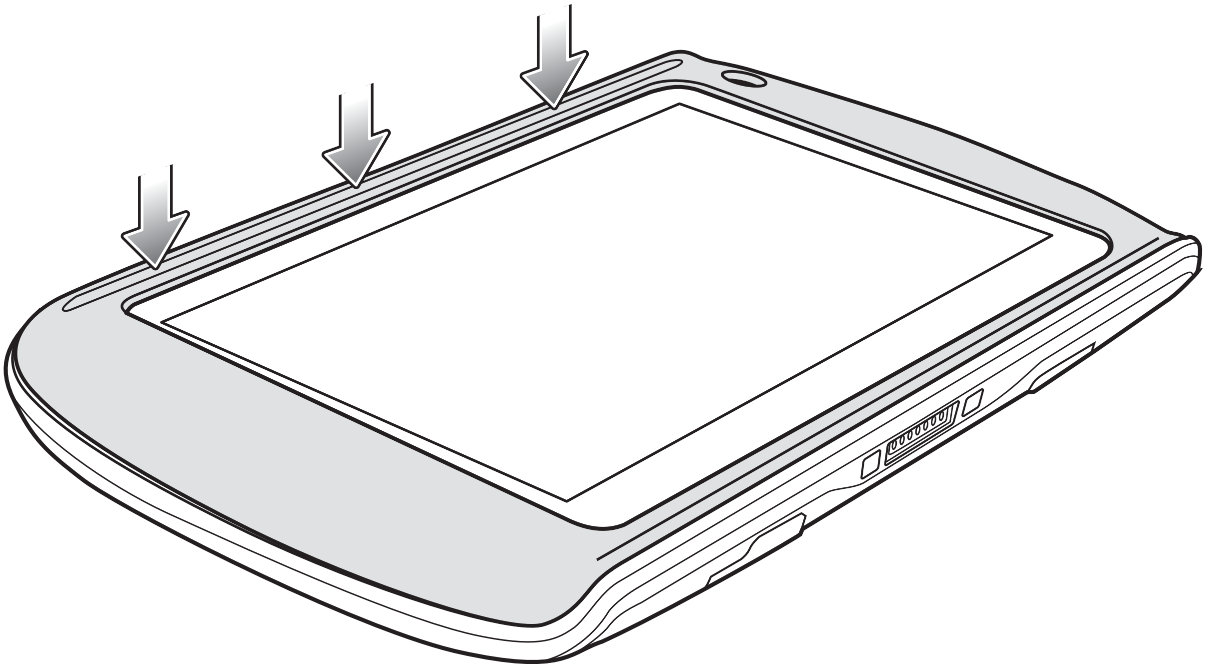
10 Place top down.

Figure 33: Align Bezel



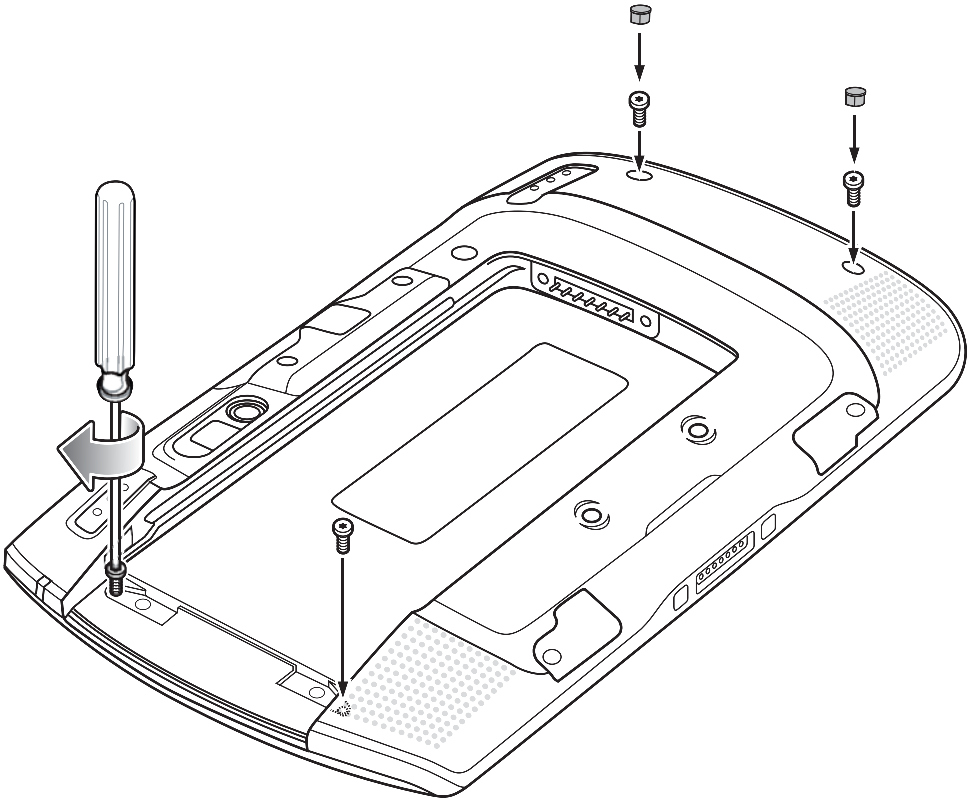
11 Push edge to snap into place.

Figure 34: Press Bezel Down



12 Using a Torx T6 screwdriver, secure bezel to ET1 using four screws.

Figure 35: Secure Bezel Using Screws



13 Replace two screw plugs.

14 Replace the battery.

Installing the Protective Rubber Bezel

Procedure:

1 Press the Power button until the Device options menu appears.

2 Touch Power off.

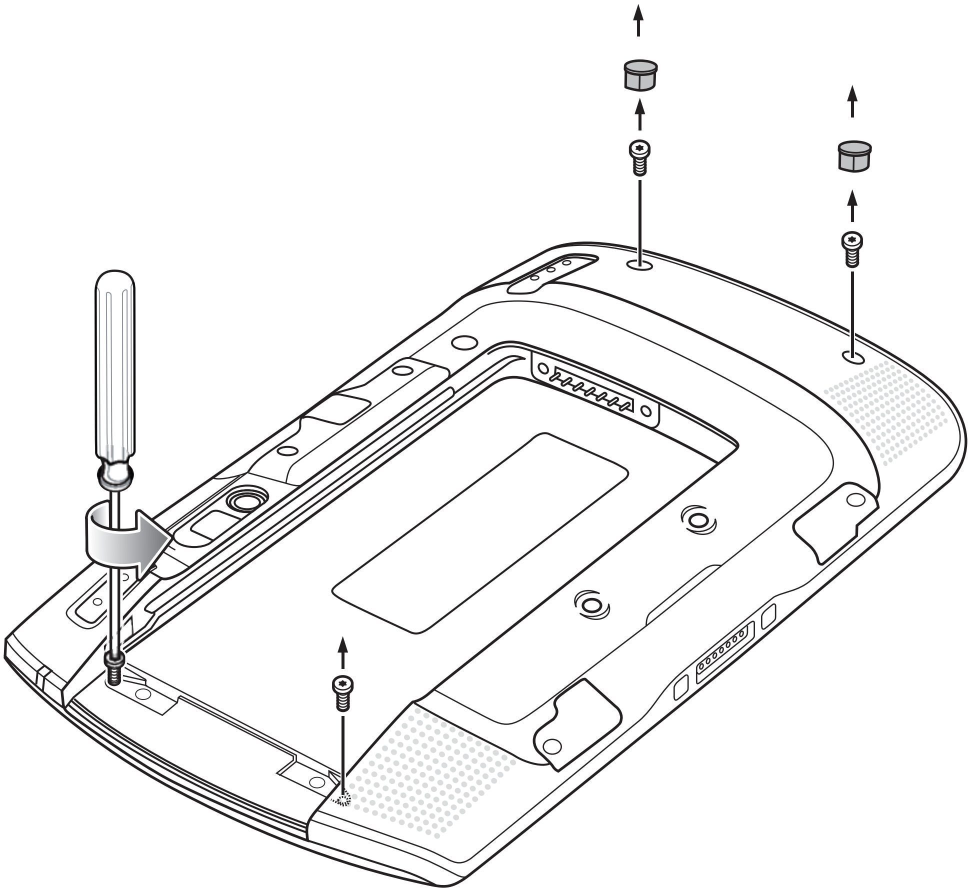
3 Remove the battery.

4 Place the ET1 face down on a table.

5 Remove two plugs covering the screws.

6 Using a Torx T6 screwdriver, remove four Torx screws.

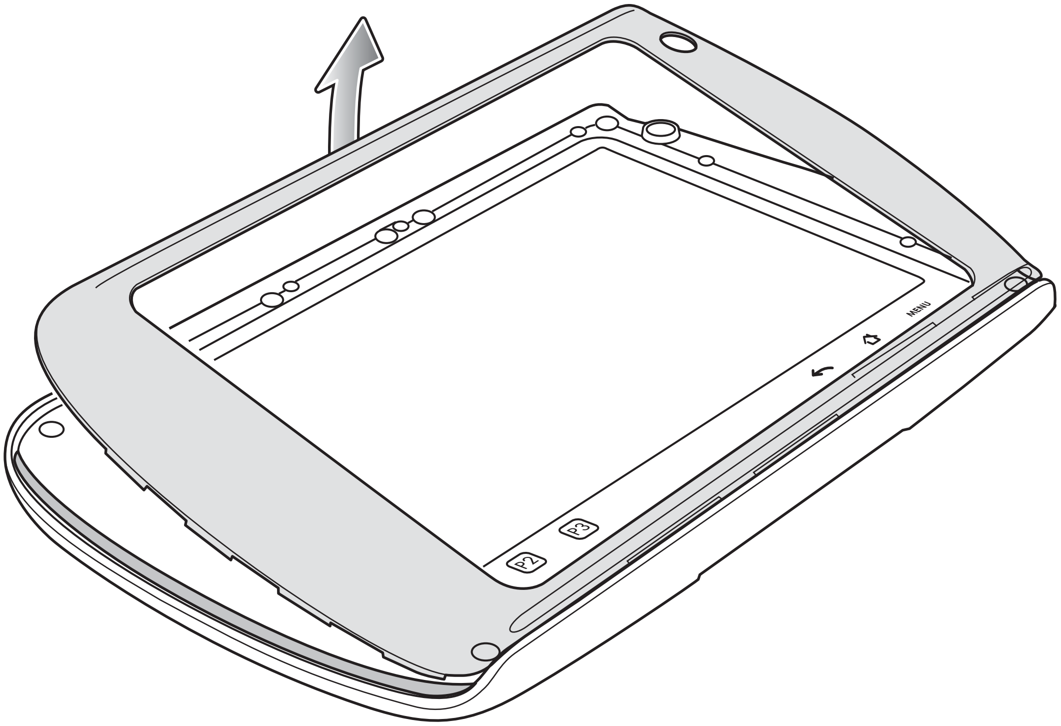
Figure 36: Remove Screws



7 Using tool, pry bezel from top of ET1.

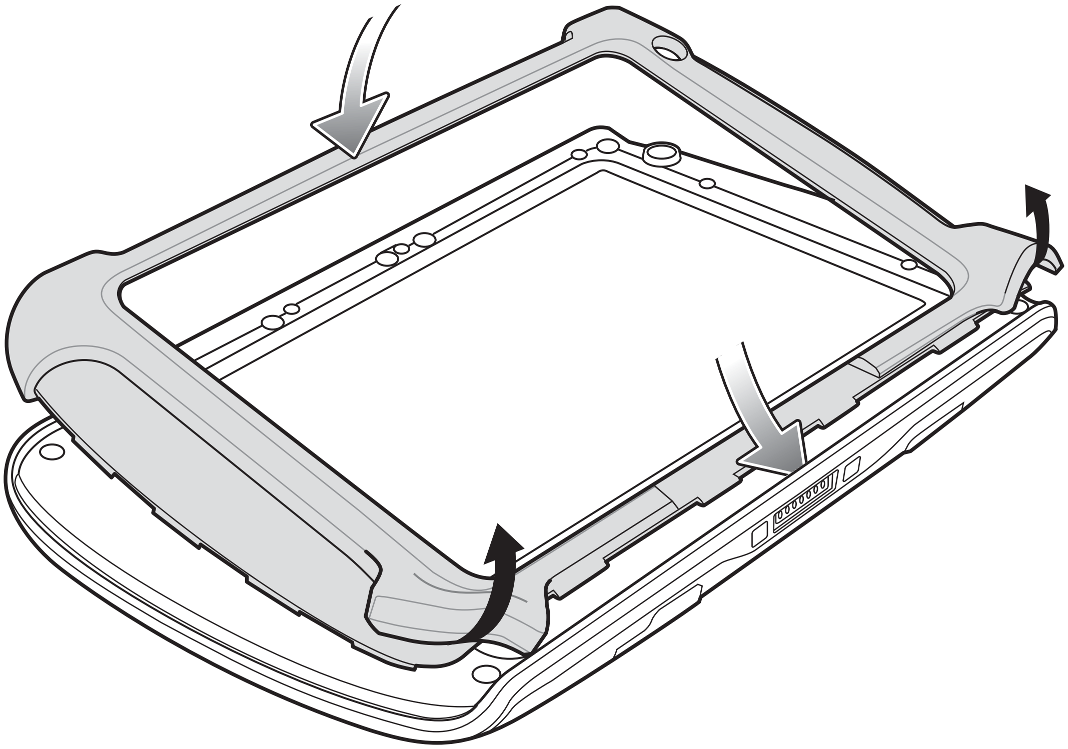
8 Lift bezel from ET1.

Figure 37: Remove Bezel



9 Lift the bottom edges of the Protective Rubber Bezel and align tab with slot is housing.

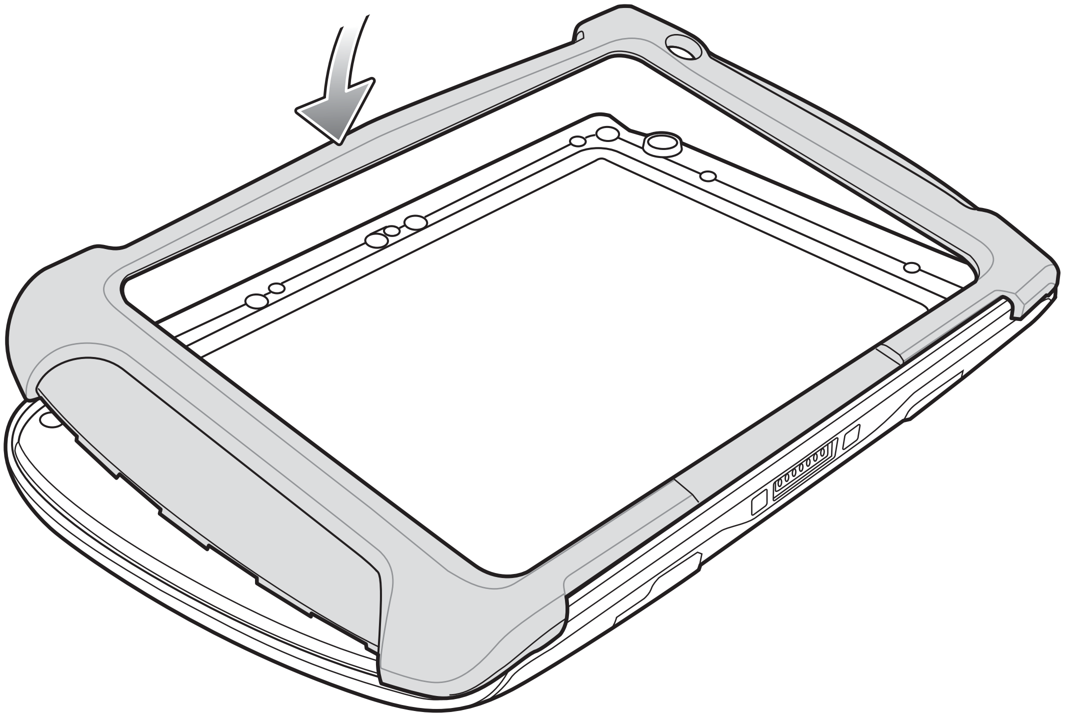
Figure 38: Align Protective Rubber Bezel



10 Place the tabs into the housing and release the bottom edges.

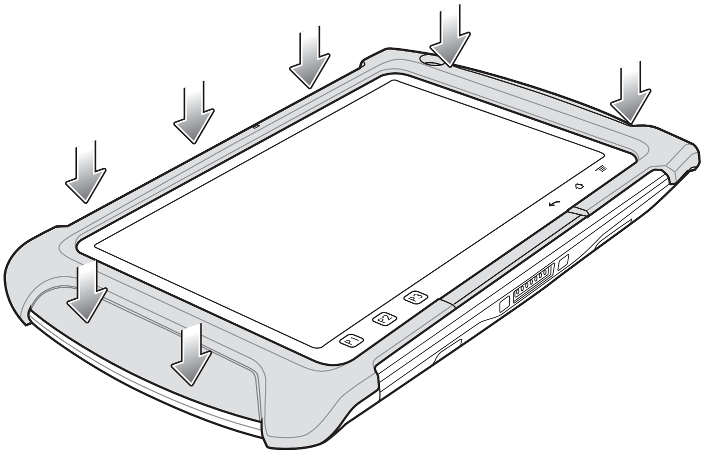
11 Push down on edges to snap into place.

Figure 39: Lay Bezel Down



12 Press down on the bezel to snap into place.

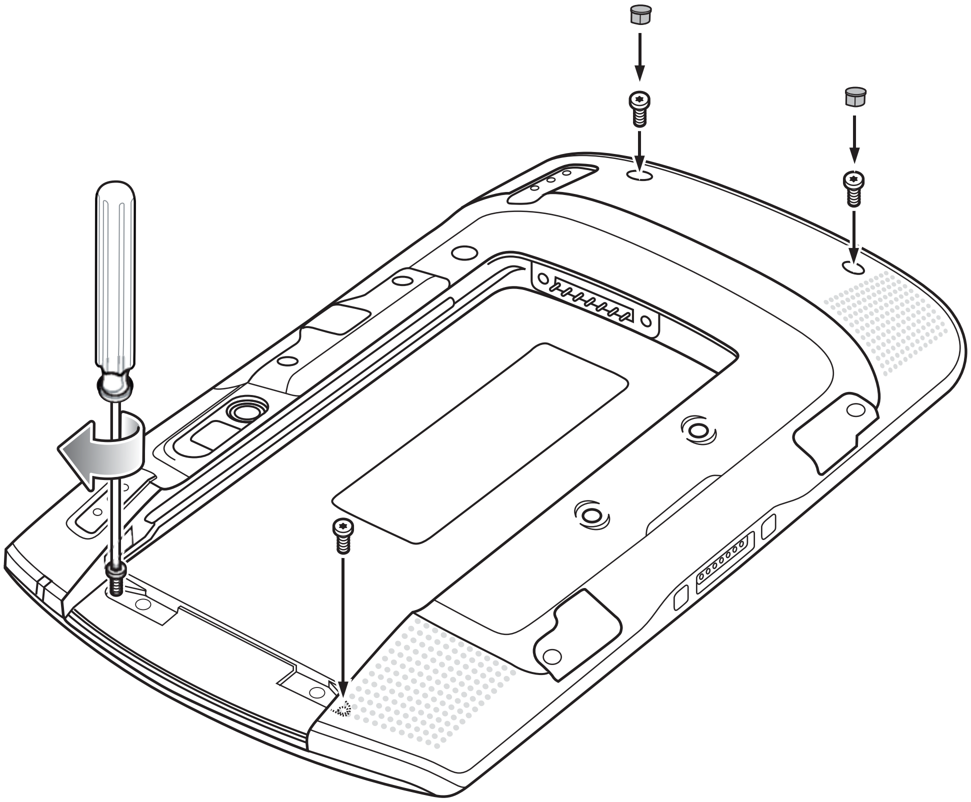
Figure 40: Press Down on Bezel



13 Turn the ET1 over

14 Using a Torx T6 screwdriver, secure bezel to ET1 using four screws

Figure 41: Secure Bezel Using Screws



15 Replace two screw plugs.

16 Replace the battery.

Chapter 3

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 ET1 to a host computer using the USB/Charge Cable or Single-slot USB Docking Cradle to transfer files between the ET1 and the host computer.

Caution:

When connecting the ET1 to a host computer and mounting its microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Procedure:

1. Setup the ET1 and either the USB/Charge Cable or the Single-slot USB Docking Cradle. See *Accessories on page 29* for setup information.
2. Place the ET1 into the cable cup or the cradle.
   Connected as a media device or **Connected as a camera** appears on the Status bar.
3. If **Connected as a camera** appears, pull down the Notification shade and touch **Connected as a camera** and then touch **Media device (MTP)**.
4. **Caution:** Ensure that all applications are not running. Loss of data may occur.

   On the host computer, open a file explorer application.
5. **Note:** While USB storage is in use, access to the microSD card is disabled on the ET1.

   Locate the ET1 as a portable device and open to view contents.
6. Copy or delete files as required.

Disconnect from the Host Computer

Caution:

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

Procedure:

1. On the host computer, unmount the microSD card.
2. Remove the ET1 from the cradle or cable.

Chapter 4

DataWedge Configuration

DataWedge is an application that reads data, processes the data and sends the data to an application.

Basic Scanning

Scanning can be performed using either the Scan Module, Scan/MSR Module or the rear-facing camera.

Using the Scan Module

To capture bar code data:

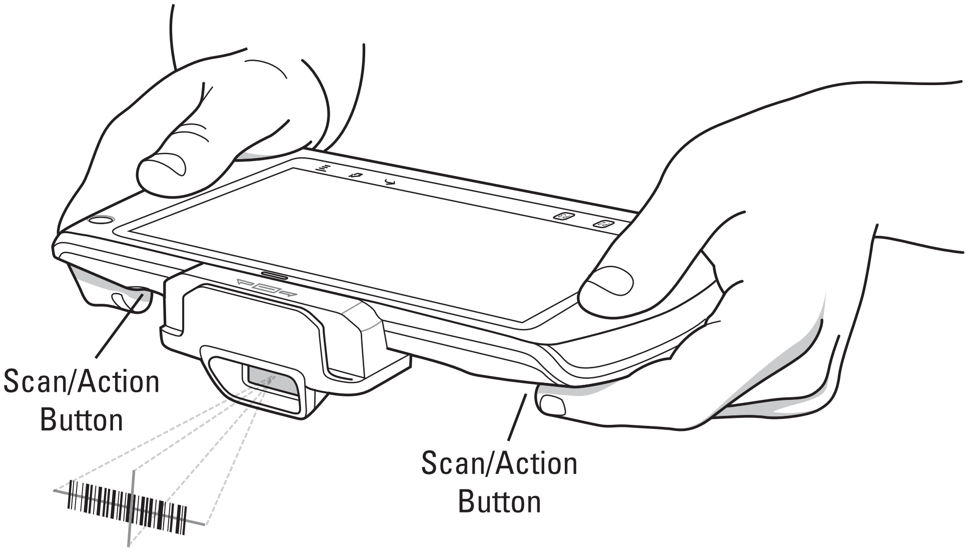
Procedure:

1 Ensure that an application is open on the ET1 and a text field is in focus (text cursor in text field).

2 Aim the Scan Module exit window at a bar code.

3 Press and hold either Scan/Action button. 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 Decode LED lights red to indicate that data capture is in process.

Figure 42: Data Capture with Scan Module or Scan/MSR Module



4 The Decode LED lights green, a beep sounds and the ET1 vibrates, by default, to indicate the bar code was decoded successfully. The captured data appears in the text field.

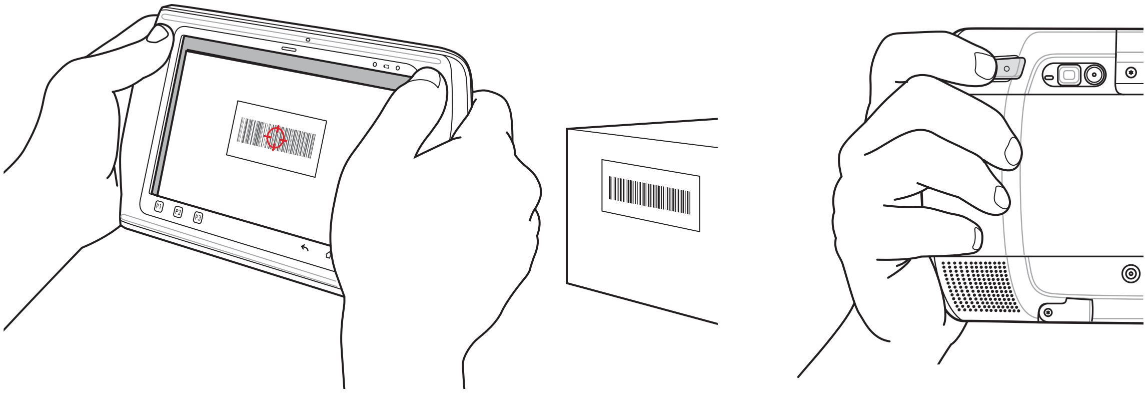
Using the Camera

To capture bar code data:

Procedure:

1. Ensure that an application is open on the ET1 and a text field is in focus (text cursor in text field).
2. Aim the Scan Module exit window at a bar code.
3. Press and hold either Scan/Action button. 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 Decode LED lights red to indicate that data capture is in process.

Figure 43: Data Capture with Rear Facing Camera



4. Move the ET1 until the bar code is centered.
5. The Decode LED lights green, a beep sounds and the ET1 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.
- **MSR Input Plug-in** – The Magnetic Stripe Reader (MSR) Input Plug-in is responsible for reading data from an MSR. Raw data read from the MSR can be processed or formatted using Process Plug-ins as required. **DataWedge** has built-in feedback functionality for the MSR 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.

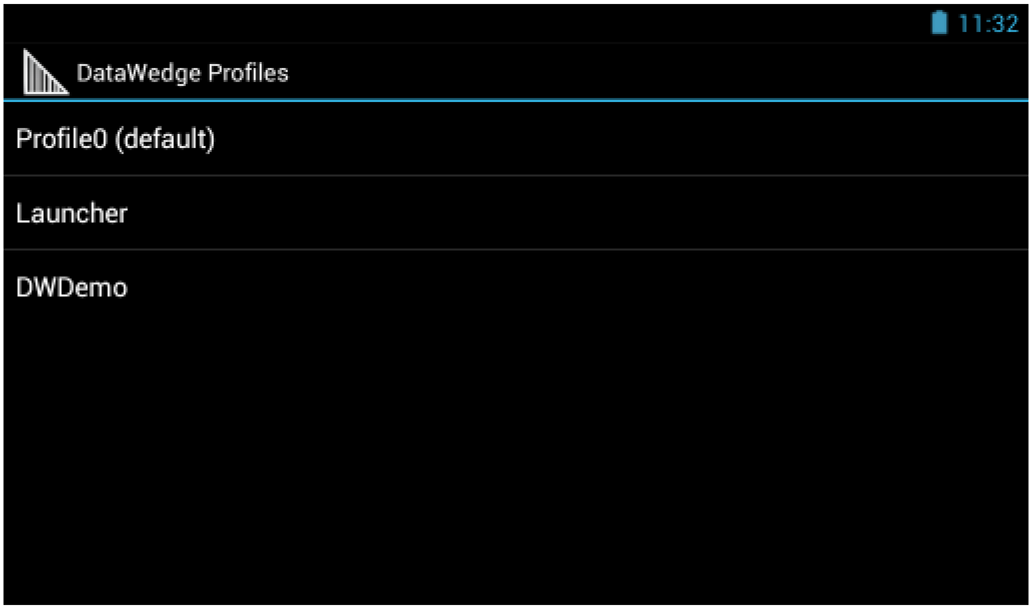
Profiles Screen

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.

Figure 44: DataWedge Profiles Screen



11:32

DataWedge Profiles

Profile0 (default)

Launcher

DWDemo

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 45: Profile Context Menu

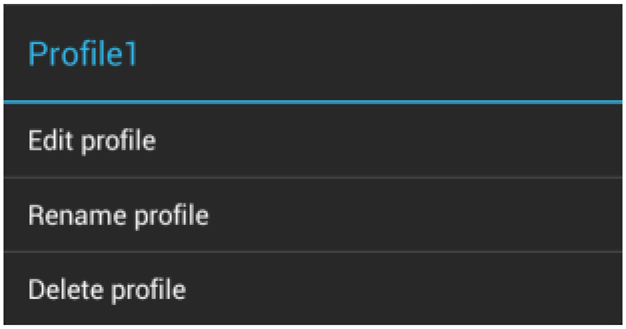
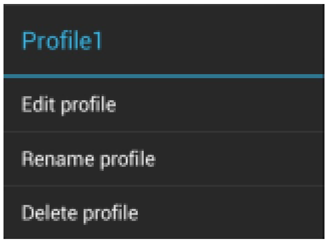


Figure 46: Profile Context Menu

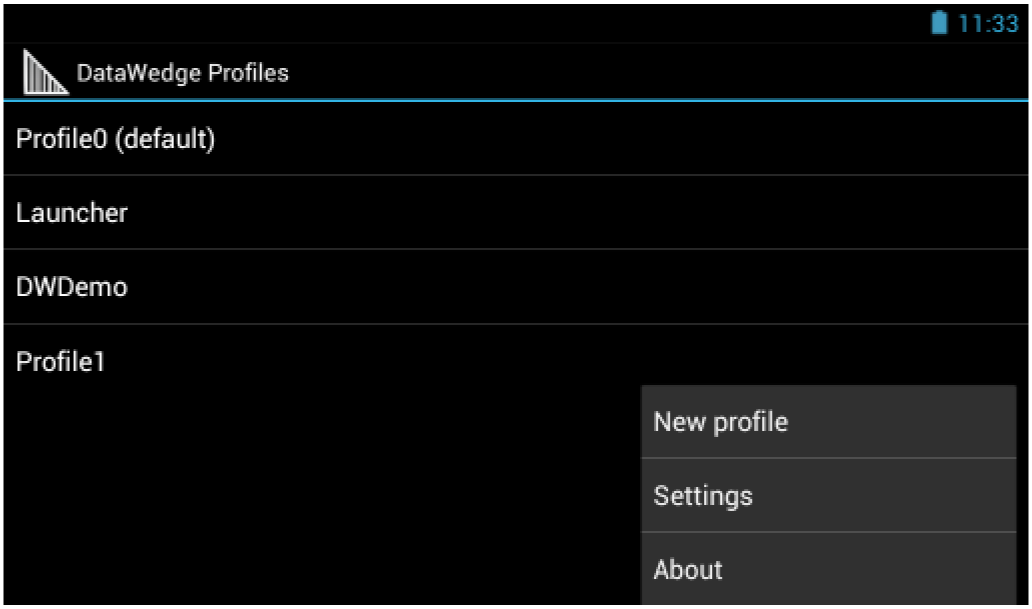


The profile context menu allows the profile to be edited (same as just tapping on a profile), renamed or deleted.

Options Menu

Touch ☰ to open the options menu.

Figure 47: DataWedge Options Menu



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

Disabling DataWedge

Procedure:

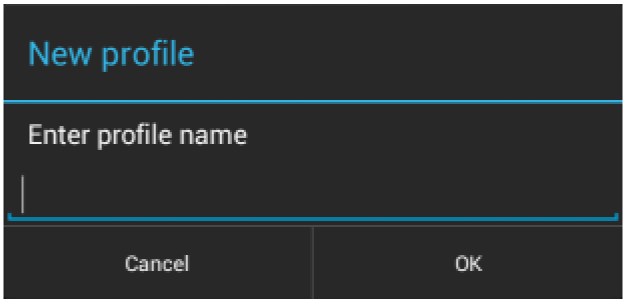
1. Touch ⊞.
2. Touch ▙.
3. Touch ☰.
4. Touch **Settings**.
5. Touch **DataWedge enabled**.
   The blue check disappears from the checkbox indicating that DataWedge is disabled.

Creating a New Profile

Procedure:

1. Touch ⊞.
2. Touch ▙.
3. Touch ☰.
4. Touch **New profile**.
5. 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).

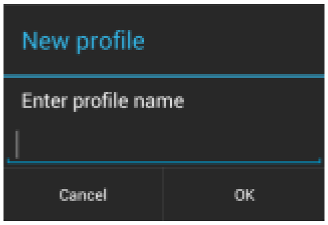
   Figure 48: New Profile Name Dialog Box

   New profile

   Enter profile name

   Figure 49: New Profile Name Dialog Box

   New profile

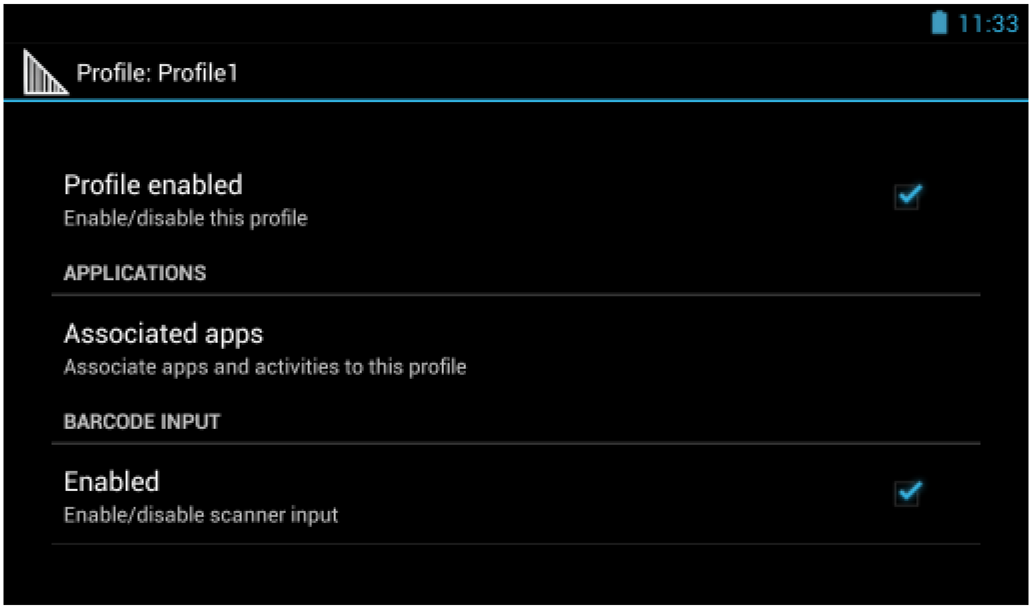
   Enter profile name

6. Touch **OK**.
   The new profile name appears in the **DataWedge profile** screen.

Profile Configuration

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

Figure 50: Profile Configuration Screen



11:33

Profile: Profile1

Profile enabled ☑
Enable/disable this profile

APPLICATIONS

Associated apps
Associate apps and activities to this profile

BARCODE INPUT

Enabled ☑
Enable/disable scanner input

The configuration screen lists the following sections:

- Profile enabled
- Applications
- Barcode Input
- MSR Input
- Keystroke output
- Intent Output
- IP Output.

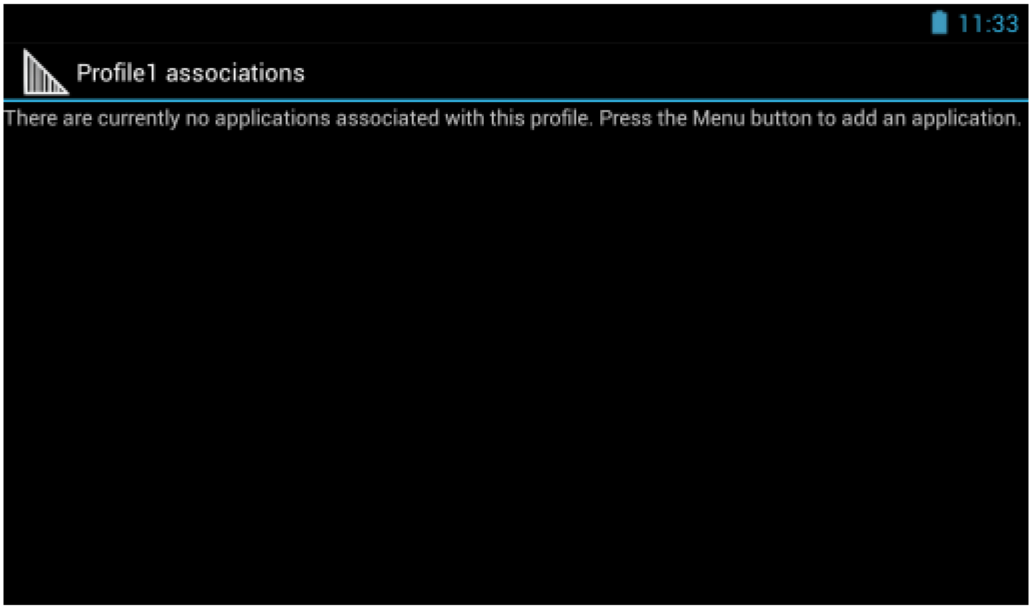
Associating Applications

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

Procedure:

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

Figure 51: Associated Apps Screen

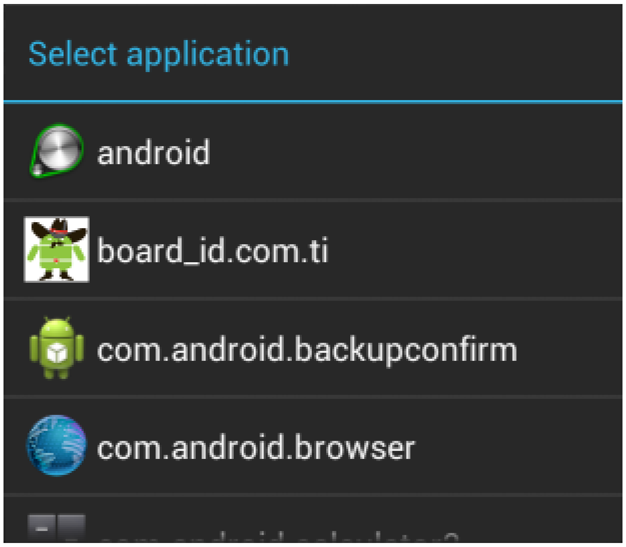


There are currently no applications associated with this profile. Press the Menu button to add an application.

2 Touch ≡.

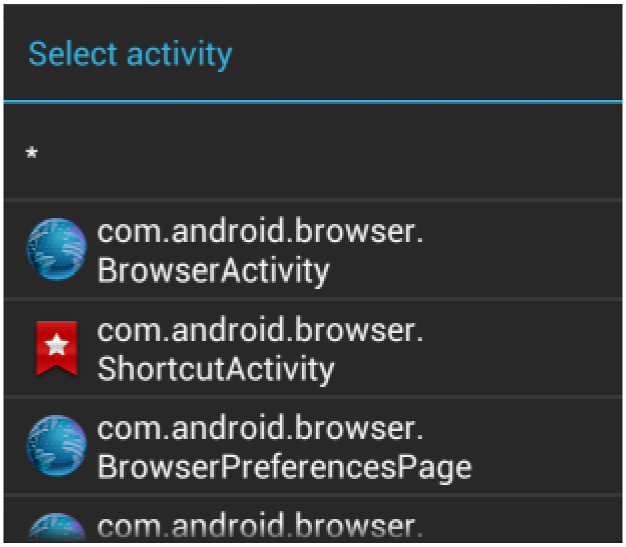
3 Touch **New app/activity**.

Figure 52: Select Application Menu



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

Figure 53: Select Activity Menu



Select activity

*

com.android.browser.
BrowserActivity

com.android.browser.
ShortcutActivity

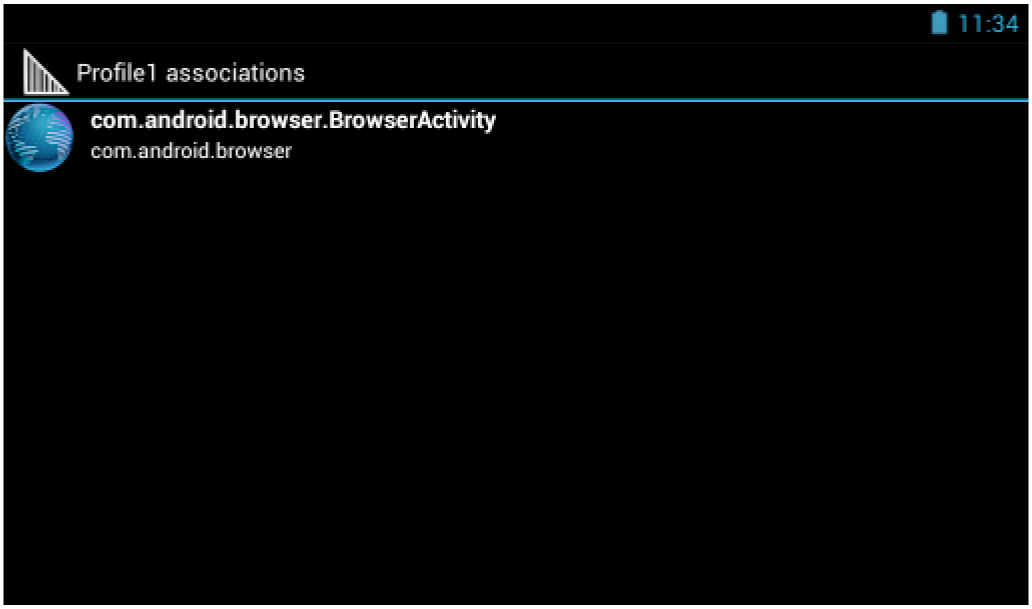
com.android.browser.
BrowserPreferencesPage

com.android.browser.

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

6 Touch ↩.

Figure 54: Selected Application/Activity



11:34

Profile1 associations

com.android.browser.BrowserActivity
com.android.browser

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 determines the best scanning device. If a Scan Module or Scan/MSR Module is installed on the ET1, then the **2D imager** is selected. Otherwise the **camera** is selected.
- **Camera scanner** - Scanning is performed with the rear-facing camera.
- **2D Imager** - Scanning is performed using the installed Scan or Scan/MSR module.

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:

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	USPostnet	USPlanet
UK Postal	Japanese Postal	Australian Postal
Canadian Postal	Dutch Postal	US4state FICS
Codabar*	MSI	Code 93
Trioptic 39	Discrete 2 of 5	Chinese 2 of 5
Korean 3 of 5	Code 11	TLC 39
Matrix 2 of 5	UPC-E1	

Touch ↩ to return to the previous screen.

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 66* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 66* 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.
- **Code39**
  - **Length1** - Use to set decode lengths (default - 0). See *Decode Lengths on page 66* for more information.
  - **Length2** - Use to set decode lengths 4 (default - 55). See *Decode Lengths on page 66* 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).

- **Interleaved 2 of 5**
  - **Length1** - Use to set decode lengths (default - 14). See *Decode Lengths on page 66* for more information.
  - **Length2** - Use to set decode lengths (default - 10). See *Decode Lengths on page 66* 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).
- **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 66* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 66* 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 66* for more information.
  - **Length 2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 66* 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 66* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 66* 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 66* for more information.
  - **Length2** - Use to set decode lengths (default - 14). See *Decode Lengths on page 66* 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 66* for more information.
  - **Length2** - Use to set decode lengths (default - 55). See *Decode Lengths on page 66* 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).
- **Matrix 2 of 5**
  - **Length1** - Use to set decode lengths (default - 10). See *Decode Lengths on page 66* for more information.
  - **Length2** - Use to set decode lengths (default - 0). See *Decode Lengths on page 66* 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 barcode 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.
- **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.

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).
  - **Centered** - Enables the Picklist mode so that only the bar code in the center of the image is decoded. This is most useful when used in conjunction with the static and dynamic reticle viewfinder modes. Note: This mode is only valid for decoder modules that supports a viewfinder. If one tries to set this for a unsupported decoder then the device would issue an error. (Camera scanner only).
  - **Reticle** - Enables the Picklist mode so that only the bar code that is directly under the cross-hair (reticle) is decoded. This is useful when used in conjunction with the static and dynamic reticle viewfinder modes. (Scan Module Only)

- **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 (Scan Module Only).
  - **Disable** - Disables the LCD mode (default).
  - **Enable** - Enables LCD mode.

  Note: When using the LCD mode, a degradation in performance may be observed and the aiming crosshair may blink until the bar code is decoded.
- **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).
- **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.
- **Viewfinder Mode** - Configures the Viewfinder modes supported for camera scanning.
  - **Viewfinder Enabled** - Enables only the viewfinder.
  - **Static Reticle** - Enables the viewfinder and a red reticle in the center of the screen which helps selecting the bar code (default).

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.
- **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).

MSR Input

Use **MSR Input** options to configure the MSR 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.

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 or MSR 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 74* 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 74* 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.motorolasolutions.emdk.datawedge.label_type”;
  - String contains the label type of the bar code.
- String DATA_STRING_TAG = “com.motorolasolutions.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.motorolasolutions.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.

The MSR 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 MSR_DATA_TAG = “com.motorolasolutions.emdk.datawedge.msr_data”;
  - String contains the output data as a String. The data from the MSR tracks is concatenated and sent out as a single string.
- String MSR_TRACK1_TAG = “com.motorolasolutions.emdk.datawedge.msr_track1”;
  - MSR track 1 data is returned as a byte array.
- String MSR_TRACK2_TAG = “com.motorolasolutions.emdk.datawedge.msr_track2”;
  - MSR track 2 data is returned as a byte array.
- String MSR_TRACK3_TAG = “com.motorolasolutions.emdk.datawedge.msr_track3”;
  - MSR track 3 data is returned as a byte array.
- String MSR_TRACK1_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track1_status”;
  - MSR track 1 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK2_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track2_status”;
  - MSR track 2 decode status as an Integer where 0 indicates a successful decode.
- String MSR_TRACK3_STATUS_TAG = “com.motorolasolutions.emdk.datawedge.msr_track3_status”;
  - MSR track 3 decode status as an Integer where 0 indicates a successful decode.

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.

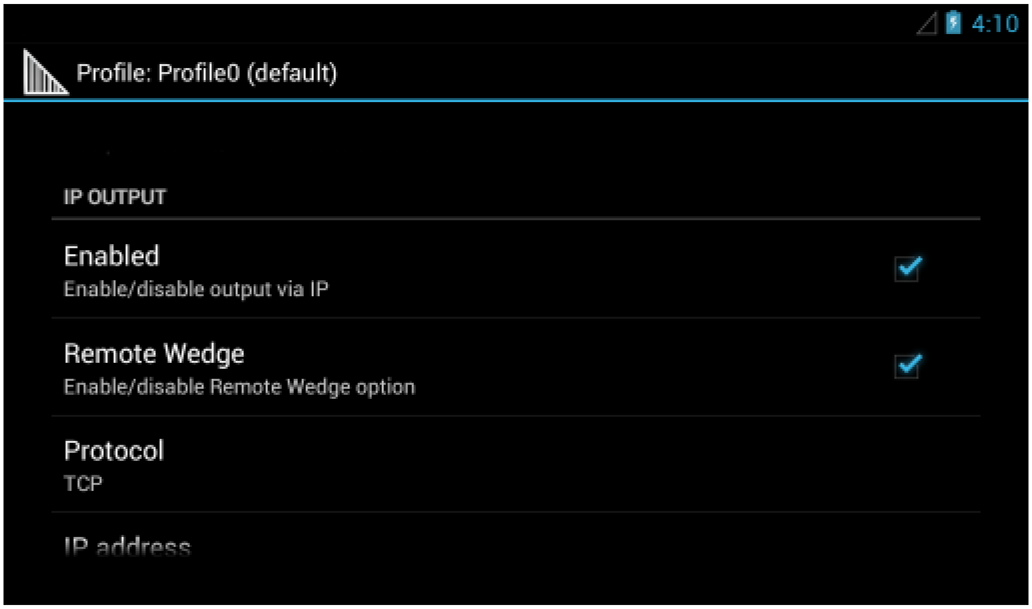
- **Enabled** - Enables or disables this plug-in. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Remote Wedge** - Enable or disable the Remote Wedge option (default - enabled). Remote Wedge is used with the IPWedge application.
- **Protocol** - Select the protocol 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 74* for more information.
- **Basic data formatting** - Allows configuration of any data formatting for the related Output Plug-in. When the plug-in is disabled any data is passed on without modification.
  - **Enabled** - Enables or disables Basic Data Formatting. A check in the checkbox indicates that it is enabled (default - enabled).
  - **Prefix to data** - Add characters to the beginning of the data when sent.
  - **Suffix to data** - Add characters to the end of the data when sent.

- **Send data** - Set to transfer the captured data to the foreground application. Disabling this option prevents the actual data from being transmitted. However, the prefix and suffix strings, if present, are still transmitted even when this option is disabled (default - enabled).
- **Send as hex** - Set to send the data in hexadecimal format. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Send TAB key** - Set to append a tab character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).
- **Send ENTER key** - Set to append an Enter character to the end of the processed data. A check in the checkbox indicates that the plug-in is enabled (default - disabled).

Usage

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

Figure 55: IP Output Screen



IP OUTPUT

Enabled ☑
Enable/disable output via IP

Remote Wedge ☑
Enable/disable Remote Wedge option

Protocol
TCP

IP address

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:

Procedure:

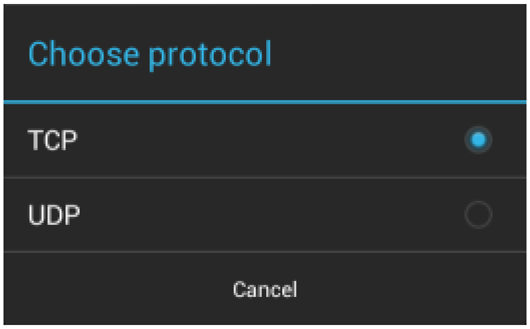
1 In **IP Output**, touch **Enabled**.
A check appears in the checkbox.

2 Ensure **Remote Wedge** option is enabled.

3 Touch **Protocol**.

4 In the **Choose protocol** dialog box, touch the same protocol selected for the **IPWedge** computer application. (TCP is the default).

Figure 56: Protocol Selection



Choose protocol

TCP ●

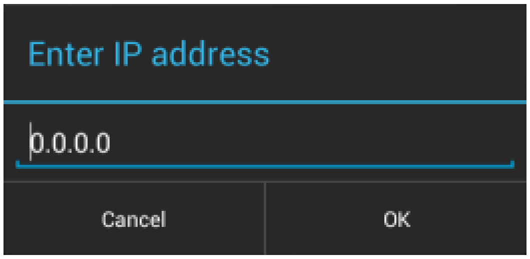
UDP ○

Cancel

5 Touch **IP Address**.

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

Figure 57: IP Address Entry



Enter IP address

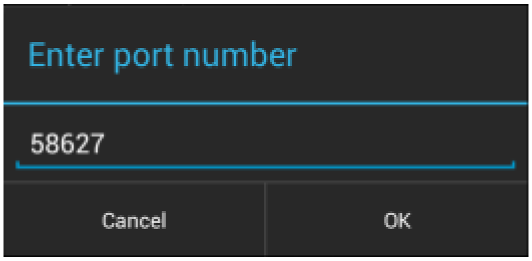
0.0.0.0

Cancel | OK

7 Touch **Port**.

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

Figure 58: Port Number Entry



Enter port number

58627

Cancel | OK

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:

Procedure:

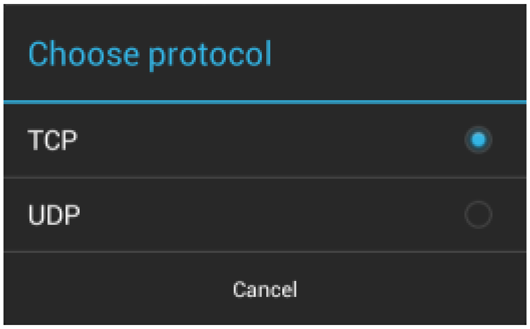
1 In **IP Output**, touch **Enabled**.
A check appears in the checkbox.

2 Ensure **Remote Wedge** option is disabled.

3 Touch **Protocol**.

4 In the **Choose protocol** dialog box, touch the same protocol selected in the client application. (TCP is the default).

Figure 59: Protocol Selection



Choose protocol

TCP ●

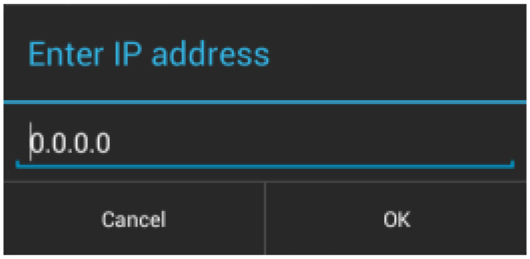
UDP ○

Cancel

5 Touch **IP Address**.

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

Figure 60: IP Address Entry



Enter IP address

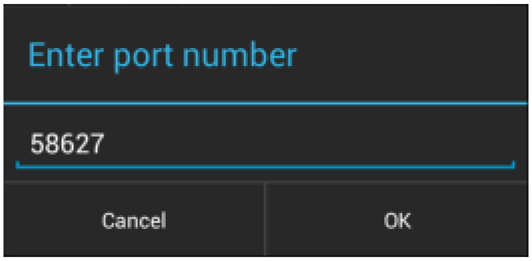
0.0.0.0

Cancel | OK

7 Touch **Port**.

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

Figure 61: Port Number Entry



Enter port number

58627

Cancel | OK

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

Generating Advanced Data Formatting Rules

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

- Rules - The ADF process plug-in consists of one or more rules. DataWedge formats the output data according to the first matching rule. A rule is a combination of criteria and a set of actions to be performed, upon fulfillment of the criteria set in the rule.
- Criteria - Criteria can be set according to Input plug-in, symbology, matching string within the data (at the specified position) and/or data length. Received data must match the defined criteria in order for the data to be processed.

- Actions - A set of procedures defined to format data. There are four types of actions which are for formatting cursor movement, data modification, data sending and delay specifications. An action can be defined to send the first number of characters to the Output plug-in, pad the output data with spaces or zeros, remove spaces in data, etc.

Configuring ADF Plug-in

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

Procedure:

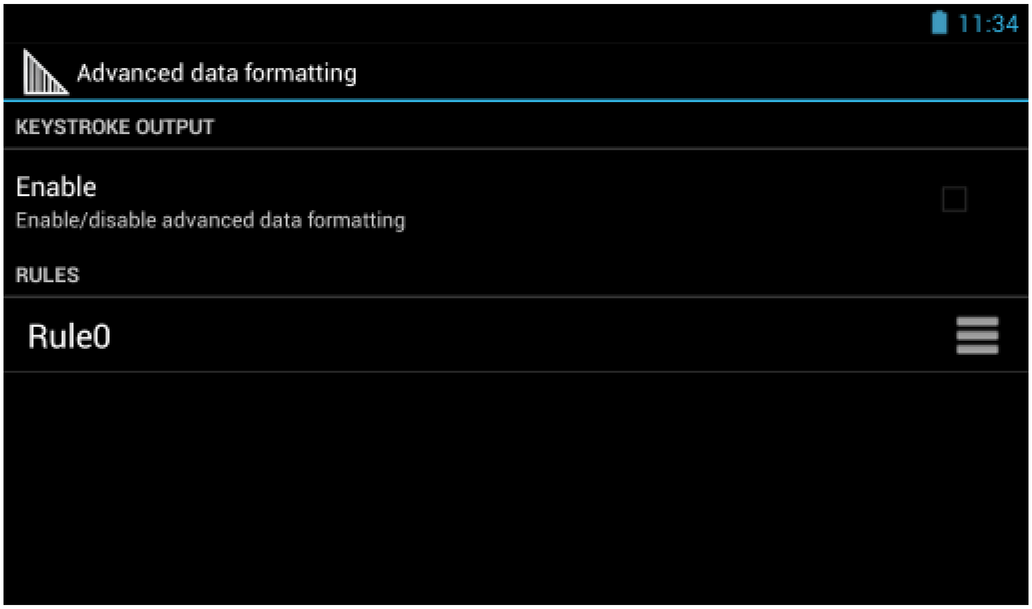
1 Touch ⊞.

2 Touch .

3 Touch a DataWedge profile.

4 In **Keystroke Output**, touch **Advanced data formatting**.

Figure 62: Advanced Data Formatting Screen



11:34

Advanced data formatting

KEYSTROKE OUTPUT

Enable □
Enable/disable advanced data formatting

RULES

Rule0 ≡

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

Creating a Rule

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

Procedure:

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**.

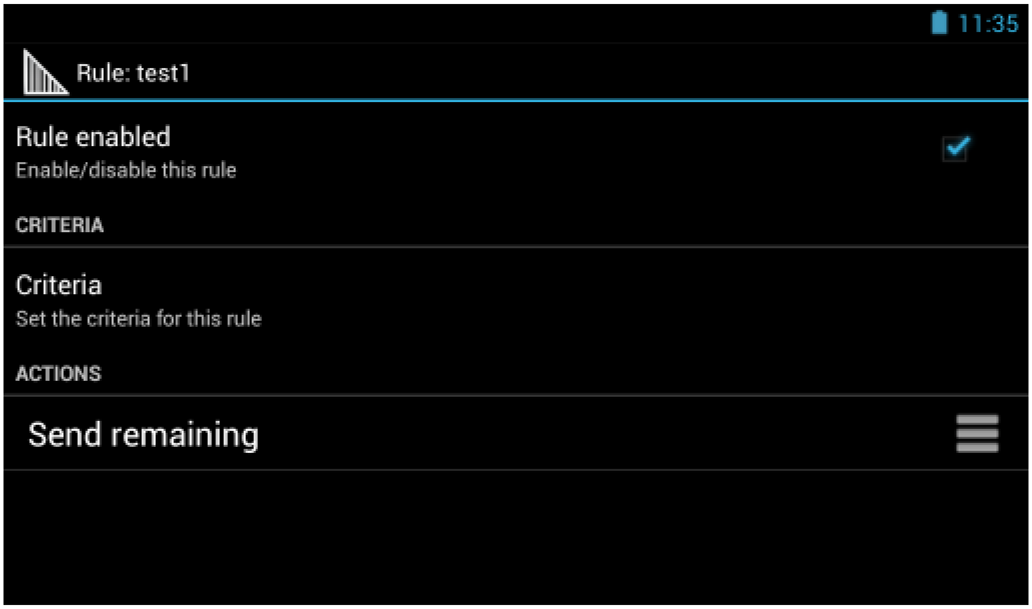
6 Touch **OK**.

Defining a Rule

Procedure:

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

Figure 63: Rule List Screen



11:35

Rule: test1

Rule enabled
Enable/disable this rule ☑

CRITERIA

Criteria
Set the criteria for this rule

ACTIONS

Send remaining

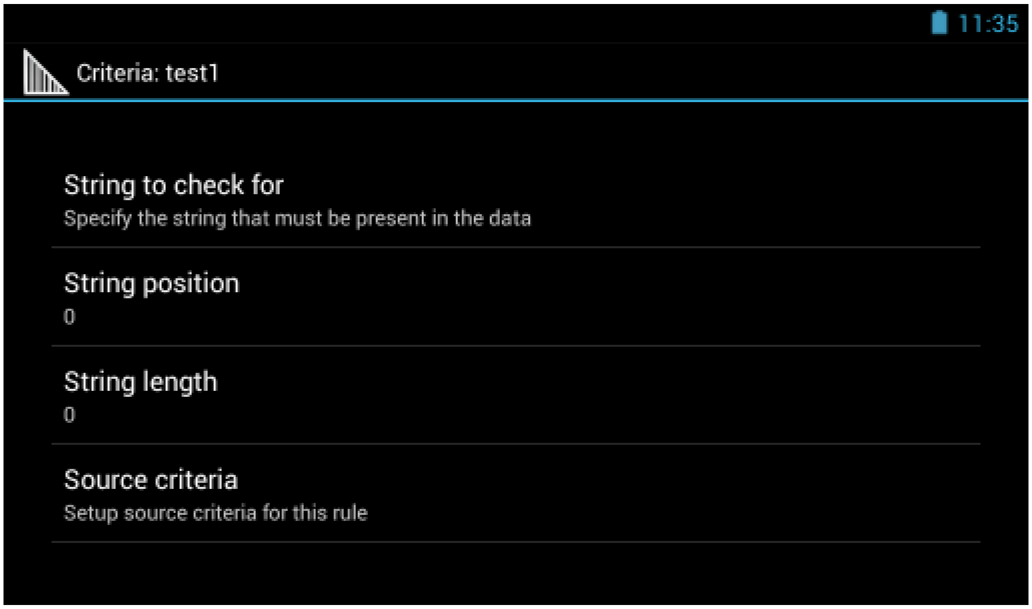
2 Touch the **Rule enabled** checkbox to enable the current rule.

Defining Criteria

Procedure:

1 Touch **Criteria**.

Figure 64: Criteria Screen



11:35

Criteria: test1

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

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 **Done**.

5 Touch **OK**.

6 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).

7 Touch the + or **-** to change the value.

8 Touch **OK**.

9 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.

10 Touch the + or **-** to change the value.

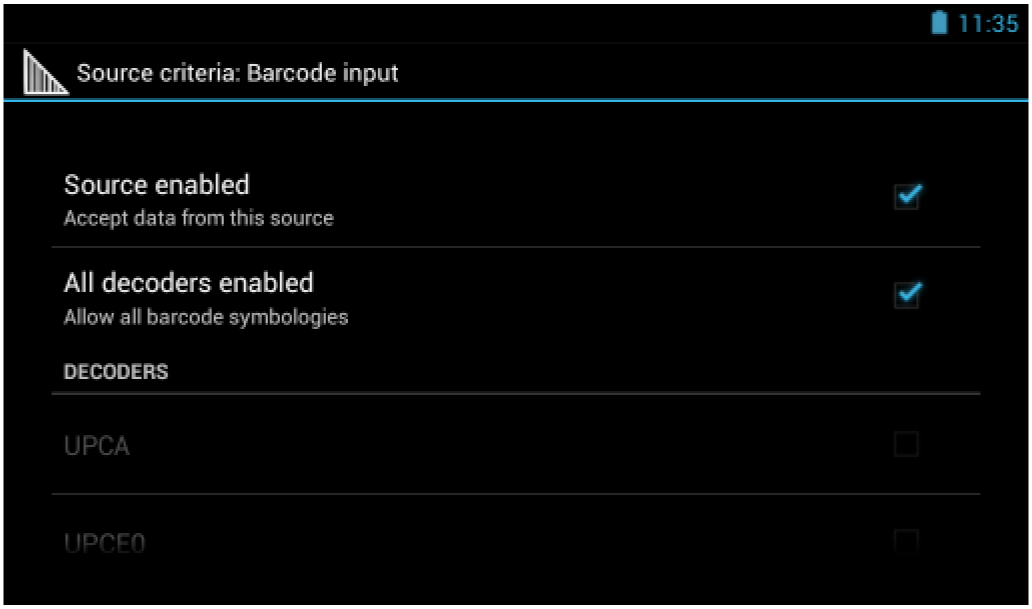
11 Touch **OK**.

12 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.

13 Touch **Barcode input** or **MSR input**. Options vary depending upon the device configuration.

14 Touch the **Source enabled** checkbox to accept data from this source.

Figure 65: Barcode Input Screen



Source criteria: Barcode input

Source enabled ☑
Accept data from this source

All decoders enabled ☑
Allow all barcode symbologies

DECODERS

UPCA □

UPCE0 □

15 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.

16 Touch ↶ until the **Rule** screen appears.

17 If required, repeat steps to create another rule.

18 Touch ↶ until the **Rule** screen appears.

Defining an Action

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

Procedure:

1 Touch ≡.

2 Touch **New action**.

3 In the **New action** menu, select an action to add to the **Actions** list. See *Table 5: ADF Supported Actions on page 78* 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

Procedure:

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.

Deleting an Action

Procedure:

1 Touch and hold the action name.

2 Select **Delete action** from the context menu.

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 5: 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.

Table continued…

Type	Actions	Description
	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.
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).

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:

Procedure:

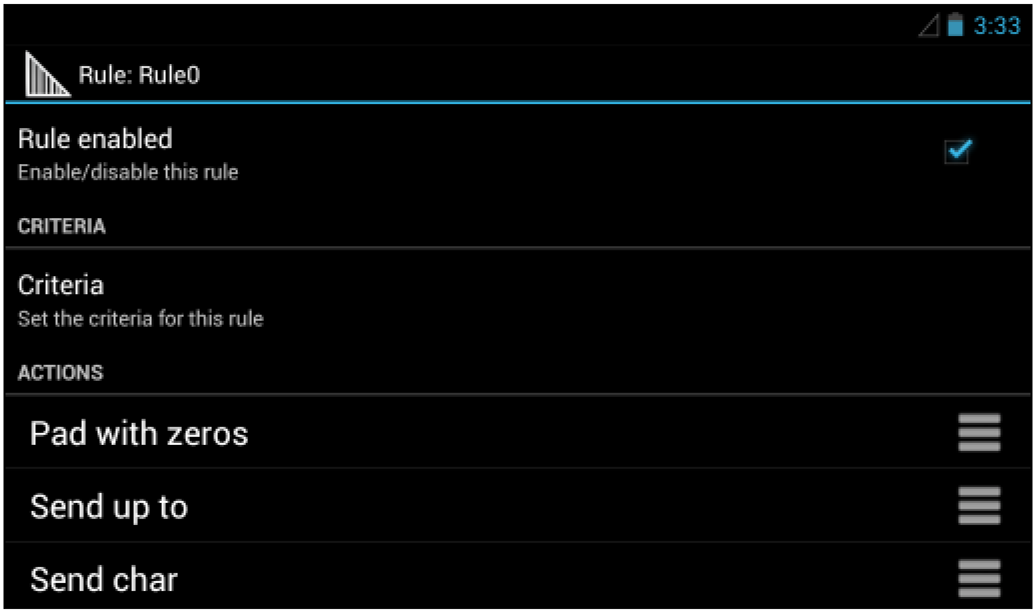
1 Touch ⊞.

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 ↩.

Figure 66: ADF Sample Screen



3:33

Rule: Rule0

Rule enabled
Enable/disable this rule ☑

CRITERIA

Criteria
Set the criteria for this rule

ACTIONS

Pad with zeros

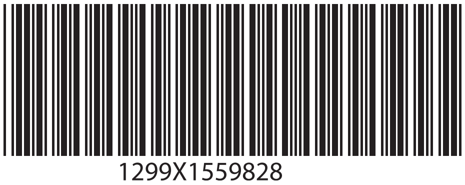
Send up to

Send char

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 67: Sample Bar Code



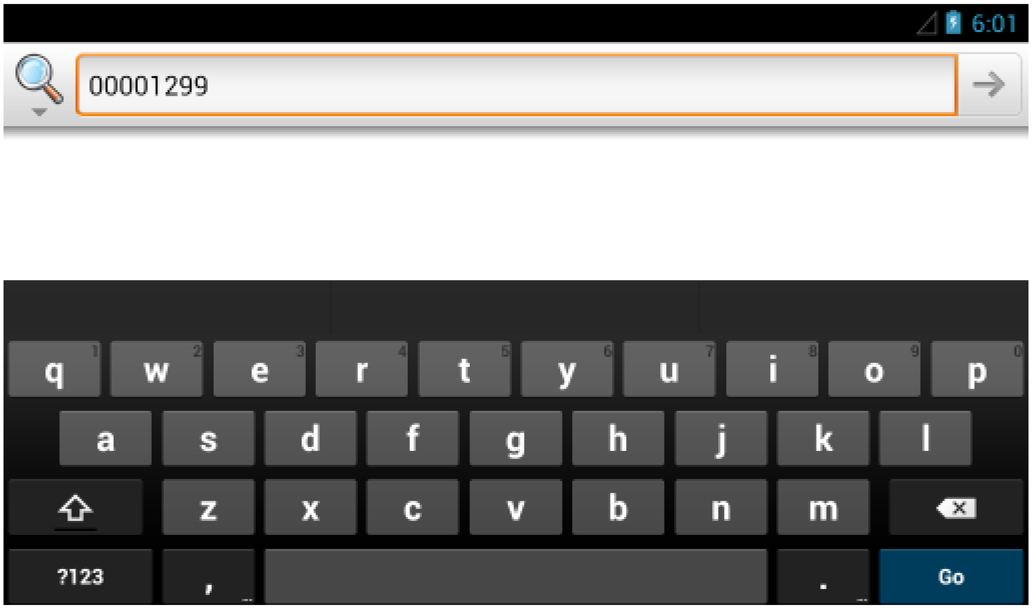
48 Press and hold the scan button.

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 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.

Figure 68: Formatted Data

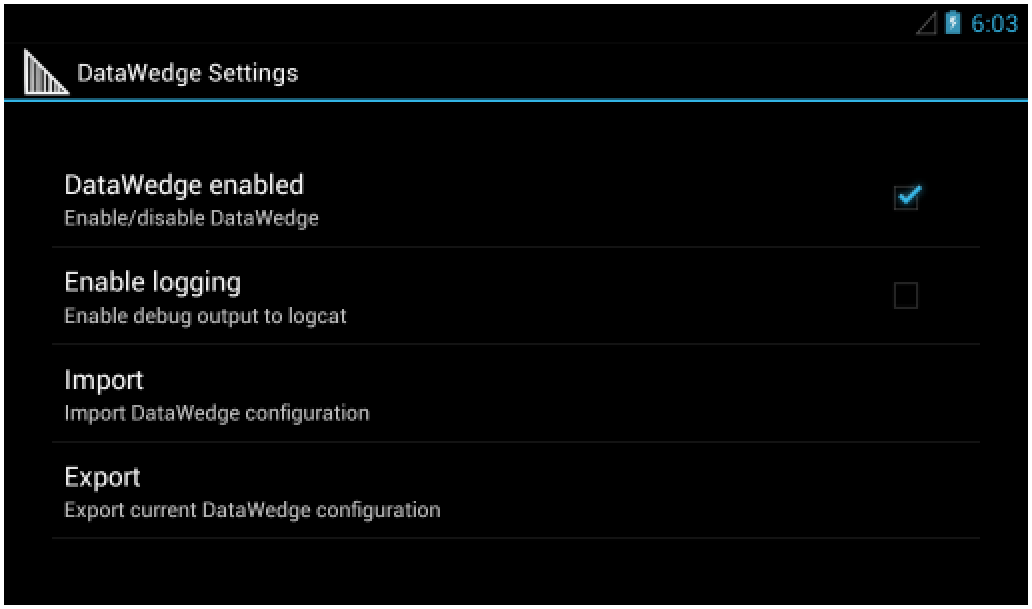


00001299

DataWedge Settings

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

Figure 69: DataWedge Settings Window



DataWedge Settings

DataWedge enabled ☑
Enable/disable DataWedge

Enable logging □
Enable debug output to logcat

Import
Import DataWedge configuration

Export
Export current DataWedge configuration

- **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 to the microSD card.
- **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

Procedure:

1. Copy the configuration file to the root of the ET1 microSD card.
2. Touch ⊞.
3. Touch ◣.
4. Touch ≡.
5. Touch **Settings**.
6. Touch **Import**.
7. Touch **SD Card**.
8. Touch **Import**. The configuration file (`datawedge.db`) is imported and replaces the current configuration.

Exporting a Configuration File

Procedure:

1. Touch ⊞.
2. Touch ◣.
3. Touch ≡.
4. Touch **Settings**.
5. Touch **Export**.
6. Touch **SD Card**.
7. Touch **Export**. The configuration file (`datawedge.db`) is saved to the root of the ET1 microSD card.

Restoring DataWedge

To restore DataWedge to the factory default configuration:

Procedure:

1. Touch ⊞.
2. Touch ◣.
3. Touch ≡.
4. Touch **Settings**.
5. Touch **Restore**.
6. 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 microSD card. 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 microSD card 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.

Remapping Keys

By default, the ET1 is configured to use the Left and Right Scan/Action keys to initiate scanning. To use the P1, P2 or P3 keys as a scan trigger:

Procedure:

1. Touch ☰.
2. Touch **Button Remap Program**.
3. Touch **P1**, **P2** or **P3**.
4. Select **L1 Button** or **R1 Button**.
5. Touch ⌂.

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.

Disable DataWedge on ET1 and Mass Deploy

To disable DataWedge and deploy onto multiple ET1 devices:

Procedure:

1 Touch ⊞.

2 Touch **DataWedge**.

3 Touch ≡.

4 Touch **Settings**.

5 Unselect the **DataWedge enabled** check box.

6 Export the DataWedge configuration. See *Exporting a Configuration File on page 83* for instructions. See *Configuration and Profile File Management on page 83* for instructions for using the auto import feature.

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 button 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.motorolasolutions.emdk.datawedge.api.ACTION_SOFTSCANTRIGGER”

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

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

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

Sample

```
Intent sendIntent = new Intent();

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

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

sendBroadcast(sendIntent);
```

Chapter 5

WLAN Configuration

The ET1 supports the following WLAN security options:

- Open
- Wireless Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)/WPA2 Personal (PSK)
- Extensible Authentication Protocol (EAP)
  - EAP-Transport Layer Security (TLS)
  - Lightweight Extensible Authentication Protocol (LEAP)
  - Protected Extensible Authentication Protocol (PEAP) - with Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2) and Generic Token Card (GTC) authentication.
  - EAP-Flexible Authentication via Secure Tunneling (FAST) - with MSCHAPv2 and GTC authentication.
  - EAP-TTLS - with Password Authentication Protocol (PAP), MSCHAP and MSCHAPv2 authentication.

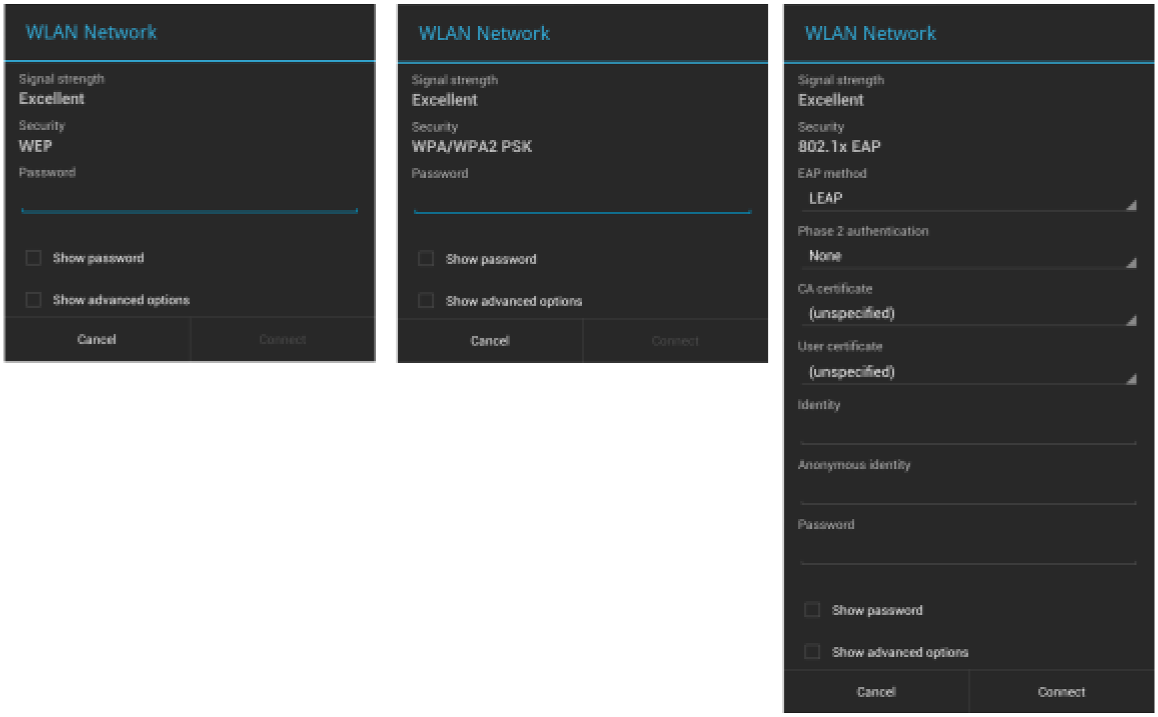
Connecting to a Wi-Fi Network

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 90* for setting connection to a proxy server and see *Configuring the Device to Use a Static IP Address on page 91* for setting the device to use a static IP address.

Procedure:

1. Touch ⊞.
2. Touch ☰.
3. Touch 📶 **Wi-Fi**.
4. Slide the Wi-Fi switch to the **On** position. The device searches for WLANs in the area and displays them in the list. Open networks are indicated with 📶 and secure networks are indicated with 📶🔒.
5. Scroll through the list and touch the desired WLAN network.

Figure 70: WLAN Network Security Dialog Boxes



WLAN Network

Signal strength
Excellent

Security
WEP

Password

WLAN Network

Signal strength
Excellent

Security
WPA/WPA2 PSK

Password

WLAN Network

Signal strength
Excellent

Security
802.1x EAP

EAP method
LEAP

Phase 2 authentication
None

CA certificate
(unspecified)

User certificate
(unspecified)

Identity

Anonymous identity

Password

6 **Note:**

Touch **Show password** checkbox to display password as it is entered.

Enter the required password. or other credentials then touch **Connect**. See the system administrator for more information.

7 The ET1 obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the ET1 with a fixed internet protocol (IP) address, see the *ET1 Enterprise Tablet Integrator Guide*.

8 The MC67 obtains a network address and other required information from the network using the dynamic host configuration protocol (DHCP) protocol. To configure the MC67 with a fixed internet protocol (IP) address, see the *MC67 Integrator Guide*.

9 When the device connects to the network, the network name appears at the top of the list and **Connected** appears below the network name.

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.

Procedure:

1 Touch .

2 Touch **Wi-Fi**.

3 Slide the Wi-Fi switch to the **On** position.

4 Touch + in the top right 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** or **TTLS**.
- Touch the **Phase 2 authentication** drop-down list and select an authentication method.
- If required, touch **CA certificate** and select a Certification Authority (CA) certificate. Note: Certificates are installed using the **Security** settings.
- If required, touch **User certificate** and select a user certificate. Note: User certificates are installed using the **Security** settings.
- If required, in the **Identity** text box, enter the username credentials.
- If desired, in the **Anonymous** identity text box, enter an anonymous identity username.
- If required, in the **Password** text box, enter the password for then given identity.

10 **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 90* for setting connection to a proxy server and see *Configuring the Device to Use a Static IP Address on page 91* for setting the device to use a static IP address.

Touch **Connect**.

11 Touch ⌂.

Viewing Connected Network Details

Procedure:

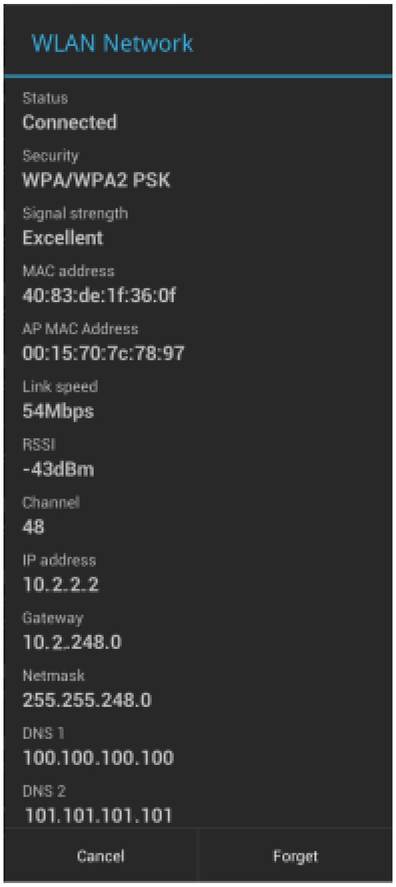
1 Touch .

2 Touch 📶 **Wi-Fi**.

3 If Wi-Fi is off, slide the Wi-Fi switch to the **On** position.

4 Touch the Connected network..

Figure 71: Connected Network Dialog Box



WLAN Network

Status
Connected

Security
WPA/WPA2 PSK

Signal strength
Excellent

MAC address
40:83:de:1f:36:0f

AP MAC Address
00:15:70:7c:78:97

Link speed
54Mbps

RSSI
-43dBm

Channel
48

IP address
10.2.2.2

Gateway
10.2.248.0

Netmask
255.255.248.0

DNS 1
100.100.100.100

DNS 2
101.101.101.101

5 Touch **OK**.

Configuring for a Proxy Server

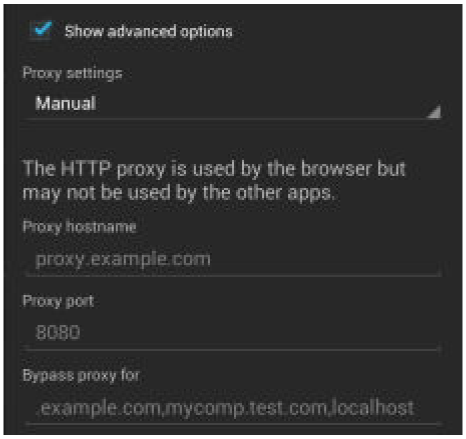
A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates 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.

Procedure:

1 In the network dialog box, touch a network.
2 Touch **Show advanced options** checkbox.
3 Touch **Proxy settings** and select **Manual**.

Figure 72: Proxy Settings



☑ 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

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 ⌂.

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:

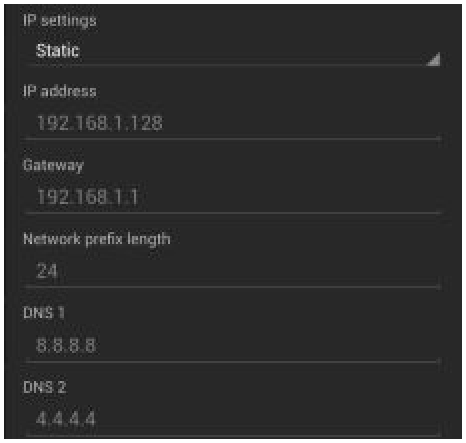
Procedure:

1 In the network dialog box, touch a network.

2 Touch **Show advanced options** checkbox.

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

Figure 73: Static IP Settings



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

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 ⌂.

11 ⌂.

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).
  - **MAC address** - Displays the Media Access Control (MAC) address of the device when connecting to Wi-Fi networks.
- **Regulatory**
  - **Enable 802.11d** - Enabled by default. The device obtains Regulatory information from the AP including country code. Displays the country code acquired from the AP.
  - **Enable 802.11d Strict mode** - Device will connect only if the acquired country matches the country broadcasted by the AP.
  - **Country selection** - Displays the acquired country code if 802.11d is enabled else it displays the currently selected country code.
  - **Region code** - Displays the current region code.
- **Band and Channel Selection**
  - **Wi-Fi frequency band** - 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**.
- **About**
  - **Version** - Displays the current Fusion information.

Remove a Wi-Fi Network

To remove a remembered or connected network:

Procedure:

1 Touch ⊞.

2 Touch ☰.

3 Touch 📶 **Wi-Fi**.

4 In the **Wi-Fi networks** list, touch and hold the name of the network.

5 In the menu, touch **Forget network**.

6 Touch ⌂.

Disabling 802.11d Feature

Procedure:

1 Touch ☰.

2 Touch **Wi-Fi**.

3 Slide the switch to the **ON** position.

4 Touch ≡.

5 Touch **Advanced**.

6 Uncheck **Enable 802.11d** checkbox.

7 On the **Warning!** dialog box, touch **Yes**.

8 Touch **Country Selection**.

9 In the **Country Selection** dialog box, select the country you are in.

10 Touch ⌂.

Chapter 6

WWAN Configuration

In order to use the WAN radio for data communication, the ET1N2 must be activated on the service provider's network. By default, the ET1N2 is configured for a GSM network. To activate on a CDMA network, manual configuration is required.

GSM Activation

When the ET1N2 turns on it automatically configures for the network. If the SIM card requires a PIN, the PIN screen appears. Enter the PIN and touch **OK**.

CDMA Activation

Prior to using the ET1N2 on a CDMA network, the ET1 must be registered with the service provider. Contact the service provider to set up an account and provide the MEID number (located under the battery).

By default, the ET1N2 is configured for a GSM network. To activate on a CDMA network:

Procedure:

1 Touch ⚙.

2 Touch **More...**.

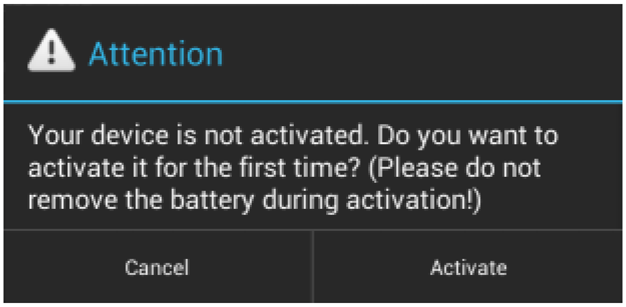
3 Touch **Mobile networks**.

4 Touch **Technology preferences**.

5 Touch **Network mode**.

6 In the **Network mode** menu, select either **Sprint** or **Verizon**. The ET1 switches the modem firmware and the Activation Dialog box appears.

Figure 74: Activation Screen



Attention

Your device is not activated. Do you want to activate it for the first time? (Please do not remove the battery during activation!)

7 Touch **Activate**. The ET1N2 begins the activation process. If the activation is unsuccessful, contact the service provider.

Switching Between Service Providers

An ET1N2 can be activated on different networks.

Note: If the ET1N2 has an ATT SIM card installed, power off the ET1N2, remove the SIM card and then turn the ET1N2 back on before switching to another network.

Procedure:

1. Touch ⚙.
2. Touch **More ...**
3. Touch **Mobile networks**.
4. Touch **Technology preferences**.
5. Touch **Network mode**.
6. Touch **Verizon**, **Sprint**, **N America** (all GSM network carriers in North America) or **Global** (all GSM network carriers outside of North America).
   The ET1N2 switches the modem firmware and connects to the network.

WAN Configuration

The user can configure various data options for WAN connectivity.

Disabling Data When Roaming

To prevent the device from transmitting data over other carriers' mobile networks when leaving an area that is covered by the carrier's networks. This is useful for controlling expenses if the service plan does not include data roaming.

Procedure:

1. Touch ⊞.
2. Touch ⚙.
3. Touch **More ...** .
4. Touch **Mobile networks**.
5. Un-check **Data roaming**.
6. Touch ↩.
7. Touch ⌂.

Limiting Data Connection to 2G Networks

Note: This feature is only available on some networks. Check with service provider.

Extend the battery life by limiting the data connections to 2G networks (GPRS or EDGE). When connected to a 2G network, the user may want to postpone activities that transmit a lot of data, such as sending, uploading, or downloading pictures or video, until they are connected to a faster mobile or other wireless network.

Procedure:

1. Touch ⊞.

2. Touch ⚙.
3. Touch **More ...** .
4. Touch **Mobile networks**.
5. Touch **GSM 2G/3G selection**.
6. Touch **2G only**.
7. Touch ⌂.
8. Touch ⌂.

Creating a New GSM Access Point Name

If the GSM wireless service provider determines that the user needs to create a new access point name (APN) or to create a new one, obtain the APN and detailed settings from the service provider.

Procedure:

1. Touch ⚙.
2. Touch **More ...** .
3. Touch **Mobile networks**.
4. Touch **Access Point Names**.
5. Touch ☰.
6. Touch **New APN**.
7. Touch each APN settings and enter the appropriate data obtained from the wireless service provider.
8. Touch **Read only** to password protect the APN information.
9. When finished, touch ☰.
10. Touch **Save**.
11. Touch the button across from the new APN name to start using it.
12. Touch ⌂.

Editing a GSM Access Point Name

If the GSM wireless service provider determines that the user needs to change the settings of the current access point name (APN), obtain the APN and detailed settings from the service provider.

Procedure:

1. Touch ⚙.
2. Touch **More ...** .
3. Touch **Mobile networks**.
4. Touch **Access Point Names**.
5. Touch an existing APN to edit.
6. If the APN is password protected, enter `moto_pct0720` in the **Enter password** dialog box and then touch **OK**.
7. Touch ☰.
8. Touch each APN settings and enter the appropriate data obtained from the wireless service provider.
9. When finished, touch ☰.
10. Touch **Save**.
11. Touch the button across from the new APN name to start using it.
12. Touch ⌂.

WAN Settings

Mobile Networks

- **Data enabled** - Uncheck to prevent the ET1N2 from transmitting data on any mobile network. This is useful if traveling in an area where the user does not have a mobile data plan and wants to avoid charges for data use on local carriers' mobile networks. Unchecking this setting does not prevent the ET1N2 from transmitting data over WLAN.
- **Data roaming** - Uncheck to prevent the ET1N2 from transmitting data on other carriers' mobile networks when it can not access its own carrier's mobile networks.
- **GSM mode settings** - On a Global network, allows user to select network and frequency band.
    - **GSM 2G/3G selection** - Options: **Automatic**, **2G only** or **3G only**.
    - **GSM frequency band selection** - Options: **All bands**, **EU only** or **NA only**.
- **Technology settings**
    - **Technology preferences** - Touch to change the network operating mode and settings.
        + **Network mode** - Options: **Verizon**, **Sprint**, **N America** (all GSM network carriers in North America) or **Global** (all GSM network carriers outside of North America).
    - **Access Point names** - On GSM networks, opens the **APNs** screen, to select mobile access point configurations; or press Menu to add a new APN. Consult your carrier about how to use the tools on this screen.
- **System select** - On CDMA networks, changes the CDMA roaming mode.
    - **Home only** - Do not roam from Home network.
    - **Automatic** - Allow automatic roaming.

Connection Data Utility

- **Ping function** - Use to test WWAN access. Enter a URL or IP address. The ET1N2 tries to access the site and reports if successful or not.
- **Modem reset** - Use to reset the modem to factory default settings.

Sprint System Options

If the ET1N2 is activated on a Sprint network, the user has the option to perform additional functions.

Start Activation

An ET1N2 that is already activated might be required to be re-activated if the device is to be reassigned to another Sprint account. The system administrator provides the device information to Sprint and then re-activate the ET1N2.

To re-activate, touch ⚙ > **System Update** > **Start Activation**.

Update Profile

Use the **Update Profile** option to move a Sprint service from another device to the ET1N2.

Update PRL

The Preferred Roaming List (PRL) is a database that contains information used during the system selection and acquisition process. The PRL indicates which bands, sub bands and service provider identifiers are scanned and in what priority order. Without a PRL, the ET1N2 may not be able to roam. To update the PRL, touch ☰ > **System Update** > **Update PRL**.

Chapter 7

Administrator Utilities

We 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 133* 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 112* for more information.

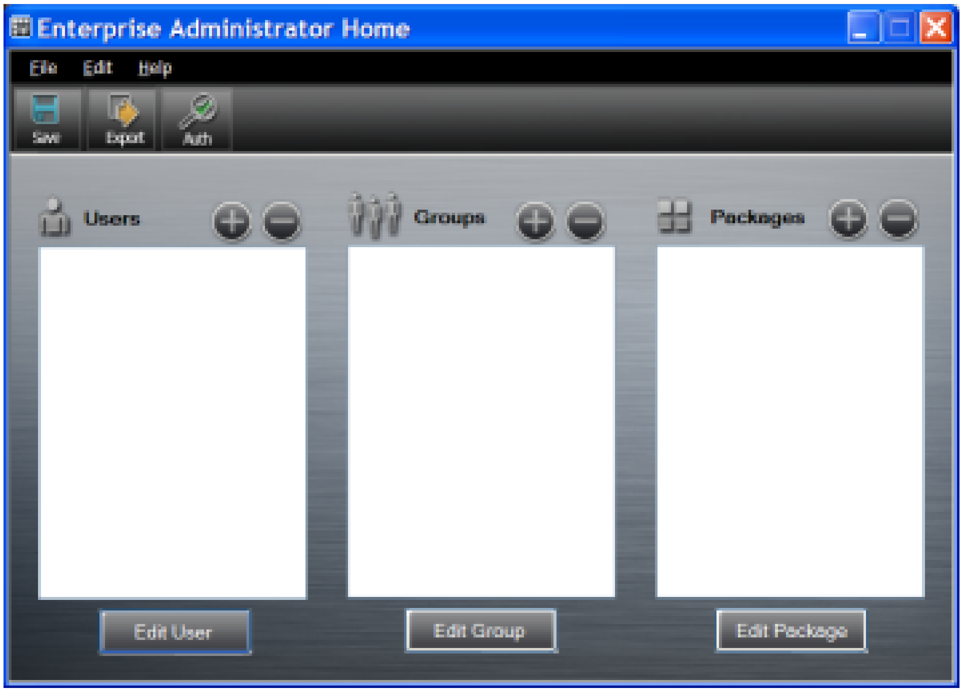
Enterprise Administrator Application

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 75: Enterprise Administrator Window



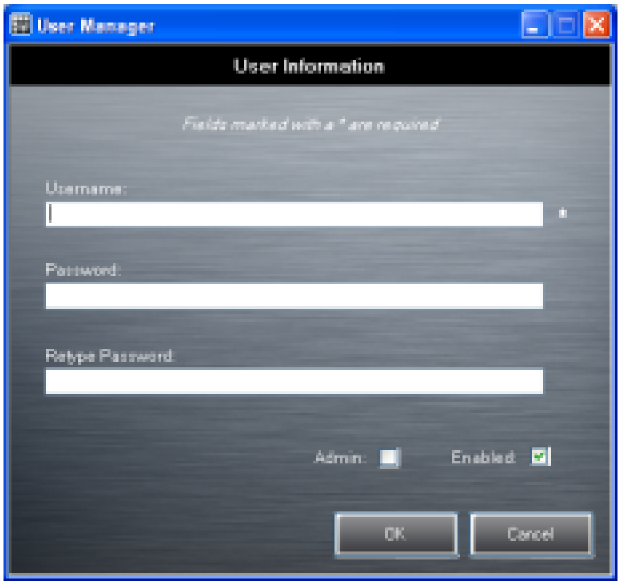
Creating Users

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

Procedure:

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

Figure 76: User Manager Window



User Manager

User Information

*Fields marked with a * are required*

Username: *

Password:

Retype Password:

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.

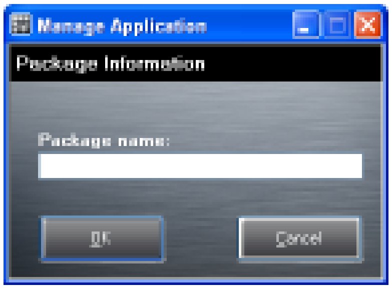
Create a list of installed applications (packages) on the device that are available for use by all the users.

Procedure:

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 113*.

Figure 77: Package Information Window



Manage Application

Package Information

Package name:

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.

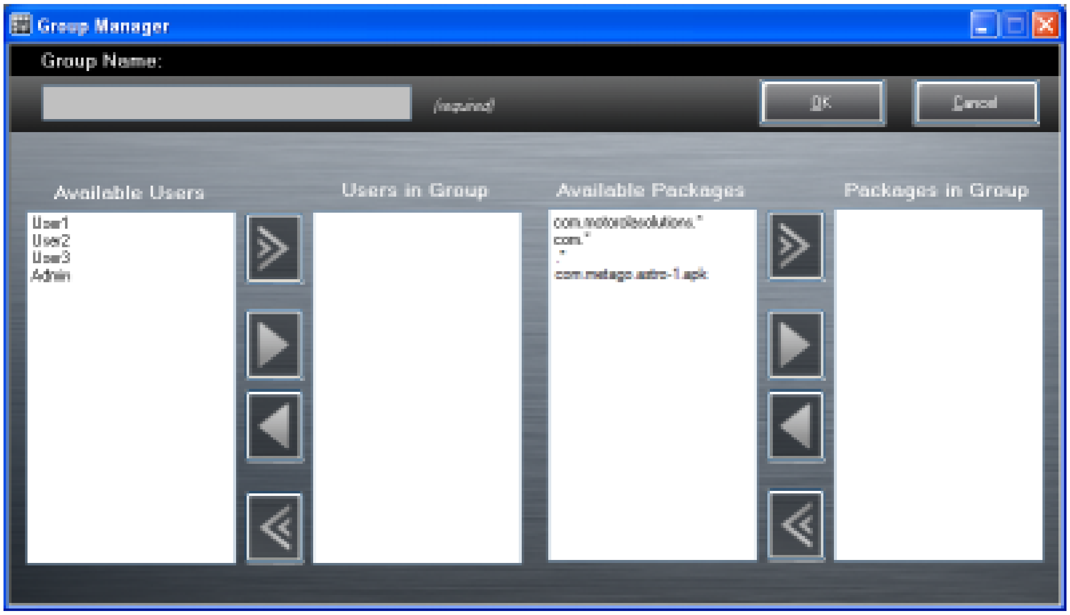
Creating Groups

Create groups of users that have access to specific applications.

Procedure:

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

Figure 78: Group Manager Window



User1
User2
User3
Admin

com.motorolasolutions.*
com.*
.*
com.metago.astro-1.apk

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**.

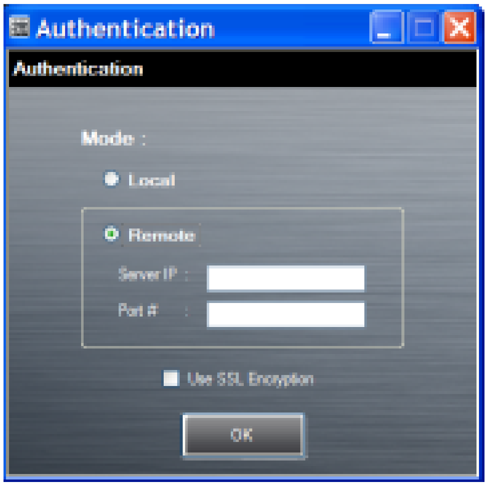
Creating Remote Authentication

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

Procedure:

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

Figure 79: 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.

Procedure:

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 microSD card. See *USB Communication on page 51* for information on copying files to the device.

Importing User List

Procedure:

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

Procedure:

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 113* for instructions for creating a Package List file):

Procedure:

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

Procedure:

1 Select a user in the **Users** list.

2 Click **Edit User**.

3 Make changes and then click **OK**.

Deleting a User

Procedure:

1 Select a user in the **Users** list.

2 Click **-**. The user name is removed from the list.

Editing a Group

Procedure:

1 Select a user in the **Groups** list.

2 Click **Edit Group**.

3 Make changes and then click **OK**.

Deleting a Group

Procedure:

1 Select a group in the **Groups** list.

2 Click **-**.

3 Click **Yes**. The group name is removed from the list.

Editing a Package

Procedure:

1 Select a package in the **Packages** list.

2 Click **Edit Package**.

3 Make changes and then click **OK**.

Deleting a Package

Procedure:

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

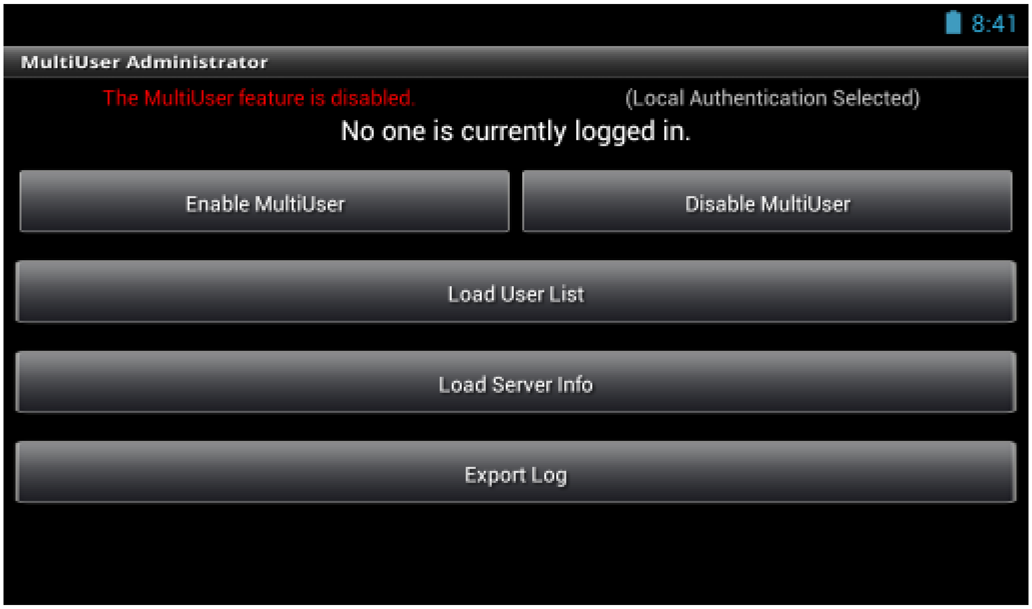
When the MultiUser Administrator is used for the first time, the password file must be imported.

Procedure:

1 Touch ⊞.

2 Touch 👥.

Figure 80: MultiUser Administrator Screen



MultiUser Administrator

The MultiUser feature is disabled.

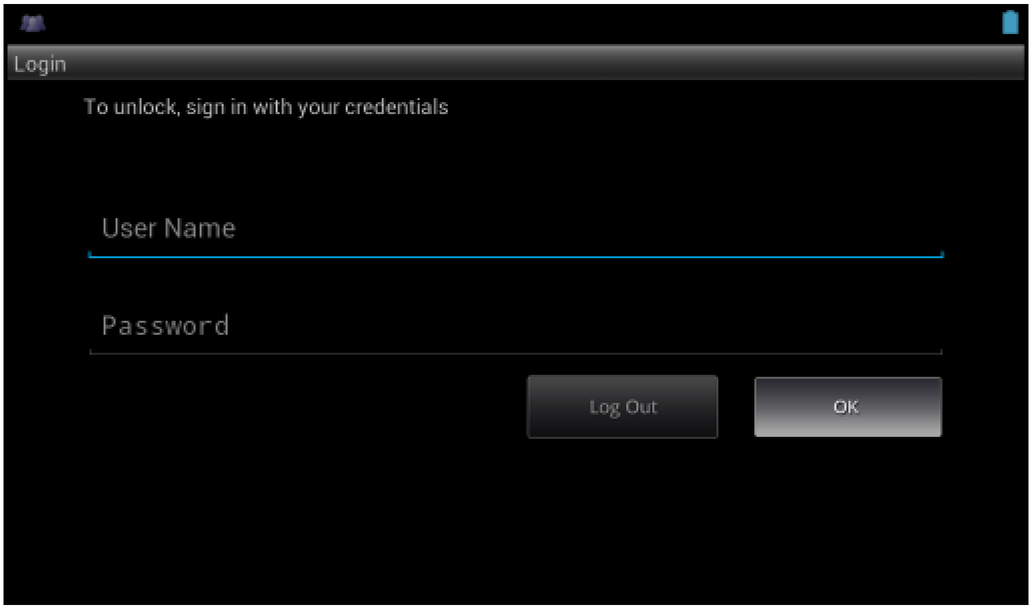
(Local Authentication Selected)

No one is currently logged in.

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

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

Figure 81: MultiUser Login Screen



Login

To unlock, sign in with your credentials

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

6 In the **Password** text box, enter the password.

7 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.

Procedure:

1 Touch ⊞.

2 Touch 👥.

3 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.

Procedure:

1 Touch ⊞.

2 Touch 👥.

3 Touch **Load Server Info**. The application reads the data from the *server* file and configures the Multi-user Login feature.

4 Touch ≡.

5 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.

Procedure:

1 Touch ⊚.

2 Touch 👥.

3 Touch ≡.

4 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:

Procedure:

1 Touch ⊚.

2 Touch 👥.

3 Touch ≡.

4 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.

Procedure:

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.

Procedure:

1 Touch ⊞.

2 Touch 👥.

3 Touch ≡.

4 Touch **Delete Individual User Data**. A dialog box displays with all of the users that currently have data associated with their log in.

5 Select each user to delete or **Select All** to delete all user data.

6 Touch **Delete** to delete the data.

Capturing a Log File

Procedure:

1 Touch ⊞.

2 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.

3 Touch **Export Log** to copy the log file to the microSD card. The log file can be captured when the multi-user feature is in either the enabled or disabled mode.

4 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.

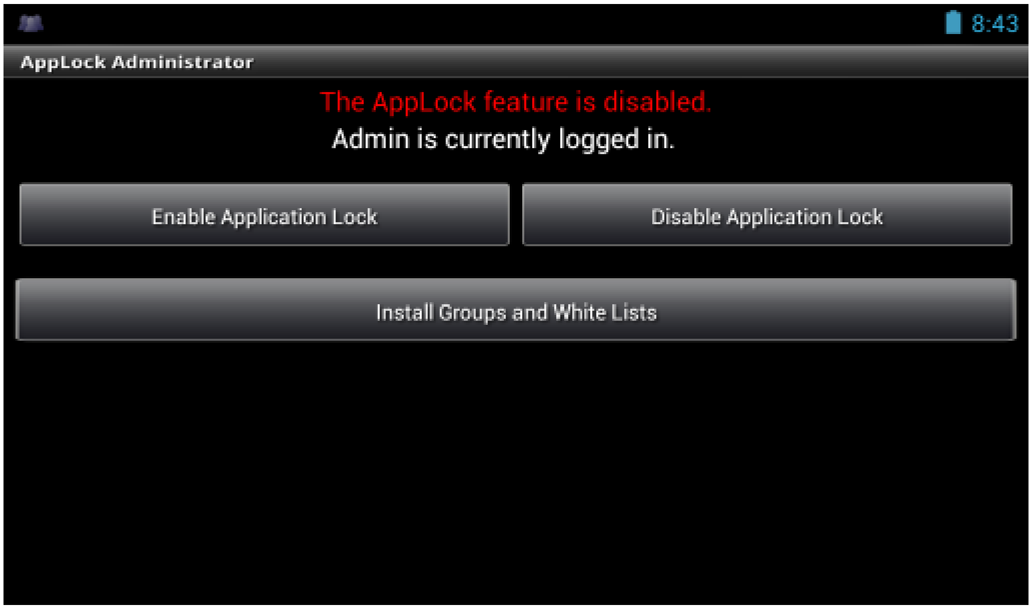
Installing Groups and White Lists

Procedure:

1 Touch ⊞

2 Touch 🔒

Figure 82: AppLock Administrator Screen



AppLock Administrator

The AppLock feature is disabled.

Admin is currently logged in.

Note:

When the application launches the current status of the Application Lock feature displays (enabled or disabled).

Log off and then log in again for the feature to take affect.

3 Touch **Install Groups and White Lists** to read the contents of the Groups and White List files from the root of the microSD card and push its contents into the AppLock framework.

Once the Group and White List files are imported and the feature enabled, the next time a user logs in, the device will be configured accordingly.

Enabling Application Lock

Procedure:

1 Touch ⊙.

2 Touch ⊞.

3 Touch **Enable Application Lock**.

Disabling Application Lock

Procedure:

1 Touch ⊙.

2 Touch ⊞.

3 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 107* 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.motorolasolutions.*
```

where:

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

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

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

`com.motorolasolutions` 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.motorolasolutions.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.motorolasolutions.example1

com.motorolasolutions.example2

com.motorolasolutions.example3

com.motorolasolutions.example4
```

Determining Applications Installed on the Device

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

Procedure:

1 Connect the device to the host computer.

Note: See *Development Tools on page 132* 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 microSD card. The file lists all the .apk files installed with their package names.

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

Procedure:

1 Touch ⊞.

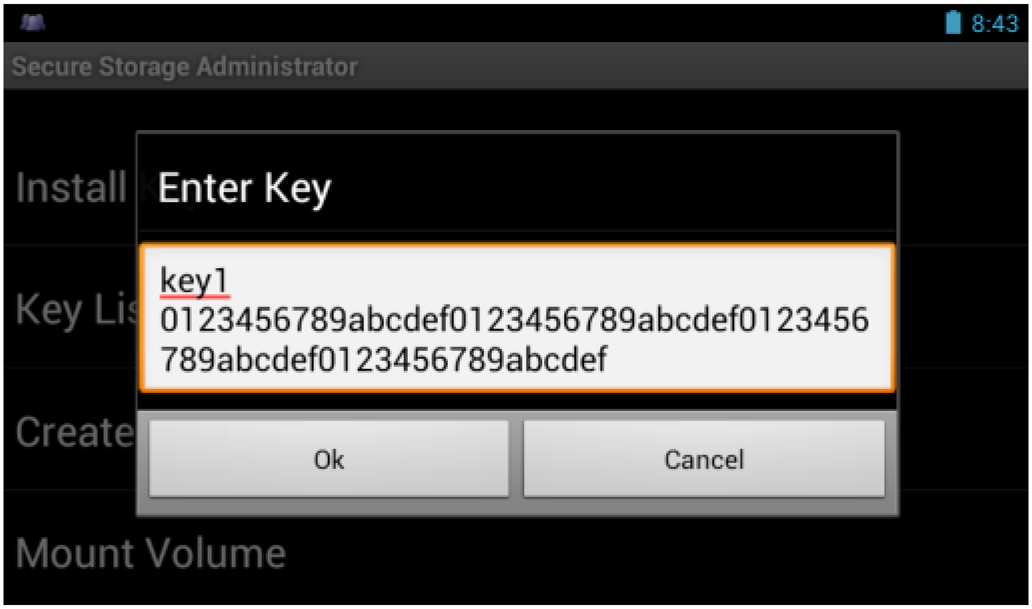
2 Touch ▦.

3 Touch **Install Key**.

4 Touch **Manual**.

5 Touch **OK**.

Figure 83: Enter Key Dialog Box



key1
0123456789abcdef0123456789abcdef0123456
789abcdef0123456789abcdef

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.

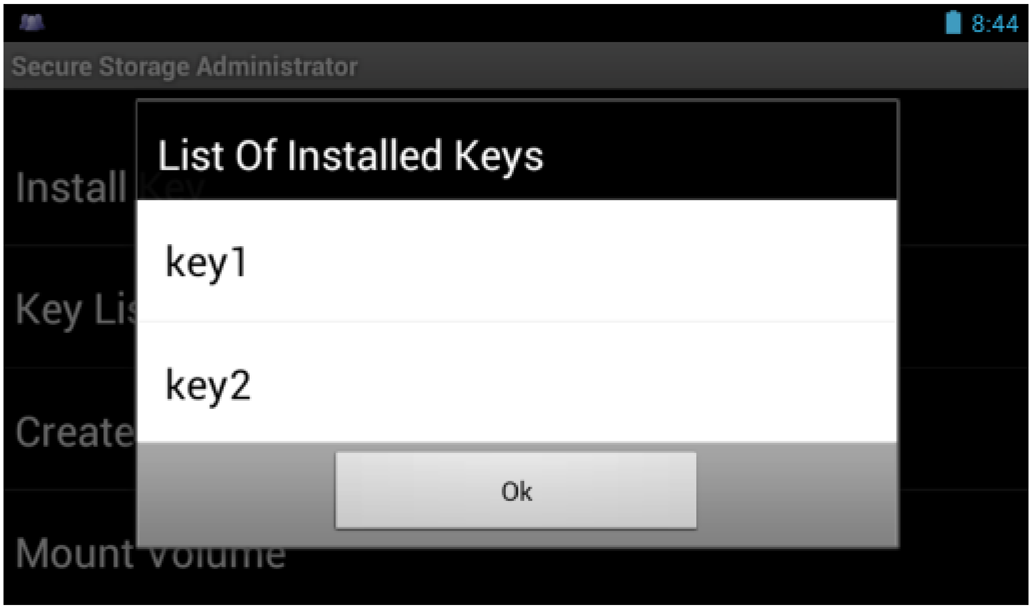
7 Touch **OK**. The key is imported into the device. The message **successfully installed the key** appears on the screen.

Viewing Key List

Procedure:

1 Touch **Key List**.

Figure 84: List of Keys



2 Touch **OK**.

Deleting a Key

Procedure:

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

Procedure:

1 Create an efs file. See *Creating an EFS File on page 117* for instruction on creating the efs file.
2 Copy the `keyfile` and `efsfile` files to root of the microSD card. See *USB Communication on page 51*.
3 Touch **Create Volume**.
4 Touch **Import**.
5 Touch **OK**. The message **Successfully Created the Volume** appears briefly.

Creating a Volume Manually

Procedure:

1 Touch **Create Volume**.
2 Touch **Manual**.
3 Touch **OK**.

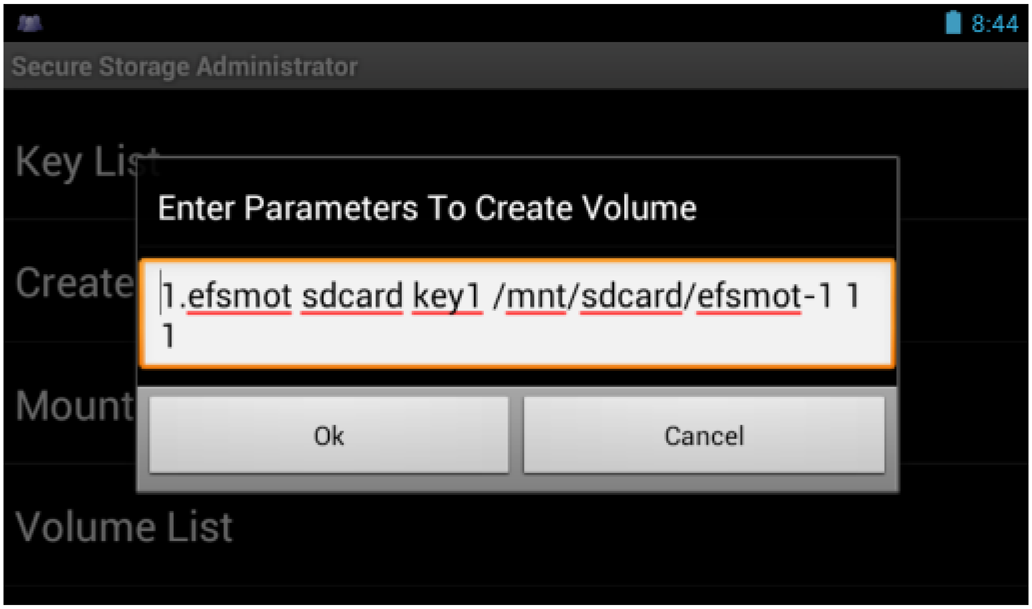
4 In the **Enter Parameters To Create Volume** text box, enter the parameters in the follow format:

<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.

Figure 85: Enter Parameter To Create Volume Dialog Box


8:44
Secure Storage Administrator
Key List
Create
Mount
Volume List
Enter Parameters To Create Volume
Ok
Cancel

1.efsmot sdcard key1 /mnt/sdcard/efsmot-1 1 1

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

Procedure:

1 Touch **Mount Volume**.

2 Touch **sdcard** or **internal**.

3 Touch **OK**.

4 Select a volume.

5 Touch **OK**.

Listing Volumes

Procedure:

1 Touch **Volume List**.

2 Touch **sdcard** to list volumes on the microSD card 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

Procedure:

1. Touch **Unmount Volume**.
2. Touch **sdcard** to list the mounted volumes on the microSD card 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

Procedure:

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

Encrypting an SD Card

Caution: All data will be erased from the microSD card when this is performed.

Procedure:

1. Touch **Encrypt SD card**. A warning message appears.
2. Touch **Yes**. The Key List dialog box appears.
3. Select a key from the list and then touch **Ok**.

   The encryption process begins and when completed, displays a successfully completed message.

Creating an EFS File

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

Procedure:

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

3 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

Procedure:

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

Procedure:

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

Procedure:

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 8

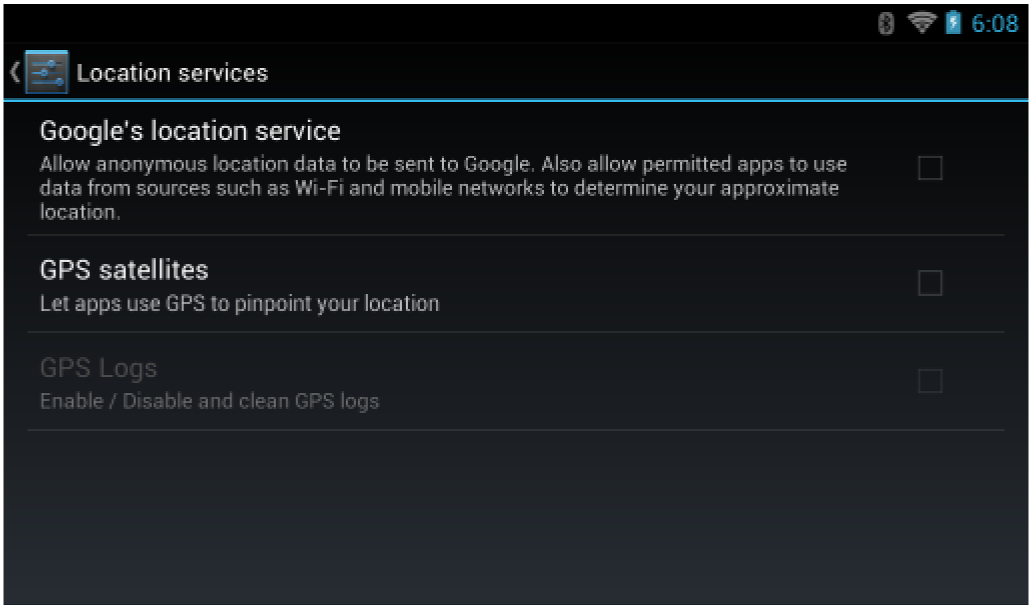
Settings

This chapter describes settings available for configuring the device.

Location Settings

Use the **Location & Security** settings to set preferences for using and sharing location information. Touch > **Location services**.

Figure 86: Location Services Window



Google's location service

Allow anonymous location data to be sent to Google. Also allow permitted apps to use data from sources such as Wi-Fi and mobile networks to determine your approximate location. □

GPS satellites

Let apps use GPS to pinpoint your location □

GPS Logs

Enable / Disable and clean GPS logs □

Check **Google's location service** checkbox to use information from Wi-Fi networks to determine approximate location.

Note: Assisted GPS is only available of ET1N2 WAN configurations.

GPS can be used in stand-alone or Assisted (A-GPS) modes. A Stand-alone GPS receiver downloads data from GPS satellites. It can take several minutes to get a fix. By using GPS Location servers, A-GPS dramatically improves the performance of the Time To First Fix (TTFF) of GPS receivers by providing them with data that they would ordinarily have to download from the GPS satellites and other aiding data that helps the acquisition. With the A-GPS data, GPS receivers can operate faster and more reliably.

Check **GPS satellites** checkbox to use the ET1's global positioning system (GPS) receiver (stand-alone) to obtain approximate location position. GPS accuracy is dependent upon a clear view of the sky and other factors.

Enabling Assisted GPS

Procedure:

1 Touch **GPS satellites**.
2 Touch **Use Assisted GPS**.
3 Touch the **Enable Assisted GPS** checkbox.
4 Touch **OK**.
5 The ET1N2 can use the Motorola Server or another location server. Touch **SUPL settings**.
6 By default, **Using Motorola Server** is selected. To change to another server deselect the checkbox.
7 In the **Server FQDN/IP** text box, enter the address of the location server.
8 In the **Port** text box, enter the port number of the server.
9 Touch **Secure connection** checkbox, if the server requires a secure connection.
10 Select the ID type to use during the SUPL session. Options: **IMSI** or **MSISDN**.
11 Touch **OK**.

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 124* for more information.
  - **PIN** - Enter a numeric PIN to unlock screen. See *Set Screen Unlock Using PIN on page 122* for more information.
  - **Password** - Enter a password to unlock screen. See *Set Screen Unlock Using Password on page 123* 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.

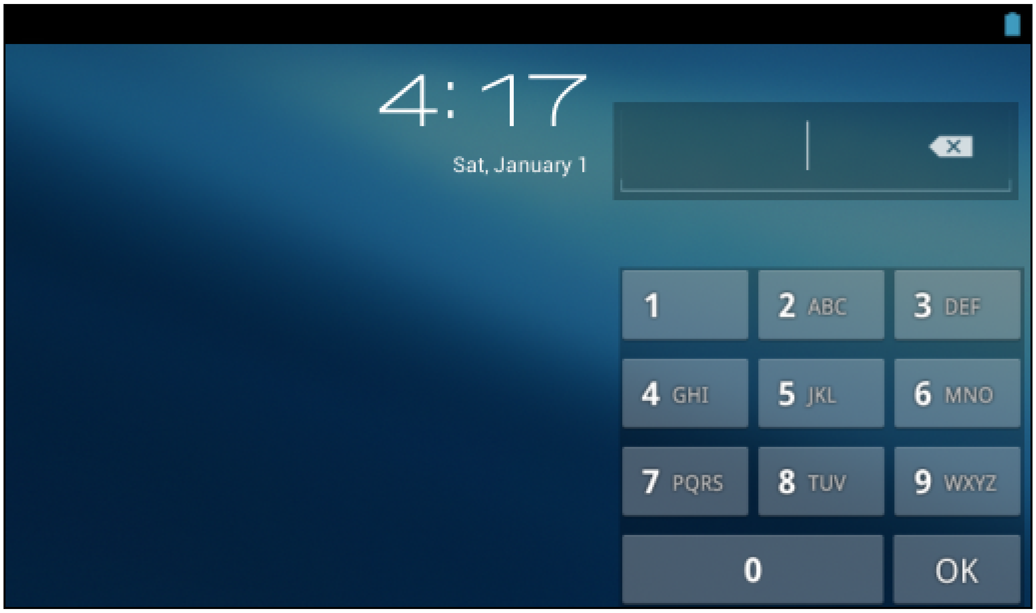
Set Screen Unlock Using PIN

Procedure:

1 Touch ⊞.

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

Figure 87: PIN Screen

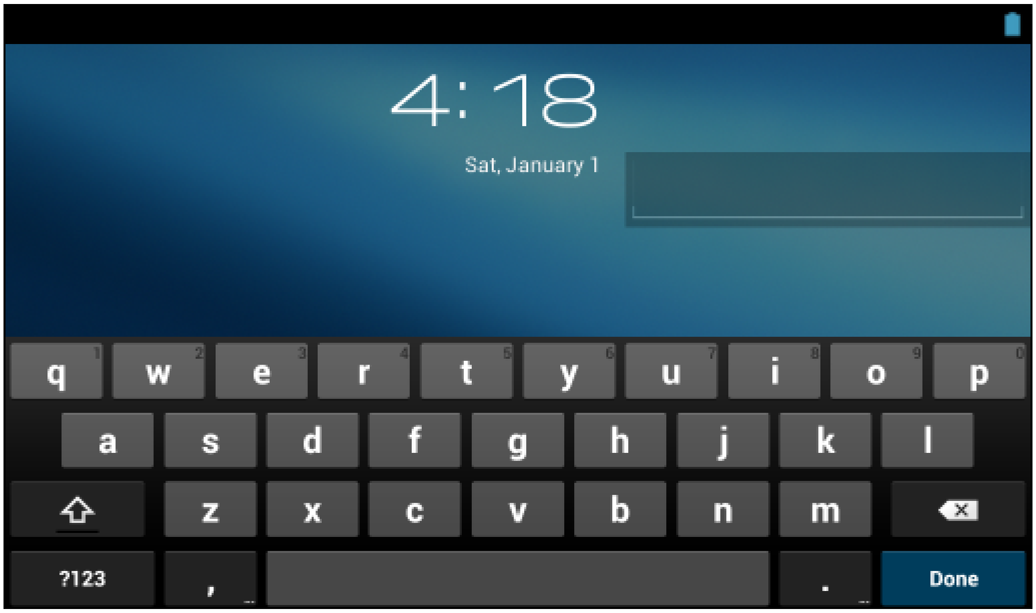


Set Screen Unlock Using Password

Procedure:

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

Figure 88: Password Screen



Set Screen Unlock Using Pattern

Procedure:

1 Touch ⊞.

2 Touch ☰.

3 Touch 🔒 **Security**.

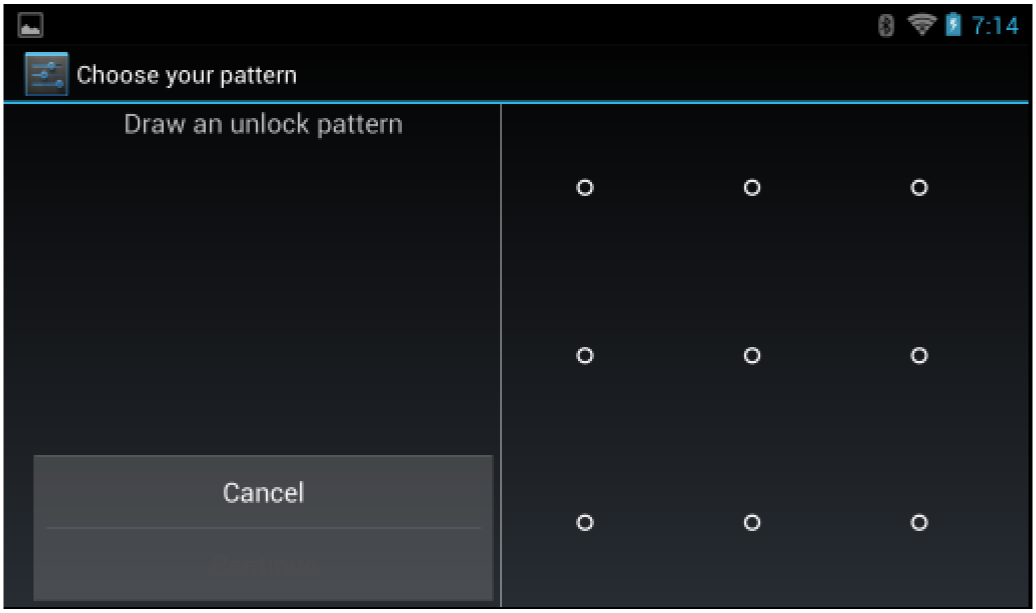
4 Touch **Screen lock**.

5 Touch **Pattern**.

6 Watch pattern example and then touch **Next**.

7 Draw a pattern connecting at least four dots.

Figure 89: Choose Your Pattern Screen



Draw an unlock pattern

8 Touch **Continue**.

9 Re-draw the pattern.

10 Touch **Confirm**.

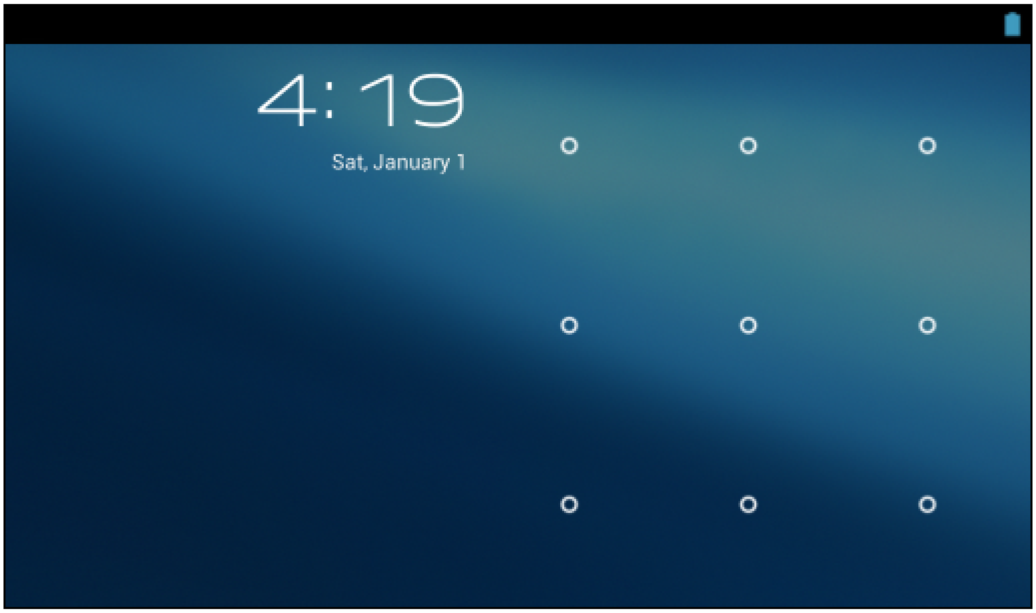
11 On the **Security** screen, touch **Make pattern visible** to show pattern when you draw the pattern.

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

13 Touch ⌂.

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

Figure 90: Pattern Screen



Multiple User Mode

For Multi-user Mode configuration, see *Administrator Utilities on page 101*.

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.

Button Remapping

The ET1’s programmable buttons, **P1**, **P2** and **P3** and the Left and Right Scan/Action buttons can be programmed to perform different functions. The **P1**, **P2** and **P3** buttons can also be programmed as shortcuts to installed applications.

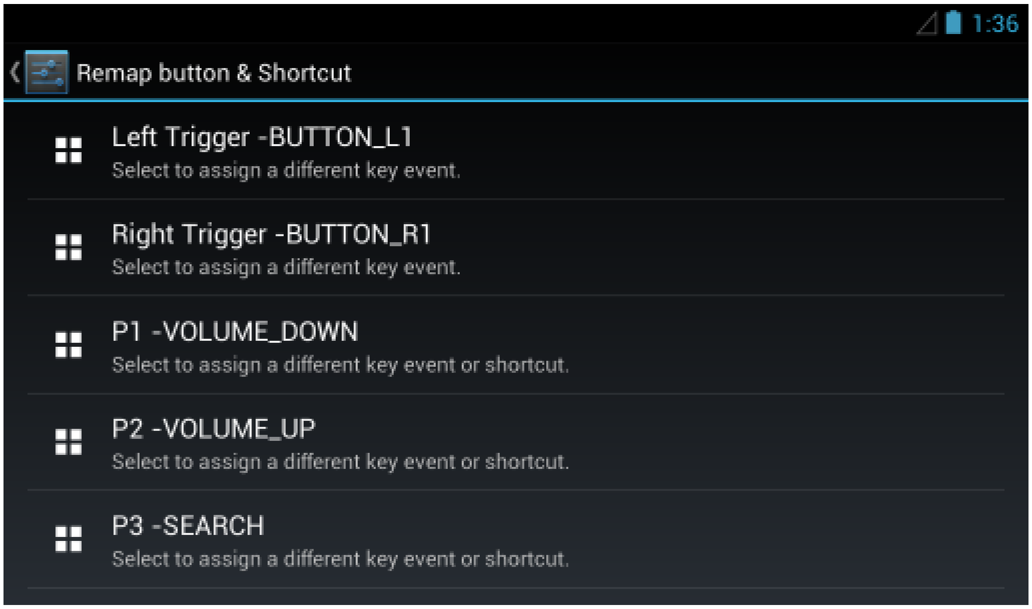
Remapping a Button

Procedure:

1 Touch ⚙.

2 Touch ▦ **Remap button & Shortcut**.

Figure 91: Remap Button & Shortcut Screen



1:36

Remap button & Shortcut

Left Trigger -BUTTON_L1
Select to assign a different key event.

Right Trigger -BUTTON_R1
Select to assign a different key event.

P1 -VOLUME_DOWN
Select to assign a different key event or shortcut.

P2 -VOLUME_UP
Select to assign a different key event or shortcut.

P3 -SEARCH
Select to assign a different key event or shortcut.

3 Select the button to remap.

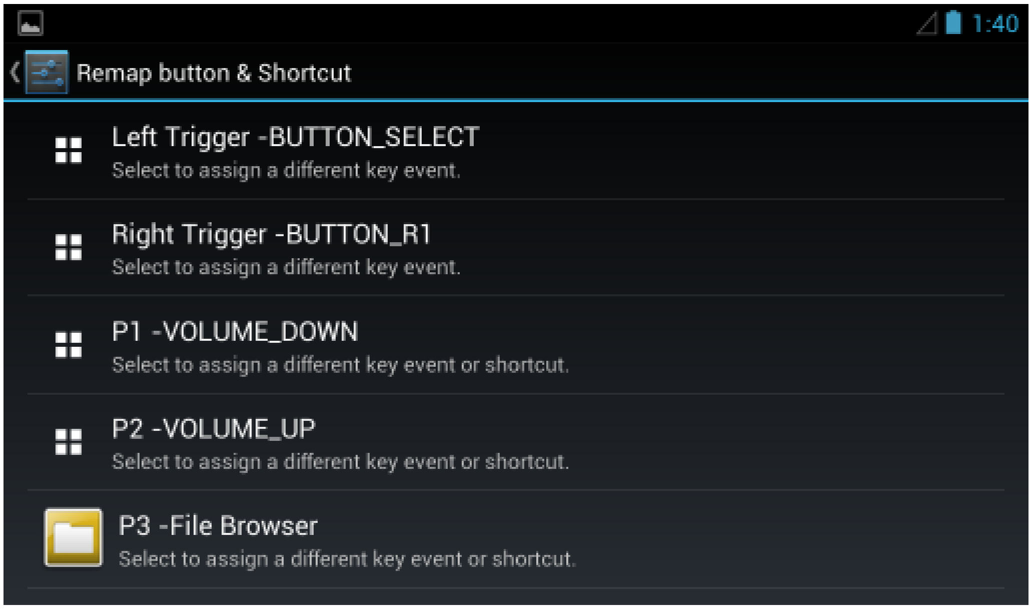
4 **Note:** If remapping the Left or Right Trigger, only the **BUTTON REMAPPING** tab displays.

Touch the **BUTTON REMAPPING** tab or the **SHORTCUT** tab that lists the available functions and applications.

5 Touch a function or application shortcut to map to the button.

Note: If you select an application shortcut, the application icon appears next to the button on the **Remap button & Shortcut** screen.

Figure 92: Remapped Button



1:40

Remap button & Shortcut

Left Trigger -BUTTON_SELECT
Select to assign a different key event.

Right Trigger -BUTTON_R1
Select to assign a different key event.

P1 -VOLUME_DOWN
Select to assign a different key event or shortcut.

P2 -VOLUME_UP
Select to assign a different key event or shortcut.

P3 -File Browser
Select to assign a different key event or shortcut.

6 Touch ⌂.

Exporting a Configuration File

The Button Remapping configuration can be exported to an xml file and imported into other ET1 devices. To export the configuration file:

Procedure:

1 Touch ⚙.

2 Touch ▦ **Remap button & Shortcut**.

3 Touch ☰.

4 Touch **Export**.

5 In the **Select export Remap file path** dialog box, touch one of the path options that displays.

6 Touch **OK**.

7 In the **Please enter xml filename** dialog box, enter a filename. Do not use spaces or include the filename extension.

Use the filename `SysKeypadRemap` to ensure that the configuration persists after an Enterprise Reset.

8 Touch **OK**. The configuration file is saved in the selected folder.

9 Copy the xml file from the folder to a host computer. See *USB Communication on page 51* for more information.

Importing a Configuration File

Procedure:

1 Copy the configuration file from a host computer to the root of the microSD card. See *USB Communication on page 51* for more information.

2 On the ET1, use File Browser to move the file from the root of the microSD card to the folder: **/enterprise/device/settings/keypad**.

3 Touch ⚙.

4 Touch ▦ **Button Remap & Shortcut**.

5 Touch ≡.

6 Touch **Import**.

7 In the **Select Import remap button config file** list, select the configuration file to import.

8 Touch **OK**.

9 In the **Warning** dialog box, touch **OK**.

Creating a Remap File

An administrator can create an xml configuration file and import it into any ET1 device. Use any text editor to create the xml file.

```
<Type>
<P1>Shortcut</P1>
<P2>Remap Button</P2>
<P3>Remap Button</P3>
<Type>
<Button_Remap>
<Left_Trigger>BUTTON_L1Left_Trigger>BUTTON_L1>
<Right_Trigger>BUTTON_R1Right_Trigger>BUTTON_R1>
<P1>VOLUME_DOWNP1>VOLUME_DOWN>
<P2>VOLUME_UPP2>VOLUME_UP>
<P3>SEARCHP3>SEARCH>
</Button_Remap>
<Shortcut>
<P1>Camera<P1>
<P2>Calculator</P2>
<P3>Gallery</P3>
</Shortcut>
```

Replace the button event strings. See *Keypad Remap Strings on page 165* for a list of available button functions.

Enterprise Reset

To ensure that the configuration persists after an Enterprise Reset, import the configuration file with the name `SysKeyRemap.xml`. After an Enterprise Reset, the ET1 looks for this file. If it exists, the Button Remap Program is configured with the settings in this file.

Accounts

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

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

- **General sync settings**

   - **Background data** - Check to permit applications to synchronize data in the background. Unchecking this setting can save battery power.
   - **Auto-sync** - Check to permit applications to synchronize data on their own schedule. If unchecked, touch ≡ > **Sync now** to synchronize data for that account. Synchronizing data automatically is disabled if **Background data** is unchecked. In that case, the Auto-sync checkbox is dimmed.
- **Manage accounts** - Lists accounts added to the device. Touch an account to open its account screen.

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

Procedure:

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

Procedure:

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 ET1. 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.
   - **Backup battery level** - Indicates the backup battery charge level.

  - **Network** - indicates the current network carrier (ET1N2 only).
  - **Signal strength** - indicates the radio signal strength (ET1N2 only).
  - **Mobile network type** - indicates the mobile network type. (ET1N2 only).
  - **Service state** - indicates the state of service. (ET1N2 only).
  - **Roaming** - indicates if the device is roaming outside the network. (ET1N2 only).
  - **Mobile network state** - indicates the mobile network state. (ET1N2 only).
  - **My phone number** - displays the phone number associated with the device. (ET1N2 only).
  - **IMEI** - displays the IMEI number for the device (ET1N2 only).
  - **IMEI SV** - displays the IMEI SV number for the device (ET1N2 only).
  - **IP address** - displays the IP address of the device.
  - **Wi-Fi MAC address** - Displays the Wi-Fi radio MAC address.
  - **Bluetooth address** - Displays the Bluetooth radio Bluetooth address.
  - **Serial number** - displays the serial number of the device (ET1N2 only).
  - **Up time** - Displays the time that the ET1 has been running since being turned on.
  - **Connect information** - displays transmit byte counter and data rates (ET1N2 only).
  - **Connect status** - displays network connection status information (ET1N2 only).
- **Hardware config** - Lists part number for various hardware on the ET1.
- **SE 13 version** - Displays date of SE13 table (ET1N2 only).
- **Legal information** - Opens a screen to view legal information about the software included on the ET1.
- **Serial number** - Displays the serial number of the device.
- **Model number** - Displays the device model number.
- **Android version** - Displays the operating system version.
- **Baseband version** - Displays WAN radio firmware version (ET1N2 only).
- **Bootloader version** - Displays the bootloader version.
- **Kernel version** - Displays the kernel version.
- **Build number** - Displays the software build number.

Chapter 9

Application Deployment

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

Security

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

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

Procedure:

1 Copy the certificate from the host computer to the root of the microSD card. See *USB Communication on page 51* for information about connecting the device to a host computer and copying files.

2 Touch ⚙.

3 Touch 🔒 **Security**.

4 Touch **Install from SD card**.

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 microSD card.

Configuring Credential Storage Settings

Procedure:

1 Touch ⚙.

2 Touch 🔒 **Security**.

- **Trusted credentials** - Touch to display the trusted system and user credentials.
- **Install from SD card** - Touch to install a secure certificate from the microSD card.
- **Clear credentials** - Deletes all secure certificates and related credentials.

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.

Touch ⚙ > { } **Developer options**. Slide the switch to the **ON** position to enable developer options.

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 133*.
- Android Debug Bridge, see *Installing Applications Using the Android Debug Bridge on page 134*.
- 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 microSD card, follow the host computer's instructions for connecting and disconnecting USB devices, to avoid damaging or corrupting files.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 51*.

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 *USB Communication on page 51*.

4 On the device, touch ⊞.

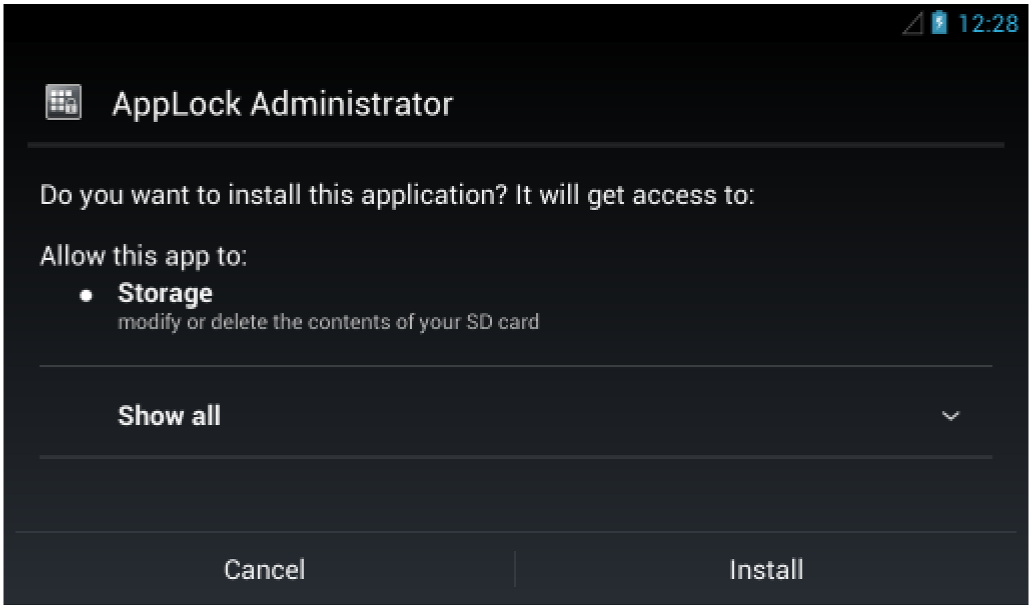
5 Touch 📁 to view files on .

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**.

Figure 93: Accept Installation Screen



AppLock Administrator

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

Allow this app to:

- **Storage**
  modify or delete the contents of your SD card

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

Prerequisites: Ensure that the ADB drivers are installed on the host computer. See *ADB USB Setup on page 133*.

Procedure:

1 Connect the device to a host computer using USB. See *USB Communication on page 51*.

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:

```
adb install <application>
```

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

8 Disconnect the device from the host computer. See *USB Communication on page 51*.

Mobility Services Platform

The MSP Client Software is a set of software components that come pre-installed on the device. The MSP Client software consists of the following components:

- The **Rapid Deployment** application provides support for MSP Staging functionality, provides support for the MSP Legacy Staging process, and provides support for backward-compatible legacy MSP 2.x Legacy Staging functionality.

- The **MSP Agent** application provides MSP Provisioning functionality and Control functionality when used with MSP Control Edition.

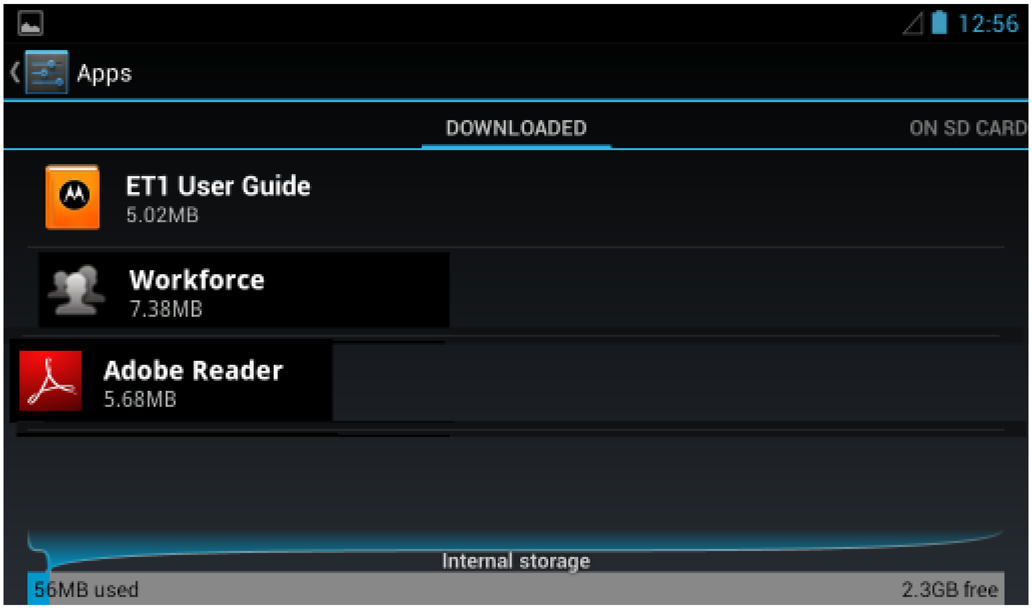
Refer to the *Mobility Services Platform User's Guide*, p/n 72E-100158-xx, for instructions for using the Rapid Deployment and MSP Agent clients.

Uninstalling an Application

Procedure:

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

Figure 94: Downloaded Screen



12:56

Apps

DOWNLOADED

ON SD CARD

ET1 User Guide
5.02MB

Workforce
7.38MB

Adobe Reader
5.68MB

Internal storage

56MB used

2.3GB free

4. Touch the application to uninstall.
5. Touch **Uninstall**.
6. Touch **OK** to confirm.

Updating the System

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

Procedure:

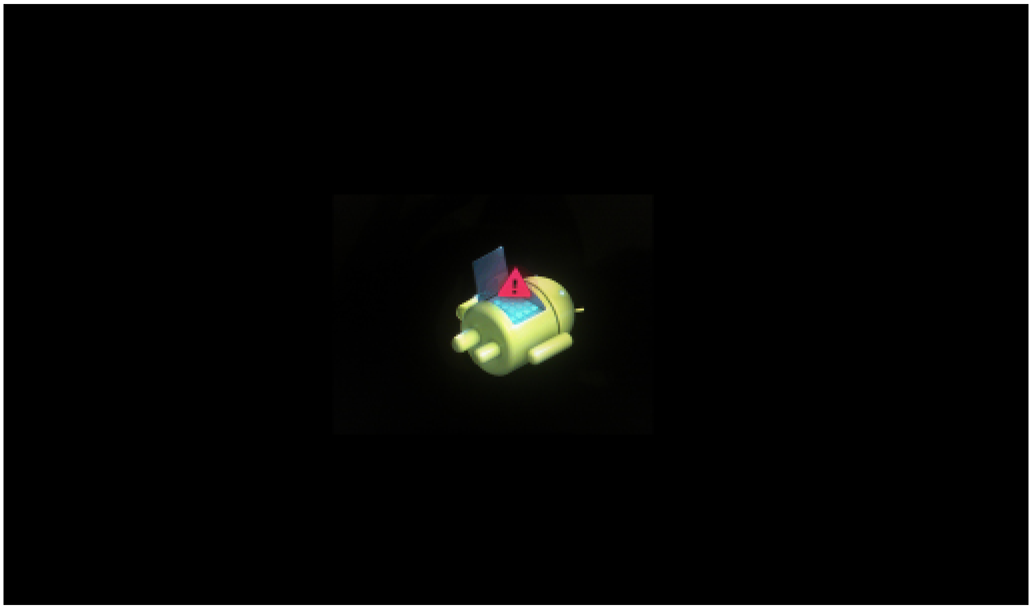
1. Download the system update package:
   a. Go to the Zebra Support Central web site, *http://www.zebra.com/support*.
   b. Download the appropriate System Update package to a host computer.
2. Copy the `ET1N0JenRUxxxxxxx.zip` (for ET1N0) or `ET1N2JenRUxxxxxxx.zip` (for ET1N2) file to the root directory of the microSD card. See *USB Communication on page 51* for more information.
3. Press and hold the Power button until the menu appears.

4 Touch **Reset**.

5 Press and hold the Right Scan/Action button.

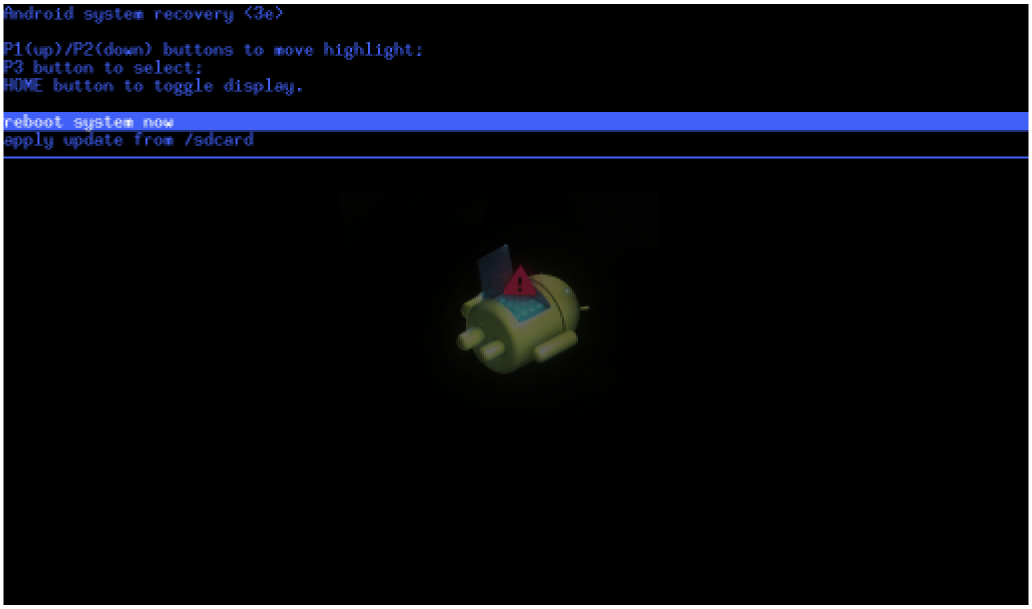
6 When the Recovery Mode screen appears, release the button.

Figure 95: Recovery Mode Screen



7 Touch ⌂.

Figure 96: System Recovery Screen



```
Android system recovery <3e>

P1(up)/P2(down) buttons to move highlight:
P3 button to select:
HOME button to toggle display.

reboot system now
apply update from /sdcard
```

8 Touch **P1** or **P2** to navigate to the **apply update from /sdcard** option.

9 Touch **P3**.

10 Touch **P1** or **P2** to navigate to the `ET1N0JenRUxxxxxxx.zip` or `ET1N2JenRUxxxxxxx.zip` file.

11 Touch **P3**. The System Update installs and then the ET1 resets.

Upgrading the Operating System from GingerBread to JellyBean

The ET1 GingerBread (AOSP V2.3) operating system can be upgraded to the JellyBean (AOSP V4.1.1) operating system.

Customers who purchased a Service Agreement option for the ET1 GingerBread version, are entitled to a one-time, operating system upgrade via the Zebra Customer Support web site: http://www.zebra.com/support. Customers must enter the serial number for each device to be upgraded. Zebra will then provide a secure web site link for the downloading the software. Customers can then install the upgrade using their own Mobile Device Management (MDM) client and or service center.

Customers who did not purchase a Service Agreement and want to upgrade to Jelly Bean, an Operating System Upgrade must be purchased separately. The software will be delivered after the customer order is placed. The link will be provided to customers by email. Customer's email address must be entered at the time the order is placed. Serial numbers for the ET1's must also be entered. Customers will install the upgrade using their own MDM client and or service center.

Refer to the MDM Client documentation for information on upgrade the ET1 using an MDM. The upgrade can be performed on an individual device using the procedure below.

Note:

Only ET1N0 with Rev. D operating system (Build number: 04-271301-2399-0601-00-M1-101712) is supported for upgrade to ET1N0 Jelly Bean. If the ET1N0 has an earlier operating system, first upgrade to Rev D, before starting this procedure.

Only ET1N2 with Rev. B operating system (Build number: 01-271301-2602-0100-00-D1-031413) is supported for upgrade to ET1N2 Jelly Bean. If the ET1N2 has an earlier operating system, first upgrade to Rev B, before starting this procedure.

The ET1 with JellyBean (V4.1.1) supports 802.11d and is enabled by default. This prevents connection with 802.11d disabled infrastructure. For deployments having 802.11d disabled infrastructure, 802.11d should be disabled in the ET1. See *Disabling 802.11d Feature on page 93* for more information.

Caution:

Backup all data and applications prior to performing the upgrade. Data on the external microSD card and in the internal /Enterprise folder will persist after the upgrade.

Ensure that power is applied to the ET1 during the system update procedure.

Procedure:

1 Download the System Upgrade package:
   - **a** Go to the Zebra Support Central web site, *http://www.zebra.com/support*.
   - **b** Download the appropriate System Upgrade package to a host computer.

If...	Then...
ET1N0	ET1N0JenRU01701580.zip
ET1N2	ET1N2JXXRU01201602.zip

2 Locate the System Upgrade package file on the host computer and un-compress the file into a separate directory.

3 Copy the `Upgrade_to_JB_0318.zip` and `FullPackageUpdate.zip` files to the root directory of the microSD card. See *USB Communication on page 51* for more information.

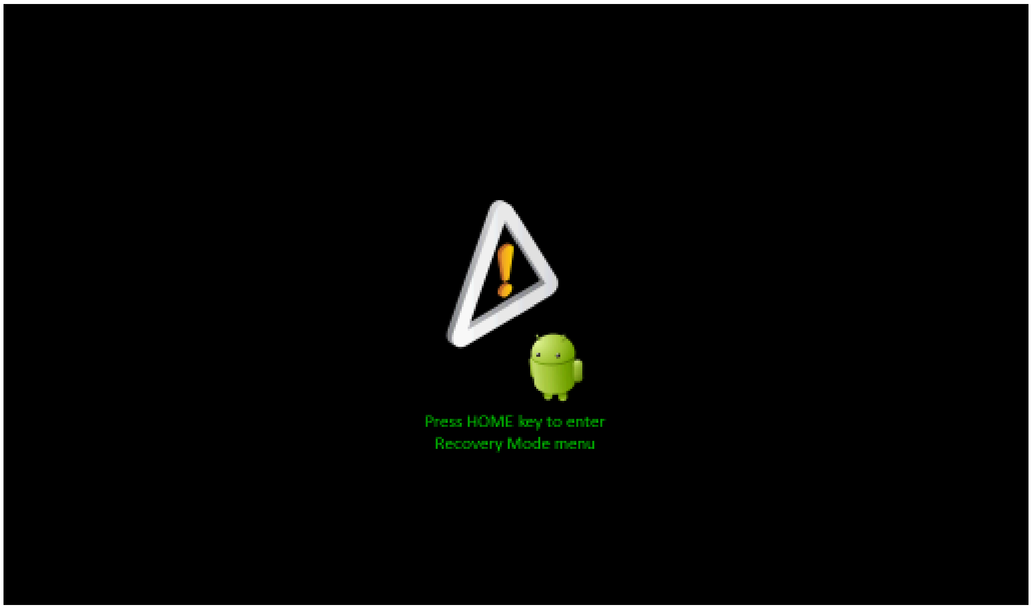
4 Press and hold the Power button until the menu appears.

5 Touch **Reset**.

6 Press and hold the Right Scan/Action button.

7 When the Recovery Mode screen appears, release the Right Scan/Action button.

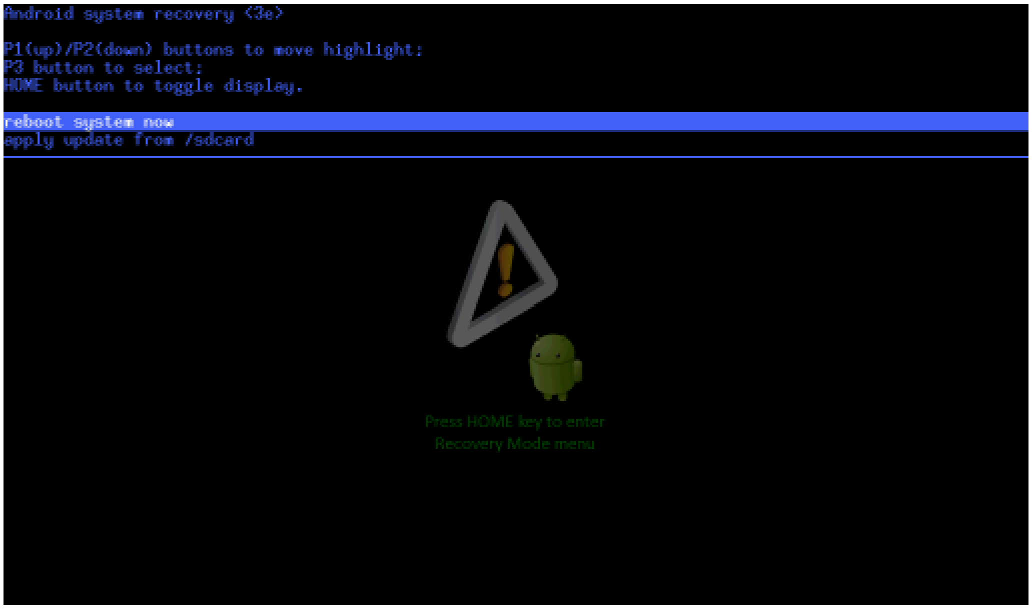
Figure 97: Recovery Mode Screen



Press HOME key to enter
Recovery Mode menu

8 Touch ⌂.

Figure 98: System Recovery Screen



```
Android system recovery <3e>

P1(up)/P2(down) buttons to move highlight;
P3 button to select;
HOME button to toggle display.

reboot system now
apply update from /sdcard
```

Press HOME key to enter
Recovery Mode menu

9 Touch **P1** or **P2** to navigate to the **apply update from /sdcard** option.

10 Touch **P3**.

11 Touch **P1** or **P2** to navigate to the `Upgrade_to_JB_0318.zip` file.

12 Touch **P3**. The System Update installs and then the ET1 resets.

13 Touch **P1** or **P2** to navigate to the **Reboot system now** option.

14 Touch **P3**.

Note: After the user presses **P3** no other user intervention is required.

The ET1 reboots. After rebooting the ET1 enters Fastboot Mode then Recovery Mode and then automatically installs the `FullPackageUpdate.zip` file. Upon completion, the ET1 reboots into the new operating system.

Storage

The device contains four types of file storage:

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

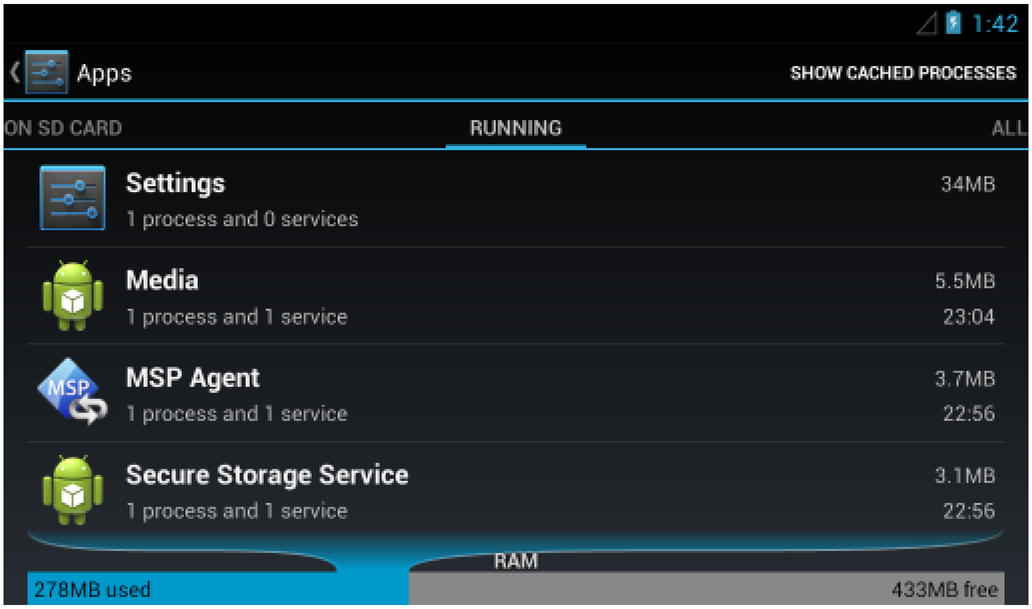
Random Access Memory

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.

Figure 99: Running Screen



Settings	1 process and 0 services	34MB
Media	1 process and 1 service	5.5MB 23:04
MSP Agent	1 process and 1 service	3.7MB 22:56
Secure Storage Service	1 process and 1 service	3.1MB 22:56

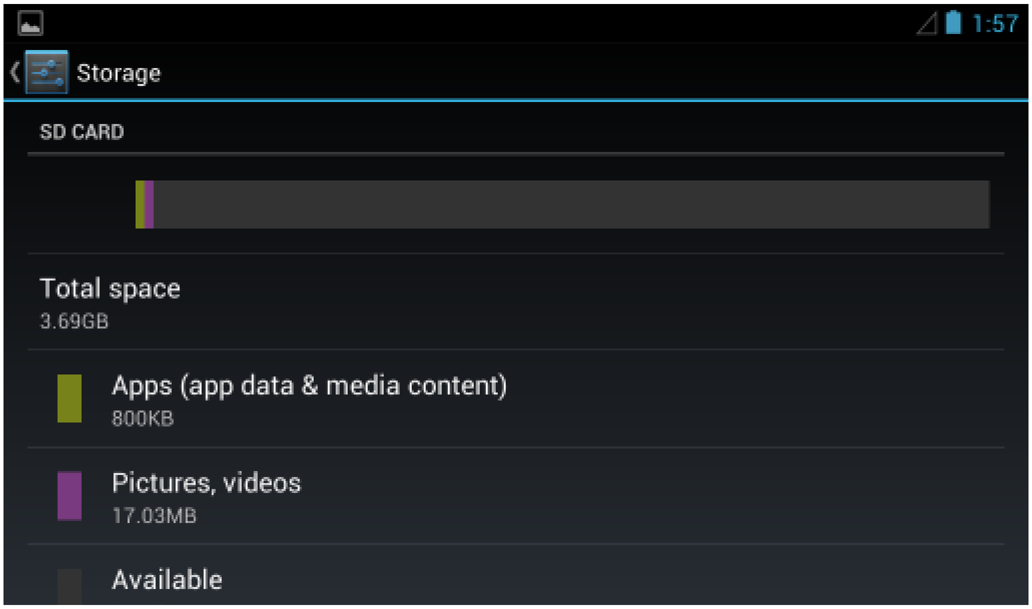
The bar at the bottom of the screen displays the amount of used and free RAM.

External Storage

The ET1 has a removable microSD card. The microSD card content can be viewed and files copied to and from when the ET1 is connected to a host computer. Some applications are designed to be stored on the microSD card rather than in internal memory.

To view the used and available space on the microSD card, touch ⚙ > ☰ **Storage**.

Figure 100: Storage Settings



1:57

Storage

SD CARD

Total space
3.69GB

🟩 Apps (app data & media content)
800KB

🟪 Pictures, videos
17.03MB

⬛ Available

- **Total space** - Displays the total amount of space on the installed microSD card.
- **Apps** - Displays the available space used for applications and media content on the installed microSD card.
- **Pictures, videos** - Displays the available space used for pictures and videos on the installed microSD card.
- **Available** - Displays the available space on the installed microSD card.
- **Unmount SD card** - Unmounts the installed microSD card from the ET1 so that it can be safely removed when the ET1 is on. This setting is dimmed if there is no microSD card installed, if it has already been unmounted or if it has been mounted on a host computer.
- **Erase SD card** - Permanently erases everything on the installed microSD card.

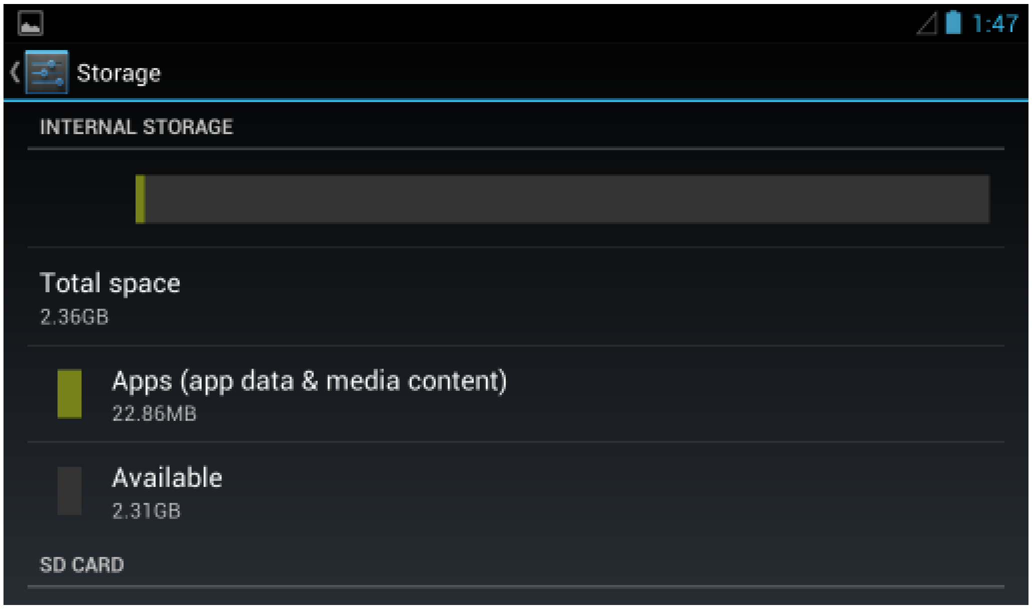
Internal Storage

Internal storage is the memory where most applications and data are stored.

The operating system protects all data and applications from power-related loss. Because the operating system mounts the entire file system in persistent storage, ET1 devices provide a reliable storage platform even in the absence of battery power. Internal Storage provides application developers with a reliable storage system available through the standard ext4 file system. Data in Internal storage is lost upon a Factory or Enterprise reset.

Internal Storage is approximately 2.3 GB (formatted). To view the available internal storage, touch ⚙ > ☰ **Storage**.

Figure 101: Storage Settings - Internal Storage



INTERNAL STORAGE

Total space
2.36GB

Apps (app data & media content)
22.86MB

Available
2.31GB

SD CARD

- **Total space** - Displays the total amount of space on the installed microSD card.
  - **Apps** - Displays the available space used for applications and media content on the internal storage.
  - **Available** - Displays the available space on the internal storage.

Enterprise Folder

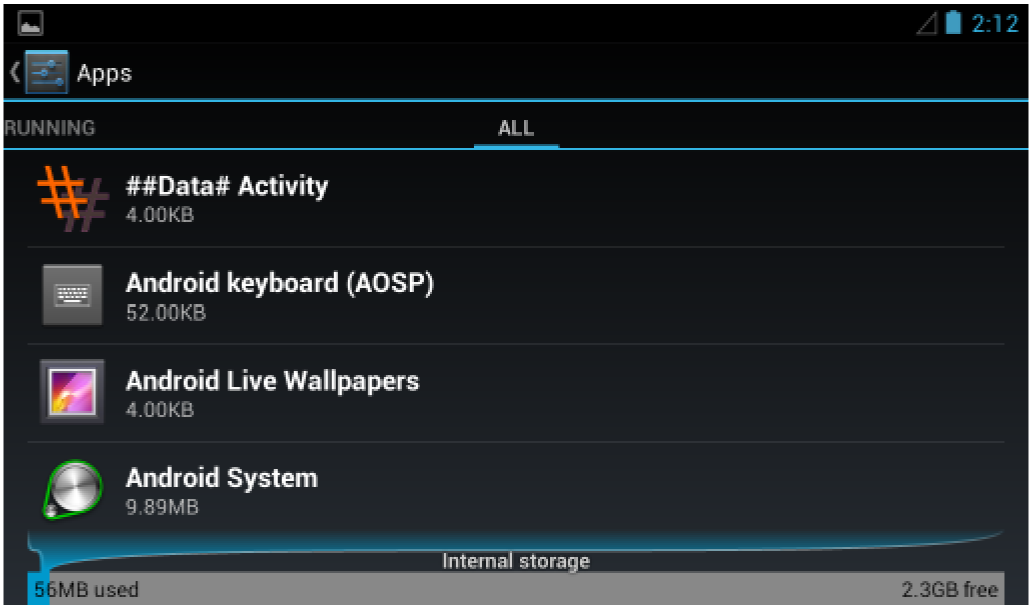
The Enterprise folder (within internal flash) is a super-persistent storage that is persistent after a reset and an Enterprise Reset. The Enterprise folder is erased during a Factory Reset. The Enterprise folder is used for deployment and device-unique data. The Enterprise folder is approximately 128 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 ≡ > **Manage apps**.

Figure 102: Manage Applications Screen



2:12

Apps

RUNNING ALL

##Data# Activity
4.00KB

Android keyboard (AOSP)
52.00KB

Android Live Wallpapers
4.00KB

Android System
9.89MB

Internal storage

56MB used 2.3GB free

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

When on the **Downloaded**, **All**, or **On SD card** tab, touch ≡ > **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 135* 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 SD card** 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.

Procedure:

1. Touch ≡ > **Manage apps**.
2. Touch an application, process, or service.

The **App Info** screen lists the application name and version number, and details about the application. Depending on the application and where it came from, it may also include buttons for managing the application's data, forcing the application to stop, and uninstalling the application. It also lists details about the kinds of information about your phone and data 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.

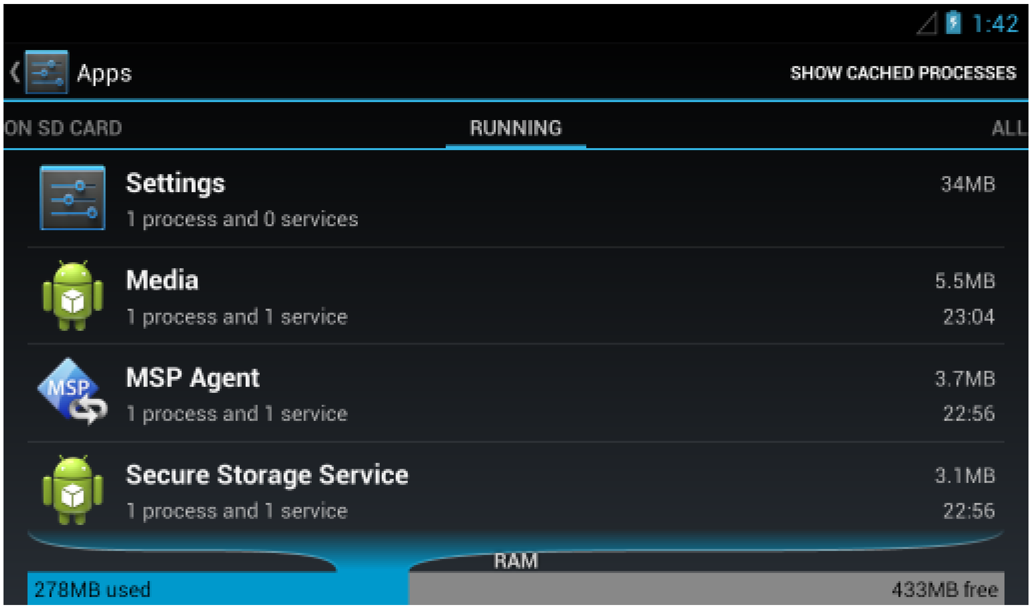
Procedure:

1 Touch ≡ > **Manage 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.

Figure 103: Running Applications



Settings 34MB
1 process and 0 services

Media 5.5MB
1 process and 1 service 23:04

MSP Agent 3.7MB
1 process and 1 service 22:56

Secure Storage Service 3.1MB
1 process and 1 service 22:56

RAM
278MB used 433MB free

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.

5 **Note:** Stopping an application or operating system processes and services disables one or more dependant functions on the device. The device may need to be reset to restore full functionality.

Touch **Stop**.

Changing Application Location

Some applications are designed to be stored on a microSD card, 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.

Procedure:

1 Touch ≡ > **Manage apps**.

2 Swipe the screen to display the **On SD card** tab.

The tab lists the applications that must be or can be stored on the microSD card. 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 the microSD card are checked.

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

3. Touch an application in the list.

   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.
4. Touch **Move to SD card** to move the bulk of the application from the device's internal storage to the microSD card.
5. 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 the microSD card in the Download directory. Use the **Downloads** application to view, open, or delete downloaded items.

Procedure:

1. Touch ⊞.
2. Touch ⬇.
3. Touch an item to open it.
4. Touch headings for earlier downloads to view them.
5. Check items to delete; then touch 🗑. The item is deleted from storage.
6. 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 10

Maintenance and Troubleshooting

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

Maintaining the ET1

For trouble-free service, observe the following tips when using the ET1:

- Do not scratch the screen of the ET1. When working with the ET1, use a finger or approved stylus or pen intended for use with a capacitive touch-sensitive screen. Never use an actual pen or pencil or other sharp object on the surface of the ET1 screen.
- The touch-sensitive screen of the ET1 is glass. Do not to drop the ET1 or subject it to strong impact.
- Protect the ET1 from temperature extremes. Do not leave it on the dashboard of a car on a hot day, and keep it away from heat sources.
- Do not store or use the ET1 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the ET1. If the surface of the ET1 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.
- Periodically replace the rechargeable battery to ensure maximum battery life and product performance. Battery life depends on individual usage patterns.

Battery Safety Guidelines

- The area in which the 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.
- Follow battery usage, storage, and charging guidelines found in this 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 ºF and +104 ºF (0 ºC and +40 ºC)
- Do not use incompatible batteries and chargers. Use of an incompatible battery or charger may present a risk of fire, explosion, leakage, or other hazard. If you have any questions about the compatibility of a battery or a charger, contact the Global Customer Support Center.
- For devices that utilize a USB port as a charging source, the device shall only be connected to products that bear the USB-IF logo or have completed the USB-IF compliance program.
- To enable authentication of an approved battery, as required by IEEE1725 clause 10.2.1, all batteries will carry a hologram. Do not fit any battery without checking it has the authentication hologram.
- 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 properly dispose of used re-chargeable batteries.
- Do not dispose of batteries in fire.
- 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, contact the Global Customer Support Center to arrange for inspection.

Cleaning Instructions

Caution:

Always wear eye protection.

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

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

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

Approved Cleanser Active Ingredients

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

Harmful Ingredients

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

Cleaning Instructions

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

Special Cleaning Notes

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

Cleaning Materials Required

- Alcohol wipes
- Lens tissue
- Cotton-tipped applicators
- Isopropyl alcohol

- Can of compressed air with a tube.

Cleaning Frequency

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

Cleaning the ET1

Housing

Using the alcohol wipes, wipe the housing including keys and in-between keys.

Display

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

Camera Window

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

Connector Cleaning

To clean the connectors:

Procedure:

1. Remove the main battery from mobile computer.
2. Dip the cotton portion of the cotton-tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton-tipped applicator back-and-forth across the connector. Do not leave any cotton residue on the connector.
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 4 through 6.

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

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

Cleaning Cradle Connectors

To clean the connectors on a cradle:

Procedure:

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

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

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

6 Remove any lint left by the cotton-tipped applicator.

7 If grease and other dirt can be found on other areas of the cradle, use a lint-free cloth and alcohol to remove.

8 Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

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

Troubleshooting

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

Troubleshooting the ET1 Enterprise Tablet

Table 6: Troubleshooting the ET1 Enterprise Tablet

Problem	Cause	Solution
When the user presses the Power button, the ET1 does not turn on.	Battery is completely discharged.	Re-charge or replace the battery.
	Battery not installed properly.	Install the battery properly. See *Installing the Battery on page 18*.
	Power button not held down long enough.	Press the Power button until the Battery Charge LED flashes three times.
	ET1 not responding.	Perform a hard reset. See *Performing a Hard Reset on page 24*.
When the user presses the Power button the ET1 does not turn on but the Decode LED blinks yellow.	Battery charge level is very low.	Re-charge or replace the battery.
Battery did not charge.	Battery failed.	Replace battery. If the ET1 still does not operate, perform a hardware reset. Simultaneously press the Power, Left Scan/Action and Right Scan/Action buttons.
	ET1 was removed from cradle while battery was charging.	Insert ET1 in cradle. The 4620 mAh battery fully charges in less than six hours.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0°C (32°F) or above 40°C (104°F).
During data communication, no data transmitted, or transmitted data was incomplete.	ET1 removed from cradle or disconnected from host com-	Replace the ET1 in the cradle, or reattach the communication cable and re-transmit.

Table continued…

Problem	Cause	Solution
	puter during communication.	
	Incorrect cable configuration.	See the system administrator.
No sound.	Volume setting is low or turned off.	Adjust the volume.
ET1 turns off.	ET1 is inactive.	The display turns off after a period of inactivity. Set this period to 15 seconds, 30 seconds, 1, 2, 10, or 30 minutes.
	Battery is depleted.	Recharge or replace the battery.
A message appears stating not enough storage memory.	Too many applications installed on the ET1.	Remove user-installed applications on the ET1 to recover memory. Select > **Apps** > **Downloaded**. Select the unused programs and touch **Uninstall**.
The ET1 does not decode when reading bar code.	DataWedge is not enabled.	Ensure that DataWedge is enabled and configured properly. Refer to the *ET1 Enterprise Tablet Integrator Guide* for more information.
	Unreadable bar code.	Ensure the symbol is not defaced.
	Distance between the ET1 and bar code is incorrect.	Place the ET1 within proper scanning range.
	ET1 is not programmed for the bar code type.	Program the ET1 to accept the type of bar code being scanned. Refer to the ET1 Enterprise Tablet Integrator Guide for DataWedge configuration.
	ET1 is not programmed to generate a beep.	If the ET1 does not beep on a good decode, set the application to generate a beep on good decode.
ET1 does not read magnetic stripe card.	Magnetic stripe on card is facing the wrong way.	Ensure that magnetic stripe card is oriented correctly. Magnetic stripe of card should be facing the display.
	MSR reading is not enabled.	Program the ET1 to accept MSR input. Refer to the *ET1 Enterprise Tablet Integrator Guide* for DataWedge configuration.
ET1 cannot find any Bluetooth devices nearby.	Too far from other Bluetooth devices.	Move closer to the other Bluetooth device(s), within a range of 10 meters (30 feet).
	The Bluetooth device(s) nearby are not turned on.	Turn on the Bluetooth device(s) to find.
	The Bluetooth device(s) are not in discoverable mode.	Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device’s user documentation for help.

Single-slot USB Docking Cradle Troubleshooting

Table 7: Troubleshooting the Single-slot USB Docking Cradle

Problem	Cause	Solution
ET1 battery is not charging.	ET1 was removed from cradle or cradle was unplugged from AC power too soon.	Ensure cradle is receiving power. Ensure ET1 is seated correctly. Confirm the battery is charging. The 4620 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The ET1 is not fully seated in the cradle.	Remove and re-insert the ET1 into the cradle, ensuring it is firmly seated.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
During data communication, no data transmits, or transmitted data was incomplete.	ET1 removed from cradle during communications.	Replace ET1 in cradle and retransmit.
	Communication software is not installed or configured properly.	Perform setup as described in the *ET1 Enterprise Tablet Integrator Guide*.

Four-slot Charge Only Docking Cradle Troubleshooting

Table 8: Troubleshooting the Four-slot Charge Only Docking Cradle

Problem	Cause	Solution
Battery is not charging.	ET1 removed from the cradle too soon.	Replace the ET1 in the cradle. The 4620 mAh battery fully charges in less than six hours. Tap ≡ > **Settings** > **About device** > **Status** to view battery status.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	ET1 is not inserted correctly in the cradle.	Remove the ET1 and reinsert it correctly. Verify charging is active. Tap ≡ > **Settings** > **About device** > **Status** to view battery status.
	Ambient temperature of the cradle is too warm.	Move the cradle to an area where the ambient temperature is between 0 °C (32 °F) and 35 °C (95 °F).

Four-slot Battery Charger Troubleshooting

Table 9: Troubleshooting the Four-slot Battery Charger

Problem	Cause	Solution
Battery not charging.	Battery was removed from the charger or charger was unplugged from AC power too soon.	Re-insert the battery in the charger or re-connect the charger's power supply. The 4620 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	Battery contacts not connected to charger.	Verify that the battery is seated in the battery well correctly with the contacts facing down.

USB/Charge Cable Troubleshooting

Table 10: Troubleshooting the USB/Charge Cable

Problem	Cause	Solution
Battery not charging.	ET1 was disconnected from AC power too soon.	Connect the power cable correctly. Confirm main battery is charging under ≡ > **Settings** > **About device** > **Status**. The 4620 mAh battery fully charges in less than six hours.
	Battery is faulty.	Verify that other batteries charge properly. If so, replace the faulty battery.
	The ET1 is not connected to power.	Detach and re-attach the power cable to the ET1, ensuring it is firmly connected.
During data communication, no data transmits, or transmitted data was incomplete.	Cable was disconnected from ET1 during communications.	Re-attach the cable and retransmit.
	Incorrect cable configuration.	See the system administrator.
	Communication software is not installed or configured properly.	Perform setup as described in the *ET1 Enterprise Tablet Integrator Guide*.

Chapter 11

Technical Specifications

The following sections provide technical specification for the device.

ET1 Technical Specifications

The following table summarize the ET1's intended operating environment and technical hardware specifications.

Table 11: ET1 Technical Specifications

Item	Description
Physical Characteristics	
Dimensions (with USB Host Expansion Module)	Height: 130.5 mm (5.14 in.) Width: 224 mm (8.82 in.) Depth: 25 mm (0.98 in.)
Weight	ET1N0: 630 g (22.4 oz.) ET1N2: 706 g (24.9 oz.)
Display	7 in. capacitive; 1024 x 600; 350 nit; Corning® Gorilla® Glass.
Touch Panel	Capacitive multi-touch.
Backlight	LED backlight.
Battery Pack	Rechargeable Lithium Ion 3.7V, 4620 mAh or 5640 mAh Smart battery.
Backup Battery	NiMH battery (rechargeable) 15 mAh 3.6 V (not user accessible).
Expansion Slot	User accessible microSD slot, up to 32 GB.
Connectivity	Two USB interfaces: one USB 2.0 OTG connector (docking connector) and one USB 2.0 Host connector (expansion module port); HDMI output; communication via cradle and expansion ports; USB 2.0 host via expansion module.
Notification	LED, audio and vibration.
Keypad Options	On-screen keyboard.
Audio	Stereo speakers, microphone and headset connector (mono, 2.5 mm jack with microphone.)
Performance Characteristics	

Table continued...

Item	Description
CPU	Texas Instruments OMAP 4430 @ 1 GHz.
Operating System	Android-based ASOP 4.1.1.
Memory	1GB RAM, 4 GB Flash plus 4 GB microSD; user accessible microsD card slot (supports up to 32 GB).
Output Power (USB)	Docking Connector: 5 VDC @ 500 mA max. Expansion Module: 5 VDC @ 500 mA max.
User Environment	
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0° C to 40° C (32°F to 104°F)
Humidity	10% to 95% RH non-condensing
Drop Specification	Multiple 1.2 m (4 ft.) drops per MIL-STD 810G specifications.
Electrostatic Discharge (ESD)	+/-15kVdc air discharge, +/-8kVdc direct discharge, +/-8kVdc indirect discharge
Sealing	IP54
Wireless LAN Data Communications	
Wireless Local Area Network (WLAN) radio	IEEE® 802.11a/b/g/n with internal antenna.
Data Rates Supported	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps. Note that 802.11n data rates may be higher.
Operating Channels	Chan 36-165 (5180 – 5825 MHz), Chan 1-13 (2412-2472 MHz); actual operating channels/frequencies depend on regulatory rules and certification agency.
Security	**Security Modes:** Legacy, WPA and WPA2 **Encryption:** WEP (40 and 128 bit), TKIP and AES **Authentication:** TLS, LEAP, EAP-FAST (MS-CHAP v2), EAP-FAST (GTC), EAP-PEAP (MSCHAPv2), EAP-PEAP (GTC), EAP-TTLS (PAP), EAP-TTLS (MSCHAP) and EAP-TTLS (MSCHAPv2).
Spreading Technique	Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM).
Wireless PAN Data and Voice Communications	
Bluetooth	Class II, v 2.1 with EDR; integrated antenna.
Wireless WAN Data (ET1N2 only)	
Wireless Wide Area Network	Data only: 3.5G GSM HSDPA and 3.5G CDMA-EVDO Rev A.
Data Capture	
Rear-facing Camera	For bar code scanning and image capture: 8 MP auto-focus camera with user controllable LED flash, illumination and aiming; captures 1D and 2D bar codes, photographs, video, signatures and documents.
Front-facing Camera	VGA camera optimized for video collaboration and low lighting condition.

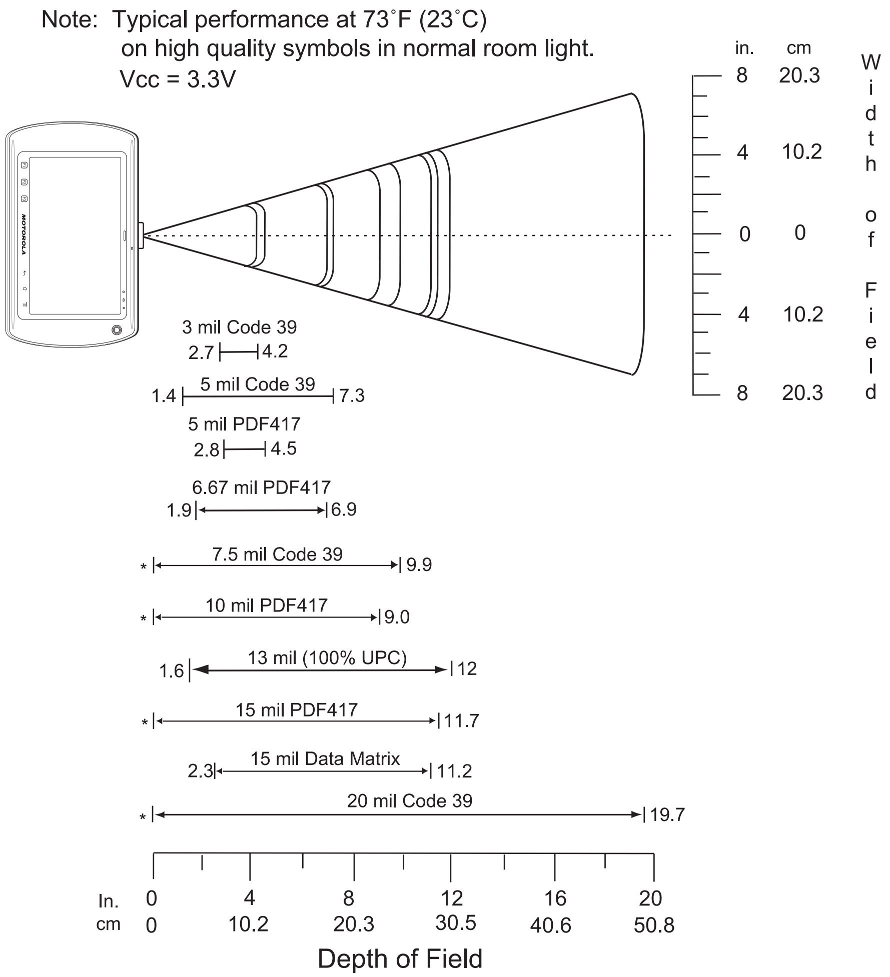
Table continued…

Item	Description
Scanning Module	For bar code scanning.
Scanning/MSR Module	For bar code scanning and reading magnetic stripe cards.
Sensors	
Gyroscope	Maintains orientation based on principles of conservation of angular momentum.
Motion Sensor	3-axis accelerometer that enables motion sensing applications for dynamic screen orientation and power management.
Ambient Light Sensor	Automatically adjusts display brightness.
Electronic Compass	Independent — does not depend on GPS.
Scanning / Scanning/MSR Module (SE4500-DL) Specifications	
Field of View	Horizontal - 39.2° Vertical - 25.4°
Optical Resolution	WVGA 752 H x 480 V pixels (gray scale)
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Outdoor: 9000 ft. candles (96,900 lux)
Focal Distance	From center of exit window: 18.5 cm (7.3 in.)
Aiming Element (VLD)	655 nm +/- 10 nm
Illumination Element (LED)	625 nm +/- 5 nm
Supported Symbologies	
1D	Chinese 2 of 5, Codabar, Code 11, Code 128, Code 39, Code 93, Discrete 2 of 5, EAN-8, EAN-13, GS1 DataBar, GS1 DataBar Expanded, GS1 DataBar Limited, Interleaved 2 of 5, Korean 2 of 5, MSI, TLC 39, Matrix 2 of 5, Trioptic, UPCA, UPCE, UPCE1, Web Code.
2D	Australian Postal, Aztec, Canadian Postal, Composite AB, Composite C, Data Matrix, Dutch Postal, Japan Postal, Maxicode, Micro PDF, Micro QR, PDF, QR Code, UK Postal, US Planet, US Postnet, US4State, US4State FICS.

Scanning and Scanning/MSR Module Decode Zone

The following figure shows the decode zone for the Scanning module and the Scanning/MSR module. Typical values appear. *Table 12: Decode Distances on page 156* lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar and space) in the symbol.

Figure 104: Scanning and Scanning/MSR Module Decode Zone



* Minimum distance determined by symbol length and scan angle.

Table 12: Decode Distances

Symbol Density/Bar Code Type	Bar Code Content/ Contrast Note 2	Typical Working Ranges	
		Near	Far
3.0 mil Code 39	80% MRD	2.7 in. 6.86 cm	4.2 in. 10.67 cm
5.0 mil Code 39	ABCDEFGH 80% MRD	1.4 in. 3.56 cm	7.3 in. 18.54 cm
5.0 mil PDF417	80% MRD	2.8 in. 7.11 cm	4.5 in. 11.43 cm
6.67 mil PDF417	4 Col, 20 Rows 80% MRD	1.9 in. 4.83 cm	6.9 in. 17.53 cm
7.5 mil	ABCDEF	Note 1	9.9 in.

Table continued...

Symbol Density/Bar Code Type	Bar Code Content/ Contrast Note 2	Typical Working Ranges	
		Near	Far
Code 39	80% MRD		25.15 cm
10 mil PDF417	3 Col, 17 Rows	Note 1	9.0 in. 22.86 cm
13 mil UPC-A	012345678905 80% MRD	1.6 in. 5.08 cm	12.0 in. 30.48 cm
15 mil PDF417	80% MRD	Note 1	11.7 in. 29.72 cm
15 mil Data Matrix	18 x 18 Modules 80% MRD	2.3 in. 5.84 cm	11.2 in. 28.45 cm
20 mil Code 39	123 80% MRD	Note 1	19.7 in. 50.04 cm

Notes:

1. Near distances are FOV limited.

2. Contrast is measured as Mean Reflective Difference (MRD) at 670 nm.

3. Working range specifications at temperature = 23 °C, pitch = 18°, roll = 0°, skew = 0°, photographic quality, ambient light ~30 ft-c, humidity 45 - 70% RH.

4. Distances measured from front edge of scan engine chassis.

ET1 I/O Connector Pin-Out

Figure 105: I/O Connector

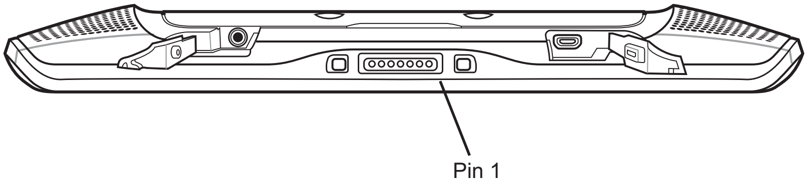


Table 13: External Connector Pin-Outs

Pin	Signal Name	Description
1	Cradle Detect	Tie to ground to indicate cradle insertion. Otherwise leave unconnected.
2	USB_ID	Tie to ground for Host mode. Leave unconnected for Client mode.
3	External Power IN	+12.0 VDC, +/- 5%, 20W
4	USB_VBUS	Host mode output = +5.0 VDC, 500mA max.

Table continued…

Pin	Signal Name	Description
		Client mode Vbus input = +5.0 VDC
5	USB_D-	USB Data Negative. High speed USB (480 Mbps) in both host and client modes. Also supports Full speed USB (12 Mbps) in both host and client modes.
6	USB_D+	USB Data Positive. High speed USB (480 Mbps) in both host and client modes. Also supports Full speed USB (12 Mbps) in both host and client modes.
7	Ground	Ground for all charging and USB communication.

ET1 HDMI Connector Pin-Out

Figure 106: Scanning and Scanning/MSR Module Decode Zone on page 158 shows the decode zone for the Scanning and Scanning/MSR Modules. Typical values appear. Table A-3 lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar and space) in the symbol.

Figure 106: Scanning and Scanning/MSR Module Decode Zone

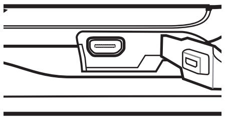


Table 14: HDMI Connector Pin-Outs

Pin	Signal Name	Description
1	Hot Plug Detect	Detect HMDI Cable Present/ Reset HMDI Device
2	Utility	Reserved
3	TMDS Data Channel 2+	Transition Minimized Differential Signaling Data Channel 2 positive
4	TMDS Data Channel 2 Shield	Transition Minimized Differential Signaling Data Channel 2 Shield Ground
5	TMDS Data Channel 2-	Transition Minimized Differential Signaling Data Channel 2 negative
6	TMDS Data Channel 1+	Transition Minimized Differential Signaling Data Channel 1 positive
7	TMDS Data Channel 1 Shield	Transition Minimized Differential Signaling Data Channel 2 Shield Ground
8	TMDS Data Channel 1-	Transition Minimized Differential Signaling Data Channel 1 negative
9	TMDS Data Channel 0+	Transition Minimized Differential Signaling Data Channel 0 positive
10	TMDS Data Channel 0 Shield	Transition Minimized Differential Signaling Data Channel 0 Shield Ground
11	TMDS Data 0-	Transition Minimized Differential Signaling Data Channel 0 negative
12	TMDS Clock+	Transition Minimized Differential Signaling Clock positive

Table continued...

Pin	Signal Name	Description
13	TMDS Clock Shield	Transition Minimized Differential Signaling Clock Shield Ground
14	TMDS Clock-	Transition Minimized Differential Signaling Clock negative
15	CEC	Consumer Electronics Control
16	Ground	System Ground
17	SCL	Display Data Channel I2C Clock
18	SDA	Display Data Channel I2C Data
19	Power (+5V)	+5 VDC Power out, 50 mA max.

ET1 Headset Pin-Out

Figure 107: Headset Connector

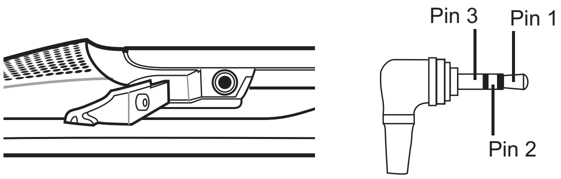


Table 15: Headset Connector Pin-Outs

Pin	Signal Name	Description
1	Mic +	Microphone positive
2	Speaker +	Speaker positive (32 ohm, 0.05 W, mono)
3	Speaker -	Speaker negative

ET1 Expansion Module Connector Pin-Out

Figure 108: Expansion Module Connector

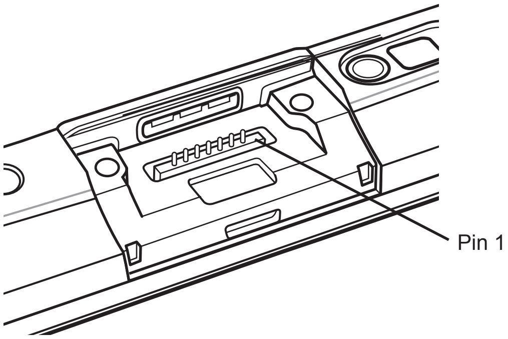


Table 16: Expansion Module Connector Pin-Outs

Pin	Signal Name	Description
1	Ground	System ground.
2	USB_D-	USB data negative. High speed USB (480 Mbps) in host mode only. Also supports Full speed USB (12 Mbps) in host mode only. NOTE: Client Mode is not supported via this USB interface.
3	USB_D+	USB Data Positive. High speed USB (480 Mbps) in host mode only. Also supports Full speed USB (12 Mbps) in host mode only. NOTE: Client Mode is not supported via this USB interface.
4	USB_VBUS	Host mode output = +5.0 VDC, 500 mA max. continuous or peak NOTE: Client Mode is not supported via this USB interface.
5	Ground	System ground.
6	System Power	Switched unregulated system power output. 3.2 VDC to 4.4 VDC, 150mA, max continuous or peak, combined from pins 6 and 7. Total system current (from battery), under any operating condition, must not exceed 1.5 A continuous.
7	System Power	Switched unregulated system power output. 3.2VDC to 4.4 VDC, 150mA, max continuous or peak, combined from pins 6 and 7. Total system current (from battery), under any operating condition, must not exceed 1.5 A continuous.

ET1 Accessory Specifications

The following sections summarize the ET1 accessories technical specifications.

Single-Slot USB Docking Cradle Technical Specifications

Table 17: Single-slot USB Docking Cradle Technical Specifications

Item	Description
Dimensions (with USB Host Expansion Module)	Height: 61.62 mm (2.43 in.) Width: 151.9 mm (5.98 in.) Depth: 138.39 mm (5.45 in.)
Weight	620 g (21.87 oz)
Input Voltage	12 VDC
Power Consumption (with ET1)	24 watts
Interface	USB
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Charging Temperature	0°C to 40°C (32°F to 104°F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Four-Slot Charge Only Cradle Technical Specifications

Table 18: Four-Slot Charge Only Cradle Technical Specifications

Item	Description
Dimensions (with USB Host Expansion Module)	Height: 83.45 mm (3.29 in.) Width: 243.28 mm (9.58 in.) Depth: 330.17 mm (13.00 in.)
Weight	1.678 kg (3.70 lbs.)
Input Voltage	12 VDC
Power Consumption (with ET1)	50 watts
Operating Temperature	0 °C to 50 °C (32 °F to 122 °F)

Table continued…

Item	Description
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

Four-Slot Battery Charger Technical Specifications

Table 19: Four-Slot Battery Charger Technical Specifications

Item	Description
Dimensions (with USB Host Expansion Module)	Height: 110.62 mm (4.36 in.) Width: 100.88 mm (3.97 in.) Depth: 245.15 mm (9.65)
Weight	580 g (20.46 in.)
Input Voltage	12 VDC
Power Consumption (with ET1)	25 watts
Operating Temperature	0 °C to 40 °C (32 °F to 104 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 40 °C (32 °F to 104 °F)
Humidity	5% to 95% non-condensing
Drop	76.2 cm (30.0 in.) drops to vinyl tiled concrete at room temperature.
Electrostatic Discharge (ESD)	+/- 15 kV air +/- 8 kV contact

USB/Charge Cable Technical Specifications

Table 20: USB/Charge Cable Technical Specifications

Item	Description
Length	160.0 cm (63.0 in.)
Operating Temperature	0 °C to 40 °C (32 °F to 104 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 kV air

Item	Description
	+/- 8 kV contact

2–Way Charge Cable Technical Specifications

Table 21: 2–Way Charge Cable Technical Specifications

Item	Description
Length	105.0 cm (41.3 in.)
Operating Temperature	-10 °C to 50 °C (14 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40°F to 158 °F)
Humidity	10% to 95% non-condensing
Electrostatic Discharge (ESD)	+/- 15 kV air, +/- 8 kV contact

Scanning Module Technical Specifications

Table 22: Scanning Module Technical Specifications

Item	Description
Dimensions (W x L x H)	3.34 cm x 5.49 cm x 3.09 cm (1.31 in. x2.16 in.x 1.22 in.)
Weight	34.3 g (1.2 oz)
Operating Temperature	°C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	10% to 95% non-condensing
Drop	4 ft. (1.22 m) drops to plywood over concrete.
Electrostatic Discharge (ESD)	+/- 15 kV air, +/- 8 kV contact
Scan Engine	
Field of View	Horizontal - 39.2° Vertical - 25.4°
Optical Resolution	752 H x 480 V pixels (gray scale)
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Outdoor: 9000 ft. candles (96,900 lux)
Focal Distance	From center of the exit window: 18.5 cm (7.3 in.)
Aiming Element (VLD)	655 nm +/- 10 nm
Illumination Element (LED)	625 nm +/- 5 nm LEDs (2x)

Scanning/MSR Module Technical Specifications

Table 23: Scanning/MSR Module Technical Specifications

Item	Description
Dimensions (W x L x H)	4.14 cm x 7.91 cm 3.97 cm (1.63 in. x 3.11 in. x 1.56 in.)
Weight	55.9 g (1.97 oz)
Operating Temperature	°C to 50 °C (32 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Humidity	5% to 95% non-condensing
Drop	4 ft. (1.22 m) drops to plywood over concrete
Electrostatic Discharge (ESD)	+/- 15 kV air, +/- 8 kV contact
Magnetic Stripe Reader	
Interface	USB
Format	ANSI, ISO, AAMVA, CA DMV, user-configurable generic format
Swipe Speed	127 to 1270 mm (5 to 50 in.) /sec, bi-directional
Decoders	Generic, Raw Data
Mode	Buffered, unbuffered
Track Reading Capabilities	Tracks 1 and 3: 210 bpi Track 2: 75 and 210 bpi, autodetect
Security	Built-in encryption engine. DES, Triple DES and AES Encryption. DUKPT key management. In-head electronics to prevent tempering.
Scan Engine	
Field of View	Horizontal - 39.2° Vertical - 25.4°
Optical Resolution	752 H x 480 V pixels (gray scale)
Roll	360°
Pitch Angle	+/- 60° from normal
Skew Tolerance	+/- 60° from normal
Ambient Light	Outdoor: 9000 ft. candles (96,900 lux)
Focal Distance	From center of the exit window: 18.5 cm (7.3 in.)
Aiming Element (VLD)	655 nm +/- 10 nm
Illumination Element (LED)	625 nm +/- 5 nm LEDs (2x)

Chapter 12

Keypad Remap Strings

Table 24: Remap Key Event/Scancodes

Key Event	Scancode
SOFT_LEFT	105
SOFT_RIGHT	106
HOME	102
BACK	158
CALL	231
ENDCALL	107
0	11
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10
STAR227	227
POUND	228
DPAD_UP	103
DPAD_DOWN	108
DPAD_LEFT	105
DPAD_RIGHT	106
DPAD_CENTER	232
VOLUME_UP	115
VOLUME_DOWN	114
CAMERA	212

Table continued…

Key Event	Scancode
A	30
B	48
C	46
D	32
E	18
F	33
G	34
H	35
I	23
J	36
K	37
L	38
M	50
N	49
O	24
P	25
Q	16
R	19
S	31
T	20
U	22
V	47
W	17
X	45
Y	21
Z	44
COMMA	51
PERIOD	52
ALT_LEFT	56
ALT_RIGHT	100
SHIFT_LEFT	42
SHIFT_RIGHT	54
TAB	15
SPACE	57
EXPLORER	150

Table continued…

Key Event	Scancode
ENVELOPE	155
ENTER	28
DEL	111
GRAVE	399
MINUS	12
EQUALS	13
LEFT_BRACKET	26
RIGHT_BRACKET	27
BACKSLASH	43
SEMICOLON	39
APOSTROPHE	40
SLASH	53
AT	215
PLUS	78
MENU	139
SEARCH	217
PAGE_UP	59
PAGE_DOWN	60
PICTSYMBOLS	61
SWITCH_CHARSET	62
BUTTON_A	63
BUTTON_B	64
BUTTON_C	65
BUTTON_X	66
BUTTON_Y	67
BUTTON_Z	68
BUTTON_L1	183
BUTTON_R1	184
BUTTON_L2	185
BUTTON_R2	186
BUTTON_THUMBL	187
BUTTON_THUMBR	188
BUTTON_START	189
BUTTON_SELECT	190
BUTTON_MODE	191

Index

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