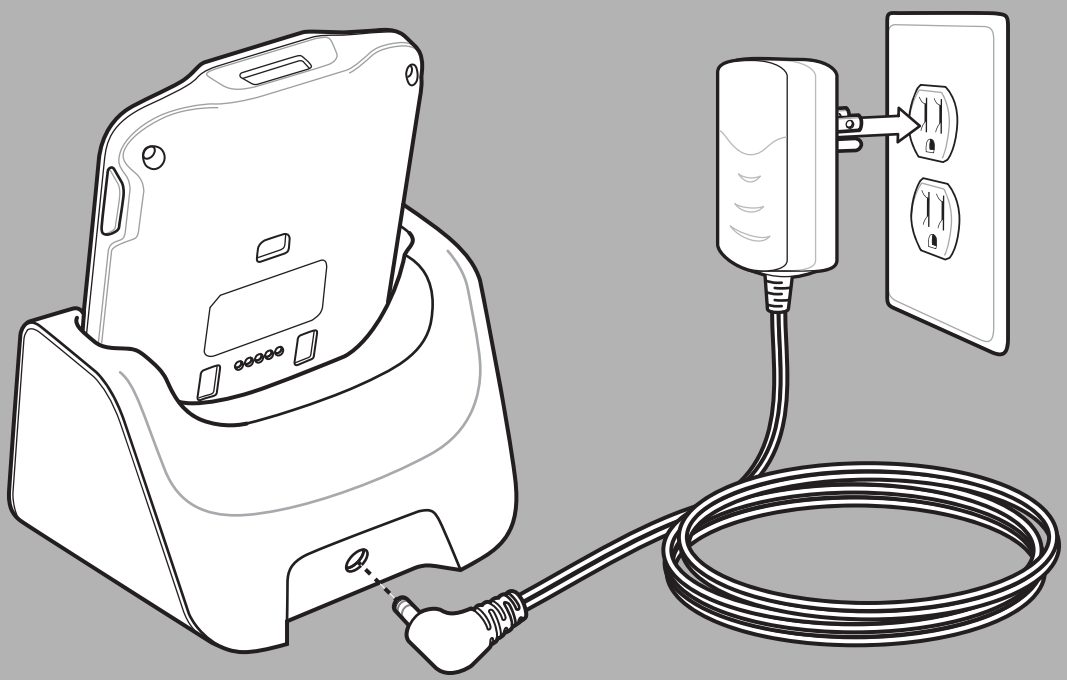
SB1
SMART BADGE
INTEGRATOR GUIDE



SB1 INTEGRATOR GUIDE

72E-164712-04
Rev. A
April 2019

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev. A	12/21/12	Initial Release.
-02 Rev. A	3/30/14	Add SB1-IAS and SB1-HC configurations and new lanyards. Add support for latest BSP.
-03 Rev. A	4/2015	Zebra Rebranding
-04 Rev. A	5/2019	Update cleaning procedures on page 5-3.

TABLE OF CONTENTS

ABOUT THIS GUIDE

Introduction

This guide provides information for configuring the SB1 and setting up SB1 accessories.

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

Documentation Set

The documentation set for the SB1 is divided into guides that provide information for specific user needs.

- *SB1 Regulatory Guide* - provides regulatory information for the SB1.
- *SB1 User Guide* - describes how to use the SB1.
- *SB1 Integrator Guide* - describes how to configure and set up the SB1 and the SB1 accessories.
- *SB1 Programmer's Guide* - describes how to write programs for use on the SB1.

Configurations

This guide covers the following configurations:

Configuration	Radio	Display	Memory	Data Capture	Audio
SB1-S	WLAN: 802.11 b/g/n	E Ink® touch screen	128 MB RAM/ 128 MB Flash	Bar code reader	Optional adapters for speaker and headset
SB1-IAS SB1-HC	WLAN: 802.11 b/g/n	E Ink® touch screen	128 MB RAM/ 128 MB Flash	Bar code reader	Built-in speaker and headset jack

Throughout this guide "SB1" refers to all configurations.

Software Versions

This guide covers various software configurations and references are made to software versions. To view the software versions:

1. Press the Home button.
2. Touch . The **Settings** screen appears.
3. Touch **More Settings**. The **More Settings** screen appears.
4. Touch **Advanced Settings**.
5. Touch **Software Version**. The **Software Version** screen lists the RhoElements and SB1 Shell versions.

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Initial Setup* - explains how to install and charge batteries and start the SB1 for the first time.
- *Chapter 2, Accessories* provide setup information for the SB1 accessories.
- *Chapter 3, Wireless Settings* - provides information for configuring the SB1 on a wireless network.
- *Chapter 4, Staging and Deployment* - provides information and guidelines for using MSP with the SB1.
- *Chapter 5, Maintenance and Troubleshooting* - includes instructions for cleaning and storing the SB1 and provides troubleshooting solutions for potential problems during operation.
- *Appendix A, Step By Step WLAN Setup Example* - provides a step by step example for setting up a WLAN using MSP.
- *Appendix B, Step By Step Creating Package Example* - provides a step by step example for creating a package using MSP.
- *Appendix C, Specifications* - lists the technical specifications for the SB1 and accessories.
- *Appendix D, Configuration* - provides special configuration information for the SB1.

Notational Conventions

The following conventions are used in this document:

- The term “SB1” refers to the Zebra SB1 smart badge.
- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Folder names

- **Bold** text is used to highlight the following:
  - Key names on a keypad
  - Button names on a screen.
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen.
- **`Courier Bold`** text is used to highlight filenames.
- ***Bold Italic*** text is used to highlight MSP package names.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents and Software

The following items provide more information about the SB1.

- *SB1 Regulatory Guide*, p/n 72-162415-xx
- *SB1 User Guide*, p/n 72E-164711-xx
- SB1 Programmer's Guide, p/n 72E-170991-xx
- *Administrating MSP 4.0*, p/n 72E-128775-04
- *Understanding Mobility Services Platform 4.0*, p/n 72E-128712-05
- Mobility Services Platform 4.0 Software Installation Guide, p/n 72E-100159-13
- Mobility Services Release Notes, p/n 72E-100160-17
- Using Mobility Services Platform 4.0, p/n 72E-128802-05

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 Global Customer Support for your region. Contact information is available at: http://www.zebra.com/support.

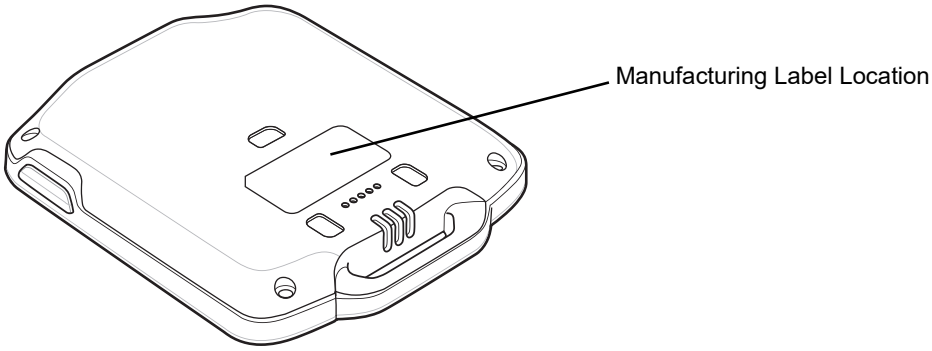
When contacting Zebra Global Customer Support, please have the following information available:

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

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

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

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



CHAPTER 1 INITIAL SETUP

This chapter provides information for setting up the SB1 for the first time and configuring the SB1.

Unpacking the SB1

Carefully remove all protective material from around the SB1 and save the shipping container for later storage and shipping. Verify that the equipment listed below is included:

- SB1
- Regulatory Guide.

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

Charging the SB1

CAUTION Follow the guidelines for battery safety described in *Battery Safety Guidelines on page 5-1*.

The SB1 must be charged within the 0 °C to +40 °C (32 °F to 104 °F) ambient temperature range.

When the SB1 is off it displays the Regulatory Label information screen.

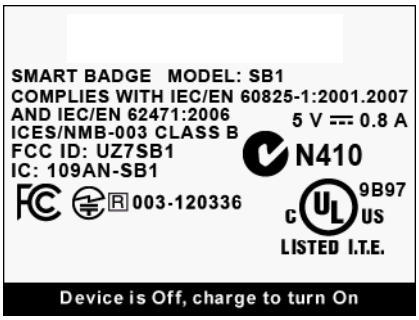


Figure 1-1 *Out of the Box Screen*

Use the Single Slot Charging cradle or Ten Slot Charge Only cradle to charge the SB1. To charge the SB1, slide it into the cradle slot with the Scan button facing up.

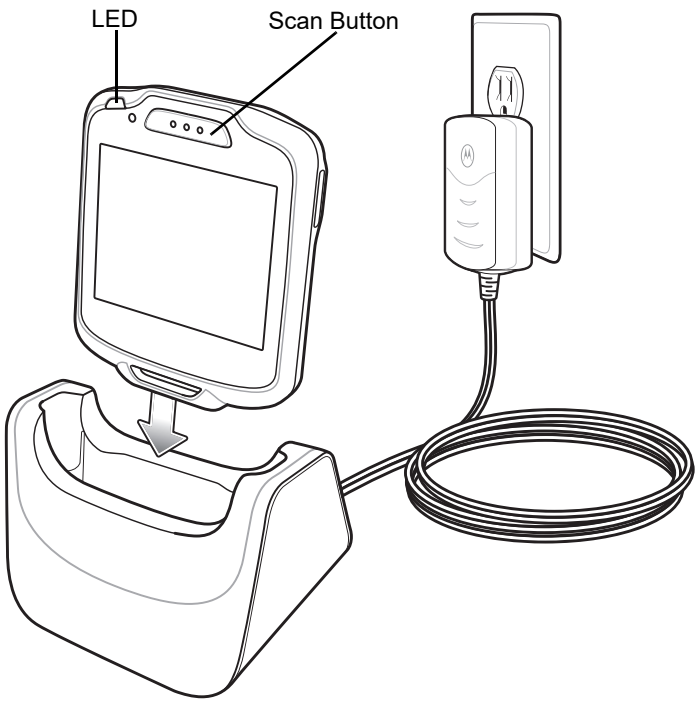


Figure 1-2 *Single Slot Charging Cradle*

NOTE If the battery is at a very low level due to the SB1 being left out overnight or stored for long periods, the SB1 might not power up immediately but the LED blinks. When the SB1 is placed in the charging cradle, it might not fully power up right away. After a few minutes, the SB1 boots normally.

When the SB1 powers up a beep sounds and the Calibration screen displays.

Leave the SB1 in the cradle until it is fully charged. The LED indicates the SB1 battery charging status. The battery fully charges in approximately four hours. See *Table 1-1 on page 1-3* for charging status indications. When the LED lights green remove the SB1 from the cradle.

Table 1-1 *LED Indicator*

LED	Indication
Off	SB1 not placed correctly in the cradle. The cradle is not powered. SB1 is not functioning properly.
Slow Blinking Amber	SB1 is charging.
Solid Green	Charging is complete.
Fast Blinking Amber	Charging error.

When using the SB1, if the battery charge falls below a predetermine level, it shuts down and displays the Battery Discharged screen.

Figure 1-3 *Battery Discharged Screen*

When this occurs, immediately recharge the SB1 battery by placing it into a charging cradle. The Battery Charging screen appears on the display when the SB1 is placed in the cradle.

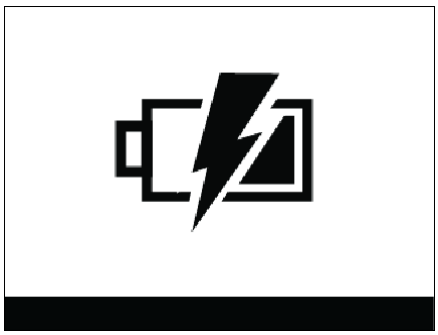


Figure 1-4 *Battery Charging Screen*

Resetting the SB1

If the SB1 stops responding to input, perform a reset (cold boot). A reset stops all running applications and any unsaved data (not specifically persisted in the *UserDrive* folder) is lost. Simultaneously press and hold the

Home and Scan buttons for five seconds. The Suspend screen appears. When the SB1 beeps release the buttons and then it resets.

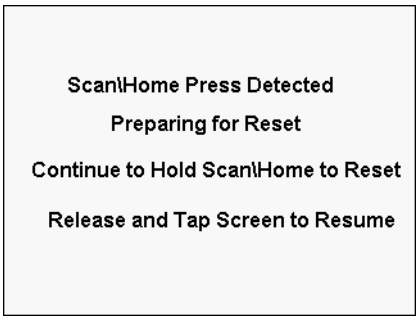


Figure 1-5 *Suspend Screen*

Start Up

After the SB1 boots up for the first time the **Home** screen displays. Refer to the *SB1 User Guide* for information on using the **Home** screen.

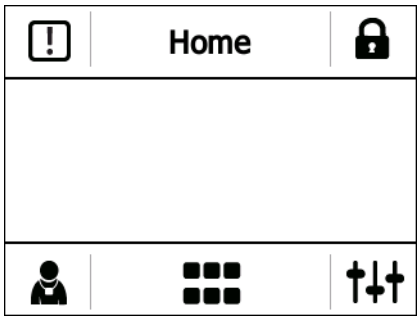


Figure 1-6 *Home Screen*

The SB1 is pre-loaded with a number of applications. Touch to open the **Applications** screen.

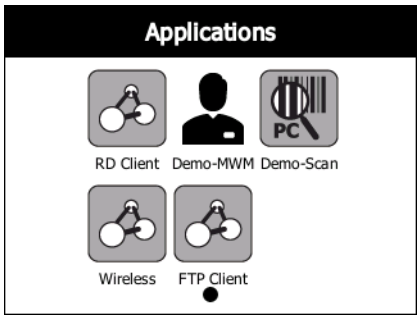


Figure 1-7 *Applications Screen*

The **Applications** screen has the following applications:

- **RD Client** - Use to stage the SB1 for initial use by initiating the deployment of settings, firmware and software. See *Chapter 4, Staging and Deployment* for detailed instructions.
- **Demo-MWM** - use to demonstrate the functionality of the SB1. Refer to the *SB1 User Guide*.
- **Demo-Scan** - use to demonstrate the SB1 scanning functionality. Refer to the *SB1 User Guide*.

- **Wireless** - use to setup the SB1 to connect to a WLAN. See *Chapter 3, Wireless Settings* for detailed instructions.
- **FTP Client** - use to copy files to the SB1 using a local ftp connection. Refer. to the *SB1 User Guide*

Advanced Settings

To access the advanced settings:

1. Press the Home button to access the **Home** screen.
2. Touch . The **Settings** screen appears.

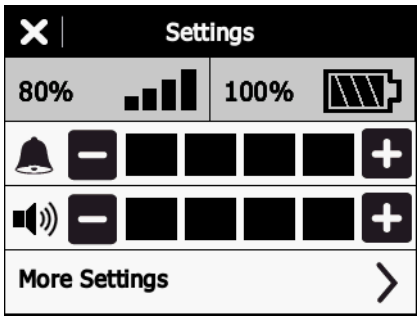


Figure 1-8 *Settings Screen*

3. Touch **More Settings**. The **More Settings** screen appears.
4. Touch **Advanced Settings**. The **Advanced Settings** screen appears.

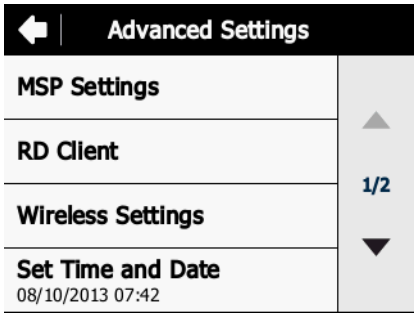


Figure 1-9 *Advanced Settings Screen*

The SB1 provides the following advanced setting:

- **MSP Settings** - Launches the MSP Agent application for monitoring and/or troubleshooting the operation of the MSP Agent. See *Chapter 4, Staging and Deployment* for detailed instructions.
- **RD Client** - Use to stage the SB1 for initial use by initiating the deployment of settings, firmware and software. *Chapter 4, Staging and Deployment* for detailed instructions.
- **Wireless Settings** - use to setup the SB1 to connect to a WLAN. See *Chapter 3, Wireless Settings* for detailed instructions.
- **Set Time and Date** - Use to set the time and date on the SB1.
- **Power Off Device** - Use to turn off the SB1.
- **Restore Factory Defaults** - Use to erase the SB1 user database.

Set Date and Time

NOTE The date and time can also be set using the MSP ***DateAndTime*** package or configuring Fusion to enable Auto Time Config. Only one method should be used to set the date and time to avoid conflicts.

To set the date and time on the SB1:

1. Touch . The **Settings** screen appears.
2. Touch **More Settings**. The **More Settings** screen appears.
3. Touch **Advanced Settings.** The **Advanced Settings** screen appears.
4. Touch **Set Date and Time**. The **Set Date and Time** screen appears.

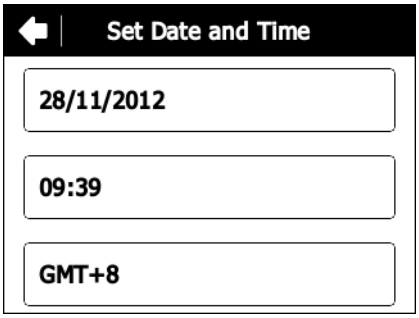


Figure 1-10 *Date and Time Screen*

5. Touch the date field. The **Set Date** screen appears.

Figure 1-11 *Set Date Screen*

6. Touch to delete the current date.
7. Use the keypad to enter the new date in the format DD/MM/YYY.
8. Touch . The **Set Date and Time** screen appears.
9. Touch the time field. The **Set Time** screen appears.

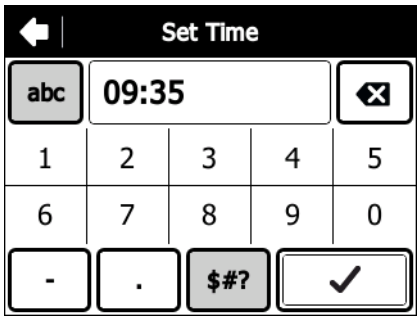


Figure 1-12 *Now Screen*

10. Touch ⌫ to delete the current time.
11. Use the keypad to enter the new date in the format HH:MM.
12. Touch ✓. The **Set Date and Time** screen appears.
13. Touch the time zone field. The **Timezone** screen appears.

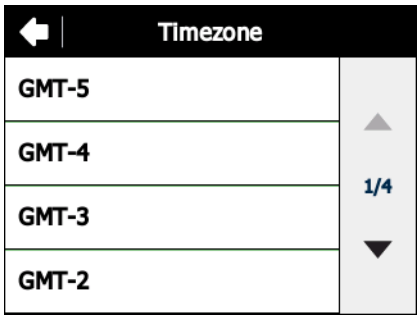


Figure 1-13 *Timezone Screen*

14. Use the up and down arrows to scroll to the time zone.
15. Touch a time zone option.
16. Touch ⬅.
17. Touch **OK** to confirm and return to the **Advanced Settings** screen.

Powering Off the SB1

Power off the SB1 when not using for long periods of time.

1. Press the Home button.
2. Touch ⚙. The **Settings** screen appears.
3. Touch **More Settings**. The **More Settings** screen appears.
4. Touch **Advanced Settings**. The **Advanced Settings** screen appears.
5. Touch the down arrow.
6. Touch **Power Off Device**.
7. Touch **OK**. The SB1 shuts down and the Regulatory Information screen appears.

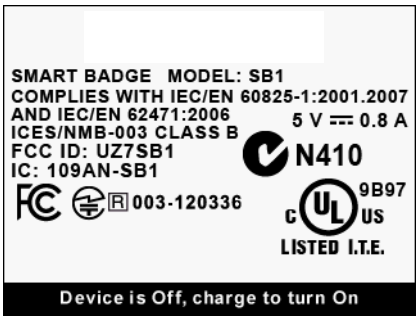


Figure 1-14 *Regulatory Information Screen*

To turn the SB1 back on, place the SB1 into a cradle.

Restore Factory Defaults

Restoring factory defaults deletes the user database information. All files installed in the *userDrive* folder are maintained. To return the SB1 to the factory default settings:

1. Press the Home button.
2. Touch . The **Settings** screen appears.
3. Touch **More Settings**. The **More Settings** screen appears.
4. Touch **Advanced Settings**. The **Advanced Settings** screen appears.
5. Touch the down arrow.
6. Touch **Restore Factory Defaults**.
7. Touch **OK** to confirm.

CHAPTER 2 ACCESSORIES

Introduction

This chapter provides information for setting up various SB1 accessories. *Table 2-1* lists the SB1 accessories.

Table 2-1 *SB1 Accessories*

Accessory	Part Number	Description
Cradles		
Single Slot Charging Cradle	CRDSB1X-1000CR	Charges the battery within the SB1.
Ten Slot Charge Only Cradle	CRDSB1X-4000CR	Charges up to ten SB1s.
Chargers		
Power Supply (5 VDC 850 mA)	PWRS-14000-XXXR	Provides power to the Single Slot Charging cradle.
Power Supply (12 VDC 4.16 A)	PWRS-14000-148R	Provides power to the Ten Slot Charge Only Cradle.
Miscellaneous		
Arm Band	SG-SB1X-WRSTB-01R	Provides a way to mount the clip-on holster for the SB1 on your arm.
Holster	SG-SB1X-HLSTR-02R	Provides a clip-on holder for wearing the SB1 on a belt.
Standard J-Hook Lanyard	KT-SB1X-LANYD-10R	Optional lanyard for holding the SB1 around the neck.
Long Neck Secure Attachment Lanyard	KT-SB1X-LANDYD2-10	Use to hold the SB1 around your neck. Contains fabric material to securely hold the SB1 (10-pack).
Long Neck Secure Attachment Lanyard	KT-SB1X-LANYD2-01	Use to hold the SB1 around your neck. Contains fabric material to securely hold the SB1.

Table 2-1 *SB1 Accessories (Continued)*

Accessory	Part Number	Description
Standard Secure Attachment Lanyard	KT-SB1X-LANYD3-01	Use to hold the SB1 around your neck. Contains fabric material to securely hold the SB1.
Mounting Bracket	KT-SB1X-MBRKT-01R	Mounts the Ten Slot Charging cradle to a rack or wall.
Headset Adapter	21-SB1XHSADP-01R KT-SB1X-HSADP-10R	Provides audio connectivity using a wired headset Single pack and 10-pack.
Speaker Adapter	21-SB1X-SKADP-01R KT-SB1X-SKADP-10R	Provides speaker for Push-To-Talk functionality. Single pack and 10-pack.
Developer Back Housing Kit	KT-SB1X-DEVLP-01R	Includes an SB1 back housing with a USB port, screw driver, six screws and a USB Cable. Allows developers to copy files to the user accessible folder.
Developer USB Dongle	KT-SB1X-DVCBL1-01	Allows developers to copy files to the user accessible folder on the SB1-IAS and SB1-HC configurations.
Speaker Headset	21-SB1X-HDSET-10R	Provides audio for hands-free PTT conversations. Contains a speaker, PTT button and volume control (10-pack).
Ear Bud Headset	21-SB1X-HDSET2-10R	Provides audio for hands-free PTT conversations. Contains ear fit speaker, PTT button and volume control (10-pack).

Single Slot Charging Cradle

Use the Single Slot Charging cradle to charge the SB1 battery.

CAUTION Ensure to follow the guidelines for battery safety described in *Battery Safety Guidelines on page 5-1*.

Setup

To set up the Single Slot Charging Cradle:

1. Plug the power plug of the power supply into the power port of the cradle.

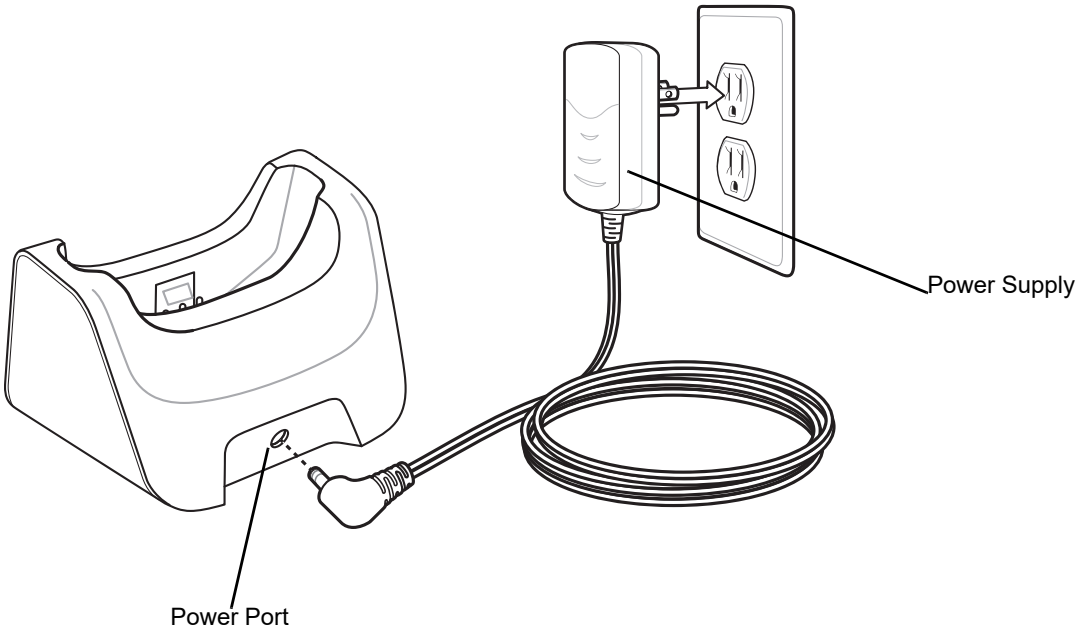


Figure 2-1 *Single Slot Charging Cradle Setup*

2. Plug the power supply into an outlet.

Charging

To charge the SB1:

1. If attached, remove SB1 from the lanyard.
2. Place the SB1 into the slot with the Scan button facing up. The LED Indicator indicates the SB1 battery charging status. The battery charges in less than four hours. See *Table 2-2* for charging status indications.

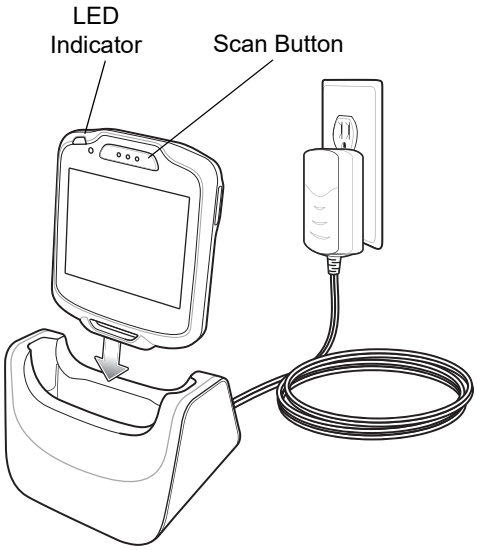


Figure 2-2 *Single Slot Charging Cradle*

3. When charging is complete, remove the SB1 from the cradle.

Table 2-2 *LED Charging Status Indicators*

LED	Indication
Off	SB1 is not placed correctly in the cradle or the cradle is not powered.
Slow Blinking Amber	SB1 is charging.
Solid Green	Charging complete.
Fast Blinking Amber	Charging error.

Ten Slot Charging Cradle

CAUTION Ensure to follow the guidelines for battery safety described in *Battery Safety Guidelines on page 5-1*.

The Ten Slot Charging cradle provides power for operating and charging up to ten SB1 devices.

Setup

To setup the Ten Slot Charging cradle:

1. Connect the power plug of the power supply to the Power Input port on the cradle.
2. Align the ferrite (Tube shape) into the cable holder and press into the holder.
3. If required, wind the cable around the wire tabs to shorten the cable.
4. Connect the AC line cord to the power supply.
5. Connect AC Line Cord to an AC outlet.

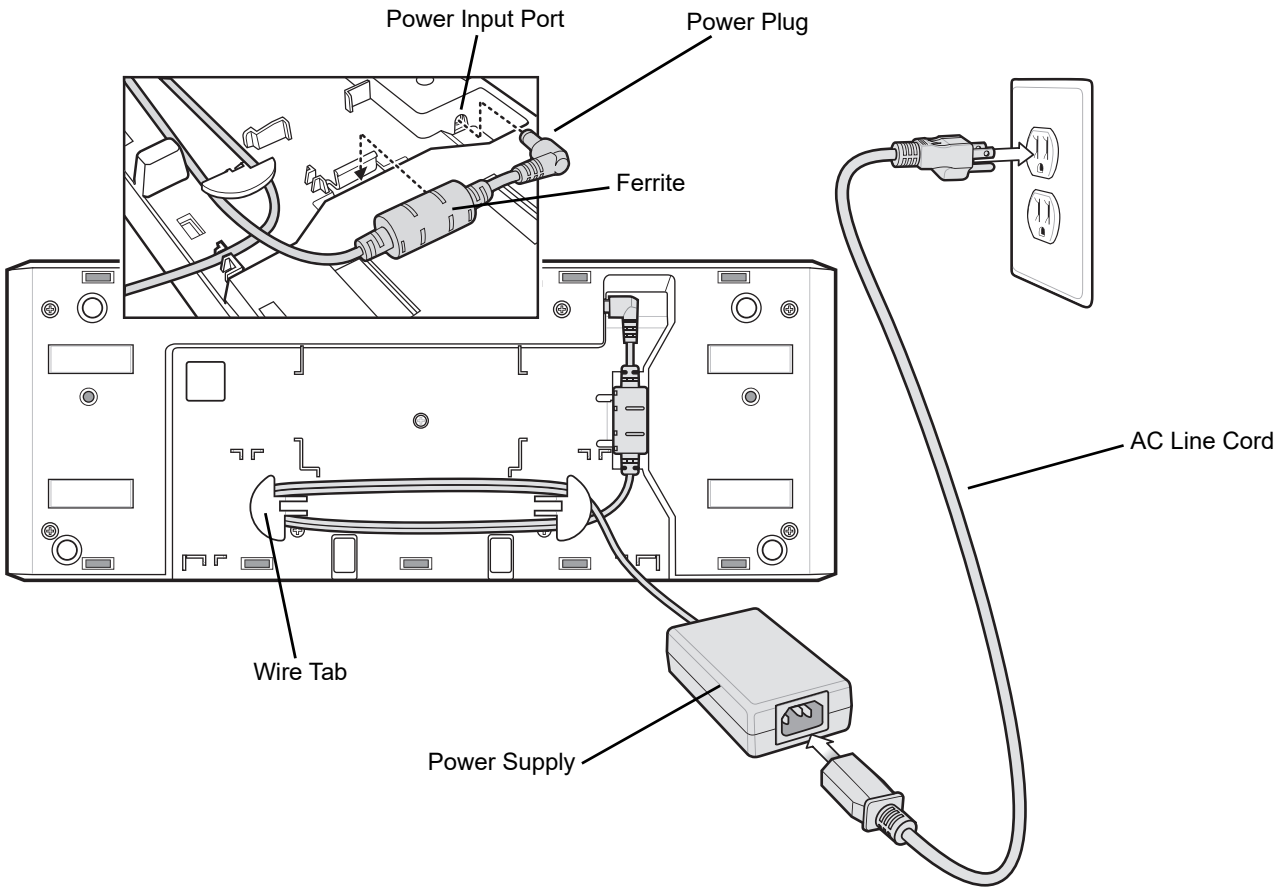


Figure 2-3 *Ten Slot Charging Cradle Setup*

Battery Charging

Place the SB1 into the slot with the Scan button and Charge LED Indicator facing up.

The SB1 Charge LED Indicator indicates the SB1 battery charging status. The battery charges in approximately four hours. See *Table 2-2 on page 2-4* for charging status indications.

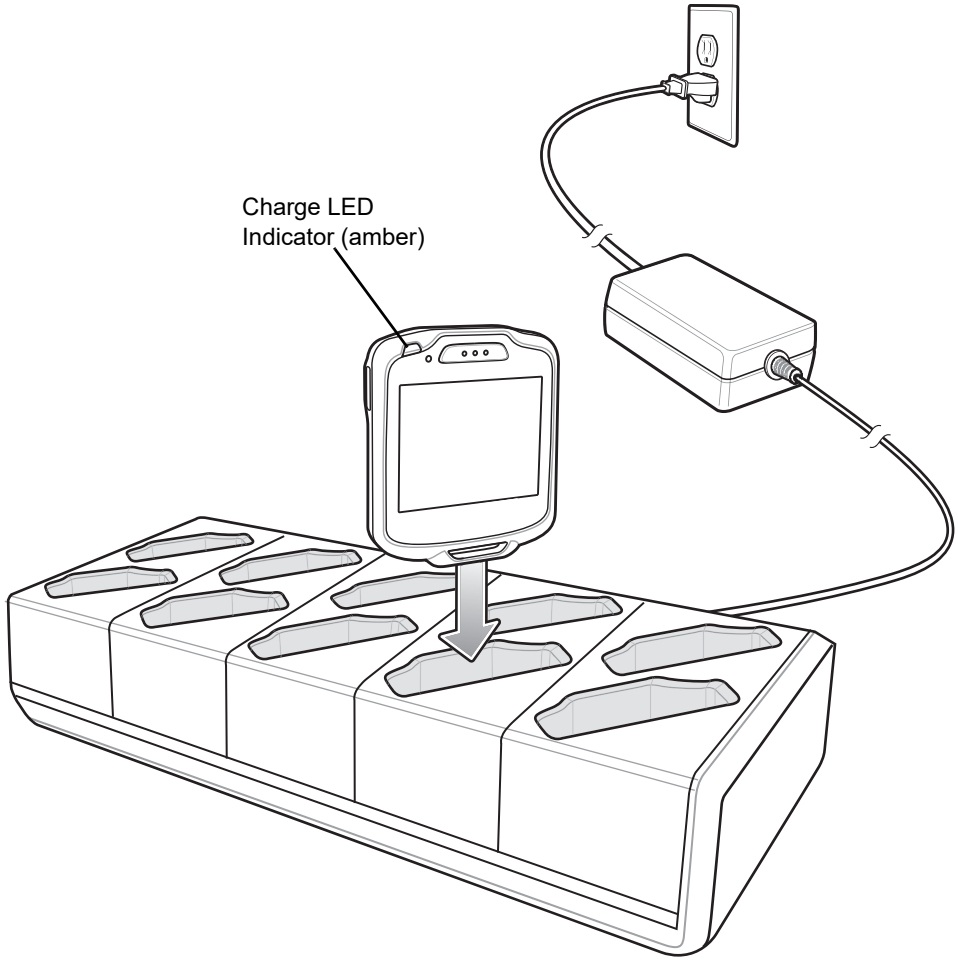


Figure 2-4 *Ten Slot Charging Cradle*

Mounting Bracket

Use the mounting bracket to mount the Ten Slot Charge Only cradle to a wall or 19 inch rack.

Setup

To set up the Ten Slot Charge Only Cradle:

1. Remove the backing from the black rubber pad and place onto the back of the Ten Slot Charging Cradle as shown.
2. Place the power supply into the mounting tabs.

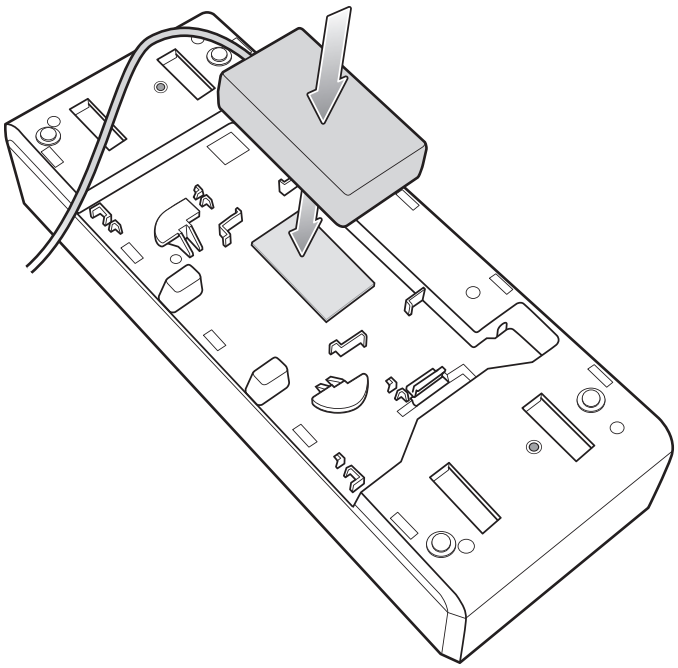


Figure 2-5 *Install Power Supply*

3. Plug the AC line cord into the power supply.
4. Wrap the power supply cord around the cable guides.

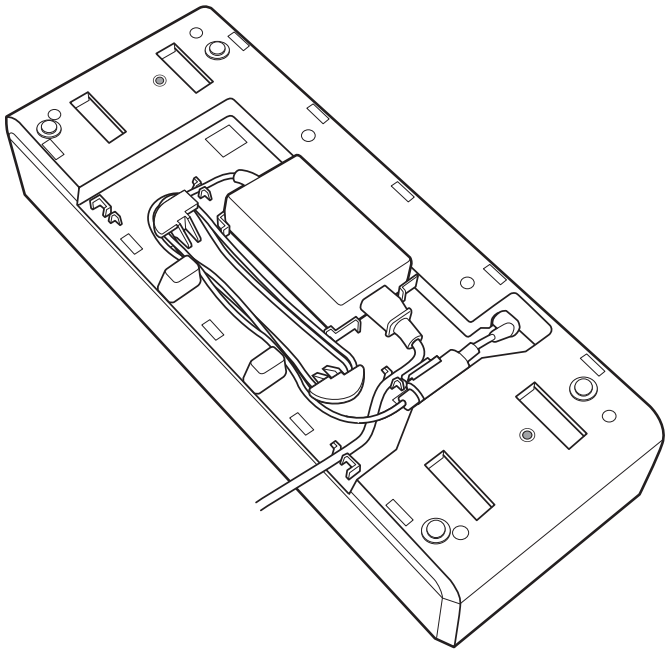


Figure 2-6 *Cable Routing*

5. Plug the power plug into the power port on the cradle.
6. Snap the ferrite into the mounting slot.
7. Place the four mounting bracket tabs into the slots on the cradle.

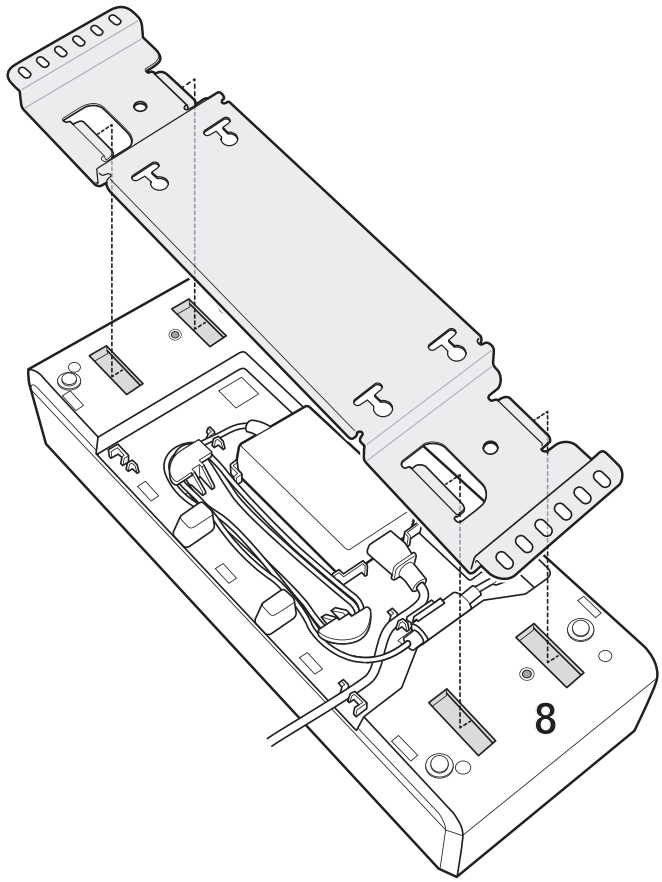


Figure 2-7 *Align Tab with Cradle*

8. Slide the mounting bracket up until the tabs enter the slots.
9. Secure the mounting bracket to the cradle using the two supplied screws. Torque to 20 kgf-cm(1.45 bf-ft).

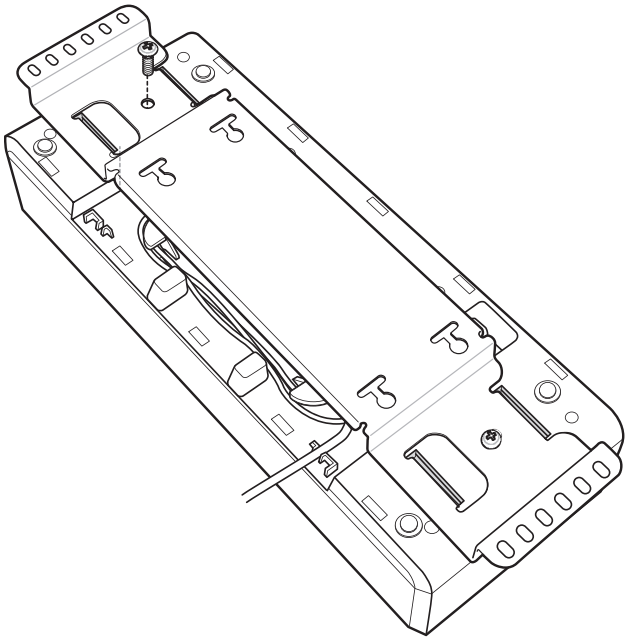


Figure 2-8 *Secure Mounting Bracket to Ten Slot Charge Only Cradle*

Wall Mounting

To mount the Ten Slot Charge Only Cradle and Mounting Bracket to a wall:

CAUTION Use mounting hardware (screws and/or anchors) appropriate for the type of wall mounting the bracket onto. The Mount Bracket mounting slots dimensions are 5 mm (0.2 in.). Fasteners must be able to hold a minimum of 4.5 Kg (10 lbs.)

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

1. Mark the four screw hole locations and drill holes.

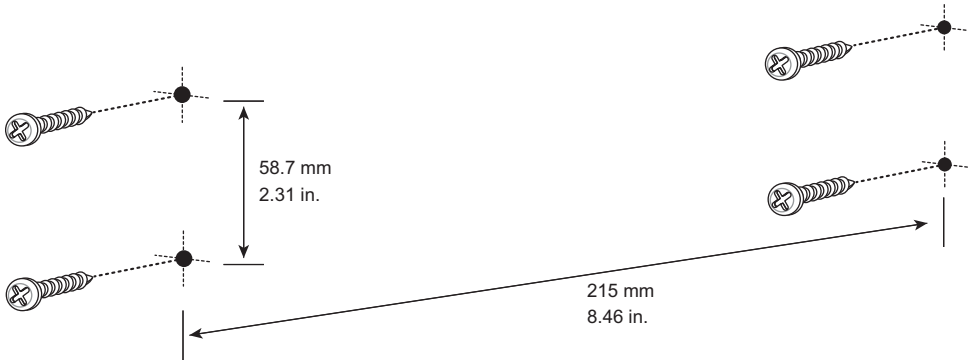


Figure 2-9 *Screw Template*

2. Install the four screws and/or anchors into the wall.
3. The screw heads should protrude 2.5 mm (0.01”) from the wall.

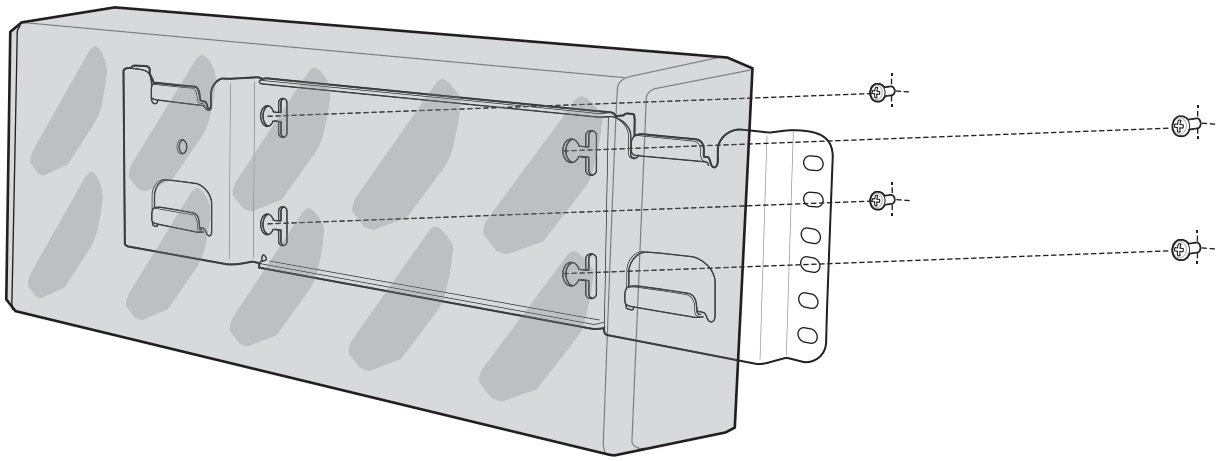


Figure 2-10 *Mounting Bracket onto Screws*

4. Align the mounting bracket’s mounting holes with the screws. Place the bracket/cradle assembly on the screws.
5. Slide the bracket/cradle assembly to the left and down.

Rack Mounting

To mount the Ten Slot Charging Cradle onto a standard rack:

1. Align the mounting holes on the bracket with the mounting holes on the rack.
2. Secure the bracket to the rack using four screws provided with the rack.

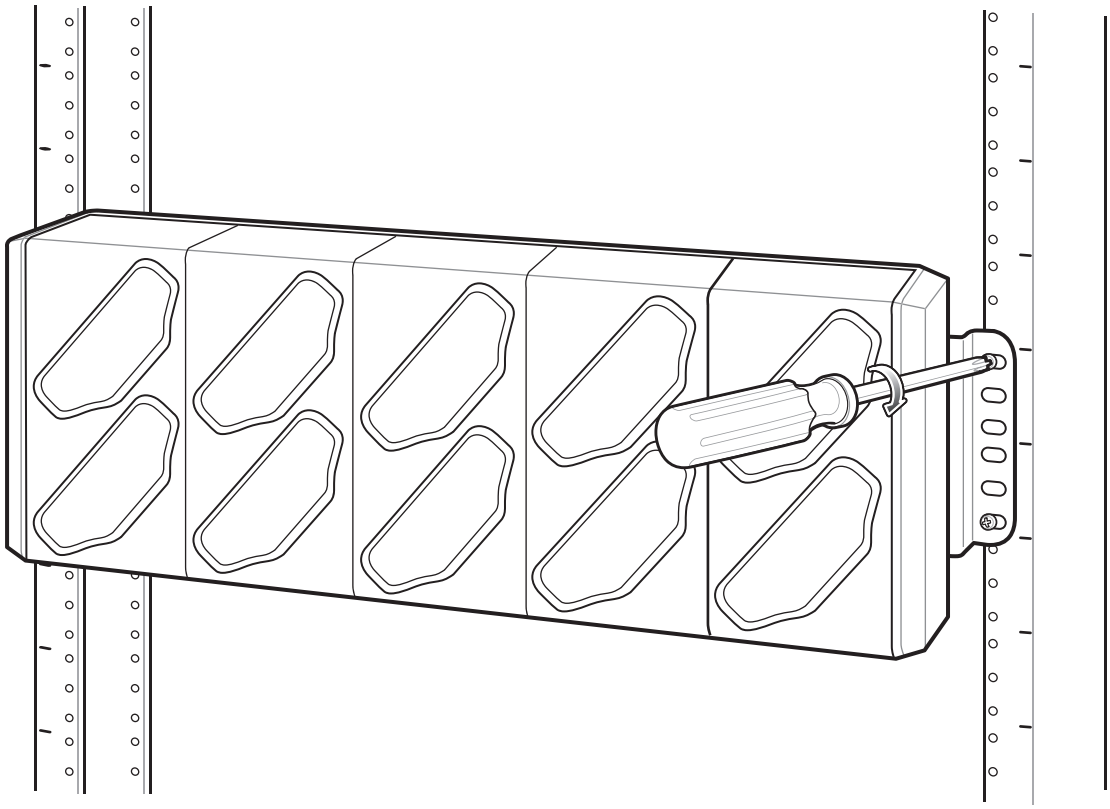


Figure 2-11 *Mounting On Rack*

Developer Back Housing

NOTE SB1-S only.

The Developer Back Housing provide USB connection for communication with a host computer.

Setup

To use the Developer Back Housing, the back housing of the SB1 must be removed and replaced with the Developer Back Housing. The Developer Back Housing Kit contains:

- Developer Back Housing
- Four long screws
- Two short screws
- Screwdriver
- USB cable.

To install the Developer Back Housing:

1. Power off the SB1.
2. Turn the SB1 face down on a table.
3. Using the supplied screwdriver, remove six screws securing the back housing to the SB1.

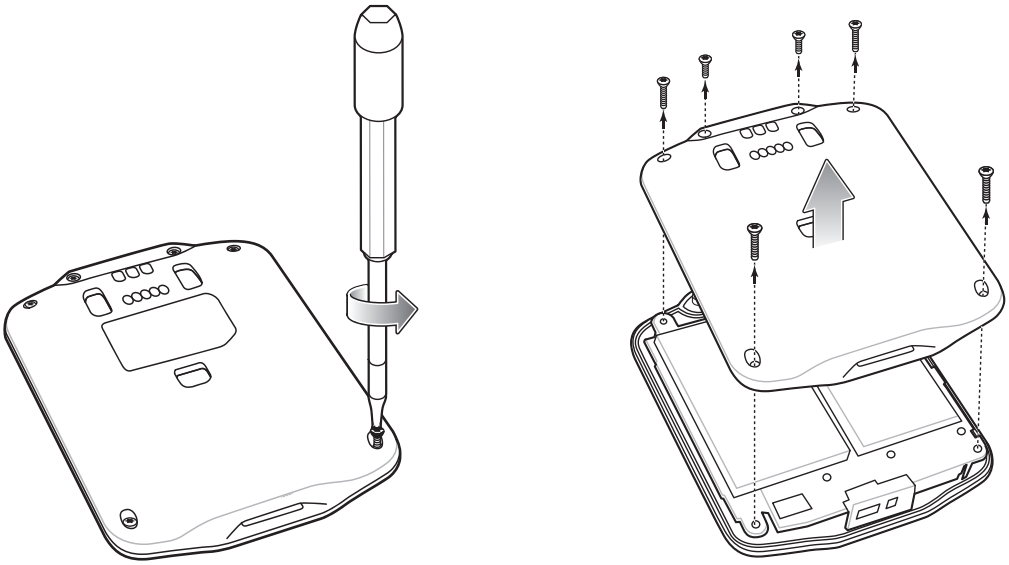


Figure 2-12 *Remove Back Housing Screws*

4. Remove the back housing.
5. Align the Developer Back Housing with the SB1.
6. Lower the Developer back Housing onto the SB1.

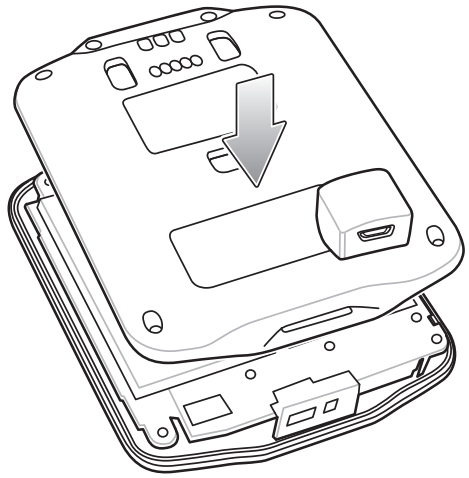


Figure 2-13 *Align and Lower New Back Housing*

7. Using the supplied screwdriver, secure the four longer screws and two shorter screws.

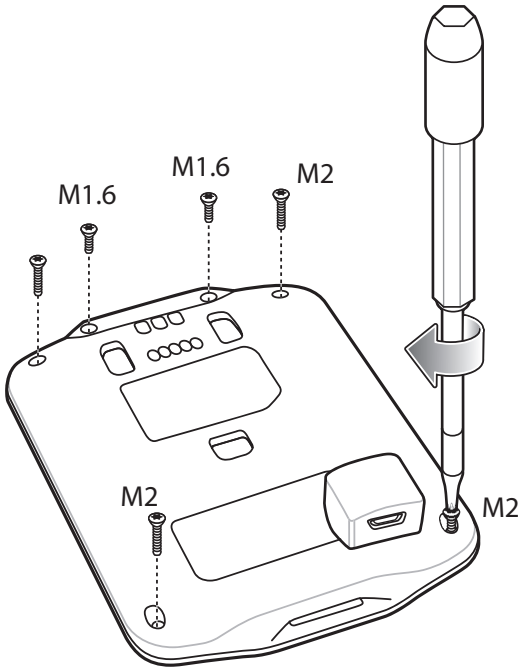


Figure 2-14 *Secure Back Housing*

8. Turn on the SB1.

Communication

To connect the SB1 to a host computer:

NOTE In order for the host computer to see the SB1 as a drive, Windows XP special file system drivers have to be installed on the host computer. Go to the following Microsoft web site: http://www.microsoft.com/en-us/download/details.aspx?id=19364 to download the drivers.

1. Connect the micro USB connector the USB cable into the USB port on the Developer Back Housing.

2. Connect the USB connector to the USB port on the host computer.

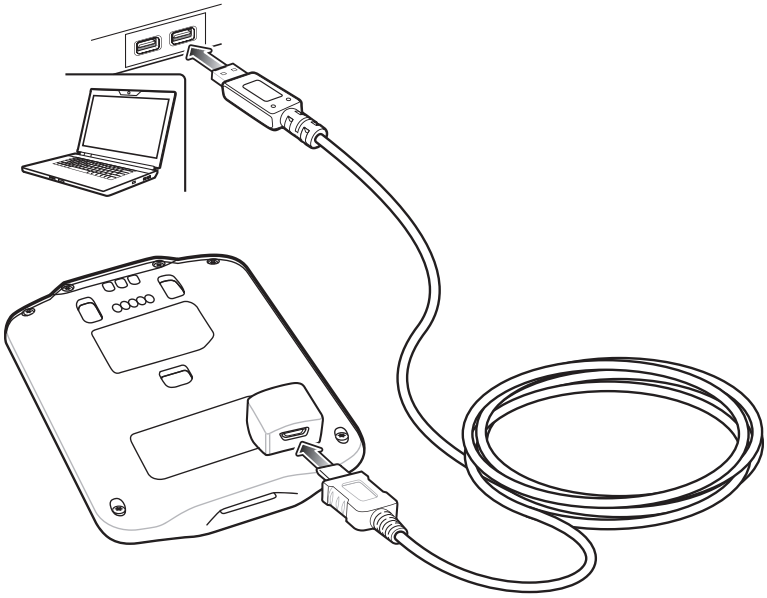


Figure 2-15 *Connect SB1 to Host Computer*

3. On the host computer, open **Windows Explorer**. The SB1 appears as a hard disk drive in **Windows Explorer**.
4. On the host computer, open another **Windows Explorer** window and locate the files to copy to the SB1.
5. Drag the files from the new window to the SB1 folder window.
6. When complete, disconnect the SB1 from the host computer.

Developer USB Dongle

NOTE SB1-IAS and SB1-HC only.

The Developer USB Dongle provide USB connection for SB1-IAS and SB1-HC communication with a host computer.

1. Insert the SB1 top first into the Developer USB Dongle.
2. Rotate the bottom of the SB1 into the dongle until it snaps into place.

NOTE In order for the host computer to see the SB1B-A as a drive, Windows XP special file system drivers have to be installed on the host computer. Go to the following Microsoft web site: http://www.microsoft.com/en-us/download/details.aspx?id=19364 to download the drivers.

3. Connect the micro USB connector the USB cable into the USB port on the Developer Back Housing.

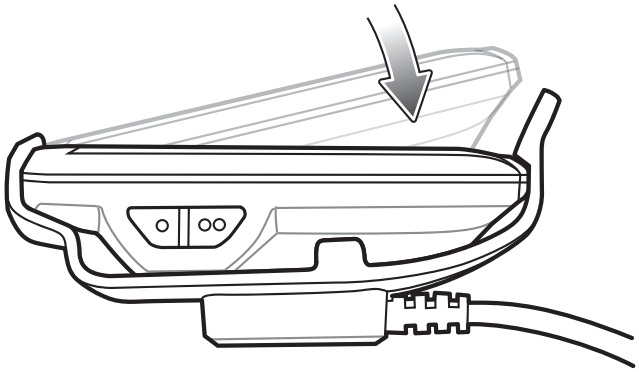


Figure 2-16 *Installing the SB1 into the Developer USB Dongle*

4. Connect the USB connector to the USB port on the host computer.

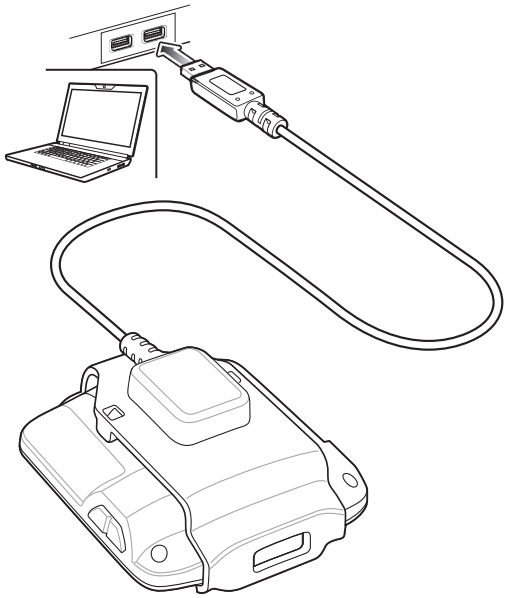


Figure 2-17 *Connect SB1B-A to Host Computer*

5. On the host computer, open **Windows Explorer**. The SB1 appears as a hard disk drive in **Windows Explorer**.
6. On the host computer, open another **Windows Explorer** window and locate the files to copy to the SB1.
7. Drag the files from the new window to the SB1 folder window.
8. When complete, disconnect the SB1 from the host computer.

CHAPTER 3 WIRELESS SETTINGS

Wireless Local Area Networks (WLANs) allow the SB1 to communicate wirelessly inside a building. Before using the SB1 on a WLAN, the facility must be set up with the required hardware to run the WLAN (sometimes known as infrastructure). The infrastructure and the SB1 must both be properly configured to enable this communication.

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

Once the infrastructure is set up to enforce the chosen WLAN security scheme, use the **Wireless Settings** software (Fusion) to configure the SB1 to match the WLAN settings.

Overview

The **Wireless Settings** software contains applications with which to create wireless profiles. Each profile specifies the security parameters to use for connecting to a particular WLAN as identified by its Extended Service Set Identification (ESSID). The software also allows the user to control which profile out of a set of profiles is used to connect. Other applications allow the user to monitor the status of the current WLAN connection and to invoke diagnostic tools for troubleshooting.

To access **Wireless Settings**, touch **Home** button > ⚙ > **More Settings** > **Advanced Settings** > **Wireless Settings**.

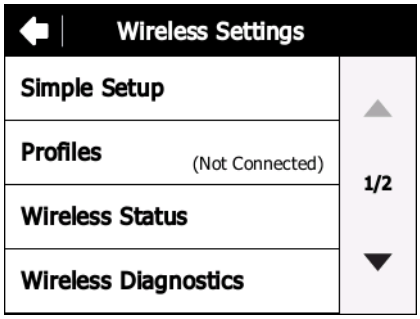


Figure 3-1 *Wireless Settings Window*

The **Wireless Settings** screen contains the following options:

- Simple Setup

- Profiles
- Wireless Status
- Wireless Diagnostics
- WLAN Enable / Disable
- Quick Options.

Use the up and down arrows to view all options.

Enable/Disable WLAN Radio

By default, the WLAN radio is on (enabled). To turn off (disabled) the WLAN radio, touch **WLAN Enabled**.

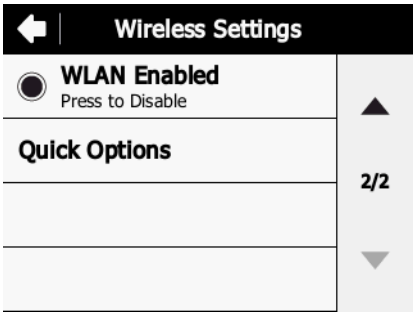


Figure 3-2 *Wireless Enabled*

The option changes to **WLAN Disabled**.

To turn on WLAN, touch **WLAN Disabled**. The option changes to **WLAN Enabled**.

Simple Setup

The **Simple Setup** application can create only a subset of wireless profiles (Open, WPA Personal (TKIP) and WPA2 Personal (AES)) by entering ESSID and passphrase, with all other settings set to default values. To create other types of wireless profiles (WPA Enterprise, WPA2 Enterprise, etc), use Mobile Device Management (MDM) software like MSP or use **Import Locally** application to import wireless configuration data which is exported from a device running Fusion X2.00 or Fusion X2.01.

Use **Simple Setup** to manually configure a wireless network connection for Open, WPA-Personal (TKIP), WPA2-Personal (AES) networks and to import a setup file stored locally from the *UserDrive*.

NOTE **Simple Setup** application displays a dialog box to enter password if a password is configured.

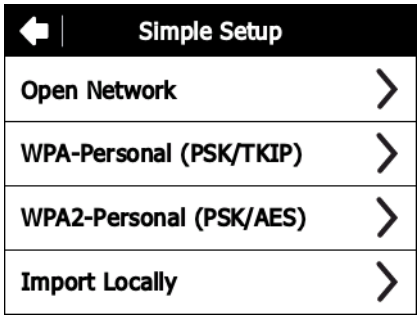


Figure 3-3 *Simple Setup Window*

Connecting to an Open Network

To connect to an open network:

1. Touch **Simple Setup**.
2. Touch **Open Network**.

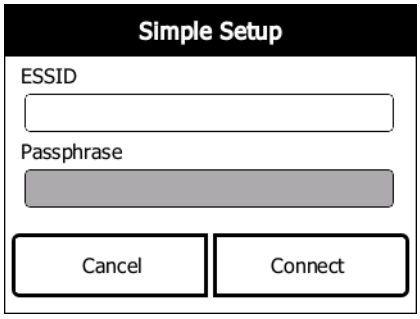


Figure 3-4 *Open Network ESSID*

3. In the **ESSID** text box, enter the ESSID name for the wireless network.
4. Touch **Connect**. The SB1 creates a profile with the provided information and connects to the wireless network.

Connecting to a Secure Network

To connect to a secured network:

1. Touch **Simple Setup**.
2. Touch **WPA-Personal (PSK/TKIP)** or **WPA2-Personal (PSK/AES)**.

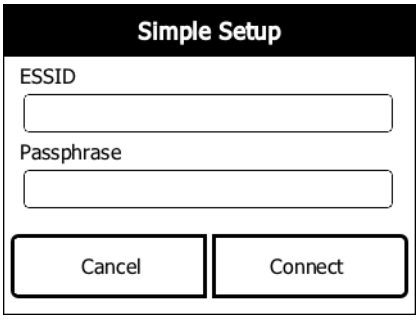


Figure 3-5 *ESSID / Passphrase Window*

3. In the **ESSID** text box, enter the ESSID for the network.
4. In the **Passphrase** text box, enter the network passphrase.
5. Touch **Connect**. The SB1 creates a profile with the provided information and connects to the wireless network.

Import

Use the **Import Locally** option to import wireless configuration data from a file stored in the *UserDrive*.

1. Copy the wireless configuration file to the *\UserDrive\Fusion-Data\Import* folder. See *Developer Back Housing on page 2-12* for instructions for copying files to the SB1.
2. Touch **Simple Setup**.
3. Touch **Import Locally**. A confirmation dialog appears.

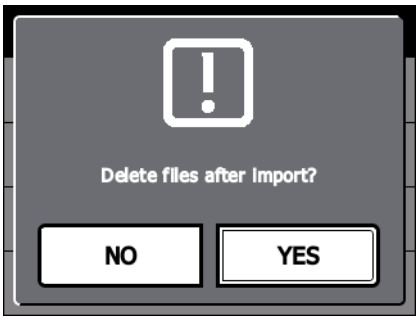


Figure 3-6 *Delete File Confirmation Message*

4. Touch **No** to leave the file on the SB1 or **Yes** to delete the file after it has been imported.

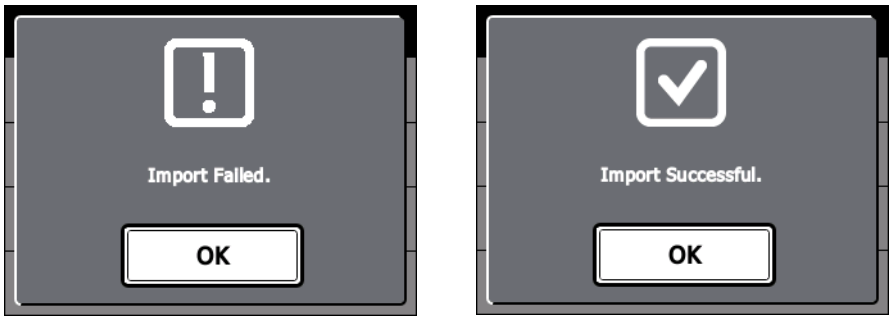


Figure 3-7 *Import Notification Message*

5. Touch **OK**.

Profiles

Touch the **Profiles** option to display a list of available profiles. The **Select a profile** window displays.

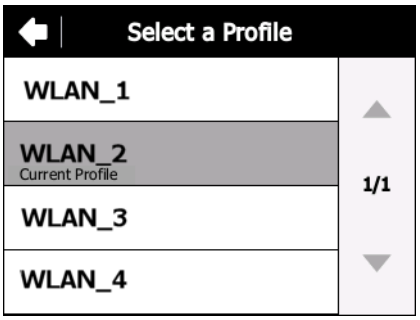


Figure 3-8 *Select a Profile Window*

Connecting to the Profile

To connect to the profile:

1. Touch a profile to connect to.

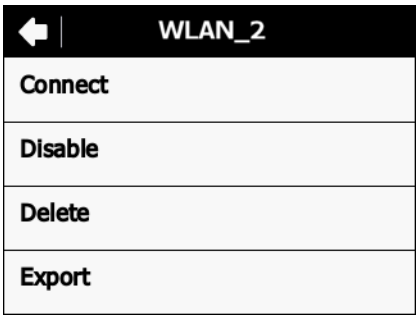


Figure 3-9 *Profile Window*

2. Touch **Connect**. The Wireless Settings screen displays with the profile name and connection status.

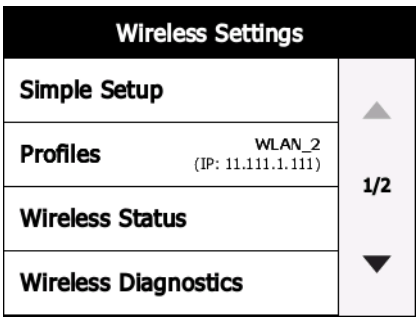


Figure 3-10 *Wireless Settings Screen*

Disabling the Profile

To disable the profile:

1. Touch a profile to disable.

2. Touch **Disable**. **Disabled** appears under the profile name.

Deleting the Profile

To delete the profile:

1. Touch a profile to delete.
2. Touch **Delete**.
3. Touch **Ok** to delete the profile from the SB1.

Exporting the Profile

You can export a profile configuration file to need info.

To export the profile:

1. Touch a profile to export.
2. Touch **Export**. The Export profile is saved to the User Drive in the Fusion-Data/Export folder. Filename: profile name_XXXXXXXXXXXX.gpdexport.
3. Touch **Ok**.

Wireless Status

NOTE The **Wireless Status** application is not finger friendly. Careful and precise touches are required when selecting options on the screen. Do not use a stylus or pointy object on the screen.

Use the **Wireless Status** option to launch the Wireless Status application. The **Wireless Status** window displays information about the wireless connection.

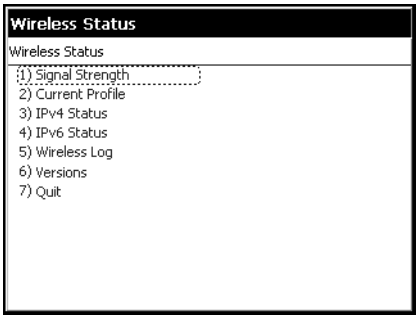


Figure 3-11 *Wireless Status Window*

The **Wireless Status** window contains the following options. Touch the option to display the option window.

- **Signal Strength** - provides information about the connection status of the current wireless profile.
- **Current Profile** - displays basic information about the current profile and connection settings.
- **IPv4 Status** - displays the current IP address, subnet, and other IP related information assigned to the mobile computer.
- **IPv6 Status** – displays IPv6 status and IPv6 related information assigned to the WLAN interface of the mobile computer.
- **Wireless Log** - displays a log of important recent activity, such as authentication, association, and DHCP renewal completion, in time order.
- **Versions** - displays software, firmware, and hardware version numbers.
- **Quit** - exits the **Wireless Status** window.

Each option window contains a back button to return to the main **Wireless Status** window.

Signal Strength Window

The **Signal Strength** window provides information about the connection status of the current wireless profile including signal quality, and other statistics described below. The BSSID address (shown as *AP MAC Address*) displays the AP currently associated with the connection. In Ad-hoc mode, the AP MAC Address shows the BSSID of the Ad-hoc network. Information in this window updates every 5 seconds.

To open the **Signal Status** window, touch **Signal Strength** in the **Wireless Status** window.

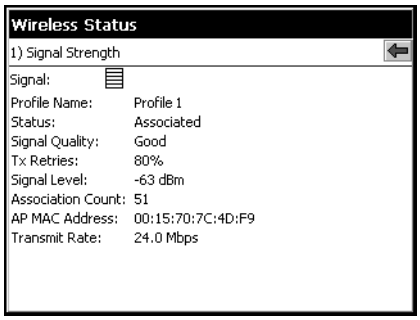


Figure 3-12 *Signal Strength Window*

After viewing the **Signal Strength** window, touch the back button to return to the **Wireless Status** window.

Table 3-1 *Signal Strength Status*

Field	Description
Signal	Displays the Relative Signal Strength Indicator (RSSI) of the signal transmitted between the AP and mobile computer. As long as the Signal Quality icon is green, the AP association is not jeopardized. If the icon is red (poor signal), an association with a different AP could be warranted to improve the signal. The signal strength icon changes depending on the signal strength.
	Excellent Signal
	Very Good Signal
	Good Signal
	Fair Signal
	Poor Signal
	Out of Range (no signal)
	The radio card is off or there is a problem communicating with the radio card.
Profile Name	Displays the name of the current profile.
Status	Indicates if the mobile computer is associated with the AP.
Signal Quality	Displays a text format of the Signal icon.
Tx Retries	Displays a percentage of the number of data packets the mobile computer retransmits. The fewer transmit retries, the more efficient the wireless network is.
Signal Level	The AP signal level in decibels per milliwatt (dBm).
Association Count	Displays the number of times the SB1 has roamed from one AP to another.
AP MAC Address	Displays the MAC address of the AP to which the mobile computer is connected.
Transmit Rate	Displays the current rate of the data transmission.

Current Profile Window

The **Current Profile** window displays basic information about the current profile and connection settings. This window updates every five seconds.

To open the **Current Profile** window, touch **Current Profile** in the **Wireless Status** window.

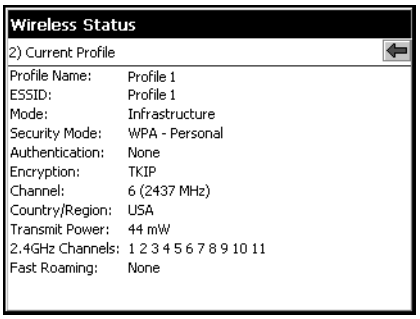


Figure 3-13 *Current Profile Window*

Table 3-2 *Current Profile Window*

Field	Description
Profile Name	Displays the name of the profile that the mobile computer is currently using to communicate with the AP.
ESSID	Displays the current profile's ESSID.
Mode	Displays the current profile's mode, either Infrastructure or Ad-hoc.
Security Mode	Displays the current profile's security mode.
Authentication	Displays the current profile's authentication type.
Encryption	Displays the current profile's encryption type.
Channel	Displays the channel currently being used to communicate with the AP.
Country	Displays the country setting currently being used.

IPv4 Status Window

The **IPv4 Status** window displays the current IP address, subnet, and other IP related information assigned to the mobile computer. It also allows renewing the IP address if the profile is using DHCP to obtain the IP information. Touch **Renew** to initiate the IP address renewal process. Touch **Export** to export IPv4 status information to a text file. The **IPv4 Status** window updates automatically when the IP address changes.

To open the **IPv4 Status** window, touch **IPv4 Status** in the **Wireless Status** window.

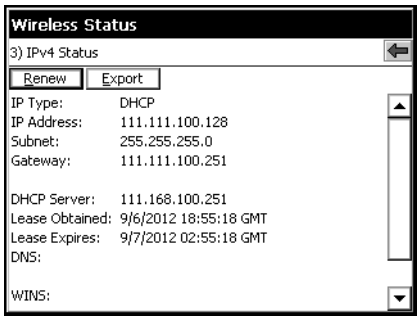


Figure 3-14 *IPv4 Status Window*

Table 3-3 *IPv4 Status Fields*

Field	Description
IP Type	Displays the IP address assignment method used for the current profile: **DHCP** or **Static**. If the IP Type is DHCP, the IP Address and other information shown is obtained from the DHCP server. In this case, the DHCP Server address and the Lease information will also be shown. If the IP Type is Static, the IP Address and other information shown are those that were entered in the profile.
IP Address	Displays the mobile computer's IP address. The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address. Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. The IP address is shown in dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.
Subnet	Displays the mobile computer's subnet mask. Most TCP/IP networks use subnets to manage routed IP addresses. All IP addresses have a network part and a host part. The network part specifies a physical network. The host part specifies a host on that physical network. The subnet mask allows a network administrator to use some of the bits that are normally used to specify the host to instead specify physical sub-networks within an organization. This helps organize and simplify routing between physical networks.
Gateway	Displays the IP addresses of the gateways. A gateway forwards IP packets to and from a remote destination.
DCHP Server	Displays the IP address of the DHCP server.
Lease Obtained	Displays the date and time that the IP address was obtained.
Lease Expires	Displays the date and time that the IP address expires.
DNS	Displays the IP addresses of the DNS server.
WINS	Displays the IP addresses of the WINS servers. WINS is a Microsoft Net BIOS name service. A WINS server provides a cache or database of NetBIOS name translations, eliminating the need to broadcast NetBIOS requests to resolve these names to IP addresses.
MAC	The IEEE 48-bit address is assigned to the network adapter at the factory to uniquely identify the adapter at the physical layer.

IPv6 Status Window

The **IPv6 Status** window displays IPv6 status, current IPv6 addresses and other IPv6 related information assigned to the WLAN interface. It also allows resetting the IPv6 address. The **IPv6 Status** window updates automatically when the IPv6 address changes.

Touch **Reset** to initiate IPv6 reset. Reset forces the TCP/IPv6 stack to re-bind to the WLAN interface. During re-bind, IPv6 stack discards its current IPv6 configuration and starts a fresh address auto configuration.

Touch **Export** to export IPv6 status information to a text file.

To open the **IPv6 Status** window, touch **IPv6 Status** in the **Wireless Status** window.

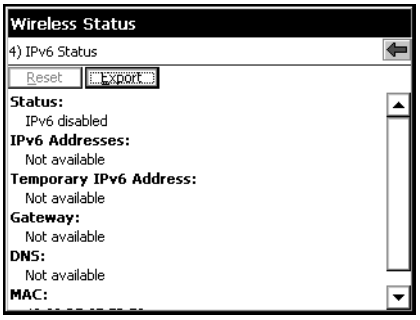


Figure 3-15 *IPv6 Status Window*

Table 3-4 *IPv6 Status Fields*

Field	Description
Status	Indicates whether IPv6 is enabled or disabled for the WLAN interface. Enable or disable IPv6 from **Options** > **Enable IPv6**.
IPv6 Addresses	Displays the SB1's IPv6 addresses assigned to WLAN interface. Displays all IPv6 addresses except Temporary IPv6 address. For each IPv6 address, it shows the scope (link local/site local/global/unknown) and remaining valid lifetime of the address.
Temporary IPv6 Address	Displays the SB1's Temporary IPv6 address assigned to WLAN interface. It displays the scope and remaining valid lifetime of the address. Temporary IPv6 addresses are based on random interface identifiers and are generated for public address prefixes that use stateless address auto configuration.
Gateway	Displays the IPv6 address of the gateway. A gateway forwards IP packets to and from a remote destination.
DNS	Displays the IPv6 address of the DNS server.
MAC	The IEEE 48-bit address is assigned to the network adapter at the factory to uniquely identify the adapter at the physical layer.

Double touch on a device **IPv6 Addresses** or **Temporary IPv6 address** to get more detailed information.

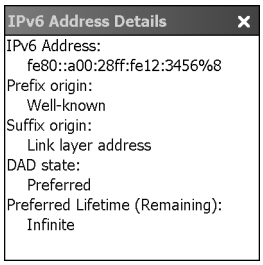


Figure 3-16 *IPv6 Address Details Example*

Table 3-5 *IPv6 Address Details Fields*

Field	Description
IPv6 Address	Displays the IPv6 address for which details are displayed.
Prefix origin	Displays the prefix origin for the IPv6 address. Possible values are Router Advertisement, Well-known, Manual, DHCPv6 or Unknown source.
Suffix origin	Displays the suffix origin for the IPv6 address. Possible values are Link layer address, Random, Well-known, Manual, DHCPv6 or Unknown source.
DAD state	Displays the Duplicate Address Detection state for the IPv6 address. Possible values are Preferred, Tentative, Deprecated, Duplicate or Invalid.
Preferred Lifetime (Remaining)	Displays the amount of time this address will remain in the Preferred state.

Wireless Log Window

The **Wireless Log** window displays a log of recent activity, such as authentication, association, and DHCP renewal completion, in time order. Save the log to a file or clear the log. The auto-scroll feature automatically scrolls down when new items are added to the log.

To open the **Wireless Log** window, touch **Wireless Log** in the **Wireless Status** window. The **Wireless Log** window displays.

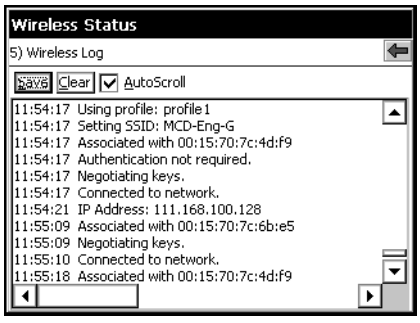


Figure 3-17 *Wireless Log Window*

Saving a Log

To save a Wireless Log:

1. Touch the **Save** button. The log.txt file is saved in the folder: \UserDrive\Fusion-Data\Export\Logs.

2. Touch **OK**.

See *Developer Back Housing on page 2-12* for information on copying the log files from the SB1.

Clearing the Log

To clear the log, touch **Clear**.

Versions Window

The **Versions** window displays software, firmware, and hardware version numbers.

To open the **Versions** window, touch **Versions** in the **Wireless Status** window.

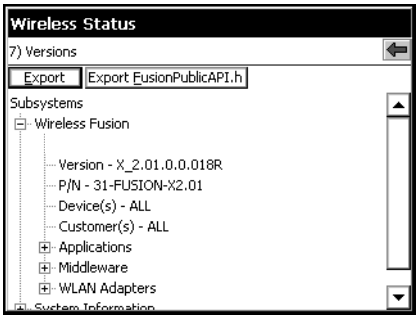


Figure 3-18 *Versions Window*

- The window displays Wireless software version numbers as well as application and middleware version information.
- Touch **Export** to export version information to a text file.
- Touch **Export FusionPublicApi.h** to export the current version of the FusionPublicAPI.h header file to the specified location.

Table 3-6 *Version Sub-categories*

Field	Description
Applications	Version information for Wireless applications.
Middleware	Version information for Wireless middleware components.
WLAN Adapters	Version and type information for WLAN adapters and the corresponding firmware and drivers.
Interface	Version and type information for the device's interface to the WLAN adapter and the corresponding firmware.
Device	Device model and identification numbers.
OS	Operating System version information.

Wireless Diagnostics

NOTE The **Wireless Diagnostics** application is not finger friendly. Careful and precise touches are required when selecting options on the screen. Do not use a stylus or pointy object on the screen.

Use the **Wireless Diagnostics** option to launch the **Wireless Diagnostics** application. The **Wireless Diagnostics** application window provides links to perform ICMP Ping, Trace Routing, and Known APs functions.

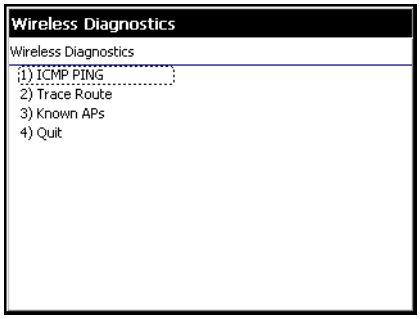


Figure 3-19 *Wireless Diagnostics Window*

The **Wireless Diagnostics** window contains the following options. Touch the option to display the option window.

- **ICMP Ping** - tests the wireless network connection.
- **Trace Route** - tests a connection at the network layer between the mobile computer and any place on the network.
- **Known APs** - displays the APs in range using the same ESSID as the mobile computer.
- **Quit** - Exits the **Wireless Diagnostics** window.

Option windows contain a back button to return to the **Wireless Diagnostics** window.

ICMP Ping Window

The **ICMP Ping** window allows testing of a connection at the network layer (part of the IP protocol) between the mobile computer and any other device on the network. Ping tests only stop when the **Stop Test** button is selected, the **Wireless Diagnostics** application is closed, or if the mobile computer switches between infrastructure and ad-hoc modes.

To open the **ICMP Ping** window, touch **ICMP Ping** in the **Wireless Diagnostics** window.

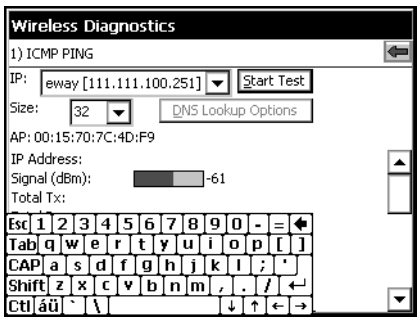


Figure 3-20 *ICMP Ping Window*

To perform an ICMP Ping:

1. In the **IP** field, enter an IP address or select an IP address from the drop-down list.
2. From the **Size** drop-down list, select a size value.
3. Touch **Start Test**. The ICMP Ping test starts. Information of the ping test displays in the appropriate fields.

The following statistics appear on the page:

- IPv4 Address or IPv6 Address – Target IP address.
- Signal - The current signal strength, measured in dBm, is provided both as a numerical value and as a histogram.
- Total Tx - The total number of pings sent is displayed numerically.
- Total Rx - The total number of valid ping responses received is displayed numerically.
- Lost - The total number of pings that were lost is displayed numerically.
- RT Times - Four round trip times: Last, Average, Minimum, and Maximum are displayed in milliseconds.
- % Rates - For each of the 14 data rates, the number of times that rate was used to transmit the ping is displayed as a percentage.

Use the **DNS Lookup Options** button to select the name resolution priority. Select the option and touch **OK** button. If a name is entered in the IP field, DNS Lookup Options setting will decide whether to use IPv4 or IPv6 address for the test. By default, this is set to IPv4 then IPv6, which indicates that it will try to resolve the name to an IPv4 address; if this fails and if IPv6 is enabled, it will try to resolve the name to an IPv6 address.

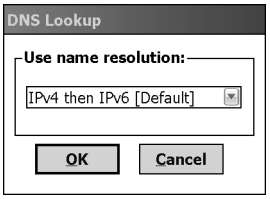


Figure 3-21 *DNS Lookup Options Window*

Graphs

A real time graph of any of the above statistics can be displayed by double touch on that statistic.

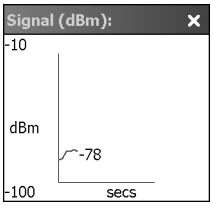


Figure 3-22 *Graph Example*

Trace Route Window

Trace Route traces a packet from a computer to a host, showing how many hops the packet requires to reach the host and how long each hop takes. The **Trace Route** utility identifies where the longest delays occur.

The **Trace Route** window allows testing a connection at the network layer (part of the IP protocol) between the mobile computer and any other device on the network.

To open the **Trace Route** window, touch **Trace Route** in the **Wireless Diagnostics** window.

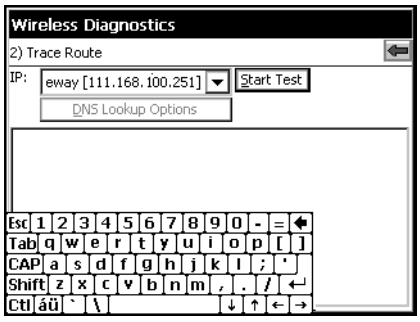


Figure 3-23 *Trace Route Window*

In the **IP** drop-down list, enter an IP address or choose one from the drop-down list, or enter a DNS Name and touch **Start Test**. When starting a test, the trace route attempts to find all routers between the mobile computer and the destination. The Round Trip Time (RTT) between the mobile computer and each router appears, along with the total test time. The total test time may be longer than all RTTs added together.

Use the **DNS Lookup Options** button to select the name resolution priority. Select the option and touch the **OK** button. If a name is entered in the IP field, DNS Lookup Options setting will decide whether to use IPv4 or IPv6 address for the test. By default, this is set to IPv4 then IPv6, which indicates that it will try to resolve the name to an IPv4 address; if this fails and if IPv6 is enabled, it will try to resolve the name to an IPv6 address.

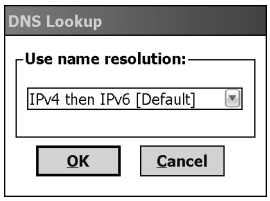


Figure 3-24 *DNS Lookup Options Window*

Known APs Window

The **Known APs** window displays the APs in range using the same ESSID as the mobile computer. This window is only available in **Infrastructure** mode. To open the **Known APs** window, touch **Known APs** in the **Wireless Diagnostics** window.

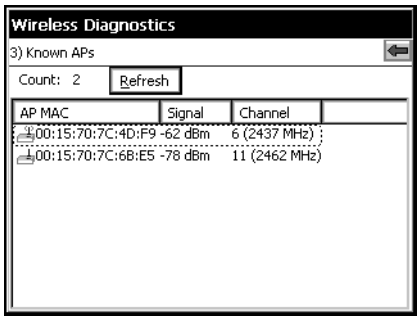


Figure 3-25 *Known APs Window*

See *Table 3-7* for the definitions of the icons next to the AP.

Table 3-7 *Current Profile Window*

Icon	Description
	The AP is the associated access point.
	The mobile computer is not associated to this AP.

Quick Options

Use the **Quick Options** to reset the WLAN radio to the factory defaults and to remove profiles from the list, set Regulatory options and Export profiles and Wireless options.

Regulatory

NOTE 802.11d is enabled by default.

Use the **Regulatory** screen to set 802.11d mode. Due to regulatory requirements, within a country, a device is only allowed to use certain channels. When 802.11d is enabled, the SB1 gets the country code from the access point (AP). When 802.11d is disabled, the country must be set manually.

To disable 802.11d and set the country code:

1. From the **Quick Options** screen, touch **Regulatory**.

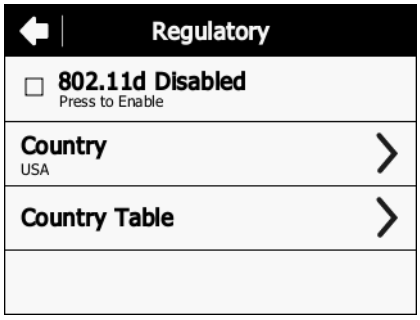


Figure 3-26 *Regulatory Settings Screen*

2. Touch **802.11d Enabled** to disable 802.11d mode.
3. Touch **Country Table**.

Figure 3-27 *Country Table Screen*

4. Scroll through the list to find the country and note the two character code associated with the country.
5. Touch ◄.
6. Touch **Country**.

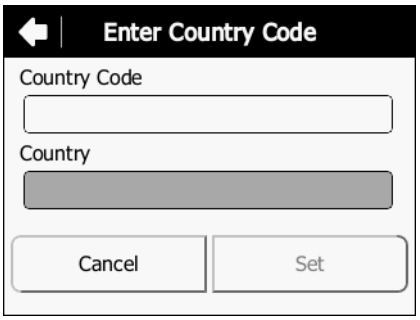


Figure 3-28 *Enter Country Code Screen*

7. In the **Country Code** text box, enter the country code for the country.
8. Touch **Set**. A Warning dialog box appears.
9. Touch **Ok**.

Export

Use **Export** to export Fusion profiles (all profiles) and Options to a pre-defined directory in the device (\UserDrive\Fusion-Data\Export). Exported Profiles and Options files are named as FusionProfiles_x.gpdexport and FusionOptions_x.gpdexport, respectively, where x is date and time of the export.

From **Quick Options**, touch **Export**.

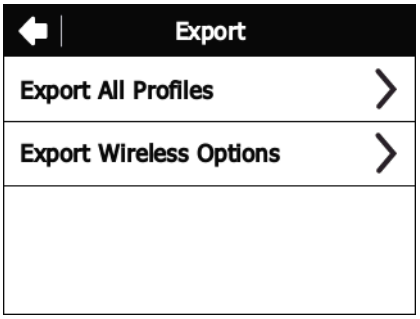


Figure 3-29 *Export Screen*

Touch **Export All Profiles** or **Export Wireless Options**.

Touch **Ok**.

Reset Wireless Settings

To reset the WLAN settings to the factory default settings:

1. Touch **Quick Options**. The **Quick Options** window appears.

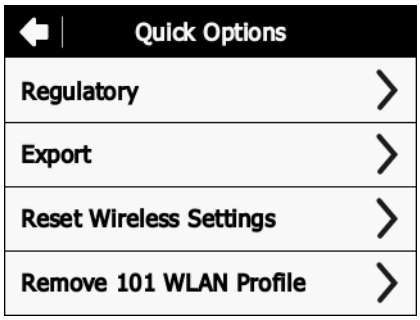


Figure 3-30 *Quick Options Window*

2. Touch **Reset Wireless Settings**.

Figure 3-31 *Confirmation Dialog Box*

3. Touch **OK** to restore factory defaults or **Cancel** to go back to the **Quick Options** screen.

Remove 101 WLAN Profile

To remove the default 101 WLAN Profile:

1. Touch **Quick Options**. The **Quick Options** window appears.

Figure 3-32 *Quick Options Window*

2. Touch **Remove 101 WLAN Profile**.

Figure 3-33 *Confirmation Dialog Box*

3. Touch **OK** to remove the 101 profile or **Cancel** to go back to the **Quick Options** screen.

Exit Wireless Settings

To exit the **Wireless Settings** application touch ⬅.

Configuring WLAN Settings

SB1 does not provide a user Interface to configure many of the WLAN configurations supported by Fusion. This includes WLAN profile configurations and WLAN options. Use of an MDM is required to configure these settings. Alternately, use the **Import Locally** application to import wireless configuration data exported from a device running Fusion X2.00 or Fusion X2.01.

Supported WLAN Profiles

Fusion in SB1 supports both Infrastructure and Ad-hoc modes of operation. Fusion supports different types of Authentication and Encryption methods. But Fusion the user interface of the SB1 allow user to create only a subset of profiles (Open, WPA Personal (TKIP) and WPA2 Personal (AES)). Other profiles like 802.1x profiles cannot be created from SB1 user interface. Use the MSP staging method or the **Import Locally** application to create/import these types of WLAN profiles.

While connecting to an 802.1x profile where the credentials are not entered as part of the WLAN profile, The SB1 prompts the user to enter credentials (username and/or password and/or domain).

Table 3-8 lists the different types of Authentication and Encryptions supported in SB1.

Table 3-8 *Security Modes*

Security Mode	Authentication Types	Encryption Types
Legacy (Pre-WPA)	None, EAP-TLS, EAP-FAST, PEAP, LEAP, TTLS	Open, WEP-40 (40/24), WEP-104 (104/24)
WPA - Personal	None	TKIP
WPA2 - Personal	None	TKIP, AES
WPA - Enterprise	EAP-TLS, EAP-FAST, PEAP, LEAP, TTLS	TKIP
WPA2 - Enterprise	EAP-TLS, EAP-FAST, PEAP, LEAP, TTLS	TKIP, AES

Table 3-9 lists the Tunneled Authentications supported for PEAP, TTLS and EAP-FAST authentications.

Table 3-9 *Tunneled Authentication Options*

Tunneled Authentication	Authentication Type		
	PEAP	TTLS	EAP-FAST
CHAP		X	
EAP-GTC	X		X
MD5		X	
MS CHAP		X	
MS CHAP v2	X	X	X
PAP		X	
TLS	X		X

Table 3-10 lists supported Performance Settings modes in SB1.

Table 3-10 Performance Settings

Mode	Description
Optimize for Data	The SB1 is tuned for data transfer. U-APSD is disabled in this mode.
Optimize for Voice	The SB1 is tuned for voice transfer. U-APSD is enabled in this mode.

Supported WLAN Options

Table 3-11 lists the supported Fusion options.

Table 3-11 *Supported WLAN Options*

Options	Description
Regulatory	802.11d mode can be changed (disable/enable). Select a country when disabling 802.11d. By default, 802.11d is enabled.
Band Selection	SB1 supports only 2.4GHz. Use this setting to select channels of operation.
802.11 Options	Pre-authentication can be enabled/disabled using this. By default, Pre-authentication is disabled.

Table 3-11 *Supported WLAN Options (Continued)*

Options	Description
System Options	**Profile Roaming** - if this is selected, profiles will be searched for an available network. By default, this is enabled. **Enable IPv4 Management** - When enabled, IPv4 address management is performed by Fusion instead of by the Operating System. By default, this is enabled. **Auto Time Config** - If enabled, Fusion will update the time on the terminal provided a Network Time Protocol server is available and the Zebra access point is enabled for this feature. By default, Auto Time Config is enabled.
Auto PAC Settings	**Allow Provisioning** - If this is allowed, and no PAC is available, device will allow server to provide one. This is disabled by default. **Allow Refreshing** - If this is allowed, and the available PAC has expired, the device will allow the Server to provide a new one. This is disabled by default.
IPv6	Enable IPv6 - if enabled, IPv6 stack will be enabled. By default, IPv6 is disabled.

Guidelines for Using MSP with Fusion

The SB1 supports the latest version of Fusion, Fusion X2.xx. WLAN Settings to configure Fusion can be created using prior MSP Settings Classes, such as Network.WLAN.FusionPublic and Network.WLAN.Fusion30Public. In addition, to support the full capabilities of Fusion X2, the new MSP Settings Class Network.WLAN.FusionX2Public is also supported.

If only SB1s are being managed, the Network.WLAN.FusionX2Public MSP Settings Class provides the best experience since it is tailored to use the capabilities of Fusion X2. Similarly, if a mixed population of Zebra Solutions devices that all support Fusion X2 are managed, the Network.WLAN.FusionX2Public MSP Settings Class is the preferred choice. In cases where a mixed population of SB1s and older devices, which do not support Fusion X2, are used, it may be preferable to use an older MSP Settings Class so a single Settings Object can target a wider number of devices.

When using an older MSP Settings Class, the capabilities supported by the Settings Class may not exactly match the capabilities of all devices with which it is compatible. Backward compatibility means that each SB1 that can accept Settings Objects created using a given MSP Settings Class supports as much WLAN functionality as it can based on the version of Fusion and the WLAN hardware present on the SB1. Certain features that can be selected in a Settings Object created via such a MSP Settings Class might not be supported on every device that can accept and process Settings Objects of that MSP Settings Class. It is important to carefully test a representative sample of each type of device to ensure that a Settings Object achieves the desired result when sent to a mixed population of devices.

Persistence Differences Between Fusion X2 and Previous Versions of Fusion

Fusion on the SB1 implements persistence as a standard feature. When configuring Fusion, the settings are automatically stored persistently in a database contained within the SB1. On all subsequent cold boots, the configuration stored in the database is automatically reapplied. There is no way to turn off the automatic persistence, but there is a way to reset Fusion back to its default state. See *Reset Wireless Settings on page 3-20* for more information.

This persistence behavior is different from all prior versions of Fusion that did not automatically store Fusion Settings persistently. This difference has the following important implications when MSP is used to configure Fusion on the SB1.

- All Fusion settings that are applied directly as part of a Staging Profile (not in a bundle) are automatically persisted by Fusion even though they are not explicitly persisted by MSP.
  - This produces different behavior from that seen on devices with older versions of Fusion. In particular, WLAN Settings that were previously transient (i.e. intentionally did not persist across subsequent cold boots) are persistent (i.e. are persist across subsequent cold boots). This could lead to confusion, especially in mixed populations of devices.
  - Fusion settings that are applied persistently, as part of a bundle, are persisted both by Fusion and MSP. While this does not result in a change of behavior, compared to older versions of Fusion, it could lead to less than optimal results. In particular, on devices with Fusion X2, WLAN Settings are unnecessarily reapplied by MSP and this could increase the time it takes for the WLAN to become usable after subsequent cold boots.
  - Choosing the “Disable all other profiles:” in a Settings Object causes all other WLAN Profiles, aside from the one being defined in that Settings Object, to be disabled. When using Fusion, the WLAN Profiles are persisted and the disabling of such WLAN Profiles are persisted. The result is approximately equivalent to that produced by older versions of Fusion, since only the WLAN Profile defined by the Settings Object will be enabled and is used after subsequent cold boots. One difference is that on Fusion X2, all defined WLAN Profiles will persist (albeit disabled) across subsequent cold boots and hence could be re-enabled, whereas in older versions of Fusion, those WLAN Profiles would not persist across subsequent Cold Boots.

- Fusion Settings that are applied persistently, as part of WLAN Settings Object in a bundle, can still be uninstalled. But since the configuration performed by the WLAN Settings Object is not removed from the Fusion persistence database, such configuration continues to persist across subsequent cold boots.
  - When using previous versions of Fusion, a WLAN Settings Object could be removed, thus causing the configuration it performed to stop persisting across subsequent cold boots. This is no longer possible with Fusion X2.
  - While a means is provided via the **Wireless Settings** to reset the persistence database, no means is provided to initiate such a reset from MSP.
- If the WLAN settings that are applied to configure Fusion reference any Certificates (e.g. for EAP-TLS), then Fusion automatically persists those certificates in its persistence database along with the rest of the Fusion configuration.
  - This ensures that everything needed to maintain WLAN connectivity persists across subsequent cold boots.
  - This produces different behavior from that seen on devices with older versions of Fusion. In particular, certificates that were previously transient (i.e. intentionally did not persist across subsequent cold boots) are be persistent (i.e. are persist across subsequent cold boots). This could lead to confusion, especially in mixed populations of devices.
  - Certificates that are installed persistently, as part of a Certificate Settings Object in a bundle, are persisted both by Fusion X2 and by MSP. While this does not result in a change of behavior, compared to older versions of Fusion, it could lead to less than optimal results. In particular, on devices with Fusion X2, Certificates are unnecessarily reinstalled by MSP and this could increase the time it takes for the WLAN to become usable after subsequent cold boots.
- Certificates that are installed persistently, as part of a Certificate Settings Object in a bundle, can be uninstalled. But since certificates are not removed from the Fusion persistence database, they continue to persist across subsequent cold boots.
  - When using prior versions of Fusion, a Certificate Settings Object could be removed, thus causing the certificates it installed to stop persisting across subsequent cold boots. This is no longer possible with Fusion X2.
  - While it is possible to reset the persistence database using **Wireless Settings**, it is not possible to reset the persistence database from MSP.

CHAPTER 4 STAGING AND DEPLOYMENT

Introduction

This chapter provides information and guidelines for staging and deploying Rho-based applications for the SB1 using the Mobility Services Platform (MSP) Server or the Remote Development Tool (RDT).

Requirements

The following items are required:

- Mobility Services Platform 4.2 Server
  - MSP 4.2 Server ISO image - The link to is software is provided in the order fulfillment email.
  - MSP 4.2 Release Notes - The link to the release notes is provided in the order fulfillment email.

  or

  Rapid Deployment Tool Solo - Application used to stage the SB1.
- MSP 4.2 Supplement for SB1 Kit - Available for download from the Zebra Support Central web site.

MSP 4.2 Supplement for SB1 Kit

The MSP 4.2 Supplement for SB1 Kit contains SB1 specific packages that can be deployed to SB1 devices and templates that can be used to simplify the creation of packages for the SB1 using the MSP Package Builder. The packages in the MSP 4.2 Supplement for SB1 Kit must be uploaded into an MSP 4.2 Server to deploy them from that MSP 4.2 Server to any SB1 device. The packages in the MSP 4.2 Supplement for SB1 Kit will be pre-loaded into RDT and hence they can be deployed to any SB1 devices without using the MSP 4.2 Supplement for SB1 Kit. The templates in the MSP 4.2 Supplement for SB1 Kit are required to be copied and registered with the MSP Package Builder if you want to use them to create SB1 application packages, using the MSP Package Builder, to be deployed to SB1 devices.

Installation

To install the MSP 4.2 Supplement for SB1 Kit:

NOTE For use only with an MSP Server.

1. Download the MSP 4.2 Supplement for SB1 Kit from the link provided in the order fulfillment email.
2. Unzip the file to a location on a host computer.
3. Install all extracted ZIP files using the MSP Admin Tool.

Template Files

The kit contains template files that are used when creating SB1 application packages using the MSP Package Builder. SB1 application packages created using the MSP Package Builder and the template files could then be uploaded to either an MSP 4.2 Server or to RDT, from which they could then be deployed to SB1 devices. The templates files must be extracted from the kit, copied, and registered with the MSP Package Builder before they can be used within the MSP Package Builder to create SB1 application packages. The MSP Package Builder must be installed before the template files can be copied or registered with the MSP Package Builder. See *Staging Using Mobility Services Platform on page 4-13* and *Staging Using Rapid Deployment Tool Solo on page 4-20* for more information.

Key SB1 Differences

The following lists key differences between the SB1 and other Zebra devices that impacts how MSP operates on the SB1.

Persistent Storage - The SB1 contains a *UserDrive* folder to store customer-specific content. Customers can develop Rho-Based applications and deploy them to the *UserDrive* folder. Customers can return the behavior of the SB1 Shell to the default state by erasing the content previously deployed to the *UserDrive* folder. A cold boot is required after *UserDrive* folder changes at the end of a bundle.

- **Reboots** - The SB1 supports program-initiated or user-initiated cold boot. Warm boots are not supported. Cold boots cause loss of all content not intentionally stored persistently. An MSP-initiated cold boot is automatically performed at the end of every update to protect against data loss.
- **Persistence** - Persistence is critical due to automatic cold boot. Content that is part of an update and is not stored persistently is lost when the cold boot is performed at the end of an update. System content is automatically stored persistently as part of OS Update. User content stored in the *UserDrive* folder is persistent. Touch Panel Calibration can be stored persistently using the ***SB1SaveCalibration*** package.
- **Application Support** - Only Rho-based applications are supported on the SB1.
- **User Interface** - The Rho-based SB1 Shell is the user interface of the SB1.
- **Update Process** - Updates to the SB1 should only be performed when the SB1 is in a cradle. Since the SB1 is not intended to be used when it is in cradle, updates should be safe to perform at any time when it is in the cradle.

  The MSP Power Condition can be attached to policies to prevent updates from occurring when the SB1 is not in the cradle. The cold boot that is automatically performed at the end of an update should be safe to perform any time the SB1 is in the cradle since it should not be in use.
  - **OS Update Packages** - Zebra supplies OS Update packages on the Support Central web site.
  - **Customer Created Packages** - Customer created packages can be deployed using a package in the same bundle as an ***OSUpdate*** package as long as it occurs before the ***OSUpdate*** package.
  - **Wireless Settings** - Wireless Settings are persistent across an OS update.

- **RD Client** - The **RD Client** application on the SB1 is not finger friendly. Careful and precise touches are required when selecting options on the screen. When launching the **RD Client**, the message **RD Client may restart your device** displays to warn the user that a cold boot is going to occur after updates are initiated using **RD Client**.
- **MSP Agent** - The **MSP Agent** does not display bundle messages, confirm conditions and power conditions that would normally be presented to a user.

  The value “Zebra SB1B” is reported to MSP for the Device Attribute *identity.deviceModel*.
- **Package Building** - A sample **User Baseline** package is provided to illustrate the Rho-based Shell configuration. This can be modified as needed to change settings and/or add applications. A Package Builder template is provided to simplify the creation of packages to deploy individual Rho-based applications to the *UserDrive* folder. These packages can be incrementally deployed or removed to add or remove their corresponding Rho-based applications. Customer-created packages should not be created to deploy content to other destinations.
- **Warm Boot Implications** - The following MSP methods are normally used to request an explicit warm boot of a device:
  - Warm boot step in a bundle
  - Warm Boot Option in a package.

  Both of these fail if used on an SB1 to prevent performing a cold boot when a warm boot is requested. The ***MSP Agent Update*** package ***abup30*** includes the Warm Boot option and fails if used alone on an SB1.

MSP Packages

The following sections describes MSP packages that can and cannot be used with the SB1.

Recommended for Use

Table 4-1 lists standard packages that are recommended for use on the SB1.

Table 4-1 *Recommended MSP Packages*

Package Name	Source	Description
DateAndTime[1]	MSP Server	Configures the SB1 to acquire the date, time and time zone from a server. The package is recommended if MSP is the Mobile Device Management (MDM). Consult the MDM documentation.The SB1 data and time can also be set using the SB1 settings, see *Set Date and Time on page 1-6*, or configuring Fusion to enable the Auto Date Config option.
GetAdapters[1]	MSP Server	Reports adapter information (especially IP address) to MSP. It is recommended if MSP is the MDM and required if **RemoteUI** or **RemoteControl** are used. Consult the MDM documentation.

[1] **Package can be used when MSP is managing the SB1.**

Table 4-1 *Recommended MSP Packages (Continued)*

Package Name	Source	Description
***GetFileVersion*[1]**	MSP 4.2 Supplement for SB1	Reports system applications and libraries versions to MSP. It is recommended because it is the only method provided to report system software versions when MSP is the MDM. Consult the MDM documentation.
***MotoRemoteUI*[1]**	MSP Server Add-On Kit	Allows remote control of the SB1 from MSP. It is recommended if MSP is the MDM and providing help desk support is desirable. Consult the MDM documentation.
[1] Package can be used when MSP is managing the SB1.		

Available for Use

Table 4-2 list the standard MSP packages available for use on the SB1.

Table 4-2 *Packages Available on the SB1*

Package Name	Source	Description
AutoStageLauncherTFTP [1] [2]	MSP Server	Sets up the SB1 to be automatically staged based on DHCP and TFTP.
GetConfigData [2]	MSP Server	Acquires and reports SB1 hardware configuration information to MSP.
GetRegistryInfo [2]	MSP Server	Extracts and reports Device Registry information to MSP.
ZebraDC [2]	MSP Server	Monitors the usage and performance of the SB1 from MSP.
SiteRefresh [2]	MSP Server	Requests the SB1 to refresh site-specific settings.
StartSmartStaging [1]	MSP Server	Transitions smoothly from Staging to MSP Provisioning.
TunnelAgent [2]	MSP Server	Supports ***MotoRemoteUI*** and ***MotoRemoteControl*** via Tunnel Service.
Universal [2]	MSP Server	Conditions activity based on registry, files and processes.
UserAttributes [2]	MSP Server	Manages Device Attributes reported to MSP.

[1] **Package is used during staging of the SB1.**
[2] **Package can be used when MSP is managing the SB1.**

Usable on the SB1

Table 4-3 lists standard MSP packages that can be used on the SB1 but with certain caveats.

Table 4-3 *Packages for Use on the SB1 with Caveats*

Package Name	Source	Description
abup30 [1] [2]	MSP Server	Updates the version of the RD Client and MSP Agent on the SB1 to a newer version. Must be preceded by the **RebootEnableOverride** package to avoid an error as a result of the lack of support for warm boot.
AdapterTime [2]	MSP Server	Conditions activity based on adapter and/or date/time. If MSP is the MDM, then the adapter parts are not very relevant, but the date/time parts may be.
AutoSiteAssign [2]	MSP Server	Configures the SB1 to automatically determine its site. If MSP is the MDM, then all modes are supported except requesting the user to disambiguate the site.

[1] **Package is used during staging of the SB1.**
[2] **Package can be used when MSP is managing the SB1.**

Table 4-3 *Packages for Use on the SB1 with Caveats (Continued)*

Package Name	Source	Description
RequestCheckin [2]	MSP Server	Allows MSP to request devices to perform expedited check-in. If MSP is the MDM, then this is fully functional, but may be of little relevance since its use may be inconsistent with the SB1 usage model.
RTMAgent [2]	MSP Server	Supports real-time management functions. If MSP is the MDM, then this is fully functional, but since it is required only to support the ***RequestCheckin*** package, it may have little relevance.

[1] Package is used during staging of the SB1.
[2] Package can be used when MSP is managing the SB1.

Discouraged from Being Used

Table 4-4 lists the MSP packages that are discouraged from being used on the SB1.

Table 4-4 *Packages Discouraged from Use*

Package Name	Source	Description
Connectivity [1]	MSP Server	The ***Connectivity*** package is an MSP feature that enables management activity to be deferred until the device has a specified form of connectivity. On devices with multiple forms of connectivity, this could be used to good advantage. Since the SB1 has only one form of connectivity, no benefit would be gained in such a scenario. Alternately, when using ***LockAndWipe***, it might make sense to configure a device to automatically lock when WLAN connectivity was lost and optionally unlock when WLAN connectivity was regained. Since these options of ***LockAndWipe*** are rejected on the SB1, no benefit would be gained in such a scenario. So, while ***Connectivity*** is fully functional on the SB1, it serves no useful purpose and is discouraged from use.
GetCabInventory	MSP Server	The ***GetCabInventory*** package is an MSP feature that enables an inventory of the .CAB files installed on a device to be reported to MSP and displayed on the MSP Console. On devices where applications are sometimes installed via .CAB files, this can be useful to detect rogue applications that may have been installed in an un-wanted manner. Since the use of .CAB files to install SB1 applications is generally not recommended, there is little value in using this package on the SB1 and is discouraged from use.

[1] Package can be used when MSP is managing the SB1.

Table 4-4 *Packages Discouraged from Use (Continued)*

Package Name	Source	Description
LockAndWipe	MSP Server	Sends messages to the SB1, request user authentication, lock/unlock the device or wipe content from a device. Discouraged since it would present a user interface that is inconsistent with the SB1 usage model.
MotoRemoteControl	MSP Server Add-On Kit	Enables a workstation to take control of the UI of a device and also to remotely perform various troubleshooting functions, such as file management, registry management, process management, etc. While ***MotoRemoteControl*** provides identical functionality on the SB1 to that provided on all other Zebra devices, its use could violate the SB1 Device Usage Model. A classic use case of ***MotoRemoteControl*** is to for a Help Desk providing support to users. Using ***MotoRemoteControl***, a Help Desk technician would be enabled to interact with the SB1 in ways that would violate the intended SB1 Device Usage Model.

[1] Package can be used when MSP is managing the SB1.

Not Supported on the SB1

Table 4-5 lists the MSP features that are not supported on the SB1.

Table 4-5 *Unsupported MSP Packages*

Package Name	Source	Description
Moto_SSL_VPN_ *	MSP Server Add-On Kit	The Zebra SSL VPN is a third-party VPN solution resold by Zebra for use on many Zebra devices. The Zebra SSL VPN has not been tested and certified for use on the SB1 and it is considered unsupported and the use of this feature should not be attempted on the SB1.
SMSStaging	MSP Server	The SMS Staging Client is an MSP feature that allows a device be staged via Staging Profiles that are sent to a device via SMS messages over a Wireless Wide Area Network (WWAN) connection. The SB1 does not offer WWAN support and the use of this feature is unsupported and should not be attempted on the SB1.
disable30 and enable30	MSP Server	Used to facilitate Staging of certain legacy devices. Not supported on the SB1 due to lack of support for warm boot.

Unlicensed Features

Certain MSP features are subject to third-party licensing that is generally included into the purchase price of the device. Since all such features are inconsistent with the SB1 Device Usage Model, it was inappropriate to burden the SB1 with the cost of these unnecessary third-party licenses. *Table 4-6* lists MSP features not licensed for use on and must never be used on the SB1.

Table 4-6 *Packages not Supported on the SB1*

Package Name	Source	Description
AppCenter	MSP Server Add-On Kit	**AppCenter** provides a means to lock down a device by controlling its UI and limiting the applications that can be run. The UI aspects of **AppCenter** are inconsistent with the SB1 Device Usage Model. The SB1 is not intended to run native applications and since the SB1 Shell does not provide any way to prevent launching of selected SB1 applications, **AppCenter** adds no value onto the SB1. As a result, **AppCenter** is not licensed for use on the SB1 and must not be used.
DeviceSecurity	MSP Server	The ***Device Security*** package is a feature containing technology licensed from a third-party that can be used on many Zebra devices. **DeviceSecurity** provides a means to control access to the device UI and which application and device features can be used. ***DeviceSecurity*** is not licensed for use on the SB1 and must not be used.
LuaScript	MSP Server	The ***LuaScript*** package is a feature containing technology licensed from a third-party that can be used on many Zebra devices. ***LuaScript*** provides a means to execute scripts written in the Lua programming language on a device and is not licensed for use on the SB1 and must not be used.
SecureStorage	MSP Server	The ***SecureStorage*** package is a feature containing technology licensed from a third-party that can be used on many Zebra devices. ***SecureStorage*** provides a means to encrypt local content stored on a device and is not licensed for use on the SB1 and must not be used.

For Use by Device Deployers

Table 4-7 lists specific packages for use by device deployers.

Table 4-7 *Packages for Use by Device Developers*

Package Name	Source	Description
EndUpdateInProgress [1] [2]	MSP 4.2 Supplement for SB1	Reverses the effects of ***UpdateInProgress***. Required after an update if ***UpdateInProgress*** was used.
RebootEnableOverride [1] [2]	MSP 4.2 Supplement for SB1	Required in a bundle just before the ***abup30*** Package to allow it to work when warm boot is not supported.
SB1SaveCalibration [1] [2]	MSP 4.2 Supplement for SB1	Required once after calibration and before cold boot if it is desired to prevent the need to recalibrate.
SB1WipeCalibration [1] [2]	MSP 4.2 Supplement for SB1	Reverses the effect of the ***SB1SaveCalibration*** package.
Sb1PrepareForOsUpdate [1] [2]	MSP 4.2 Supplement for SB1	Prepares the SB1 for OS Update. Required before any ***OSUpdate*** package to allow the update to work correctly.
UpdateInProgress [1] [2]	MSP 4.2 Supplement for SB1	Informs the user that an update is in progress and block the starting of new applications. Can optionally be used in a bundle before non-OS Update Packages.
WipeUserDrive [1] [2]	MSP 4.2 Supplement for SB1	Wipes the contents of the *UserDrive* folder. Optional to revert the SB1 back to the factory default (empty) state and restore the default behavior of the SB1 Shell.
FinishStaging [1]	MSP 4.2 Supplement for SB1	Optional to suppress the “Your Device is Ready to Use” message after staging is complete.

[1] Package is used during staging of the SB1.
[2] Package can be used when MSP is managing the SB1.

Developing and Packaging Applications

The following sections provide information for developing and packaging Rho-based application for the SB1.

Folder Structures

It is recommended to follow the folder structures described below when developing applications for the SB1:

SB1 Folder Structure

Application content must be designed to reside on the *UserDrive* folder. The content should be designed as additive to a baseline and should be located in a sub-folder under the *\UserDrive\apps* folder that is named for the application (e.g. \UserDrive\apps\myapp). All inter-files references should assume that all files are located in that application sub-folder. Optionally, files of different types may be segregated in additional sub-folders.

Refer to the *SB1 Programmer's Guide* for detailed information on folder structures.

Workstation Folder Structure

The entire content of the application sub-folder for a given Rho-based application should be placed inside another folder named *UserDrive*. If multiple Rho-based applications are stored on the same workstation, then the *UserDrive* folder for each application should be stored under another folder named for the application.

The following is an example of a workstation application folder structure.

```
\MySB1Applications\
        MyApp1\UserDrive\apps\
                MyApp1\
                        MyApp1.app
                        MyApp1.html
                        other.html
        MyApp2\UserDrive\apps\
                MyApp2\
                        MyApp2.app
                        MyApp2.html
                        jpg\
                                image.jpg
```

Development

Start a new Rho-based application by creating an appropriate application content folder. See *Folder Structures on page 4-10*.

At a minimum, this should include an application HTML file named for the application. For example, myapp.html. It may also include additional files referenced from the application HTML file. This should also include a simple apps.json file that defines a single icon to launch the application HTML file.

Refer to the *SB1 Programmer's Guide* for more information on developing Rho-baed applications for the SB1.

Testing

To test an application on the SB1:

1. Install a Developer Back Housing onto the SB1. See *Developer Back Housing on page 2-12* for more information.
2. Connect the SB1 to a workstation using a micro USB cable. Ensure that the *UserDrive* folder can be accessed on the workstation.
3. Copy the baseline content to the *config* and/or *apps* folders on the SB1.
4. Copy the application content (under the *apps* folder) to the SB1 *apps* folder.
5. Copy the simple **`apps.json`** file for the application to the SB1 *config* folder.
6. Disconnect the micro USB cable.
7. Reboot the SB1 by pressing and holding the Scan and Home buttons for about five seconds until a beep is heard.
8. Touch the application icon in the **Applications** screen and test the application functionality.
9. Modify application content and repeat above the steps until behavior is acceptable.

Sample Baseline Package Customization

The ***Sample Baseline*** package is provided to a sample package to create new packages from. To customize the ***Sample Baseline*** package:

1. Locate the sample **`Sb1SampleBasline.apf`** package file in the folder to which you extracted the MSP 4.2 Supplement for SB1.
2. Using the MSP Package Builder, open the **`sb1samplebasline.apf`** package file.
3. Select **Tools** > **Convert to Project**.
4. Enter a name for the new package.
5. Enter the location for the new package project file (.MSPPROJ) and the extracted content files.
6. Select **OK**.
7. Select **File** > **Save** to save the new package project file.
8. Modify the files in the folder to which the sample package content files were extracted based on application requirements and by following the *SB1 Programmer's Guide*.
9. Open the package project file in MSP Package Builder.
10. Select the **Files** section of the project and delete the *UserDrive* folder.
11. Drag the *UserDrive* folder into the **Client File System** pane of the project.
12. Select **File** > **Save** to save the modified package project file.
13. Select **Tools** > **Generate APF File** to make a package file containing the modified content.
14. Enter a package version number.

Creating Application Packages

To create a Rho-based application package:

1. Develop a new Rho-based application. See *Development on page 4-10*.
2. Rename the **`apps.json`** file for the application based on the name of the application (for example, if the application name is **`myapp`**, then rename the **`apps.json`** file to **`myapp.app`**). Place the **`myapp.app`** file into the application folder for the application. See *Folder Structures on page 4-10*.
3. Launch the MSP Package Builder.
4. Select **File** > **New Project**.
5. Select the **RhoApplication** template.
6. Enter a name for the package (based on the name of the application).
7. Select a location for the package (the workstation folder containing the UserDrive folder for the application).
8. Select the **Files** section of the project.
9. Drag the *UserDrive* folder for the application into the **Client File System** pane of the project.
10. Select **Tools** > **Generate APF File** to make a package file containing the modified content.
11. Enter a version for the package to be created.

Staging Using Mobility Services Platform

This section provides information for staging the SB1 using the MSP Server. MSP is available in three editions: MSP Stage Edition, MSP Provision Edition and MSP Control Edition. MSP Provision Edition includes all the functionality of MSP Stage Edition. MSP Control Edition includes all the functionality of MSP Provision Edition and MSP Stage Edition. The Staging Edition is a free to use with the SB1 and can be used to perform all staging activities described in this guide. When using the MSP Provision Edition or the MSP Control Edition only to stage the SB1, the number of licenses tied to these editions are not affected. If management of the SB1 is desired, suitable licenses for MSP Provision Edition and MSP Control Edition are required.

Setting Up the MSP Server

To prepare the SB1 for staging using MSP and a workstation:

1. Install the latest available MSP 4.2 Supplemental deliverables to ensure that all client software is up to date and that all available server patches are installed.
2. Install the MSP 4.2 Server software onto suitable workstation according to the *Mobility Services Platform 4.2 Software Installation Guide*.
3. Install the MSP 4.2 Supplement for SB1 Kit. See *MSP 4.2 Supplement for SB1 Kit - Available for download from the Zebra Support Central web site. on page 4-1*.
4. Install the MSP Package Builder onto the Windows-based workstation according to the *Mobility Services Platform 4.2 Software Installation Guide*.
5. Install the Package Builder Template for Rho-Based Applications for the SB1 into the MSP Package Builder. See *MSP 4.2 Supplement for SB1 Kit - Available for download from the Zebra Support Central web site. on page 4-1*.
6. Launch the MSP Console from the workstation and ensure that log in is successfully.

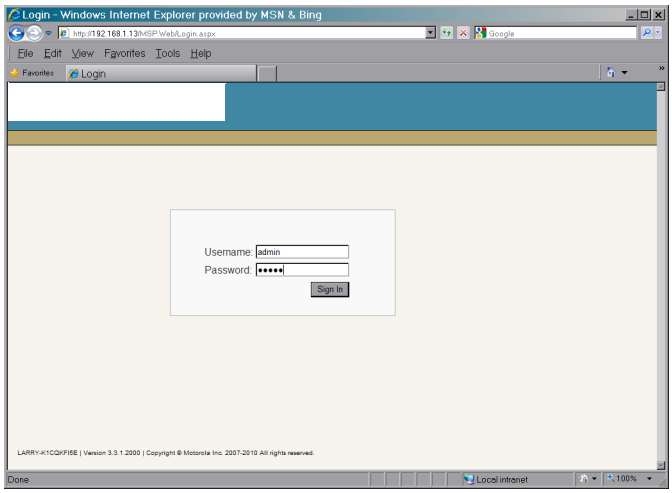


Figure 4-1 *Mobility Services Platform Console*

7. Copy the contents of the extracted *Templates* folder to the folder where the MSP Package Builder is installed, for example:

   D:\Program Files\Motorola MSP\MSP Package Builder.
8. Launch **MSP Package Builder**.
9. Select **Tools** > **Options**. The **Options** window appears.

10. Select **Default File Templates**.

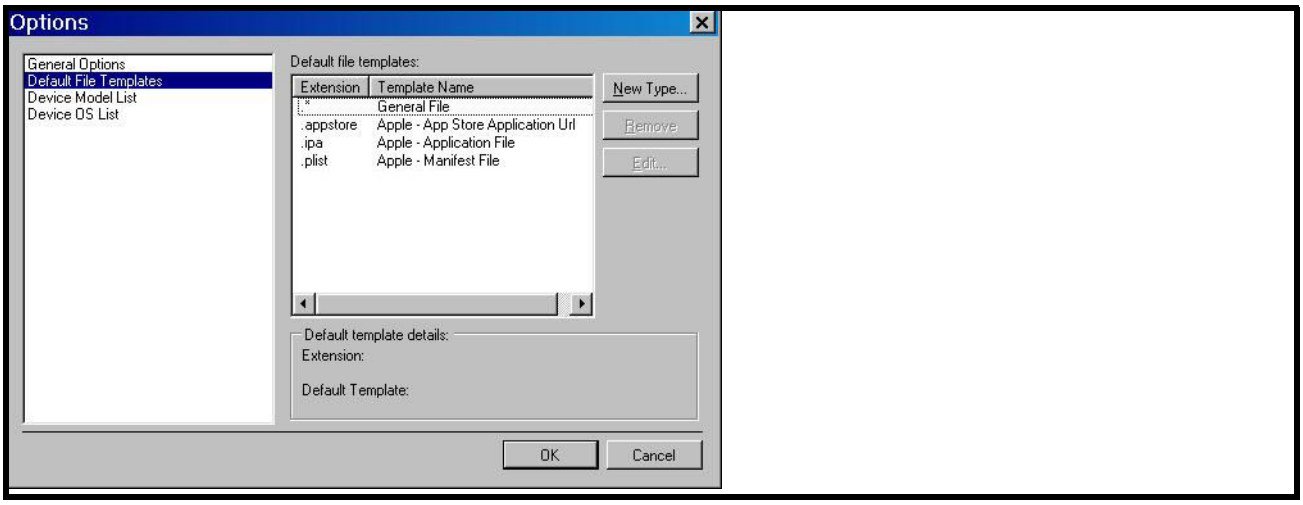


Figure 4-2 *Options Window*

11. Click the **New Type** button. The **Default File Template** dialog box appears.

Figure 4-3 *Default File Template Window*

12. In the **File Extension** text box, enter **.app**.
13. In the **Default Template** drop-down list box, select **RhoApp. 1.0**.
14. Click **OK**.
15. Repeat for RhoFont (.ttf) and Rho App1 (.app1). Once you are done, the **Default Template** list should look as shown in *Figure 4-4*.

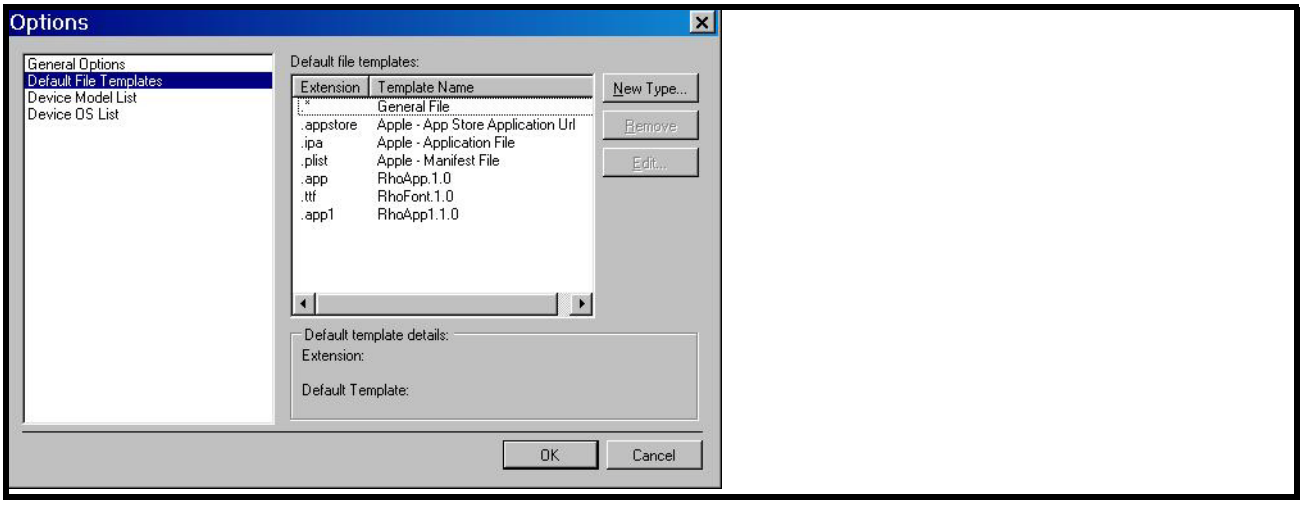


Figure 4-4 *Options Window with Extensions*

16. Click **OK**.

Preparing Generic Staging Content

To prepare the generic staging content:

1. Determine all WLAN(s) that will be used when staging the SB1.
2. Determine the WLAN(s) that will be used by the SB1 after staging.
3. Log in to the MSP Console and create one WLAN Settings Object for each unique WLAN.
   - Enter a unique name for the WLAN.
   - Enter the configuration information for each unique WLAN.
4. Determine which FTP servers will be used when staging the SB1.
5. Ensure that an MSP Relay Server Object has been created by the MSP Administrator to represent each FTP server.

Preparing Infrastructure to Support a Well-Known Staging WLAN

Configure the WLAN infrastructure to support a local WLAN with the following characteristics:

- SSID = “airbeam”
- Authentication = Open
- Encryption = WEP128 or WEP104
- WEP Key Index = 1
- Hex WEP Key 1 = “1011121314151617181 91a1b1c”

Since this Staging WLAN uses low security, limit access to the WLAN by:

a. Locating it in a secure area.
b. Lowering the RF power or using a limited range antenna.
c. Enabling the Staging WLAN only when staging is being performed.

UserDrive Update

To prepare *UserDrive* folder content using the MSP Server:

1. Customize the sample baseline ***Sb1SampleBasline*** package as required to suit the requirements for the customer application environment. See *Sample Baseline Package Customization on page 4-11*.
2. Create one or more Rho-based application packages using the MSP Package Builder and the RhoApplication template See *Creating Application Packages on page 4-12*.
3. Create a bundle containing the following deployment steps:
   a. The customized baseline package from step 1.
   b. Any Rho-based application packages created in step 2.
4. Create a Staging Profile with some or all of the following:
   a. WLAN settings (see *Preparing Generic Staging Content on page 4-15*.
   b. Relay Server settings (see *Preparing Generic Staging Content on page 4-15*.

c. Bundle created in step 3.

Enrollment for Management by MSP

> ***NOTE*** In order to manage the SB1 using MSP, the MSP Provision Edition and MSP Control Edition servers are required. Each managed SB1 requires an MSP Provision or MSP Control license depending upon the functionality being used.

The MSP Agent is installed on the SB1 but is initially dormant until it is activated via staging. Activating the MSP Agent causes the SB1 to become managed by MSP and is referred to as Enrolling the SB1 for On-going Management by MSP.

The following requirements must be met for the SB1 to be managed by MSP:

- The SB1 must have network connectivity to reach a defined Relay Server. This requirement is typically accomplished for an SB1 by applying a WLAN Settings Object during staging.
- The SB1 must have the information (address, credentials, etc.) needed to reach the Relay Server with which it checks-in. This requirement is typically accomplished for an SB1 by specifying a Relay Server during staging.
- The SB1 must have been configured to check-in with MSP via its defined Relay Server on some scheduled basis. This requirement is typically accomplished for an SB1 by applying an Agent.30 Settings Object during staging.

Since staging is an activity that must be invoked by a user, it is often desirable to reduce the number of times staging must be performed, preferably to a single staging operation. The above requirements can often be combined into the same staging operations that perform other tasks, an OS Update, deploying application content or an MSP Agent update.

1. Create a bundle containing the desired deployment steps:
   a. ***SB1SaveCalibration*** package, if required.
   b. Packages for MSP Agent Update, if required.
   c. UserDrive packages, if required.
   d. An Agent.30 Settings Object specifying desired MSP Agent configuration.
2. Create a Staging Profile with some or all of the following:
   a. WLAN settings. See *Preparing Generic Staging Content on page 4-15*.
   b. Relay Server settings. See *Preparing Generic Staging Content on page 4-15*.
   c. Bundle created in step 1.

Print a Bar Code Sheet

To print a bar code sheet:

1. Log into the MSP Console.
2. Locate the desired Staging Profile.

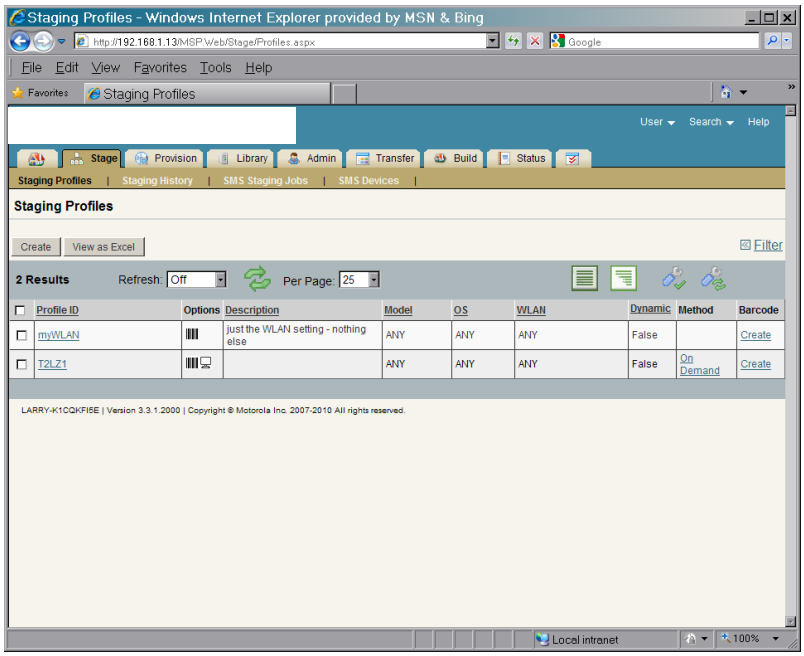


Figure 4-5 *Staging Profiles Screen*

3. Select **Create**. The **Barcode Sheet Generation** screen appears.

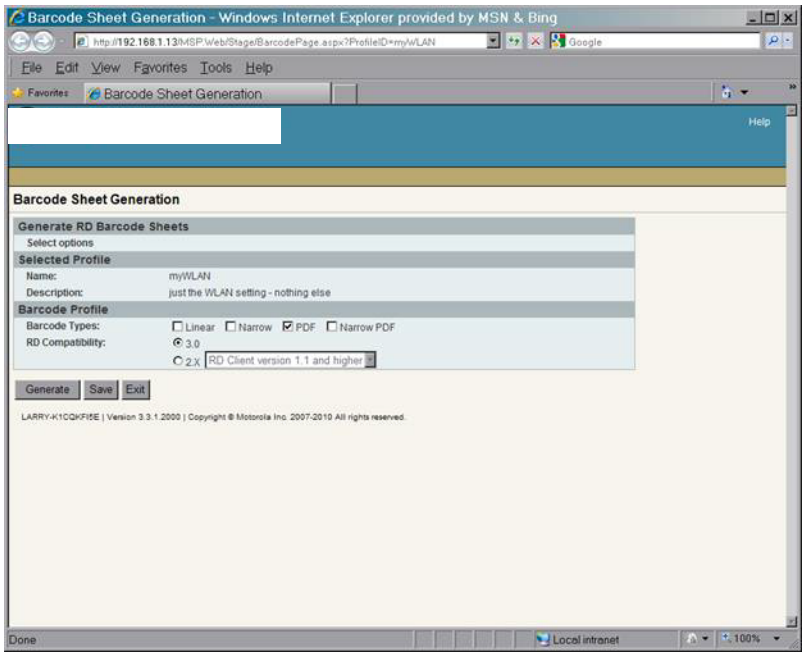


Figure 4-6 *Barcode Sheet Generation Screen*

4. In the **Barcode Profile** section:
   - Select the **Barcode Types - PDF** checkbox.
   - Select the **RD Compatibility - 3.0** radio button.
5. Click the **Generate** button. MSP creates the bar code sheet and displays it on the screen.

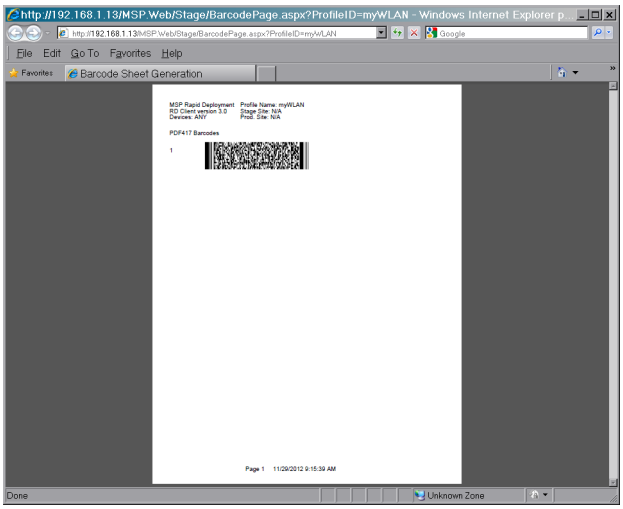


Figure 4-7 *Bar Code Sheet*

6. Print the bar code sheet.

Using the RD Client

Use the **RD Client** to stage an SB1 using a printed bar code sheet or using Well-known WLAN.

Bar Code Sheet

To stage an SB1 using a printed bar code sheet:

1. Generate and print a bar code sheet. See *Print a Bar Code Sheet on page 4-16*.
2. On the SB1, press the Home button (if required).
3. Touch > > **Advanced Settings**. Enter password (if required).

   or

   Touch **Applications**.
4. Touch **RD Client**.
5. Touch **OK**. Wait for the **Waiting…** message to display.

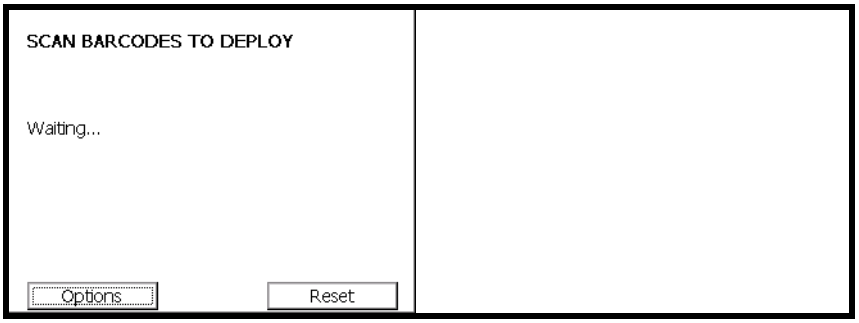


Figure 4-8 *Scan Barcodes to Deploy Screen*

6. Press the Scan button and aim at the bar code(s).
7. When the message **Your Device is Ready To Use** displays, touch **OK**.

Well-Known WLAN

To stage an SB1 using a Well-known WLAN:

1. Prepare the Well-Known Staging WLAN. See *Preparing Infrastructure to Support a Well-Known Staging WLAN on page 4-15*.
2. Log into the MSP Console from a workstation that is on the same subnet as the Well-Known Staging WLAN.
   a. Locate the desired Staging Profile and click the **On-Demand** link or the **Staging – On-Demand** link.
   b. Within the On-Demand Server Applet screen, click the **Turn staging server on** button.
3. On the SB1, press the Home button (if required).
4. Touch > > **Advanced Settings**. Enter password (if required).

   or

   Touch **Applications**.
5. Touch **RD Client**.

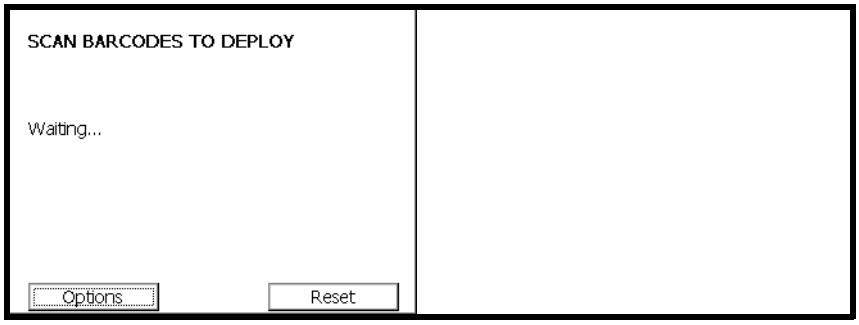


Figure 4-9 *Scan Barcodes to Deploy Screen*

6. When the **Waiting…** message displays, touch **Options**. The **Main Menu** screen appears.

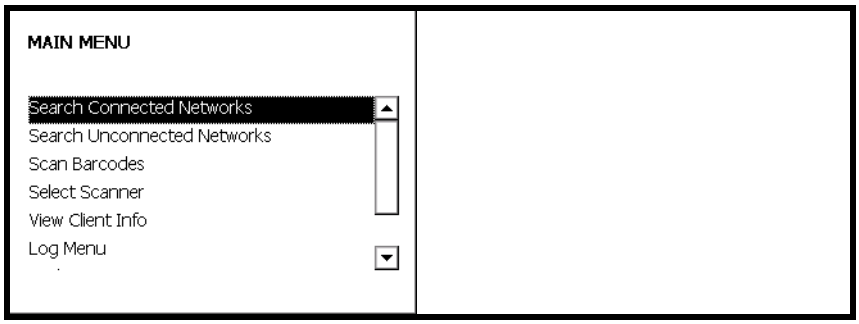


Figure 4-10 *Main Menu Screen*

7. Touch **Search Unconnected Networks**.
8. When the message **Your Device is Ready To Use** appears, touch **OK**.

Staging Using Rapid Deployment Tool Solo

This section provides information for staging the SB1 using the RDT Solo.

Setting Up RDT Solo

To prepare the SB1 for staging using RDT Solo on a workstation:

1. From a Windows-based workstation, launch RDT Solo. The **RDT Solo** Home Screen appears.

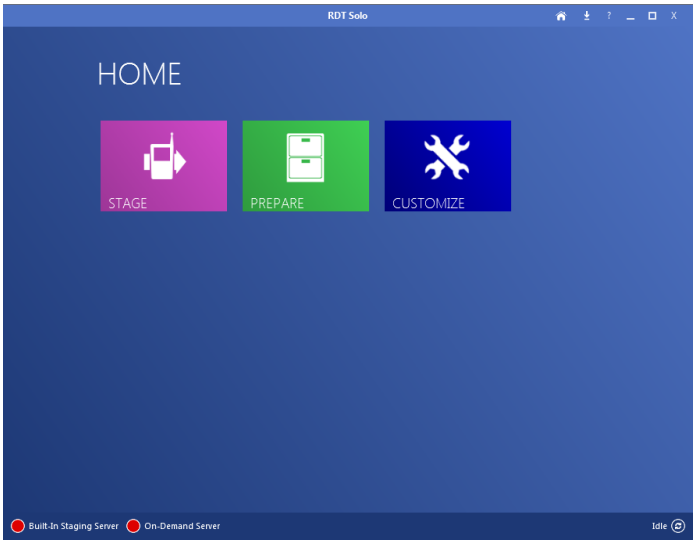


Figure 4-11 *Remote Deployment Tool Solo Home Screen*

2. Copy the contents of the extracted *Templates* folder to the folder where the MSP Package Builder is installed, for example:

   D:\Program Files\Motorola MSP\MSP Package Builder.

3. Launch **MSP Package Builder**.
4. Select **Tools** > **Options**. The **Options** window appears.
5. Select **Default File Templates**.

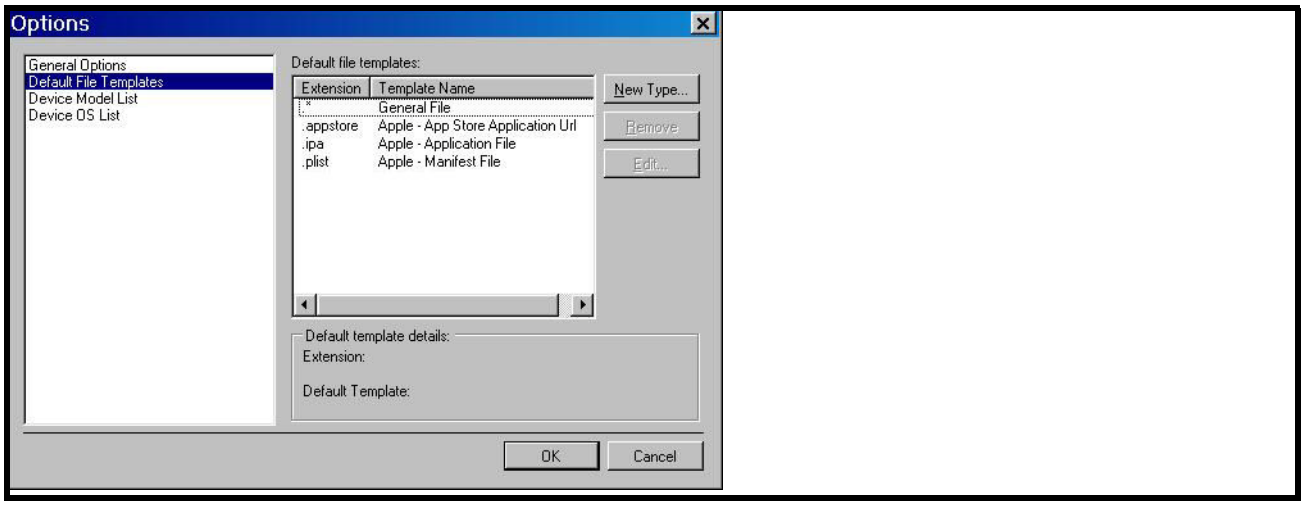


Figure 4-12 *Options Window*

6. Click the **New Type** button. The **Default File Template** dialog box appears.

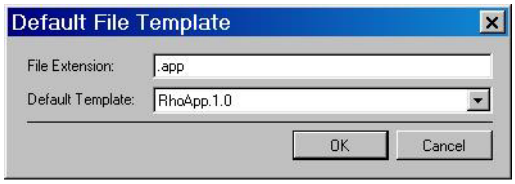


Figure 4-13 *Default File Template Window*

7. In the **File Extension** text box, enter **.app**.
8. In the **Default Template** drop-down list box, select **RhoApp. 1.0**.
9. Click **OK**.
10. Repeat for RhoFont (.ttf) and Rho App1 (.app1). Once you are done, the **Default Template** list should look as shown in *Figure 4-14*.

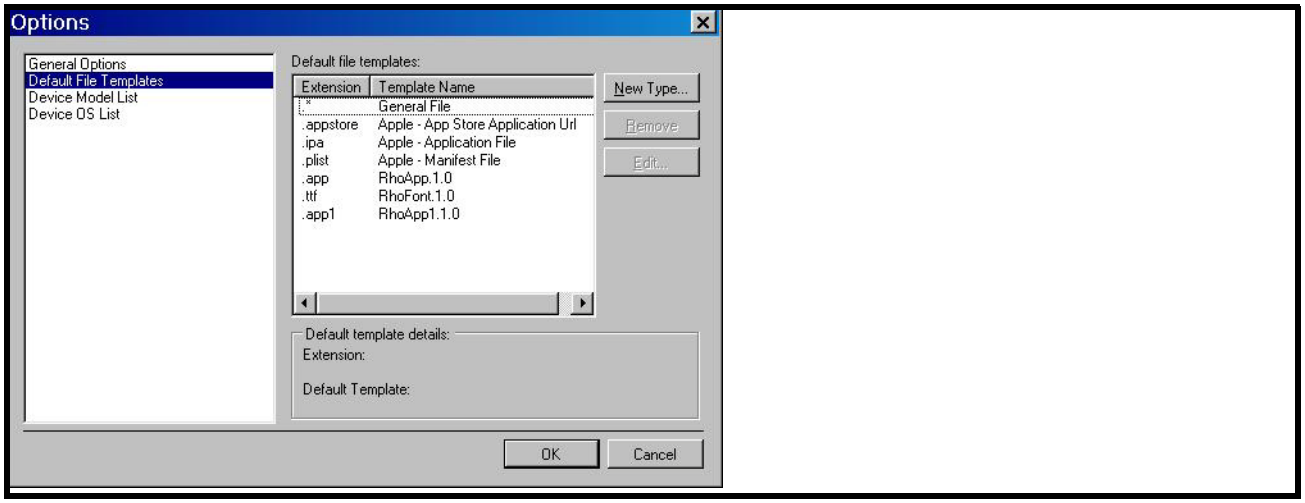


Figure 4-14 *Options Window with Extensions*

11. Click **OK**.

Preparing Generic Staging Content

To prepare generic staging content:

1. Determine all WLAN(s) that will be used when staging the SB1.
2. Determine the WLAN(s) that will be used by the SB1 after staging.
3. Launch RDT Solo and for each unique WLAN:
   a. Enter a unique name for the WLAN.
   b. Enter the configuration information for each unique WLAN.
4. Determine if additional FTP servers (other than the one built-into the RDT) will be used to stage the SB1.
5. Ensure the information for each FTP server into the RDT Solo.

UserDrive Update

To prepare content using the RDT Solo:

1. Customize the sample Baseline ***Sb1SampleBasline*** package as required to suit the requirements for the customer application environment. See *Sample Baseline Package Customization on page 4-11*.
2. Optionally create one or more Rho-Based Application package using the MSP Package Builder and the RhoApplication Template. See *Creating Application Packages on page 4-12*.
3. Login to RDT Solo and define a Staging Profile:
   a. Enter a unique name for the Staging Profile.
   b. Identify the WLAN to be used for staging.
   c. Identify the Staging Server.
   d. Specify the customized baseline package from step 1.
   e. Specify any Rho-Based Application packages created in step 2.
   f. Save the Staging Profile.

Printing a Bar Code Sheet

To print a bar code sheet:

1. Launch RDT Solo.
2. Click **Stage**.
3. Select the RDProfile to stage.
4. Click **Continue**.
5. Select the staging server.
6. Click **Continue**.
7. Click BARCODE.
8. Select the PDF417 bar code type.
9. Click the **View** button. RDT Solo creates the bar code sheet and displays it on the screen.
10. Print the bar code sheet.

Using the RD Client

Use the **RD Client** to stage an SB1 using a printed bar code sheet or using Well-known WLAN.

Bar Code Sheet

To stage an SB1 using a printed bar code sheet:

1. Generate and print a bar code sheet. See *Printing a Bar Code Sheet on page 4-22*.
2. On the SB1, press the Home button (if required).
3. Touch > **More Settings**> **Advanced Settings**. Enter password (if required).

   or

   Touch **Applications**.
4. Touch **RD Client**.
5. Touch **OK**. Wait for the **Waiting…** message to display.

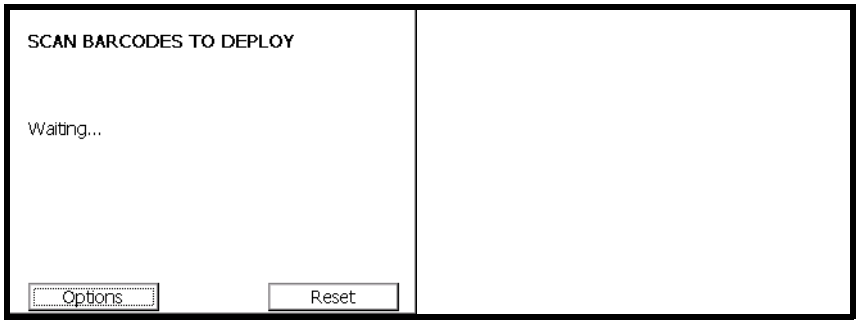


Figure 4-15 *Scan Barcodes to Deploy Screen*

6. Press the Scan button and aim at the bar code(s).
7. When the message **Your Device is Ready To Use** displays, touch **OK**.

Well-known WLAN

To stage an SB1 using a Well-known WLAN:

1. Prepare the Well-Known Staging WLAN. See *Preparing Infrastructure to Support a Well-Known Staging WLAN on page 4-15*.
2. Log into the RDT from a workstation that is on the same subnet as the Well-Known Staging WLAN.
   a. Locate the desired named Staging Profile.
   b. Click the **On-Demand** link.
   c. Click the **Turn staging server on** button.
3. On the SB1, press the Home button (if required).
4. Touch > More Settings > **Advanced Settings**. Enter password (if required).

   or

   Touch **Applications**.
5. Touch **RD Client**.

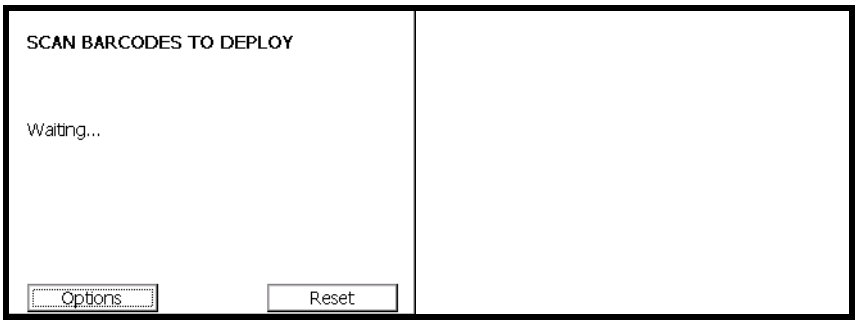


Figure 4-16 *Scan Barcodes to Deploy Screen*

6. When the **Waiting…** message displays, touch **Options**. The **Main Menu** screen appears.

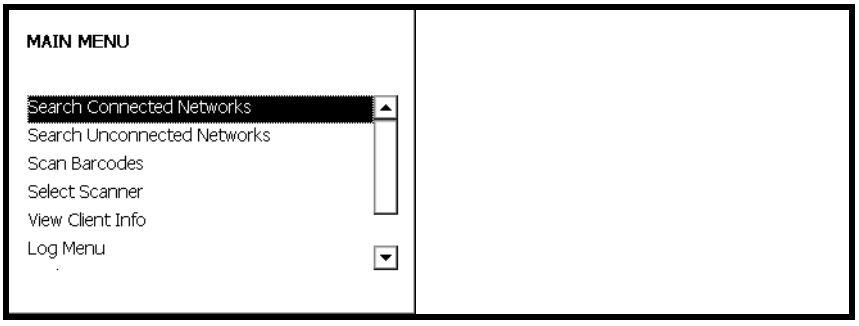


Figure 4-17 *Main Menu Screen*

7. Touch the **Search Unconnected Networks**.
8. When the message **Your Device is Ready To Use** appears, touch **OK**.

On-going MSP Management

This section provides additional information for managing the SB1 using MSP features. In order to manage the SB1 using MSP, the MSP Agent on the SB1 must first be activated via staging. See *Enrollment for Management by MSP on page 4-16* for more information.

NOTE For use with MSP only.

Reboot Deployment Steps

On the SB1, a reboot is always performed automatically at the end of every bundle. If the intent is to just perform a reboot of the SB1, then use a bundle with no deployment steps. If the intent is to reboot the SB1 between each package, include a reboot deployment step between the packages but do not end the bundle with a reboot deployment step to avoid a double reboot. One from the reboot deployment step and the other from the end of the bundle.

Send Jobs Only When SB1 is in Cradle

To send a bundle only when the SB1 is in a cradle:

1. Create a Power Condition Object where:
   - First line prompt, Second line prompt, and Third line prompt are all set to empty.
   - Delay (seconds) is set to 0.
   - Enable countdown is set to False.
   - Require power level is set to A/C.
2. For any Policy or Action that is applicable to any SB1 and where it is desired that Jobs occur only when the SB1 is in the cradle:
   - On the Readiness Conditions page of the Policy or Action, select the Condition created in step 1.
3. When the Policy fires or the Action is executed:
   - A Job is sent and is evaluated by the SB1.
   - If the SB1 is not in the cradle, then the Job is deferred.
   - On each subsequent check-in, the Job is re-evaluated and, if the SB1 is in the cradle, then the Job is executed.

Customizing the UpdateInProgress Package

To customize the ***UpdateInProgress*** package:

1. Locate the **`UpdateInProgress.APF`** package file in the folder to which you extracted the MSP 4.2 Supplement for SB1.
2. Using the **MSP Package Builder** open the **`UpdateInProgress.APF`** package file.
3. Select **Tools** > **Convert to Project**.
   a. Enter a name for the new package.
   b. Enter the location for the new package project file (.MSPPROJ) and the extracted content files.

c. Click **OK**.

4. Select **File** > **Save** to save the new package project file.
5. Modify the **`ld.txt`** file in the folder to which the package content files were extracted.
6. Select **File** > **Save** to save the modified package project file.
7. Select **Tools** > **Generate APF File** to make a package file containing the modified content.
8. Enter a package version.

Table 4-8 Customized ld.txt File Example

Original File Contents	Example Custom Contents
@lock Zebra MSP A Software Update is in progress Please do not use this device Until further notice Button *	@lock My Company Name This device is being updated and should not be used until this message disappears Button *

NOTE The ld.txt file must always contain exactly 7 text lines, as shown above.

Only text lines 2, 3, 4, and 5 should be changed, if desired, to alter the text that will be displayed on the SB1 screen.

Be sure to test any long text strings to ensure that they do not get truncated when they are displayed on the device screen.

How to Protect an Update Using UpdateInProgress

This section describes the steps required to protect an update when using the ***UpdateInProgress*** package:

1. Create a bundle containing the following:
   - The ***SB1SaveCalibration*** package - The Force Install option should not be set for this deployment step so the package is skipped if it is already present on the SB1.
   - The ***UpdateInProgress*** package - This package can optionally be customized, if desired. See *Customizing the UpdateInProgress Package on page 4-25*. The Force Install option should be set for this deployment step so the package is deployed even if it is already present on the SB1.
   - Deployment steps to perform whatever update is desired.
   - The ***EndUpdateInProgress*** package - The Force Install option should be set for this deployment step so the package is always deployed even if it is already present on the SB1.
2. Create a policy or action to deploy the bundle.
   - When a job to execute the bundle from step 2 is executed, a dialog box displays on the SB1 screen when the ***UpdateInProgress*** package is installed. The dialog box re-displays even following cold boots that occur during the update. The dialog box is removed when the ***EndUpdateInProgress*** package is installed.

Performing OS Updates from MSP

To push an OS Update to the SB1:

1. Obtain an *SB1* ***OSUpdate*** package from the SB1 page on the Zebra Support Central web site.
2. Create a bundle containing the following deployment steps in the exact order:
   a. ***SB1SaveCalibration*** package.

      The Force Install option should not be set for this deployment step so the package is skipped if it is already present on the SB1.

      The package is only installed if it is not already installed on the SB1. This ensures that the Touch Panel Calibration information produced when the user successfully performed a Touch Panel Calibration is stored persistently if it has not already been stored. Since this bundle results in two cold boots, failure to ensure that Touch Panel Calibration information is stored persistently requires the user to perform Touch Panel Calibration following each cold boot.

   b. ***WipeUserDrive*** package.

      This package is optional and would be installed to satisfy two key use cases.

      If the intent of the bundle includes loading new content in the *UserDrive* folder, then installing this package with the Force Install flag set to True ensures that the package is installed, and that the *UserDrive* partition is erased, regardless of whether the package is already installed on the SB1. If any packages are used to deploy content to the *UserDrive* folder, then it is advisable to first ensure that the *UserDrive* folder is empty. This ensures a predictable result no matter what state the SB1 may be in when staging is initiated.

      If the intent of the bundle is to return the SB1 to factory default state, then installing this package with the Force Install flag set to True ensures that the *UserDrive* partition is empty, as it is when the SB1 is shipped from the factory. Perform an OS Update in this way places the SB1 in the state it would have been in had it come from the factory loaded with the OS to which it was just updated.

   c. An SB1 Baseline Package, with the Force Install flag set to True.

      If the intent of the bundle is to populate content into the *UserDrive* folder, and to prepare an SB1 for production use, then a suitable SB1 Baseline Package should be installed. Installing an SB1 Baseline Package with the Force Install flag set to True ensures that the specified content is deployed to the *UserDrive* folder whether or not the package is already on the SB1. This is especially important if the ***WipeUserDrive*** package was installed previously in the bundle because while the ***WipeUserDrive*** package removes content from the *UserDrive* folder, it does not uninstall any package(s) that may have deployed that content. Forcing the SB1 Baseline Package to be reinstalled in such a case guarantees that the content is always deployed.

   d. One or more SB1 application package(s), with the Force Install flag set to True.

      If the intent of the bundle is to populate content into the *UserDrive* folder, and to prepare an SB1 for production use, then one or more SB1 applications packages may be installed. Installing an SB1 application package with the Force Install flag set to True ensures that the specified content is deployed to the *UserDrive* folder whether or not the package is already on the SB1. This is especially important if the ***WipeUserDrive*** package was installed previously in the bundle because while the ***WipeUserDrive*** package removes content from the *UserDrive* folder, it does not uninstall any package(s) that may have deployed that content. Forcing an SB1 application package to be reinstalled in such a case guarantees that the content is always deployed.

   e. The ***Sb1PrepareForOsUpdate*** Package.

      The Force Install option should be set for this deployment step, so the package is always deployed even if it is already present on the SB1.

Every bundle that installs an ***OSUpdate*** package to an SB1 must include the ***Sb1PrepareForOsUpdate*** package just before the ***OSUpdate*** package. Installing the ***Sb1PrepareForOsUpdate*** package places the SB1 into a state in which the OS Update can be successfully performed. Since the ***Sb1PrepareForOsUpdate*** package might have been previously installed on the SB1 during a prior OS Update, installing it with the Force Install flag set to True ensures that the SB1 is placed the state required to allow the OS Update to be performed.

The ***Sb1PrepareForOsUpdate*** package causes an explicit cold boot to occur which is mandatory in order to place the SB1 into the state required to allow the OS Update to be performed. After the cold boot, the processing of the bundle by the **RD Client** continues. As previously noted, the ***SB1SaveCalibration*** package should generally be used to suppress the need for the user to perform Touch Panel Calibration following that cold boot.

f. ***SB1WipeCalibration*** package (optional), with the Force Install flag set to True.

If the intent of the bundle is to return a SB1 to factory default state, then it may be desirable to remove any Touch Panel Calibration information that was saved. If the ***SB1WipeCalibration*** package is installed between the ***Sb1PrepareForOsUpdate*** package and the ***OSUpdate*** package, then Touch Panel Calibration is suppressed on the cold boot initiated by the ***Sb1PrepareForOsUpdate*** package (before the OS ***Update*** package) but Touch Panel Calibration is be required after the OS Update is complete, as it would be on a fresh out of the box device.

Since the ***SB1WipeCalibration*** package may have been previously installed on the SB1, installing the ***SB1WipeCalibration*** package with the Force Install flag set to True ensures that the Touch Panel Calibration information is always removed. Note that unless it is specifically desired to require that Touch Panel Calibration be performed by the user, then this package should not be included in the bundle.

g. The ***OSUpdate*** package from step 1.

In some cases, an ***OSUpdate*** package might be applied more than once to the same SB1. For example, a package might be used to return an SB1 to the factory default state even if the OS in the SB1 was previously deployed using that same package. Installing an ***OSUpdate*** package with the Force Install flag set to True ensures that the OS Update is always performed and that the SB1 is always placed into the desired state.

3. Create a Policy or Action to deploy the bundle from step 2.

- When a Job to execute the bundle from step 2 is executed, the SB1 reboots into a mode where the Rho-based Shell is not running. This allows the *Application* partition and OS to be safely updated.

When the OS Update is complete, the SB1 reboots again into a mode where the Rho-based Shell and PTT Express are running. Under normal circumstances, Wireless Settings connectivity and manageability by MSP is preserved across the application and OS Update.

In the event that the OS Update reformats the *Application* and/or *UserDrive* folders, then Wireless Settings connectivity and/or manageability by MSP may not be preserved across the application and OS Update.

Pushing an MSP Agent Update

To update the MSP Agent using MSP:

1. Choose the most appropriate MSP Agent Update package.

- Most commonly, the ***abup30*** package with a version of ddd_xxx should be used.
- Alternately, the ***abup30*** package with a version of ddp_xxx could be used, if support for Detached Jobs is required. Refer to the *MSP Client Software Guide* for more information).

2. Create a bundle containing the desired deployment steps:

a. The ***RebootEnableOverride*** package. The **abup30** package from in step 1.

3. Create a Policy or action to deploy the bundle from step 2.
   - When a job to execute the bundle from step 2 is executed, the MSP Agent is updated and a cold boot is performed to activate the new updated MSP Agent.
   - It is generally recommended to have a policy to deploy the latest version of the MSP Agent to all devices managed by MSP and to update the bundle referenced by that policy whenever a new version of the MSP Agent becomes available.

MSP Agent Update Using an MSP Server and the RD Client

The MSP Client software is pre-installed on the SB1 and can be updated by installing an ***MSP Client Software Update*** package. When an SB1 is managed by MSP on an ongoing basis, it is highly recommended to update to the latest available version of the MSP Client software. If only staging is used, it may not be necessary or even advisable to update to the MSP Client software from the version that is pre-installed.

Initial staging when the SB1 is out of the box must be performed using the version of the RD Client pre-installed on the SB1. While newer versions of the MSP Client software might be available, and while a newer version might include additional RD Client features, such features could not be utilized unless staging was performed multiple times. A first staging operation would need to be performed to update the RD Client then a second staging operation would need to be performed. The first staging operation would need to stay within the capabilities of the original RD Client and only the second staging operation could utilize any new capabilities of the new RD Client.

In addition, if new capabilities are required to get onto a desired network, it may be impractical to perform the first staging operation over that network. While there may be cases in which multiple staging operations might be acceptable, in most cases a single staging operation is preferred, thus requiring that staging to be performed using the capabilities of the RD Client that is part of MSP Client software that is pre-installed on the SB1.

To update the MSP Agent using an MSP Server:

1. The SB1 is supported by the standard MSP Agent Update packages.
   - Most commonly, ***abup30*** package with a version of ddd_xxx should be used.
   - Alternately, the ***abup30*** package with a version of ddp_xxx could be used, if support for Detached Jobs is required. Refer to the *MSP Client Software Guide* for more information.

2. Since the SB1 does not support warm boot, the standard ***MSP Agent Update*** packages fail if used by itself. The ***RebootEnableOverride*** package is used to override default behavior and allow the standard ***MSP Agent Update*** packages.

3. Create a bundle containing the desired deployment steps:
   a. ***RebootEnableOverride*** package from step 2.
   b. ***abup30*** package from step 1.

4. Create a Staging Profile with some or all of the following:
   a. WLAN settings. See *Preparing Generic Staging Content on page 4-15*.
   b. Relay Server settings. See *Preparing Generic Staging Content on page 4-15*.
   c. Bundle created in step 3.

CHAPTER 5 MAINTENANCE AND TROUBLESHOOTING

Introduction

This chapter includes instructions on cleaning and storing the SB1, and provides troubleshooting solutions for potential problems during SB1 operation.

Maintaining the SB1

For trouble-free service, observe the following tips when using the SB1:

- Do not scratch the screen of the SB1. When working with the SB1, use only your finger. Never use an actual pen, pencil, stylus or other sharp object on the surface of the SB1 screen.
- Although the SB1 is water and dust resistant, do not expose it to rain or moisture for an extended period of time. In general, treat the SB1 as a pocket calculator or other small electronic instrument.
- The screen of the SB1 is glass. Do not to drop the SB1 or subject it to strong impact.
- Protect the SB1 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 SB1 in any location that is dusty, damp, or wet.
- Use a soft lens cloth to clean the SB1. If the surface of the SB1 screen becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution. See *Cleaning on page 5-2*.
- Do not place in pocket. Use holster or armband.

Battery Safety Guidelines

WARNING! Failure to follow these guidelines may result in fire, explosion, or other hazard.

- 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 user 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 +95 ºF (0 ºC and +35 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 Zebra Global Customer Support.
- 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 Zebra Global Customer Support to arrange for inspection.

Cleaning

CAUTION Always wear eye protection.

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

If you have to use any other solution for medical reasons please contact Zebra 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[1](see Important note below), hydrogen peroxide or mild dish soap.

IMPORTANT Use pre-moistened wipes and do not allow liquid to pool.

[1] When using sodium hypochlorite (bleach) based products always follow the manufacturer's recommended instructions: use gloves during application and remove the residue afterwards with a damp alcohol cloth or a cotton swab to avoid prolonged skin contact while handling the device.

Due to the powerful oxidizing nature of sodium hypochlorite, the metal surfaces on the device are prone to oxidization (corrosion) when exposed to this chemical in the liquid form (including wipes). Avoid allowing any bleach based product to come in contact with the metal electrical contacts on the device, the battery, or the cradle. In the event that these types of disinfectants come in contact with metal on the device, prompt removal with alcohol-dampened cloth or cotton swab after the cleaning step is critical.

Harmful Ingredients

The following chemicals are known to damage the plastics on the SB1 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. In addition, bleach solutions are known to corrode gold contacts over time.

Cleaning Instructions

Do not apply liquid directly to the SB1. 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. If solution containing bleach is used on the gold contacts, it is recommended that an immediate wipe down using isopropyl alcohol (IPSA) be administered to remove residuals. 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 SB1. The SB1 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 SB1, such as hand sanitizer that contain ethanolamine, hands must be completely dry before handling the SB1 to prevent damage to the plastics.

Materials Required

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

Cleaning the SB1

Housing

Using the alcohol wipes, wipe the housing including buttons.

Display

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

Reader Exit Window

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

Contacts

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

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

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

Cleaning Cradle Connectors

To clean the connectors on a cradle:

1. Remove the DC power cable from the cradle.
2. Dip the cotton portion of the cotton tipped applicator in isopropyl alcohol.
3. Rub the cotton portion of the cotton tipped applicator along the pins of the connector. Slowly move the applicator back-and-forth from one side of the connector to the other. Do not let 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 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. Ensure that there is no lint left by the cotton tipped applicator, remove lint if found.
7. If grease and other dirt can be found on other areas of the cradle, use lint free cloth and alcohol to remove.
8. Allow at least 10 to 30 minutes (depending on ambient temperature and humidity) for the alcohol to air dry before applying power to cradle.

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

Cleaning Frequency

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

Troubleshooting

SB1

Table 5-1 *Troubleshooting the SB1*

Problem	Cause	Solution
SB1 does not turn on.	Battery not charged.	Charge the SB1.
	SB1 was turned off.	Place the SB1 into a powered cradle. The SB1 turns on when power is applied.
	System error.	Perform a reset. If the SB1 still does not turn on, contact the system administrator. For more information see, *Resetting the SB1 on page 1-4*.
Battery did not charge.	Battery failed.	Perform a reset. For more information see, *Resetting the SB1 on page 1-4*.
	SB1 removed from cradle while battery was charging.	Place in cradle and begin charging. The battery requires up to four hours to recharge fully.
	Extreme battery temperature.	Battery does not charge if ambient temperature is below 0 °C (32 °F) or above 40 °C (104 °F).
SB1 does not emit sound.	Volume setting is low or turned off.	Increase the volume. Refer to the *SB1 User Guide* for more information.
	Audio Adapter not installed properly.	Remove and replace Audio Adapter. When connected properly the SB1 emits two beeps.
	Headset not plugged into Adapter correctly.	Remove headset plug and insert into Audio Adapter audio jack.
	Speaker Adapter not installed properly.	Remove and replace Speaker Adapter. When connected properly the SB1 emits three beeps.

Table 5-1 *Troubleshooting the SB1 (Continued)*

Problem	Cause	Solution
Tapping the screen buttons or icons does not activate the corresponding feature.	Touch screen not calibrated correctly.	Re-calibrate the screen. Refer to the *SB1 User Guide* for more information.
	Battery depleted.	Recharge the battery.
The SB1 stops responding.	User pressed the Home and Scan buttons simultaneously for less than five seconds suspending the SB1.	Touch the screen to wake the SB1 from suspend.
Cannot capture bar code data.	Scanning application is not running.	Verify the SB1 a scanning application is running. See the system administrator.
	Unreadable bar code.	Ensure that the bar code is of good quality.
	Distance between SB1 and bar code is incorrect.	Ensure that the SB1 is within proper scanning range.
	SB1 is not programmed for the bar code type.	See system administrator.
	Battery is low.	Check the battery level. When the battery is low, the SB1 automatically goes into suspend mode.
	Bar Code Reader window is dirty.	Clean the window. See *Cleaning on page 5-2*.
Low Battery message appears.	Battery charge level is getting low.	Place the SB1 into a cradle or charger to charge the battery.
Cannot Reload message appears on the screen.	Network communication error has occurred.	Touch **Wait** button to allow the SB1 to re-establish communication with the network. If problem persists, contact system administrator.

Single Slot Charging Cradle

Table 5-2 *Troubleshooting the Single Slot Charging Cradle*

Problem	Cause	Solution
SB1 battery is not charging.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	The SB1 is not fully seated in the cradle.	Remove and re-insert the SB1 into the cradle, ensuring it is correctly seated.
	Battery is faulty.	Verify that other SB1 devices charge properly. If so, contact system administrator.

Ten Slot Charge Only Cradle

Table 5-3 *Troubleshooting the Four Slot Charge Only Cradle*

Problem	Cause	Solution
SB1 battery is not charging.	Cradle is not receiving power.	Ensure the power cable is connected securely to both the cradle and to AC power.
	The SB1 is not fully seated in the cradle.	Remove and re-insert the SB1 into the cradle, ensuring it is correctly seated.
	Battery is faulty.	Verify that other SB1 devices charge properly. If so, contact system administrator.

Audio Adapter

Table 5-4 *Troubleshooting the Audio Adapter*

Problem	Cause	Solution
Audio cannot be heard through headset.	Audio Adapter not connected properly.	Remove Audio Adapter and reinstall.
	Headset is not connected properly.	Remove headset from Audio Adapter and reinstall.
	Volume is too low.	Increase audio volume.

Speaker Adapter

Table 5-5 *Troubleshooting the Speaker Adapter*

Problem	Cause	Solution
Audio cannot be heard through Speaker Adapter.	Speaker Adapter not connected properly.	Remove Speaker Adapter and reinstall.
	Volume is too low.	Increase audio volume,

APPENDIX A STEP BY STEP WLAN SETUP EXAMPLE

Introduction

This appendix provides a step-by-step sample procedure for setting up WLAN settings for staging an SB1. Note that the information is an example and settings are dependent upon the network that you are connecting to.

Procedure

This sample procedure provides instructions for setting up the WLAN settings for staging the SB1.

1. Connect to the MSP Server.

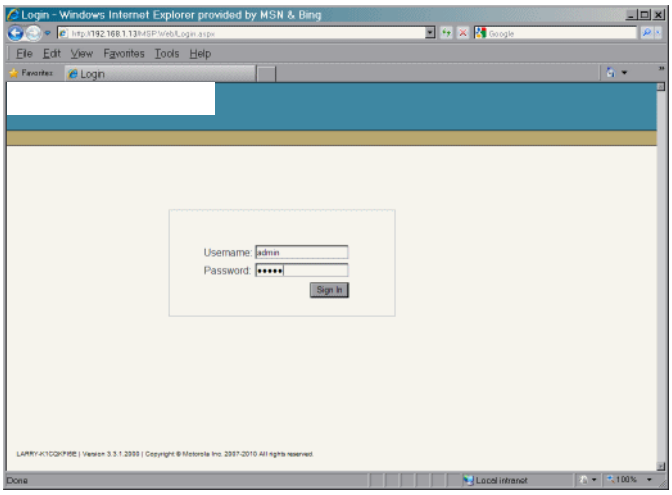


Figure A-1 *MSP Console*

2. Login using the username and password set up during MSP installation. After login the **Start Page** displays.

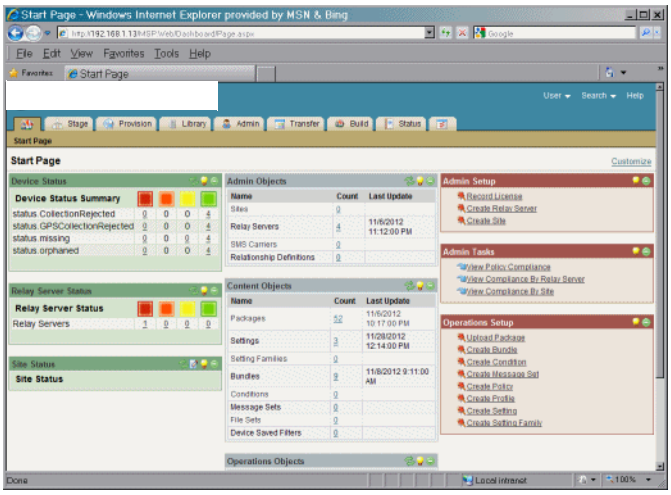


Figure A-2 *MSP Start Page*

3. Click the **Library** tab.

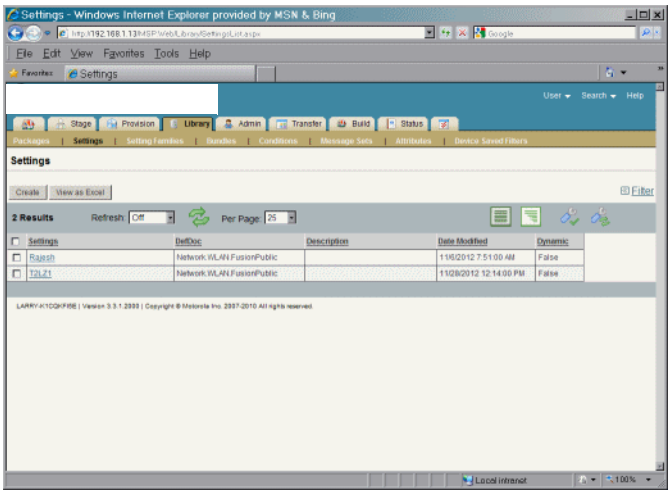


Figure A-3 *Library Tab*

4. Under the **Library** tab, click on the **Settings**. A list of all the settings created displays. Initially, it is blank.
5. Click the **Create** button. The **Setting Create** screen appears.

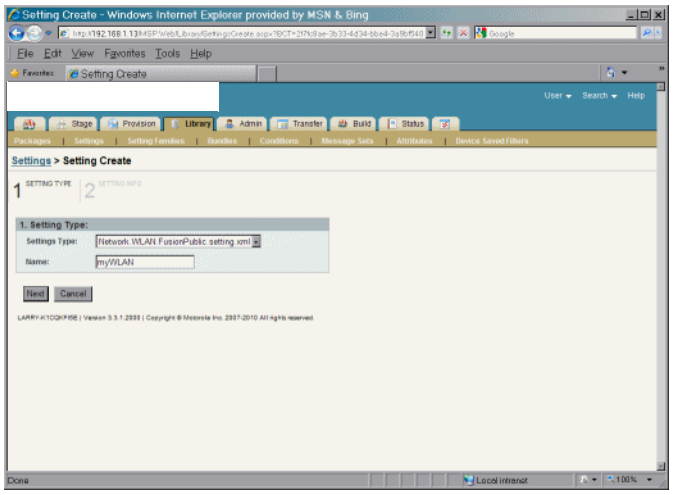


Figure A-4 *Setting Create - Setting Type Screen*

6. In the **Settings Type** drop-down list, select **Network.WLAN.FusionPublic.setting.xml**.
7. In the **Name** text box, enter a name for this setting type. Do not use spaces.
8. Click the **Next** button. The **Setting Info** screen appears.

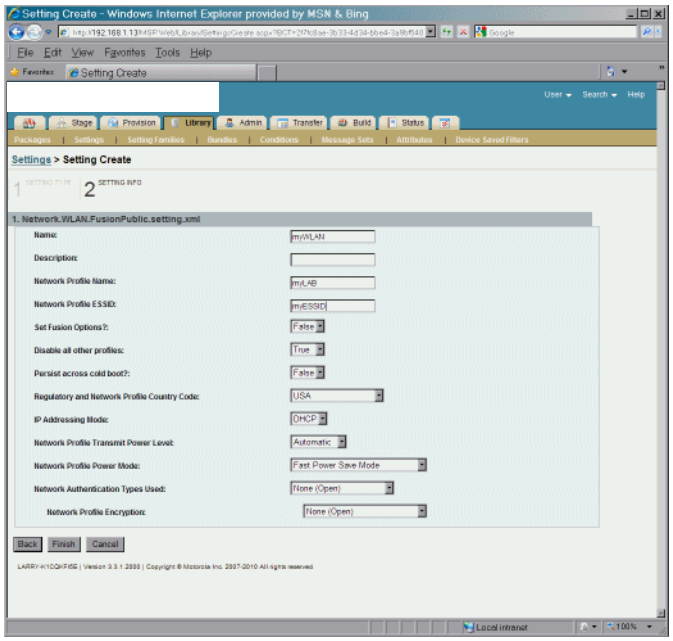


Figure A-5 *Setting Create - Setting Info Screen*

9. The system displays a template designed for creation of settings of the type selected.
10. In the **Name** text box, enter a name for the settings.
11. In the **Network Profile Name** text box, enter a name for the network profile.
12. In the **Network Profile ESSID** text box, enter a name for the network profile ESSID.
13. In the **Set Fusion Options** drop-down list, select **True**. Selecting **True** expands the option fields.

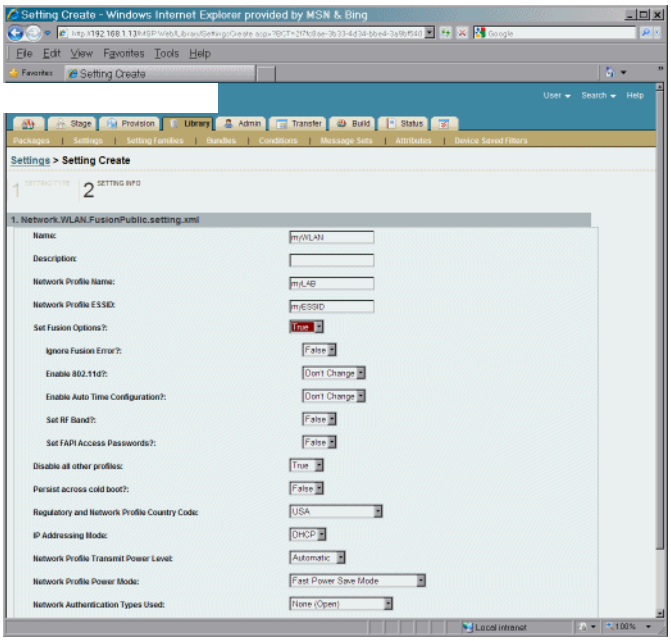


Figure A-6 *Set Fusion Options*

14. This is typical of this kind of screen in MSP and you may see the same behavior. If you choose an authentication type or an encryption type.
15. In the **Ignore Fusion Error** drop-down list, select **True**.
16. In the **Enable 802.11d?** drop-down list, select **False** if not using 802.11d or **True** if using 802.11d.
17. I am defaulting all the other fields except Network Profile Encryption. For that field. I choose WPA–PSK(TKIP), because that is the kind of encryption I am using.
18. In the **Network Profile Encryption** drop-down list, select the type of encryption the network is supporting.
19. In the **Pre-shared Pass Key** text box, enter the pre-shared passkey.
20. Click **Finish**. The **Related Tasks** window appears.

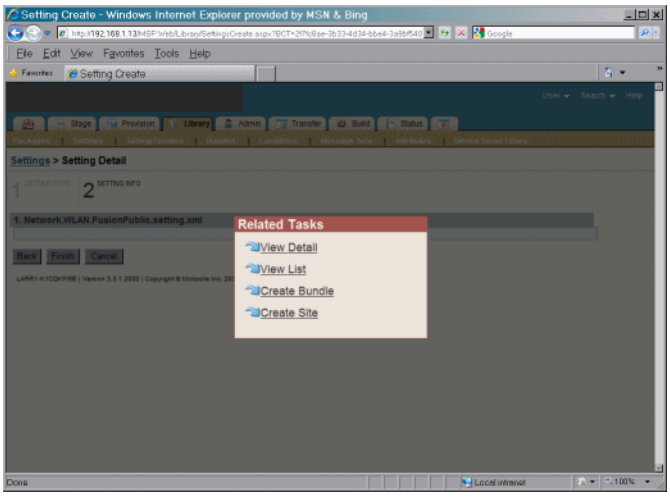
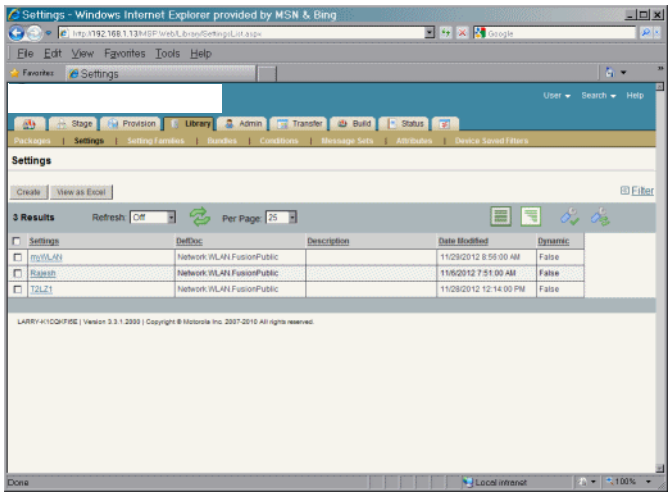


Figure A-7 *Related tasks*

21. Click **View List**. The setting just created appears in the list.



22. Click the **Stage** tab. A list of Staging Profiles defined in the MSP Server displays. The list is initially blank.

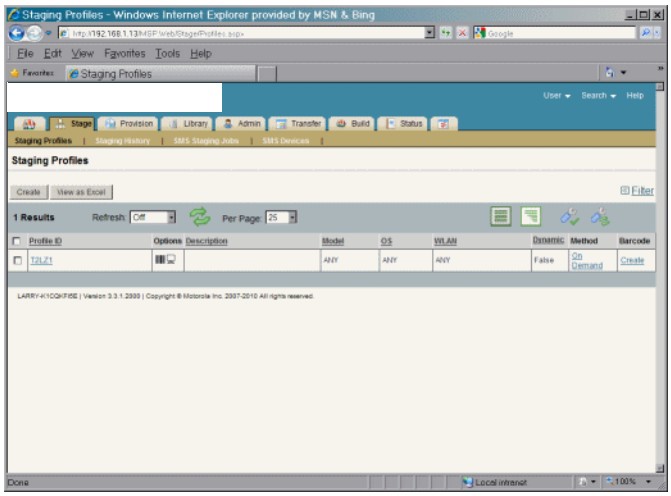


Figure A-8 *Staging Profiles Screen*

23. Click the **Create** button. The Profile Create screen appears.

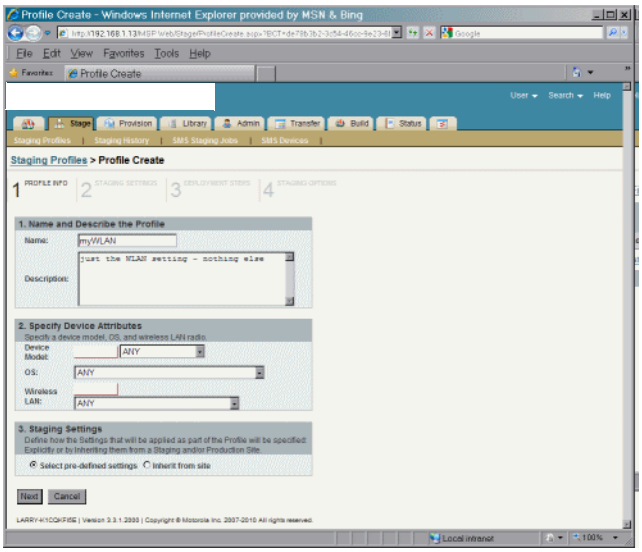


Figure A-9 *Profile Create Screen*

24. In the **1. Name and Describe the Profile** section, enter a name for the profile in the **Name** text box.
25. In the **description** text box, enter a description of the profile.
26. Profile Info page, enter a name for the new Staging Profile, and optionally enter a description.
27. In the **3. Staging Settings** section, select the **Select pre-defined settings** radio button.
28. Click the **Next** button.

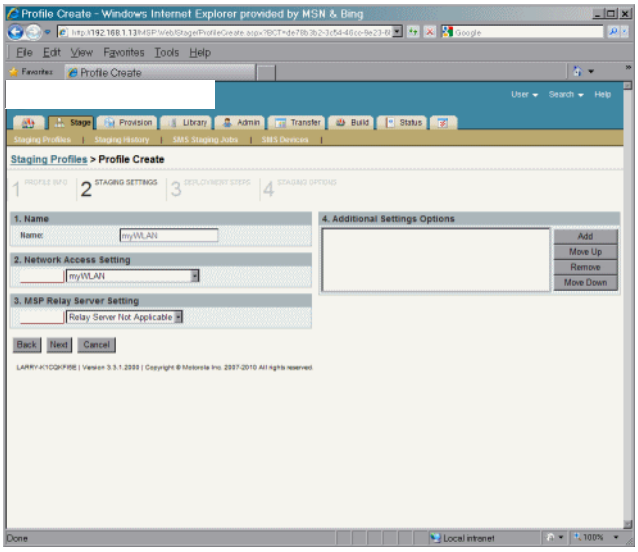


Figure A-10 *Profile Create - Staging Settings Screen*

29. In the **2. Network Access Setting** section, use the drop-down box to select the WLAN profile that just created. Do not select a Relay Server or make any other entries on this page.
30. Click the **Next** button.

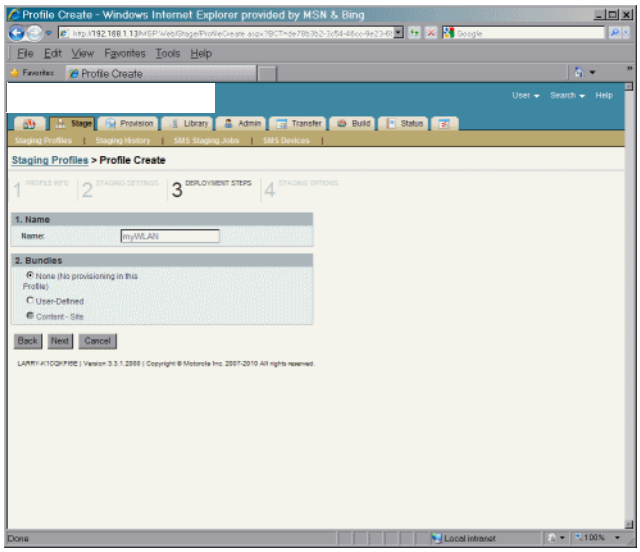


Figure A-11 *Profile Create - Deployment Steps Screen*

31. Click the **Next** button.

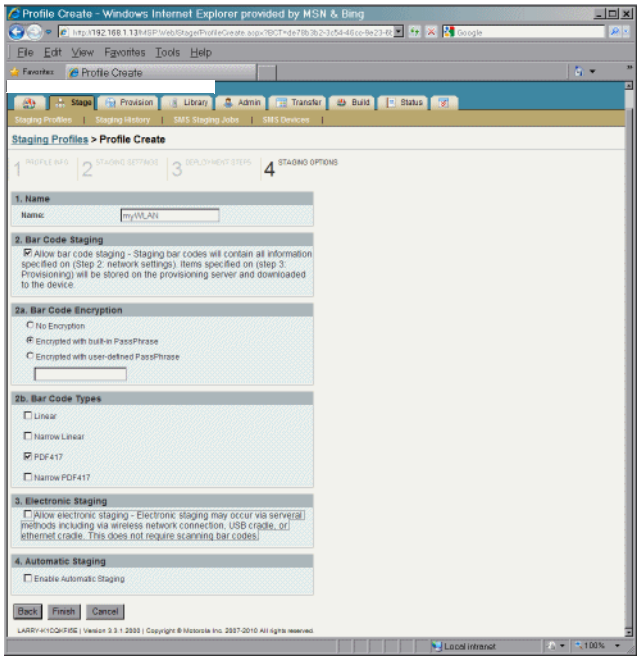


Figure A-12 *Profile Create - Staging Options Screen*

32. In **2b. Bar Code Types** section, deselect all checkboxes except for the **PDF417** checkbox.

33. In **3. Electronic Staging** section, uncheck **Allow Electronic Staging** checkbox.

34. Click the **Finish** button. The **Related Tasks** window appears.

35. Click **View List**. The new Staging Profile appears in the list.

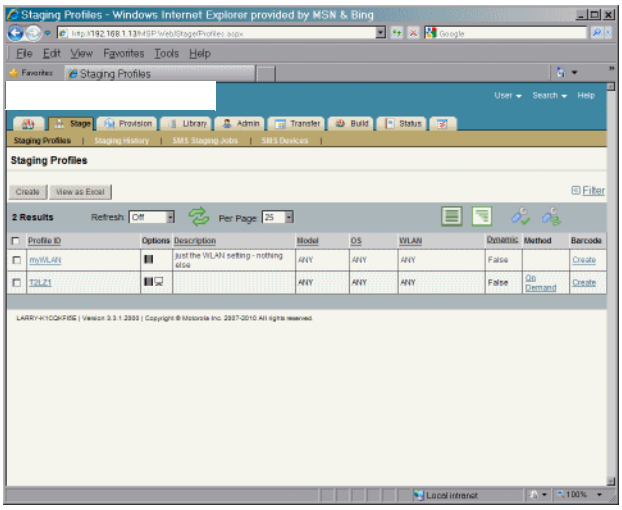


Figure A-13 *Staging Profiles Screen*

36. Click the **Create** link to generate the bar codes for this Staging Profile. The **Barcode Sheet Generation screen** appears.

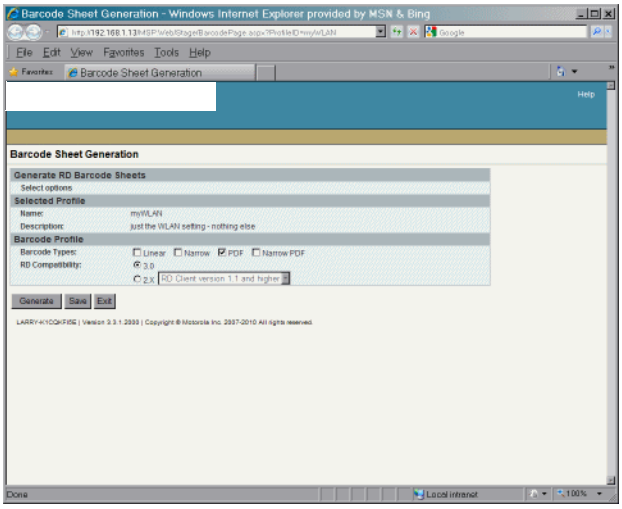


Figure A-14 *Barcode Sheet Generation Screen*

37. Click the **Generate** button. After a moment, a PDF document containing the Staging Profile bar code displays.

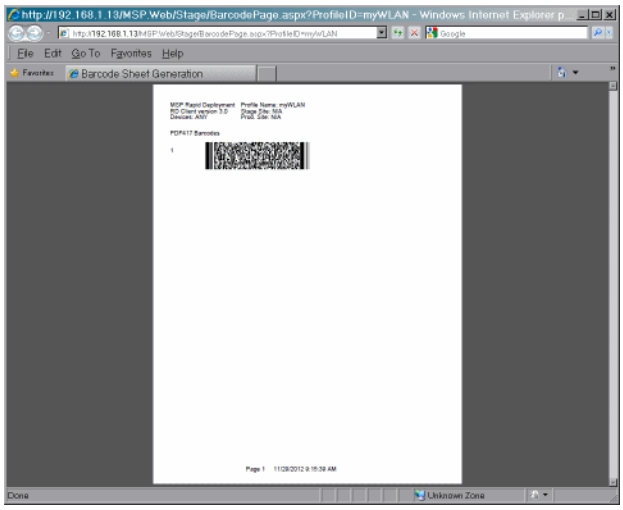


Figure A-15 *Barcode Sheet Screen*

38. Save the file to email or to print later, or send the file directly to a printer. Use the Adobe Reader controls to zoom in on the bar code.
39. On the SB1, press the Home button (if required).
40. Touch > > **Advanced Settings**. Enter password (if required).

    or

    Touch **Applications**.
41. Touch **RD Client**.
42. Touch **OK**. Wait for the **Waiting…** message to display.

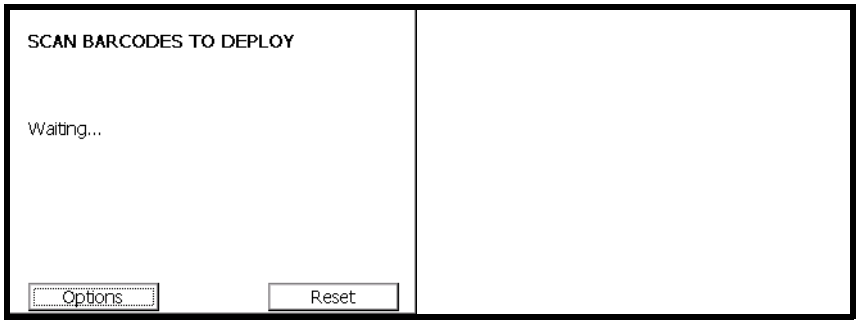


Figure A-16 *Scan Barcodes to Deploy Screen*

43. Press the Scan button and aim at the bar code. If trying to read the bar code from the screen and not paper, try to hold the SB1 a little above the perpendicular with the screen to avoid reflection.
44. The SB1 beeps and begins applying the WLAN settings.
45. When the message **Your Device is Ready To Use** displays, touch **OK**.

APPENDIX B STEP BY STEP CREATING PACKAGE EXAMPLE

Introduction

This appendix provides a step-by-step sample procedure for creating a package and deploying it to the SB1. Note that the information is an example and settings are dependent upon the package you are creating.

See *Appendix A, Step By Step WLAN Setup Example* example procedure for setting up the WLAN connection.

Procedure

This sample procedure provides instructions for creating a package, placing the package into a bundle, creating a staging profile to instruct the SB1 to download and install the bundle.

1. Connect to the MSP Server.

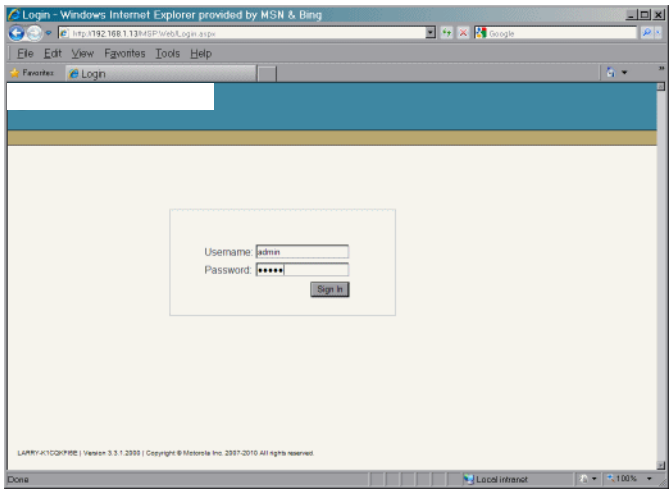


Figure B-1 *MSP Console*

2. Login using the username and password set up during MSP installation. After login the Start Page displays.

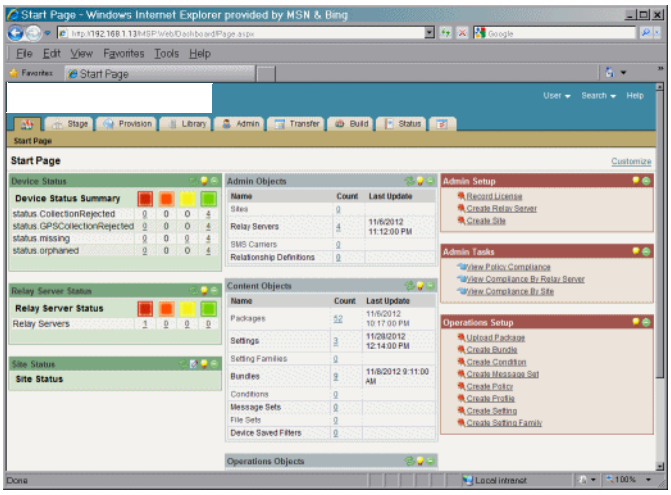


Figure B-2 *MSP Start Page*

3. Click the **Library** tab. This list shows all the package known to the MSP server, including the packages that come with MSP and any packages that have already been created.

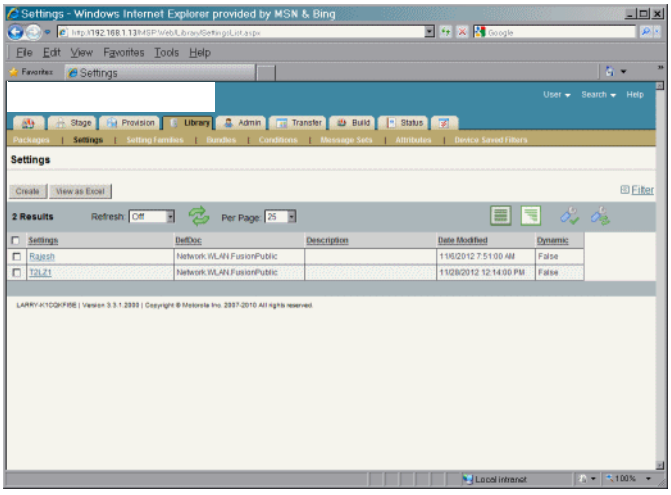


Figure B-3 *Library Tab Screen*

4. Click the **Build** tab. The **Build Tab** screen appears.

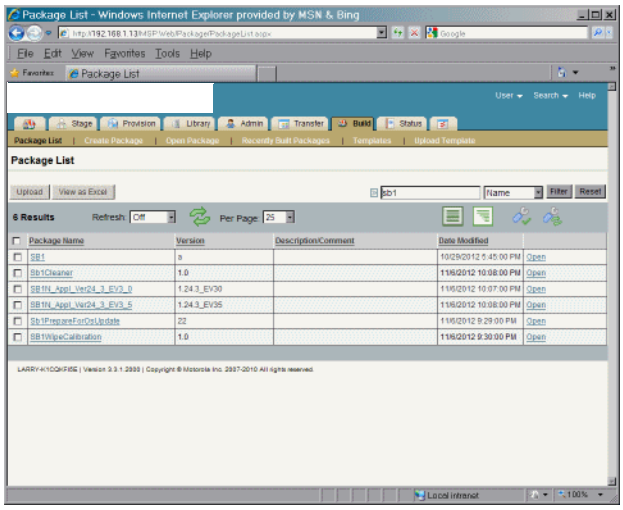


Figure B-4 *Build Tab Screen*

5. If needed, filter the list to list only SB1 packages.
6. Click **Create Package**. The **Package Info** screen appears.

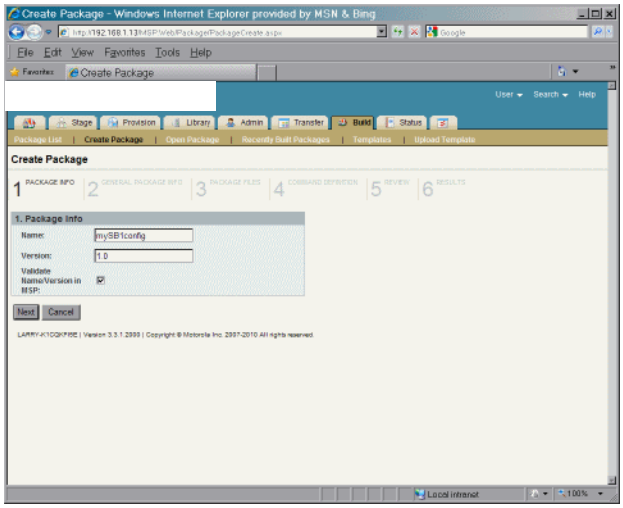


Figure B-5 *Create Package - Package Info Screen*

7. In the **Name** text box, enter a name for the package.
8. In the **Version** text box, enter a version number for the package.
9. Ensure that **Validate Name/Version** in MSP is checked.
10. Click **Next**. The **General Package Info** screen appears.

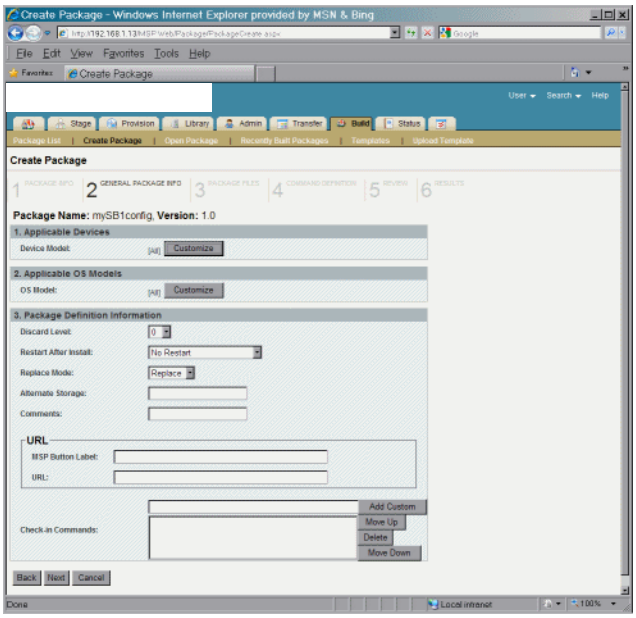


Figure B-6 *Create Package - General Package Info Screen*

11. Click **Next**. The **Package Files** screen appears.

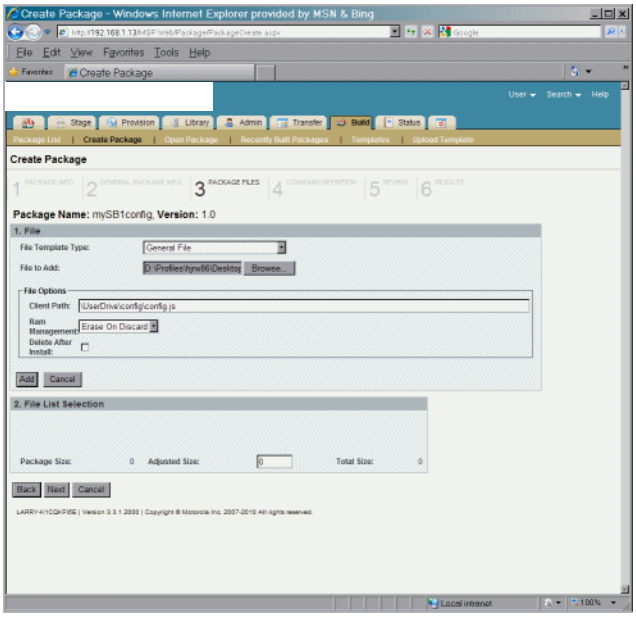


Figure B-7 *Create Package - Package Files Screen*

12. In the **File Template Type** drop-down list, select **General File**.
13. Click the **Browse** button next to **File to Add**.
14. In the **Choose File to Open** window, locate the first file to go into the package and then click **Open**.
15. In the **File Options** - **Client Path** text box, enter the full path name the file will load into on the SB1.

    For the SB1, all files should be deployed to the *\UserDrive* folder. Refer to the*SB1 Programmer's Guide* for specific information regarding folder structures.
16. Click the **Add** button to add the file to the package.

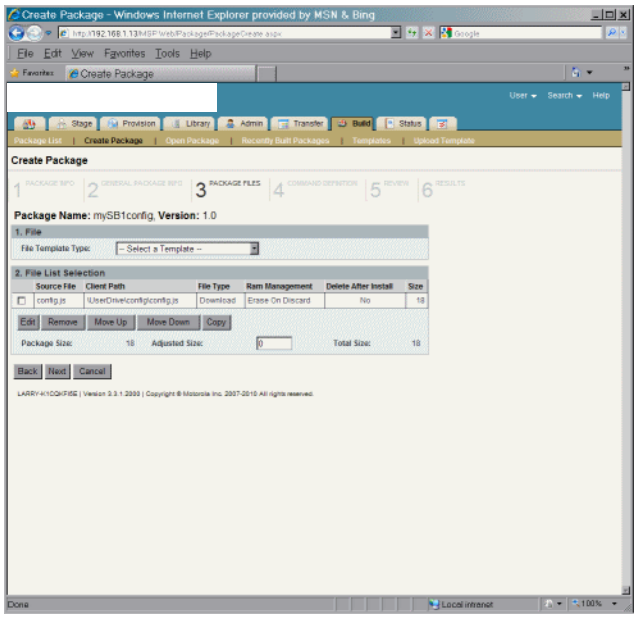


Figure B-8 *Create Package - Package Files Screen*

17. Repeat the process to add all the remaining files to the package.

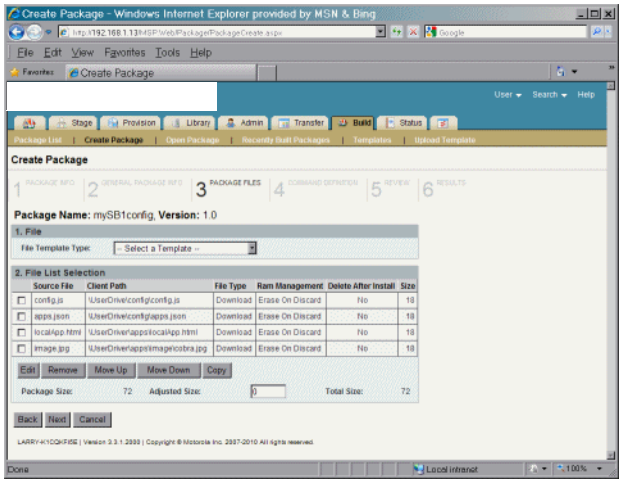


Figure B-9 *Create Package - Package Files Screen, Multiple Files in Package*

18. Click **Next**. The **Command Definition** screen appears.

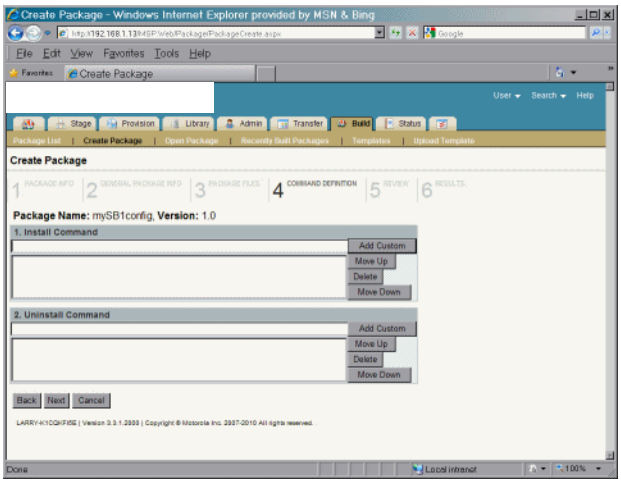


Figure B-10 *Create Profile - Command Definition Screen*

19. For this example, click **Next**. The **Review** screen appears.

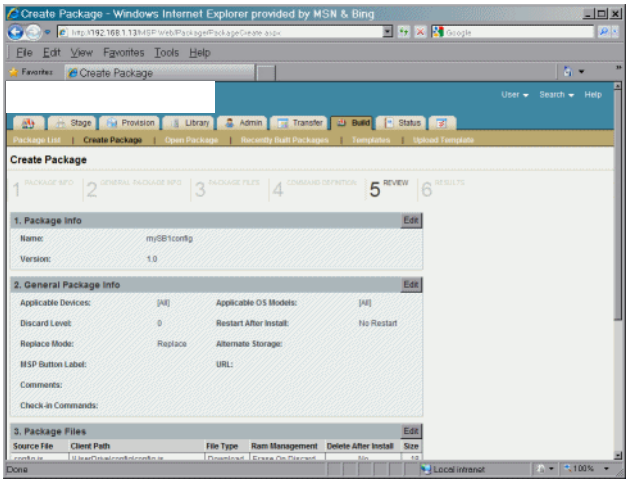


Figure B-11 *Create Package - Review Screen*

20. Scroll to the bottom of the screen.

21. Click the **Create Package** button to create the package.

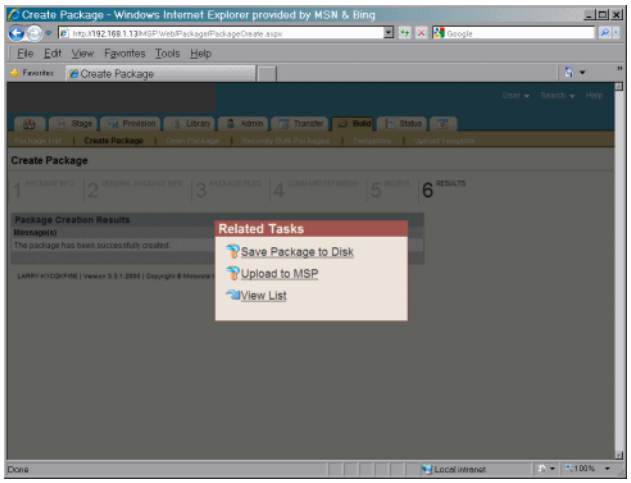


Figure B-12 *Related Tasks Screen*

22. Select **Save Package to Disk** to save the package as a .apf file or select **Upload to MSP** to upload the package to the MSP server. For this example, select **Upload to MSP**.

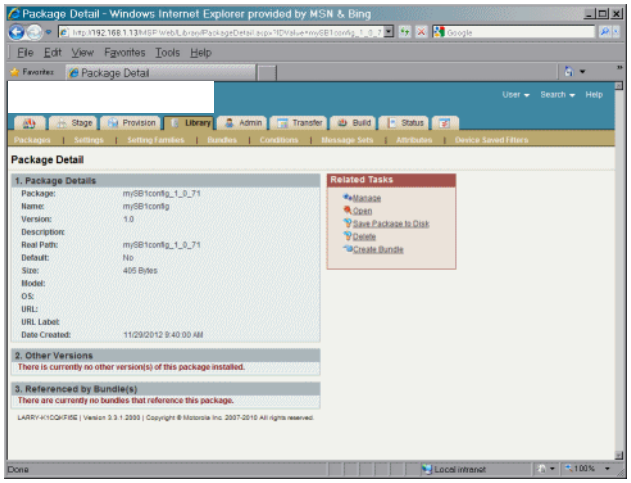


Figure B-13 *Package Details Screen*

23. The screen shows that the package has been uploaded to the MSP server. In the **related tasks** window, click **Create Bundle**. The **Bundle Create** screen appears.

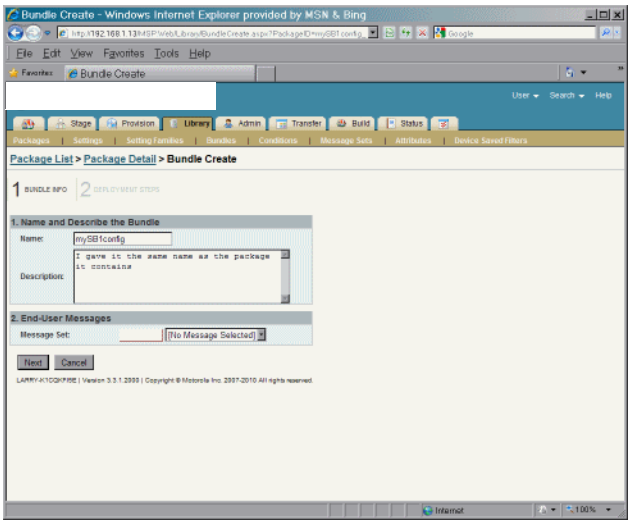


Figure B-14 *Create Bundle Screen*

24. In the **Name** text box, enter a name for the bundle.

25. In the **Description** text box, enter a description for the bundle.

26. Click the **Next** button. In this example, MSP has already created a bundle step to install the package.

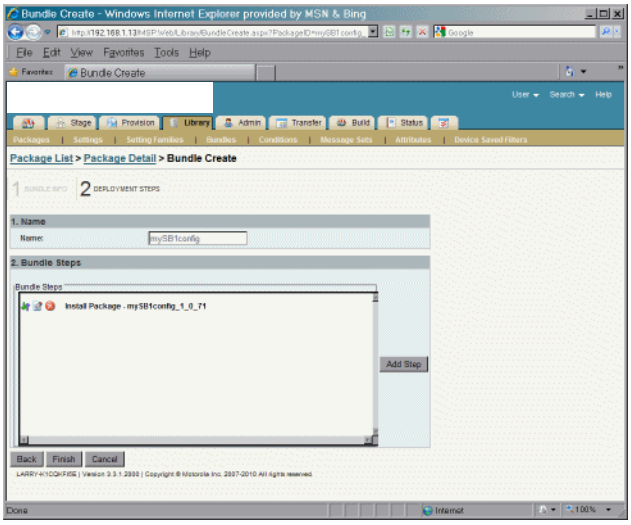


Figure B-15 *Bundle Create - Bundle Steps Screen*

27. Click **Finish**. The **Related Tasks** screen appears.

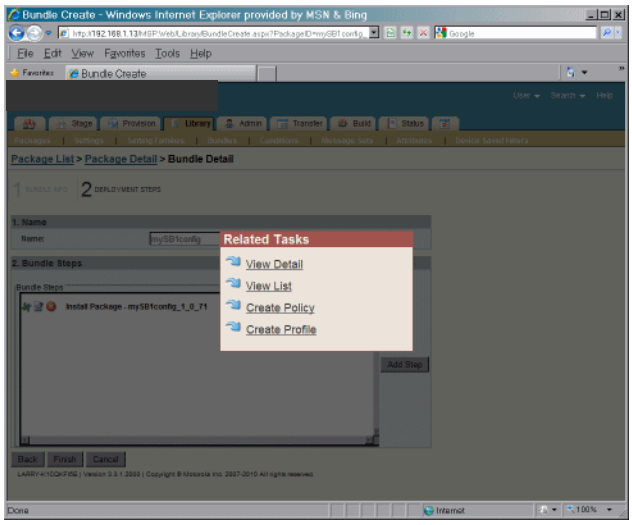


Figure B-16 *Related Tasks Screen*

28. Click **Create Profile**. The **Create Profile** screen appears.

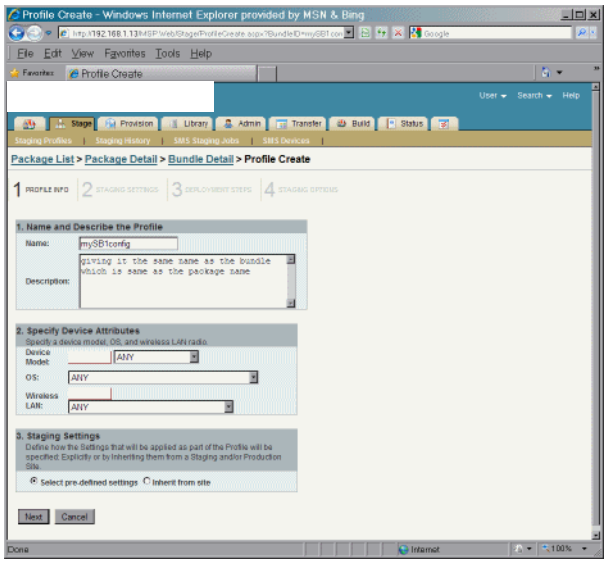


Figure B-17 *Create Profile Screen*

29. In the **Name** text box, enter a name for the profile.

30. In the **Description** text box, enter a description for the profile.

31. Ensure that the **Select pre-defined settings** radio button is selected.

32. Click the **Next** button. The **Staging Settings** screen appears.

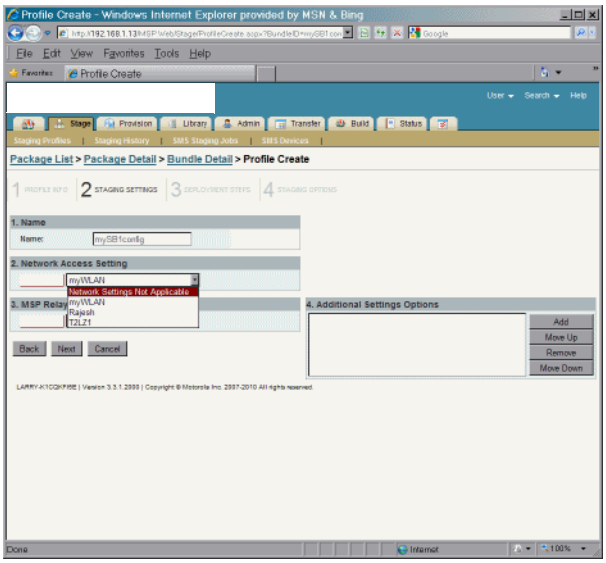


Figure B-18 *Create Profile - Staging Settings Screen*

33. Since the SB1 is already on a network (see Appendix A) it is not required to select a network option.

34. Specify a Relay Server. Refer to the MSP documentation for information on creating a Relay Server. At least one Relay Server is required to hold the content for deployment and must be reachable over the network by the SB1.

35. Click the **Next** button. The **Deployment Steps** screen appears.

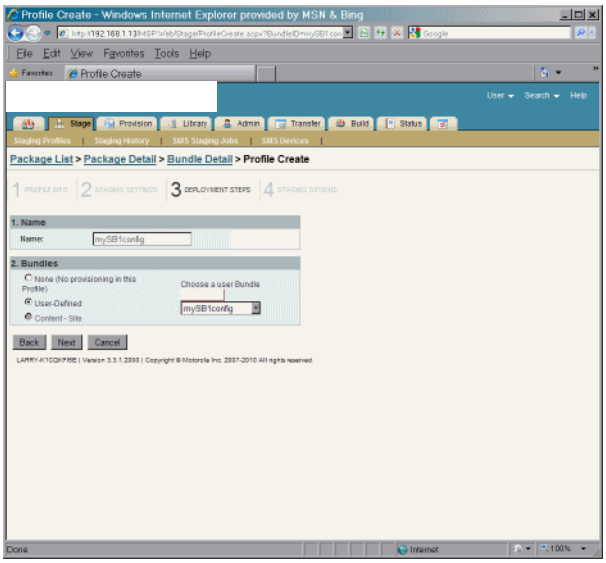


Figure B-19 *Create Profile - Deployment Steps Screen*

36. Click **Next**. The **Staging Options** screen appears.

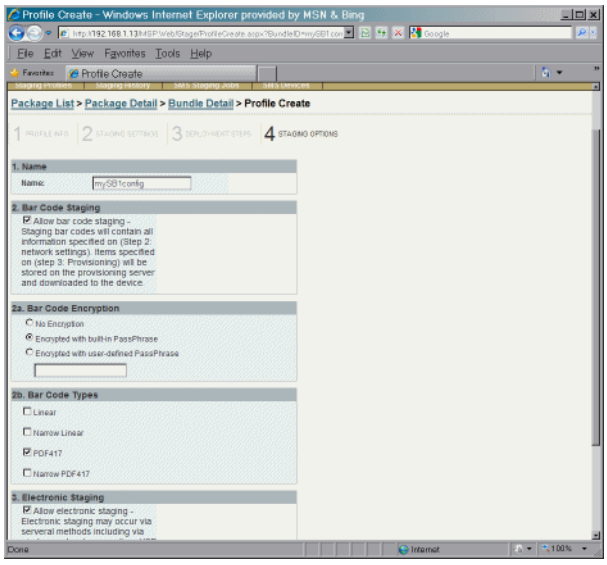


Figure B-20 *Create Profile - Staging Options Screen*

37. Uncheck the barcode type checkboxes.

38. Click **Finish**. The **related Tasks** screen appears.

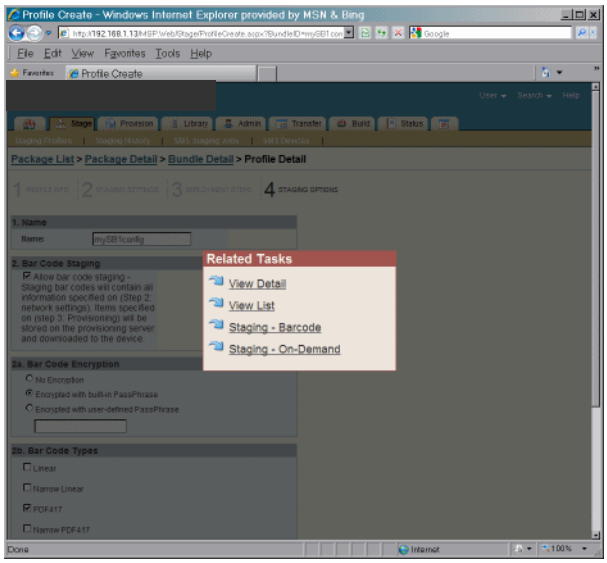


Figure B-21 *Related Tasks Screen*

39. Select **Staging - Barcode**. The **Barcode Sheet Generation** screen appears.

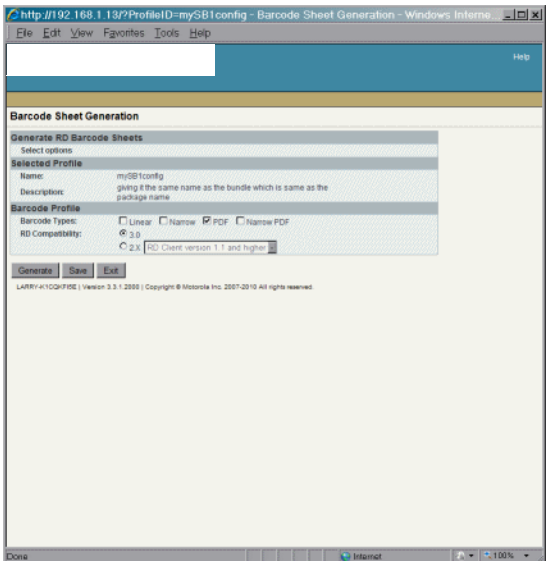


Figure B-22 *Barcode Sheet Generation Screen*

40. Click the **Generate** button. After a moment, a PDF document containing the Staging Profile bar code displays.

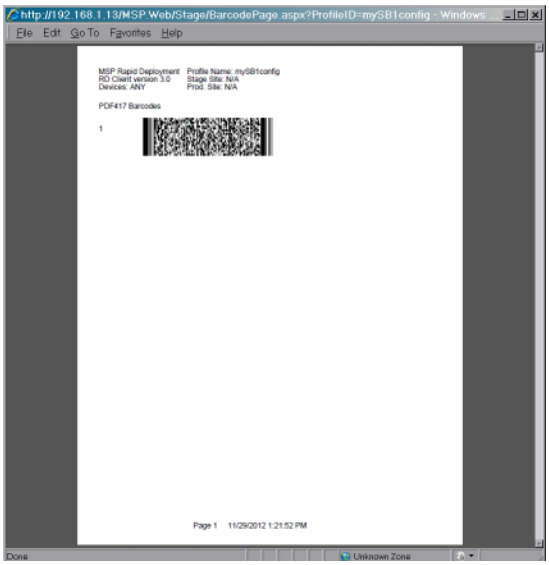


Figure B-23 *Barcode Sheet Screen*

41. Save the file to email or to print later, or send the file directly to a printer. Use the Adobe Reader controls to zoom in on the bar code.
42. On the SB1, press the Home button (if required).
43. Touch > > **Advanced Settings**. Enter password (if required).

    or

    Touch **Applications**.
44. Touch **RD Client**.
45. Touch **OK**. Wait for the **Waiting…** message to display.

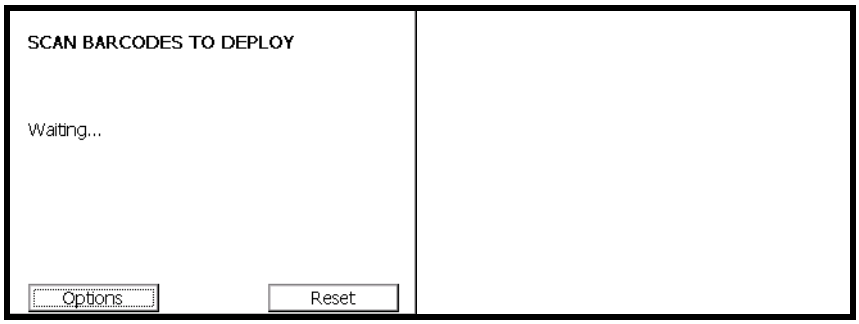


Figure B-24 *Scan Barcodes to Deploy Screen*

46. Press the Scan button and aim at the bar code. If trying to read the bar code from the screen and not paper, try to hold the SB1 a little above the perpendicular with the screen to avoid reflection.
47. The SB1 beeps and begins installing the bundle.
48. When the message **Your Device is Ready To Use** displays, touch **OK**.

APPENDIX C SPECIFICATIONS

SB1 and Accessory Technical Specifications

Table C-1 summarizes the SB1 technical specifications and intended operating environments.

Table C-1 *SB1 Technical Specifications*

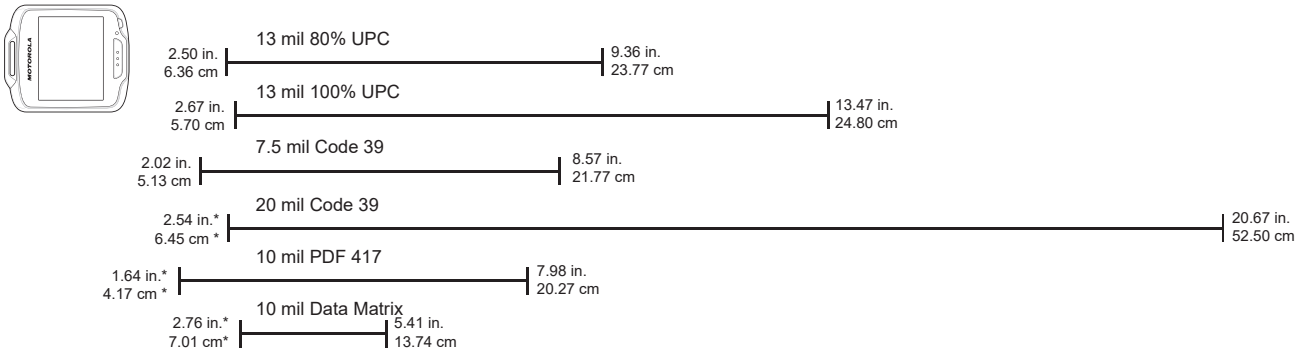
Item	Description
Physical Characteristics	
Dimensions	SB1-S: 92 mm L x 81 mm W x 14 mm D (3.62 in. L x 3.19 in. W x 0.55 in. D) SB1-IAS and SB1-HC: 92 mm L x 81 mm W x 24 mm D (3.62 in. L x 3.19 in. W x 0.94 in. D)
Weight	SB1-S: 110 g (3.88 oz.) SB1-IAS and SB1-HC: 124 g (4.4 oz.)
Display	3.0” E Ink Pearl, 4-bit grayscale (16 shades). QVGA 320 x 240 resolution.
Touch Panel	Full screen resistive touch; finger operation (no stylus)
Battery	Rechargeable Lithium-ion 910 mAh
Network Connections	Wireless Local Area Network (WLAN)
Notification	Audio: beeper; Visual: multi-color LED
Audio	SB1-S: Integrated microphone; accessories include optional Speaker Adapter with push-to-talk and Audio Adapter. SB1-IAS and SB1-HC: Integrated microphone, speaker, two PTT buttons and headset jack.

Table C-1 *SB1 Technical Specifications (Continued)*

Item	Description
Performance Characteristics	
CPU	IMX35 (532 MHz)
Applications	Supports thin client applications and HTML 5 with RhoElements extensions.
Memory	128 MB RAM/128 MB Flash
User Environment	
Operating Temperature	0 °C to 35 °C (32 °F to 95 °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 Specification	Multiple 1.22 m (4 ft) drop to tile over concrete per MIL STD 810G specifications
Electrostatic Discharge (ESD)	+/-15 kV air discharge +/- 8 kV direct discharge
Sealing	IP54
Wireless LAN Data and Voice Communications	
WLAN radio	Wi-Fi IEEE® 802.11b/g/n
Data Rates Supported	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps and MCS0-7
Operating Channels	Channel 1-13 (2412-2472 MHz), Channel 14 (2484 MHz) Japan only; actual operating channels/frequencies depend on regulatory rules and certification agency
Security	**Security Modes:** Legacy, WPA and WPA2 **Encryption:** WEP (40 or 128 bit), TKIP and AES **Authentication:** TLS, TTLS (MS-CHAP), TTLS (MS-CHAP v2), TTLS (CHAP), TTLS (MD5), TTLS (PAP), PEAP-TLS, PEAP (MS-CHAP v2), PEAP (EAP-GTC), EAP-FAST-TLS, EAP-FAST (MS-CHAP v2), EAP-FAST (EAP-GTC) and LEAP
Spreading Technique	Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency Division Multiplexing (OFDM)
Data Capture	
Bar Code Reader	Omni-directional bar code reader with integrated aiming and illumination.
Supported 1D Symbologies	UPC/EAN, Code 128, GS1-128, GS1-Databar, Code 39, Interleaved 2 of 5, Discrete 2 of 5, Codabar, Coupon Code, MSI, Code 93, Code 11.
Supported 2D Symbologies	DataMatrix, PDF417, QR Code, Aztec Code, MaxiCode, Composite Code, Postal codes.

Bar Code Reader Decode Zones

Figure C-1 shows the decode zone for the bar code reader. The figures are typical values. *Table C-2* lists the typical distances for selected bar code densities. The minimum element width (or “symbol density”) is the width in mils of the narrowest element (bar or space) in the symbol.



* Dependent upon bar code width

Figure C-1 *Bar Code Reader Decode Graph*

Table C-2 *Bar Code Reader Decode Distances*

Symbol Density/ Bar Code Type	Typical Working Ranges	
	Near	Far
13 mil 80% UPC	2.50 in 6.35 cm	9.36 in 23.77 cm
13 mil 100% UPC	2.67 in 5.70 cm	13.47 in 24.8 cm
7.5 mil Code 39	2.02 in 5.13 cm	8.57 in 21.77 cm
20 mil Code 39	2.54* in 6.45* cm	20.67 in 52.50 cm
10 mil PDF 417	1.64* in 4.17* cm	7.98 in 20.27 cm
10 mil Data Matrix	2.76* in 7.01* cm	5.41 in 13.74 cm

Notes:
1. Distances are measured from the edge of the SB1.
2. The distances marked with asterisk (*) are a result of the field of view (FOV) limitation and depend upon the bar code length.
3. 300 lux artificial ambient light.
4. Bar codes at 20° pitch.
5. Photographic quality short bar codes.
6. Reading of long and large code is limited by effective system resolution

Accessory Specifications

Single Slot Charging Cradle

Table C-3 *Single Slot Charging Cradle Technical Specifications*

Feature	Description
Dimensions	Height: 13.02 cm (5.13 in.) Width: 15.24 cm (6.0 in.) Depth: 15.24 cm (6.0 in.)
Input Power	5.4 VDC
Power Consumption	12 W
Operating Temperature	-25 °C to 50 °C (-13 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 35 °C (32 °F to 95 °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

Ten Slot Charge Only Cradle

Table C-4 *Ten Slot Charge Only Cradle Technical Specifications*

Feature	Description
Dimensions	Height: 10.16 cm (4.0 in.) Width: 48.77 cm (19.00 in.) Depth:15.24 cm (6.0 in.)
Input Power	12 VDC
Power Consumption	50 W
Operating Temperature	-25 °C to 50 °C (-13 °F to 122 °F)
Storage Temperature	-40 °C to 70 °C (-40 °F to 158 °F)
Charging Temperature	0 °C to 35 °C (32 °F to 95 °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

APPENDIX D CONFIGURATION

Log Backup

By default the SB1 saves a RhoElements log file (**`log.txt)`** in the **`\UserDrive`**. However, when the SB1 is rebooted, the log file is overwritten. The LogBackup utility makes a backup copy of the log file (named **`RELogBkup.txt`**). This is helpful for debugging SB1 RhoElements applications.

The required files are in the SB1 Toolbox. Download the SB1 Toolbox from the Zebra Support Web Site, http://www.zebra.com/support.

In the SB1 Toolbox, locate the **`LogBackup\UserDrive`** folder.

Copy the **`LogBkup.cpy`** file to the root of the **`\UserDrive`** on the SB1.

After the next reboot, a file with name **`RELogBkup.txt`** will be created from the previous running RhoElements activities (prior to reboot).

Extract the file from the SB1 when appropriate.

NOTE This utility is for debugging purpose only. Remove the file from the SB1 after debugging.

Reboot Service

The reboot service is a new performance feature, which allows the SB1 device to be automatically rebooted (cold boot) without the need of an external tool (e.g. MSP or another MDM). Experience has shown that all devices need to be rebooted periodically. When this service is configured, the SB1 will manage the reboot. The current control feature(s) include:

- Enable/Disable – controlled by the “Enabled” setting. Disabled by default.
- Running Time – running time is how long the SB1 will run before the next reboot. Running time starts from the last reboot. Controlled by the “Period” setting.

  When the running time elapses the SB1 schedules a reboot which will execute three minutes after the Sb1 is placed (and remains) in the cradle.

The required files are in the SB1 Toolbox. Download the SB1 Toolbox from the Zebra Support Web Site, http://www.zebra.com/support.

In the SB1 Toolbox, locate the **Reboot_Service\UserDrive** folder.

Using a text editor, open the **SB1_StandAlone_Reboot_Sample.reg** file.

Edit the registry keys:

[HKEY_LOCAL_MACHINE\Software\Motorola\Services\reboot]

"Enabled"=dword:1

where:

0 = disabled (default)

1 = enabled.

"Period"=”01-00-00”

where:

01-00-00 = Period of scheduled reboot in the format DD-HH-MM.

DD = days (0 to 30)
HH = hours (0 to 23)
MM = minutes (0 to 59).

For example, 1 day 12 Hours and 16 minutes should be entered as “01-12-16”.

Save the **SB1_StandAlone_Reboot_Sample.reg** file.

Copy the file to the root on the **\UserDrive** folder.

Reboot the SB1 to have the registry setting take effect.

SetTimeZone

The SetTimeZone feature configures the SB1 for a specific time zone. The default time zone (out-of-box) is GMT-8.

The required files are in the SB1 Toolbox. Download the SB1 Toolbox from the Zebra Support Web Site, http://www.zebra.com/support.

In the SB1 Toolbox, locate the **SetTimeZone-Setup** folder. Using a text editor, open the **SetDefaultTZ.reg** file.

The .reg file lists all the valid text strings for all time zones. Replace the default time zone (“Eastern Standard TIme”) with the desired time zone. Save the file.

Copy the following files from the **SetTimeZone-SetUp** folder to the root of **\UserDrive**:

- SetTimeZoneById.exe
- SetTimeZoneById.cpy
- SetTimeZoneById.lnk
- SetTimeZoneById.reg

Cold boot the SB1 for changes to take effect. The Time Zone setting will be set to the new value.

Display Full Update Interval

Display Full Update Interval feature defines how often the display driver will perform a full refresh of the E-ink display. A full refresh of the display sets all the bits to black then white and then renders the screen. The purpose is to clear the screen of unwanted display artifacts left over from previously drawn graphic images. These artifacts are called ghosted images.

If the developer feels that they are seeing too much ghosting on the screen then they can set the FullUpdateInterval to 1. This will cause the display to perform more full screen refreshes providing less ghosting at the expense of speed and power consumption. If they can live with some minor ghosting then they can relax the value (increase it) to improve speed and reduce power consumption.

The required files are in the SB1 Toolbox. Download the SB1 Toolbox from the Zebra Support Web Site, http://www.zebra.com/support.

In the SB1 Toolbox, locate the **`Specific Registries Configuration\UserDrive`** folder. Using a text editor, open the **`Display_Full_Update_Interval.reg`** file.

Edit the registry key:

[HKEY_LOCAL_MACHINE\Drivers\Display\DDIPU]

"FullUpdateInterval"=dword:2

where:

1 = perform a full refresh on every 3/4 screen redraws

2 = perform a full refresh on every other screen redraw

3 = perform a full refresh on every third screen redraw

Save the **`Display_Full_Update_Interval.reg`** file. Copy the file to the root of **`\UserDrive.`**

Reboot the SB1 to have the registry setting take effect.

Enable or Disable Rotation

SB1 screen will rotate when the SB1 is rotated. This feature can be changed so that applications can control rotation.

The required files are in the SB1 Toolbox. Download the SB1 Toolbox from the Zebra Support Web Site, http://www.zebra.com/support.

In the SB1 Toolbox, locate the **`Specific Registries Configuration\UserDrive`** folder. Using a text editor, open the **`Enable_Rotation.reg`** file.

Edit the registry key:

[HKEY_LOCAL_MACHINE\Drivers\BuiltIn\IST\Settings]Rotation

"Enabled"=dword:1

where:

0 = application rotates the screen

1 = SB1 IST driver rotates the screen (default).

Save the **`Enable_Rotation.reg`** file. Copy the file to the root of **`\UserDrive.`**

Reboot the SB1 to have the registry setting take effect.

Timeout for Rotation

The time between rotation from normal orientation to badge orientation can be controlled by changing this registry. Default value is 5 seconds. Note that this timeout value has no effect on the time between badge orientation to badge screen (which is controlled by the SB1 Shell. Refer to the SB1 Programmer's Guide for more information. Also when the device orientation changes from badge back to normal, the rotation shall be immediate.

Note: This is not a dynamically configurable parameter. A cold boot with the appropriate registry key in the root folder of UserDrive is required for the respective change to come into effect.

The required files are in the SB1 Toolbox. Download the SB1 Toolbox from the Zebra Support Web Site, http://www.zebra.com/support.

In the SB1 Toolbox, locate the **`Specific Registries Configuration\UserDrive`** folder. Using a text editor, open the **`Enable_Rotation.reg`** file.

Edit the registry key:

[HKEY_LOCAL_MACHINE\Drivers\BuiltIn\IST\Settings]Rotation

"Enabled"=dword:1

where:

0 = rotation to be handled by application

1 = IST driver rotates the screen (default).

Save the **`Enable_Rotation.reg`** file. Copy the file to the root of **`\UserDrive.`**

Reboot the SB1 to have the registry setting take effect.

INDEX

L

M

P

Q

R

S

T

U

W

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

72E-164712-04 Revision A - May 2019