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

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

Zebra reserves the right to make changes to any software or product to improve reliability, function, or design.

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

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

---

**Warranty**

For the complete Zebra hardware product warranty statement, go to:


---

**Revision History**

Changes to the original manual are listed below:

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-01 Rev A</td>
<td>10/2006</td>
<td>Initial Release</td>
</tr>
<tr>
<td></td>
<td>1/2008</td>
<td>Added External Antenna&lt;br&gt;Software Update Version 1.1&lt;br&gt;Updated Chapter 5, Wireless Applications&lt;br&gt;Added new Demo Application in Chapter 7&lt;br&gt;Replaced Chapter 8, Bluetooth Setup</td>
</tr>
<tr>
<td>-02 Rev A</td>
<td>5/2016</td>
<td>Rebranding</td>
</tr>
</tbody>
</table>
# Table of Contents

Warranty ............................................................................................................................................... ii  
Revision History ................................................................................................................................... ii  

**About This Guide**  
Introduction ........................................................................................................................................... xi  
  - Documentation Set .......................................................................................................................... xi  
Configurations....................................................................................................................................... xii  
Chapter Descriptions ............................................................................................................................ xiii  
  - Notational Conventions......................................................................................................................... xiii  
Related Documents and Software ........................................................................................................ xiv  
Service Information ............................................................................................................................... xiv  
  - Support Information .......................................................................................................................... xiv  

**Chapter 1: Getting Started**  
Introduction ........................................................................................................................................... 1-1  
Unpacking the Reader ........................................................................................................................... 1-1  
Connections and Ports ......................................................................................................................... 1-2  
Accessories ....................................................................................................................................... 1-4  
Getting Started .................................................................................................................................... 1-4  
Installing and Removing the Battery ................................................................................................. 1-5  
  - Installing the Battery ......................................................................................................................... 1-5  
  - Removing/Replacing the Main Battery .............................................................................................. 1-6  
Charging the Battery ............................................................................................................................. 1-7  
  - Charging the Main Battery and Memory Backup Battery ............................................................... 1-7  
  - Charging the Battery ......................................................................................................................... 1-7  
  - Serial Communications ...................................................................................................................... 1-8  
Charging Spare Batteries .................................................................................................................... 1-9  
Connect a USB Cable ............................................................................................................................ 1-10  
Connect an External Antenna .............................................................................................................. 1-11  
Starting the Reader .............................................................................................................................. 1-13  
  - Host Computer Display Setup ........................................................................................................... 1-13  
Checking Battery Status ..................................................................................................................... 1-13  
Battery Management ............................................................................................................................ 1-13
Chapter 2: Installation

Introduction .................................................................................................................. 2-1
RD5000 Installation ........................................................................................................... 2-1
  Mounting Location ........................................................................................................... 2-2
  Installing The Mounting Brackets .................................................................................. 2-2
  Installing The Shock Isolators on The Mounting Brackets ........................................... 2-6
  Locally Fabricated Mounting Platform ........................................................................... 2-7
    Mounting Platform Fabrication .................................................................................... 2-7
  Installing The Shock Isolators on The Locally Fabricated Mounting Platform .............. 2-8
  Mounting The Reader .................................................................................................... 2-9
    Mounting on The Mounting Brackets ......................................................................... 2-9
  External Antenna Installation .......................................................................................... 2-12

Chapter 3: Accessories

Introduction .................................................................................................................. 3-1
Power Supply .................................................................................................................. 3-2
Battery ............................................................................................................................. 3-2
Four Slot Spare Battery Charger ...................................................................................... 3-3
  Setup .............................................................................................................................. 3-3
  Spare Battery Charging with the Four Slot Spare Battery Charger ................................ 3-4
  Battery Charging Indicators ......................................................................................... 3-4
Universal Battery Charger (UBC) Adapter ........................................................................ 3-5
  Inserting and Removing a Battery ............................................................................... 3-5
  Setup .............................................................................................................................. 3-6
  Battery Charging Indicators ......................................................................................... 3-6
Charging Cable ............................................................................................................... 3-7
Charging Cable With Serial Communications .................................................................. 3-8
USB Communications Cable ........................................................................................... 3-9
  USB Connection Setup (Windows CE 5.0) ................................................................... 3-9
  USB Connection Setup (Windows CE 5.0) ................................................................... 3-10
External Antenna ............................................................................................................ 3-11

Chapter 4: ActiveSync

Introduction .................................................................................................................... 4-1
Installing ActiveSync ....................................................................................................... 4-1
Connect the RD5000 USB Communications Cable .......................................................... 4-2
Setting Up an ActiveSync Connection (with no Partnership) on the Host Computer ........ 4-2
  Setting up a Partnership ............................................................................................... 4-6
RFID Reader Setup ......................................................................................................... 4-11
  USB Connection Setup (Windows CE 5.0) .................................................................. 4-11
Chapter 5: Wireless Applications

Introduction .............................................................................................................................. 5-1
Signal Strength Icon ............................................................................................................. 5-2
Turning the WLAN Radio On and Off .............................................................................. 5-3
  Windows CE 5.0 with Fusion 2.4 and Higher ................................................................. 5-3
Find WLANs Application ................................................................................................... 5-4
Profile Editor Wizard ........................................................................................................... 5-5
  Profile ID ........................................................................................................................... 5-5
  Operating Mode ................................................................................................................ 5-6
  Ad-Hoc ............................................................................................................................. 5-8
Authentication ..................................................................................................................... 5-9
  Tunneled Authentication ................................................................................................. 5-9
User Certificate Selection .................................................................................................. 5-11
  User Certificate Installation ............................................................................................ 5-11
Server Certificate Selection .............................................................................................. 5-12
Credential Cache Options ................................................................................................. 5-13
  User Name ....................................................................................................................... 5-15
  Password ....................................................................................................................... 5-15
Advanced Identity ............................................................................................................. 5-16
Encryption ......................................................................................................................... 5-16
  Key Entry Page ............................................................................................................... 5-18
  Passkey Dialog ............................................................................................................... 5-18
IP Address Entry ............................................................................................................... 5-19
Transmit Power .................................................................................................................. 5-21
Battery Usage ..................................................................................................................... 5-22
Manage Profiles Application ............................................................................................. 5-22
  Changing Profiles .......................................................................................................... 5-23
  Editing a Profile .............................................................................................................. 5-24
  Creating a New Profile ................................................................................................. 5-24
  Deleting a Profile .......................................................................................................... 5-24
  Ordering Profiles .......................................................................................................... 5-25
  Export a Profile .............................................................................................................. 5-25
Wireless Status Application ............................................................................................... 5-25
  Signal Strength Window ............................................................................................... 5-26
  Current Profile Window ................................................................................................. 5-27
  I Pv4 Status Window .................................................................................................... 5-28
  Wireless Log Window .................................................................................................. 5-30
    Saving a Log ................................................................................................................. 5-30
    Clearing the Log .......................................................................................................... 5-30
  Versions Window .......................................................................................................... 5-30
Wireless Diagnostics Application ...................................................................................... 5-31
  ICMP Ping Window ....................................................................................................... 5-32
  Trace Route Window .................................................................................................... 5-33
  Known APs Window ...................................................................................................... 5-33
Options ............................................................................................................................... 5-34
  Operating Mode Filtering .............................................................................................. 5-34
  Regulatory Options ....................................................................................................... 5-35
  Band Selection ............................................................................................................. 5-36
  System Options ............................................................................................................ 5-36
  Change Password ........................................................................................................ 5-37
Chapter 6: Application Deployment for WinCE 5.0

Software Installation on Development PC ................................................................. 6-1
Required System Configurations ............................................................................ 6-2
DCP for RD5000 ........................................................................................................ 6-2
To install the DCP for RD5000: .............................................................................. 6-3
Components .............................................................................................................. 6-3
Platform SDK ............................................................................................................ 6-4
Symbol Mobility Developer Kits .............................................................................. 6-5
SMDK for C Contents and Locations ........................................................................ 6-6
SMDK Patch for RD5000 .......................................................................................... 6-6
Installing Other Development Software ................................................................. 6-6
Software Updates ..................................................................................................... 6-6
Deployment ............................................................................................................... 6-7
ActiveSync ................................................................................................................ 6-7
Adding Programs ...................................................................................................... 6-9
Adding a Program from the Internet ........................................................................ 6-9
Creating Hex Images ................................................................................................. 6-10
Starting Terminal Configuration Manager .............................................................. 6-11
Defining Script Properties ....................................................................................... 6-13
Creating The Script For The Hex Image ................................................................. 6-14
Opening a New or Existing Script .......................................................................... 6-14
Copying Components to the Script ....................................................................... 6-15
Saving the Script .................................................................................................... 6-15
Building the Image .................................................................................................. 6-15
Downloading Partitions to the RFID Reader ......................................................... 6-16
Software Upgrade Using The OSUpdate Utility ..................................................... 6-16
Flash Storage .......................................................................................................... 6-17
FFS Partitions .......................................................................................................... 6-17
Working with FFS Partitions ................................................................................. 6-17
RegMerge.dll ......................................................................................................... 6-17
CopyFiles ............................................................................................................... 6-18
Non-FFS Partitions ................................................................................................. 6-18
AirBEAM Smart ...................................................................................................... 6-19
AirBEAM Package Builder ...................................................................................... 6-19
AirBEAM Smart Client .......................................................................................... 6-19
AirBEAM License .................................................................................................... 6-20
Configuring the AirBEAM Smart Client ............................................................... 6-20
Packages(1) Tab .................................................................................................... 6-20
Packages(2) Tab .................................................................................................... 6-21
Server Tab ................................................................................................................ 6-21
Misc(1) Tab ............................................................................................................. 6-22
Misc(2) Tab ............................................................................................................. 6-23
## Chapter 7: RFID Applications

**Introduction** ..................................................................................................................  7-1

- **RFIDSocketBridge** ........................................................................................................  7-2
  - **Registry File** ...............................................................................................................  7-2

**RFIDDemo Application** ......................................................................................................  7-3

- **Using RFIDDemo to Read Tags From a Remote Reader** ..................................................  7-3
- **Using RFIDDemo to Forward/Log Tags to Remote Device** ..............................................  7-4

**Launching the RFIDDemo Application** ..............................................................................  7-5

- **File Menu Options** ........................................................................................................  7-6
  - **About** ..........................................................................................................................  7-6
  - **Device Settings** ..........................................................................................................  7-7
    - **Reader Device Settings:** ............................................................................................  7-7
    - **Tag Logging** .............................................................................................................  7-7
    - **Registry Settings Description** ..................................................................................  7-8
  - **MPS Settings** ..............................................................................................................  7-12
    - **Reader MPS Settings:** ..............................................................................................  7-12
  - **Proximity Initiated Tag Read** .......................................................................................  7-13
  - **Motion Initiated Tag Read** ..........................................................................................  7-13
  - **Tag Access Parameters** ..............................................................................................  7-14
  - **Reader Settings:** ........................................................................................................  7-14
  - **Program Tag** ..............................................................................................................  7-16
    - **Reader Program Tag Settings:** ................................................................................  7-16
  - **Lock Options** .............................................................................................................  7-18
    - **Reader Lock Option Settings:** ...............................................................................  7-18
    - **Tag Locking** ............................................................................................................  7-19
  - **Read Tags** ..................................................................................................................  7-21

**Test Applications and Utilities** ..........................................................................................  7-22

- **AtmelFlasher Utility** ......................................................................................................  7-26

**Launching the GeminiRFID Demo Application** ..................................................................  7-28

- **Reading Tags** ..............................................................................................................  7-29
- **Selecting Tags** .............................................................................................................  7-30
- **Clearing the Display** ....................................................................................................  7-30
- **Saving Tag Data** ..........................................................................................................  7-31

**File Menu** ..........................................................................................................................  7-31

- **About** ..........................................................................................................................  7-32
- **Log** ...............................................................................................................................  7-32
- **Reboot** ........................................................................................................................  7-32
- **Settings** .......................................................................................................................  7-33
- **Gen2 Operational Settings** ...........................................................................................  7-34
- **Exit** ..............................................................................................................................  7-34
Chapter 8: Bluetooth Setup

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>8-1</td>
</tr>
<tr>
<td>Adaptive Frequency Hopping</td>
<td>8-2</td>
</tr>
<tr>
<td>Security</td>
<td>8-2</td>
</tr>
<tr>
<td>Turning the Bluetooth Radio Mode On and Off</td>
<td>8-3</td>
</tr>
<tr>
<td>Disable Bluetooth</td>
<td>8-3</td>
</tr>
<tr>
<td>Enable Bluetooth</td>
<td>8-3</td>
</tr>
<tr>
<td>Bluetooth Power States</td>
<td>8-4</td>
</tr>
<tr>
<td>Cold Boot</td>
<td>8-4</td>
</tr>
<tr>
<td>Warm Boot</td>
<td>8-4</td>
</tr>
<tr>
<td>Suspend</td>
<td>8-4</td>
</tr>
<tr>
<td>Bluetooth Profiles</td>
<td>8-5</td>
</tr>
<tr>
<td>Modes</td>
<td>8-6</td>
</tr>
<tr>
<td>Wizard Mode</td>
<td>8-6</td>
</tr>
<tr>
<td>Explorer Mode</td>
<td>8-9</td>
</tr>
<tr>
<td>Discovering Bluetooth Device(s)</td>
<td>8-10</td>
</tr>
<tr>
<td>Bonding with DISCOVERED Device(s)</td>
<td>8-11</td>
</tr>
<tr>
<td>Renaming a Bonded Device</td>
<td>8-12</td>
</tr>
<tr>
<td>Deleting a Bonded Device</td>
<td>8-13</td>
</tr>
<tr>
<td>Accepting a Bond</td>
<td>8-14</td>
</tr>
<tr>
<td>Discovering Services</td>
<td>8-15</td>
</tr>
<tr>
<td>File Transfer Services</td>
<td>8-16</td>
</tr>
<tr>
<td>Connect to Internet Using Access Point</td>
<td>8-17</td>
</tr>
<tr>
<td>OBEX Object Push Services</td>
<td>8-18</td>
</tr>
<tr>
<td>Send a Picture</td>
<td>8-18</td>
</tr>
<tr>
<td>Headset Services</td>
<td>8-19</td>
</tr>
<tr>
<td>Serial Port Services</td>
<td>8-20</td>
</tr>
<tr>
<td>Personal Area Network Services</td>
<td>8-20</td>
</tr>
<tr>
<td>Bluetooth Settings</td>
<td>8-21</td>
</tr>
<tr>
<td>Device Info Tab</td>
<td>8-21</td>
</tr>
<tr>
<td>Services Tab</td>
<td>8-22</td>
</tr>
<tr>
<td>Dial-Up Networking Service</td>
<td>8-22</td>
</tr>
<tr>
<td>File Transfer Service</td>
<td>8-23</td>
</tr>
<tr>
<td>OBEX Object Push Service</td>
<td>8-24</td>
</tr>
<tr>
<td>Personal Area Networking Service</td>
<td>8-24</td>
</tr>
<tr>
<td>Serial Port Service</td>
<td>8-25</td>
</tr>
<tr>
<td>Headset Service</td>
<td>8-25</td>
</tr>
<tr>
<td>Security Tab</td>
<td>8-26</td>
</tr>
<tr>
<td>Discovery Tab</td>
<td>8-27</td>
</tr>
</tbody>
</table>
Table of Contents

Virtual COM Port Tab ..................................................................................................................... 8-28
Miscellaneous Tab ......................................................................................................................... 8-29
Tag Logging Setup Using RFID Demo Example .............................................................................. 8-30

Chapter 9: Maintenance & Troubleshooting
Introduction ........................................................................................................................................ 9-1
Maintaining the RFID reader ........................................................................................................... 9-1
Battery Safety Guidelines .............................................................................................................. 9-1
Troubleshooting ............................................................................................................................ 9-2
  RFID Reader ................................................................................................................................. 9-2
  Bluetooth Connection .................................................................................................................. 9-4
  Four Slot Spare Battery Charger ............................................................................................... 9-4

Appendix A: Technical Specifications
Technical Specifications .................................................................................................................. A-1
  RFID Reader ................................................................................................................................ A-1

Appendix B: Motion Sensor Parameters
Introduction ....................................................................................................................................... B-1
API Calls ........................................................................................................................................ B-1
Possible Extensions ......................................................................................................................... B-2
Parameter Details ............................................................................................................................ B-3

Index
About This Guide

Introduction

This guide provides information about setting up and configuring RD5000 RFID reader and accessories.

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

Documentation Set

The documentation set for the RD5000 RFID reader is divided into guides that provide information for specific user needs.

- **Microsoft Application Guide** - describes how to use Microsoft developed applications.
- **Symbol Application Guide** - describes how to use Zebra developed applications.
- **RD5000 Quick Reference Guide (QRG)** - describes how to use the RD5000 RFID reader and provides the regulatory information.
- **RD5000 Integrator Guide** - describes how to set up the RD5000 RFID reader and the accessories.
- **SMDK Help File** - provides API information for writing applications.
The RD5000 User Guide information is presented in the Quick Start Guide.

## Configurations

This guide covers the following configurations:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Radios</th>
<th>Memory</th>
<th>Data Capture</th>
<th>Operating System</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>RD5000</td>
<td>WLAN: 802.11a/b/g</td>
<td>64 MB RAM</td>
<td>RFID</td>
<td>Windows CE 5.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WPAN: Bluetooth</td>
<td>64 MB Flash</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter Descriptions

Topics covered in this guide are as follows:

- **Chapter 1, Getting Started**, provides information on charging the RFID reader battery and resetting.
- **Chapter 2, Installation**, provides information on installing and setting up the reader.
- **Chapter 3, Accessories**, describes the accessories available for the RFID reader and how to set up power connections and battery charging capabilities, where applicable.
- **Chapter 4, ActiveSync**, provides instructions on installing ActiveSync and setting up a partnership between the RFID reader and a host computer.
- **Chapter 5, Wireless Applications**, provides instructions using and configuring the reader on a wireless network.
- **Chapter 6, Application Deployment for WinCE 5.0**, describes the application deployment for WinCE 5.0.
- **Chapter 7, RFID Applications**, describes RFID applications, and procedures for deploying applications.
- **Chapter 8, Bluetooth Setup**, describes Bluetooth setup procedures and features.
- **Chapter 9, Maintenance & Troubleshooting**, includes instructions on cleaning and storing the RFID reader, and provides troubleshooting solutions for potential problems during RFID reader operation.
- **Chapter A, Technical Specifications**, includes the technical specifications for the RFID reader.
- **Chapter B, Motion Sensor Parameters**, describes the Motion/Proximity sensor setting for the RFID reader.

Notational Conventions

The following conventions are used in this document:

- "RFID Reader", "reader" or "mobile computer" refers to the Zebra RD5000 RFID reader.
- *Italics* are used to highlight the following:
  - Chapters and sections in this guide
  - Related documents and links
- **Bold** text is used to highlight the following:
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.
Related Documents and Software

The following documents provide more information about the RD5000 RFID reader.

- **RD5000 Quick Reference Guide**, p/n 72-89955-xx
- **RD5000 Integrator Guide**, p/n 72-89956-xx
- **Symbol Application Guide for Symbol Devices**, p/n 72E-68901-xx
- **Microsoft Applications for Mobile and WinCE 5.0 User Guide**, p/n 72E-78456-xx
- **Symbol Mobility Developer Kit (SMDK) Help File**, p/n 72E-38880-03
- **Symbol Mobility Developer Kits**, available at: [http://support.symbol.com](http://support.symbol.com)
- **RD5000 RFID Reader DCP Update**, available at: [http://support.symbol.com](http://support.symbol.com).
- **Device Configuration Package and Platform SDK for 9090c50 (for RD5000 with Windows CE 5.0)**, available at: [http://support.symbol.com](http://support.symbol.com).

For the latest version of this guide and all guides, go to: [http://support.symbol.com](http://support.symbol.com).

Service Information

If an equipment problem occurs, contact the appropriate regional Support Center for contact information. Before calling, locate the model number and serial number.

Call the Support Center from a phone near the scanning equipment so that the service person can try to talk through the problem. If the equipment is found to be working properly and the problem is symbol readability, the Support Center will request samples of bar codes for analysis at our plant.

If the problem cannot be solved over the phone, the equipment may need to be returned for servicing. If that is necessary, specific directions will be provided.

**NOTE** 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.

Support Information

For service information, warranty information or technical assistance contact or call the Support Center. Contact information is provided on the Zebra contact web site go to: [http://www.zebra.com/support](http://www.zebra.com/support).

If the Zebra product was purchased from a Zebra Business Partner, contact that Business Partner for service.
Chapter 1 Getting Started

Introduction

This chapter provides an overview of the RD5000 RFID reader, explains how to charge the battery and how to start the reader.

*Figure 1-1 on page 1-2* provides the reader parts location and *Figure 1-2 on page 1-3* provides the locations of the reader ports and connectors. *Table 1-1* lists the reader ports and connectors.

A list of the accessories is provided in *Table 1-2*.

Unpacking the Reader

Carefully remove all protective material from around the reader and save the shipping container for later use.

Verify that all equipment was received:

- RD5000 RFID reader
- Lithium-ion battery
- Shock Isolators and mounting hardware
- QRG (Quick Reference Guide)

Inspect the equipment for damage. If any equipment is missing or if any equipment is damaged, contact the Symbol Technologies Support Center immediately. See *Service Information on page xiv* for contact information.
Connections and Ports

The RD5000 RFID reader has connections for:

- Power input (battery charging) and serial communication
- USB communication
- External antenna
**Figure 1-2**  RD5000 RFID Reader Ports/Connectors and Antenna Locations

**Table 1-1**  RD5000 RFID Reader Ports/Connections

<table>
<thead>
<tr>
<th>Port/Connectors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power/Serial</td>
<td>Connection for external power, battery charging and serial communications.</td>
</tr>
<tr>
<td>USB Client</td>
<td>USB client connection.</td>
</tr>
<tr>
<td>External Antenna</td>
<td>Supports one external antenna.</td>
</tr>
</tbody>
</table>
Accessories

Table 1-2 lists the RD5000 accessories.

Table 1-2  RD5000 Accessories

<table>
<thead>
<tr>
<th>Accessory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>Provides battery charging power and external power.</td>
</tr>
<tr>
<td>Spare lithium-ion battery</td>
<td>Replacement battery.</td>
</tr>
<tr>
<td>Four Slot Spare Battery Charger</td>
<td>Charges up to four spare batteries.</td>
</tr>
<tr>
<td>Universal Battery Charger Adapter</td>
<td>Adapts the UBC for use with the reader batteries.</td>
</tr>
<tr>
<td>Charging Cable</td>
<td>Connects to the power supply to provide battery charging power.</td>
</tr>
<tr>
<td>Charging Cable with Serial</td>
<td>Connects to the power supply and the battery charging and serial</td>
</tr>
<tr>
<td>Communications</td>
<td>communications connector to provide battery charging power. This cable also</td>
</tr>
<tr>
<td></td>
<td>has a 9-pin serial connector.</td>
</tr>
<tr>
<td>USB Communications Cable</td>
<td>Connects to the USB mini connector to provide USB communications.</td>
</tr>
<tr>
<td>External Antenna</td>
<td>Provides a remotely mounted antenna location.</td>
</tr>
<tr>
<td></td>
<td>Device Configuration Package and Platform SDK for 9090c50 (for RD5000 with</td>
</tr>
</tbody>
</table>

Getting Started

In order to start using the reader for the first time:

- Install the main battery
- Charge the main battery and backup battery
- Start the reader
- Configure the reader

The main battery can be charged before or after it is installed. Use one of the spare battery chargers to charge the main battery (out of the reader) or the Power Supply and Charging cable to charge the main battery installed in the reader.
Installing and Removing the Battery

Installing the Battery

Before using the reader, install the battery into the reader. If the battery was fully charged before installation the unit is ready to use. If the battery is not charged when it was installed then it must be charged in the unit prior to use.

1. Rotate the door latch (see Figure 1-1 on page 1-2) counterclockwise 1/4 turn to disengage the battery door latch and open the battery door.

2. Insert the battery into the battery slot as shown in Figure 1-3 on page 1-5. Ensure the battery is fully inserted, the battery release engages the battery when it is fully inserted.

3. Close the battery door and rotate the door latch clockwise 1/4 turn to engage the battery door latch.

4. If the battery was not fully charged before it was installed, then the battery must be charged before the unit can be used. To charge the battery proceed to Charging the Battery on page 1-7.

When a charged battery is fully inserted in the reader and the battery door is locked, the reader can be turned on.

Figure 1-3 Installing the Main Battery
Removing/Replacing the Main Battery

The main battery may be periodically replaced with a charged battery as an alternative to connecting the unit to the external battery charger.

Prior to removing the main battery, press the Power button to place the reader in suspend mode (off). The Battery LED must be off.

1. Rotate the door latch (see Figure 1-1 on page 1-2) counterclockwise 1/4 turn to disengage the battery door latch and open the battery door.

2. The battery door switch detects the door opening and initiates a battery removal shutdown. Pause 3-4 seconds while the reader performs battery removal shutdown.

3. Hold the battery release up and pull the battery out.

4. If a replacement battery is being used, insert the battery into the battery slot as shown in Figure 1-3 on page 1-5. Ensure the battery is fully inserted, the battery release engages the battery when it is fully inserted. If no battery is being inserted the unit can maintain the configuration settings for approximately 1/2 hour (with a fully charged internal backup battery).

5. Close the battery door and rotate the door latch clockwise 1/4 turn to engage the battery door latch.

Figure 1-4 Removing the Main Battery

NOTE When main battery door is opened and closed or if the battery is replaced, RD5000 RFID reader may not properly power itself back on. To power up the reader, manually initiate a cold boot (see Performing a Cold Boot on page 1-16) or momentarily apply external power to initiate a cold boot.

The device recovery method is a cold boot, see Performing a Cold Boot on page 1-16. All user data that was not stored in persistent memory (\Application and \Platform) will have to be manually restored.
Charging the Battery

Charging the Main Battery and Memory Backup Battery

Before using the reader for the first time, connect the reader to the optional power supply (see Figure 1-5 on page 1-8) and charge the battery until the amber charge indicator light remains lit (see Table 1-3 on page 1-5) for charge status indications. After the initial charge cycle, charge time is less than four hours.

The reader is equipped with a memory backup battery which automatically charges from the fully-charged main battery. When the reader is used for the first time, the backup battery requires approximately 15 hours to fully charge. This is also true any time the backup battery is discharged, which occurs when the main battery is removed for several hours. The backup battery retains data in memory for at least 30 minutes when the main battery is removed. When the reader reaches a very low battery state, the combination of main battery and backup battery retains data in memory for at least 72 hours.

Use the following to charge the main battery:

- Accessories: The reader charging cable provides charging capability.
  - Power supply and a charging cable
- The reader charging accessories are used to charge batteries that are removed from the reader.
  - Four Slot Spare Battery Charger
  - Universal Battery Charger (UBC)

Charging the Battery

After the initial charging, charge the battery in the reader using the charging cable with the appropriate power supply. Or the battery may be removed and charged in a spare battery charger (see Charging Spare Batteries on page 1-9). The battery fully charges in less than four hours.

1. Ensure the power supply is connected to the appropriate power source (see Chapter 3, Accessories for setup information).
2. Connect the power supply to the reader.
3. The reader starts to charge automatically. The amber Battery LED, lights to show the charge status. See Table 1-3 for charging indications.
Serial Communications

Serial communications are connected in the same way that the battery charging is connected. Except that the Charging Cable with Serial Communications (see Figure 3-7 on page 3-8) is used instead of the Charging Cable. Serial communication is only used for software de-bugging and for image uploading.

![Power Supply Connection](image)

**Figure 1-5** *Power Supply Connection*

**Table 1-3** *RD5000 LED Indicators*

<table>
<thead>
<tr>
<th>LED Indication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BATTERY LED</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>Reader is on, battery charge is greater than 80%.</td>
</tr>
<tr>
<td>Green-Red Flash</td>
<td>Reader is on, green LED flashes red when charge is less than 80%. Duration of the red flash increases as the battery charge drops. At 79% very short red flash, at 41% longer red flash.</td>
</tr>
<tr>
<td>Solid Red</td>
<td>Battery charge is less than 40%, at 20% a beeper sounds every ½ second, at 13% the unit turns off.</td>
</tr>
<tr>
<td>Off</td>
<td>Reader is off.</td>
</tr>
<tr>
<td>Slow Blinking Amber</td>
<td>Reader is charging.</td>
</tr>
<tr>
<td>Solid Amber</td>
<td>Charging complete.</td>
</tr>
<tr>
<td>Fast Blinking Amber</td>
<td>Error in charging; check the reader.</td>
</tr>
</tbody>
</table>
Charging Spare Batteries

Use the following accessories to charge spare batteries (outside of the reader):

- Four Slot Spare Battery Charger
- Universal Battery Charger (UBC) Adapter.

To charge a spare battery:

1. Ensure the accessory used to charge the spare battery is connected to the appropriate power source (see Chapter 3, Accessories for setup information).

2. Insert the spare battery into the spare battery charging slot with the charging contacts facing down (over the charging pins) and gently press down on the battery to ensure proper contact.

3. The battery starts to charge automatically. The amber charge LED on the accessory lights to show the charge status. See Chapter 3, Accessories for charging indications for the accessory.

The battery usually fully charges in less than four hours.
Connect a USB Cable

The USB port is protected by the USB port cover. To access the USB port, remove the USB port cover.

**CAUTION** With the USB port cover removed the reader should only be operated in a clean, dry environment (for setup and configuration only). The USB port cover must be replaced before operating the reader outside of a lab environment. With the USB port cover removed the reader is not properly sealed.

1. Loosen the two phillips head screws and lift off the USB port cover (see Figure 1-6).

![Figure 1-6 Remove the USB Port Cover](image)

2. Connect the USB cable to the reader as shown in Figure 1-7.

![Figure 1-7 Connect the USB Cable](image)
Connect an External Antenna

The external antenna looks very similar to the RD5000 and it provides a remotely mounted antenna location (see Figure 3-13 on page 3-11).

When the reader is used without an external antenna the external antenna port is protected by the 50 ohm termination resistor/cover. Remove the external antenna port termination resistor/cover to access the external antenna port shown in Figure 1-8. The external antenna cable must be routed to the external antenna connector shown in Figure 1-10 on page 1-12. See External Antenna Installation on page 2-12 for external antenna installation procedures.

**CAUTION** With the external antenna port termination resistor/cover removed the reader should only be operated in a clean, dry environment (for setup and configuration only). The external antenna port termination resistor/cover (or an external antenna connector Reverse-Polarity N) must be used.

3. Unscrew and remove the external antenna port termination resistor/cover as shown in Figure 1-8.

![Figure 1-8 Remove the External Antenna Port Termination Resistor/Cover](image-url)
4. Connect the external antenna to the external antenna port as shown in Figure 1-9.

Figure 1-9  Connect an External Antenna Cable to the Reader

5. Connect the external antenna to the external antenna port as shown in Figure 1-10.

Figure 1-10  External Antenna Connection
Starting the Reader

Confirm that the reader has a charged battery and press the **Power** button to turn on the reader. If the reader does not power on, perform a cold boot (see *Performing a Cold Boot on page 1-16*).

Host Computer Display Setup

The RD5000 does not have a display. To view the system menus use an application such as the Microsoft *Remote Display Control for Pocket PC*. For more information and the *Remote Display Control for Pocket PC* download go to [http://www.microsoft.com/downloads/](http://www.microsoft.com/downloads/) and search for *Remote Display Control for Pocket PC*. Download the application and follow the provided installation and setup procedures.

After the remote display application has been installed on the host computer, set up an ActiveSync connection between the host computer and the RD5000 reader (see *Setting Up an ActiveSync Connection (with no Partnership) on the Host Computer on page 4-2*).

Start the remote display application to access the RD5000 RFID reader application.

Checking Battery Status

The Battery LED displays the battery status, see *Table 1-3* for status indications.

Battery Management

Battery Saving Tips

- Connect the reader to external power when not in use.
- Turn off the reader during periods of non-use.
- Power off the reader when charging, to charge at a faster rate.
- Use the Motion and Proximity sensor features to control the time the RFID engine is active, see *MPS Settings on page 7-12* and *Appendix B, Motion Sensor Parameters*. 
Status Icons (Windows CE 5.0)

The Taskbar at the bottom of the window displays the active programs, current time, battery status and communication status.

![Taskbar with status icons](image)

Figure 1-11  Taskbar

Status icons are shown in the taskbar to indicate present status of the reader. Double tapping each status icon displays the corresponding setup window and the settings enables to be changed or adjusted.

<table>
<thead>
<tr>
<th>Status Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📝</td>
<td>This icon indicates that the keyboard input panel is selected.</td>
</tr>
<tr>
<td>🗓️</td>
<td>This icon indicates that the keyboard input panel is hidden.</td>
</tr>
<tr>
<td>⚡</td>
<td>This icon indicates that the main battery is charging or that the reader is operating on AC power. Double tapping on this icon opens the <strong>Power Properties</strong> window.</td>
</tr>
<tr>
<td>🌋</td>
<td>This icon indicates the battery is fully charged and the reader is running on external power.</td>
</tr>
<tr>
<td>🍃</td>
<td>This icon indicates that the battery is fully charged (100% charged). The battery status icons provide the battery status in 10% increments from 10% to 100%.</td>
</tr>
<tr>
<td>📦</td>
<td>This icon indicates that the reader is connected to a host computer with a serial cable.</td>
</tr>
<tr>
<td>📤</td>
<td>Wireless connection status icon. Indicates WLAN signal strength.</td>
</tr>
<tr>
<td>📱</td>
<td>The <strong>Bluetooth Enabled</strong> icon appears in the task tray and indicates that the Bluetooth radio is on.</td>
</tr>
<tr>
<td>📱</td>
<td>The <strong>Bluetooth Disabled</strong> icon appears in the task tray and indicates that the Bluetooth radio is off.</td>
</tr>
<tr>
<td>📱</td>
<td>The <strong>Bluetooth Communication</strong> icon appears in the task tray and indicates that the reader is communicating with another Bluetooth device.</td>
</tr>
<tr>
<td>🍃</td>
<td>The <strong>RFIDSocketbridge</strong> application manages incoming wireless connections, supports the TCP/IP, or Bluetooth connections, monitors battery life, controls battery LEDs, and beeps on low battery.</td>
</tr>
</tbody>
</table>
Resetting the Reader

If the reader stops responding, reset it. There are two reset functions; warm boot and cold boot.

A warm boot restarts the reader by closing all running programs.

A cold boot also restarts the reader, but erases all stored records and entries in RAM. Data saved in flash memory is not lost. In addition, it returns formats, preferences and other settings to the factory default settings.

Perform a warm boot first. This restarts the reader and saves all stored records and entries. If the reader still does not respond, perform a cold boot.

Performing a Warm Boot

Hold down the Power button (see Figure 1-1 on page 1-2) for approximately five seconds. As soon as the reader battery LED turns off release the Power button. As the RD5000 starts to perform a warm boot it beeps twice.
Performing a Cold Boot

A cold boot restarts the reader and erases all user stored records and entries that are not saved in flash memory (Application and Platform folders). *Never perform a cold boot unless a warm boot does not solve the problem.*

> **CAUTION** Performing a cold boot restores formats, preferences and other settings to the factory default settings. User data may be deleted.

> **NOTE** Any data previously synchronized with a computer can be restored during the next ActiveSync operation.

To perform a cold boot:

1. Rotate the door latch (see *Figure 1-1 on page 1-2*) counterclockwise 1/4 turn to and open the battery door. The battery door switch detects the door opening and initiates a battery removal shutdown.

> **NOTE** There is an access hole located directly below the battery door switch (see *Figure 1-12*). The reset switch is recessed within the access hole.

2. Press and hold the **Power** button (see *Figure 1-1 on page 1-2*) while simultaneously using a paper clip (or other thin object), to press and hold the reset switch (see *Figure 1-12*). Hold both for five seconds.

3. Release the reset switch and the **Power** button. The battery LED flashes yellow to indicate that a cold boot has initiated.

4. Close the battery door and rotate the door latch (see *Figure 1-1 on page 1-2*) counterclockwise 1/4 turn to lock.

The LED flashes several more times as the reader reboots and the battery LED lights green when the reader has completed the cold boot.

![Figure 1-12  Reset Button Location](image-url)
Chapter 2 Installation

Introduction

The RD5000 RFID reader is designed for use on a mobile platform such as a forklift. The unit may be used both indoors and outside and is resistant to outside elements such as sun, rain, snow and splashed water. The RD5000 RFID reader requires a mounting platform. The platform may be locally fabricated or the Zebra designed mounting brackets may be used.

RD5000 Installation

The reader must be professionally installed.

Installing the RD5000 RFID reader consists of the following procedures:

- Determine the mounting location
- Install the Zebra mounting brackets, or prepare the mounting platform
- Install the shock isolators
- Mount the reader

Mounting Location

Select a mounting location that is free from obstructions that might inhibit reading and/or interfere with the Proximity Sensor field of view and/or WAN communications. The location should also allow easy access to the reader for changing the battery and/or connecting the charging cable. Finally, the location should not subject the reader to possible damage during loading and unloading of products.
Installing The Mounting Brackets

The mounting brackets are designed to provide the proper clearances, as well as provide protection from a flat object impacting the reader. The brackets are designed to be welded in place and a welding jig is available for this purpose.

To install the mounting brackets:

✓ **NOTE** When mounting the welding jig, do not use the lock washers to mount the shock isolators.

1. Attach the shock isolators (provided with the reader) to the mounting brackets (using the post side of the shock isolator) and the provided nut. Center the shock isolator post in the mounting hole and finger tighten the nut.

2. Repeat the shock isolator mounting procedure for the second mounting bracket.

![Diagram of Mounting Brackets](Image)

**Figure 2-1 Mounting the Shock Isolators, for the Welding Jig**
3. Attach the welding jig to the shock isolators using the four allen head screws and the four lock washers. The mounting brackets are identical so either bracket can be used on the left or right hand sides.

![Welding Jig Installation Diagram]

**Figure 2-2  Welding Jig Installation**

4. Position the mounting brackets/welding jig assembly in the final mounting location and secure the assembly so that it will not move.
5. Tack weld the mounting brackets in the six locations marked (see Figure 2-3). The welds should be 1/2 inch to 3/4 inch long, with a 1/4 inch bead and 1/16 inch penetration.

Figure 2-3  Tack Welds, Location

6. Remove the welding jig, and remove the shock isolators.
7. Finish welding the mounting brackets (see Figure 2-4) with a 1/4 inch bead and 1/16 inch penetration.

![Figure 2-4](image)

*Figure 2-4  Finish Welding the Brackets*

8. Clean and inspect the welds. Re-weld any areas that require touch-up.

9. Allow the brackets to cool before continuing with the installation.

10. Clean and apply touch-up paint (as required) to inhibit corrosion.
Installing The Shock Isolators on The Mounting Brackets

**CAUTION** The shock isolators are required. Do not mount the unit without the shock isolators.

When permanently mounting the shock isolators use the lock washers between the nut and the mounting bracket, as shown in Figure 2-5.

1. Attach the shock isolators (provided with the reader) to the mounting brackets (using the post side of the shock isolator) with the provided nut and lock washer. Center the shock isolator post in the mounting hole and tighten the nut. Repeat the shock isolator mounting procedure for all four shock isolators.

![Figure 2-5 Mounting the Shock Isolators](image)

2. The mounting brackets are ready to accept the RD5000 RFID reader. Proceed to Mounting The Reader on page 2-9.
Locally Fabricated Mounting Platform

✓ **NOTE** The locally fabricated mounting platform is only used when the mounting brackets are not (or cannot) be used.

The mounting platform may be locally fabricated, or the mounting brackets may be used (recommended) as the mounting platform.

**Mounting Platform Fabrication**

⚠️ **CAUTION** The supplied shock isolators are required and must be used with any user developed mounting platform.

The mounting platform must be designed to provide the raised mounting for the reader. The mounting design must be strong enough to support the unit taking into account the shocks and vibration the reader will experience. *Figure 2-6 on page 2-7* provides the placement and size specifications for the mounting platform.

![Figure 2-6 Mounting Platform Specifications](image-url)

**Figure 2-6** Mounting Platform Specifications
Installing The Shock Isolators on The Locally Fabricated Mounting Platform

The locally fabricated mounting platform must provide the proper clearances (see Figure 2-6 on page 2-7).

1. Attach the shock isolators (provided with the reader) using the post side of the shock isolator as appropriate for the mounting platform design. Center the shock isolator post in the mounting hole and secure. Repeat the shock isolator mounting procedure for all four shock isolators.

2. Proceed to Mounting The Reader on page 2-9 and adapt the procedure to fit the locally fabricated mounting platform requirements.
Mounting The Reader

The steps provided are to mount the RD5000 RFID reader to the mounting brackets. Adjust the steps accordingly if a fabricated platform is being used.

1. Prior to starting the installation confirm that the reader has been configured for the local wireless network and that the battery has been fully charged.

2. Press the Power switch (located between the Battery and Error LEDs) and confirm that the reader boots up properly and that the green Battery LED lights. The reader may take a couple of minutes to fully boot up. If the reader does not properly boot up, return it to the local IT specialist to confirm operation.

3. Once the proper boot up has been confirmed, press the Power switch again to turn the reader off before proceeding with the installation. The Battery LED should now be off.

Mounting on The Mounting Brackets

The mounting brackets provide the proper clearances and provide protection from a flat object impacting the reader. The brackets must be welded in place (see Installing The Mounting Brackets on page 2-2) before proceeding with the reader mounting procedure.

**CAUTION** The shock isolators are required. Do not mount the unit without the shock isolators

1. Tilt and angle the reader to fit the battery door between the shock isolators (see Figure 2-7).
2. Slide the reader under the mounting bracket far enough to clear the external antenna terminating resistor and lower the reader onto the shock isolators.

Figure 2-8  Mounting the RD5000 RFID Reader

3. Slide the reader over the shock isolators to align the shock mount holes with the reader mounting holes.

4. If the holes do not align properly loosen the nuts at the bottom of the shock isolators and move the shock isolators to properly align the holes.

5. When the holes are properly aligned, insert the allen head screws, and finger tighten.
6. Once all of the allen head screws are in place, use a 3/16 inch allen wrench and a 7/16 open end wrench to tighten the allen screws and the shock isolator nuts to a torque of 3.3 ft.-lbs.

The reader is now ready for use.
External Antenna Installation

The external antenna must be professionally installed. Select an accessible mounting location that is free from obstructions that might inhibit reading.

The external antenna uses the same mounting brackets or mounting platform that the RD5000 uses.

The location should not subject the external antenna to possible damage during loading and unloading of products. Use the following steps to install the external antenna:

Installing the external antenna is the same as the RD5000 installation procedures:

- Determine the mounting location.
- Install the mounting brackets, or prepare the mounting platform. See Installing The Mounting Brackets on page 2-2 or Locally Fabricated Mounting Platform on page 2-7 for detailed procedures.
- Install the shock isolators, see See Installing The Shock Isolators on The Mounting Brackets on page 2-6 or Installing The Shock Isolators on The Locally Fabricated Mounting Platform on page 2-8 for detailed procedures.
- Mount the external antenna the same way that the RD5000 is mounted. See Mounting The Reader on page 2-9 for detailed procedures.
- Connect the external antenna cable as described in Connect an External Antenna on page 1-11.
Chapter 3 Accessories

Introduction

The RD5000 RFID reader and the MC9000 Series mobile computers share some of the same accessories. These accessories provide a wide variety of product support capabilities. Accessories include a power supplies, spare batteries and battery charging solutions. The RD5000 accessories include:

- **Power Supply**
  Provides battery charging power.

- **Spare lithium-ion battery**
  Spare/replacement battery.

- **Four Slot Spare Battery Charger**
  Charges up to four spare batteries.

- **Universal Battery Charger Adapter**
  Adapts the UBC for use with the mobile reader batteries.

- **Charging Cable**
  Connects to the power supply and the Battery Charging to provide battery charging power.

- **Charging Cable with Serial Communications**
  Connects to the power supply and the Battery Charging and Serial Communications connector to provide battery charging power. In addition the cable has a “Y” connector with a 9-pin serial connector.

- **External Antenna**
  Provides an externally mounted antenna location.

- **USB Communications Cable**
  Connects to the USB mini connector to provide USB communications.
**Power Supply**

The Zebra approved power supply output rated at 12 Vdc and a minimum of 3.33 A is required to maintain warranty coverage and regulatory approvals. The power supply is certified to EN60950-1 with SELV outputs. Use of an alternative power supply will invalidate any approval given to this device and may be dangerous.

The power supply is self-regulating and can accept inputs within the range of 100-250 VAC and 50-60 Hz. Power cords are available to fit most local power delivery systems.

**Battery**

The Zebra approved battery is a removable, rechargeable 7.2 V Lithium Ion battery pack, rated at 2200 mAh, 15.8 watt hours.

The Zebra rechargeable battery packs are designed and constructed to the highest standards within the industry. However, there are limitations to how long a battery can operate or be stored before needing replacement. Many factors affect the actual life cycle of a battery pack, such as heat, cold, harsh environmental conditions and severe drops.

When batteries are stored over six (6) months, some irreversible deterioration in overall battery quality may occur. Store batteries discharged in a dry, cool place, removed from the equipment to prevent loss of capacity, rusting of metallic parts and electrolyte leakage. When storing batteries for one year or longer, they should be charged and discharged at least once a year. If an electrolyte leakage is observed, avoid any contact with affected area and properly dispose of the battery. Batteries must be charged within the 32° to 104° F (0° to +40° C) ambient temperature range. Replace the battery when a significant loss of run time is detected.

Standard warranty period for all Zebra batteries is 30 days, regardless if the battery was purchased separately or included as part of the RFID reader. For more information on Zebra batteries, please visit:

http://mysymbolcare.symbol.com/battery/batbasics1.html
Four Slot Spare Battery Charger

This section describes how to set up and use the Four Slot Spare Battery Charger to charge up to four spare batteries.

![Four Slot Spare Battery Charger](image)

**Setup**

*CAUTION* Use only a Zebra approved power supply output rated 15 VDC and minimum 5 A. Use of an alternative power supply will void the product warranty and may cause product damage.

![Four Slot Spare Battery Charger Power Connection](image)
Spare Battery Charging with the Four Slot Spare Battery Charger

1. Connect the charger to a power source as shown in Figure 3-2.

2. Insert the battery into a spare battery charging slot and gently press down on the battery to ensure proper contact.

Battery Charging Indicators

An amber LED is provided on each battery charging well (see Figure 3-1 on page 3-3). See Table 3-1 for charging status indications.

The battery usually charges in less than four hours.

<table>
<thead>
<tr>
<th>LED</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Charger is not attached to the power supply correctly, power supply is not powered or a battery is not inserted in the slot.</td>
</tr>
<tr>
<td>Fast Blinking Amber</td>
<td>Charging error; check placement of spare battery.</td>
</tr>
<tr>
<td>Slow Blinking Amber</td>
<td>Spare battery is charging.</td>
</tr>
<tr>
<td>Solid Amber</td>
<td>Charging complete.</td>
</tr>
</tbody>
</table>
Universal Battery Charger (UBC) Adapter

This section describes how to use the UBC adapter to charge a spare battery.

The UBC can be used with a power supply as a standalone spare battery charger or it can be used with the four station UBC2000 to provide charging to simultaneously charge up to four spare batteries. For additional information about the UBC2000, see the *UBC 2000 Universal Battery Charger Product Guide* (p/n 70-33188-xx).

![UBC Adapter Diagram]

**Figure 3-3  UBC Adapter**

Inserting and Removing a Battery

Insert the battery into the battery well with the charging contacts facing down (over charging pins) and gently press down on the battery to ensure proper contact.

To remove the battery, press the battery release and lift battery out of the well.
Setup

**CAUTION** Use only a Zebra approved power supply output rated 15 VDC and minimum 1.5 A. Use of an alternative power supply will void the product warranty and may cause product damage.

![UBC Adapter Power Connection](image)

**Figure 3-4  UBC Adapter Power Connection**

**Battery Charging Indicators**

To charge a spare battery using the UBC adapter, connect the power supply to the UBC (see *Figure 3-4 on page 3-6*), then insert the spare battery. The spare battery begins charging automatically. The charge LEDs (see *Figure 3-5*) show the battery charging. *Table 3-2* shows battery charging status indications. The battery usually charges in three hours.

![UBC Adapter LEDs](image)

**Figure 3-5  UBC Adapter LEDs**
Charging Cable

The Charging Cable is used to connect the power supply to the RD5000. The pin-outs for the Power/Serial Connector are provided in Table 3-3.

Table 3-2  UBC Adapter Charge LED Status Indications

<table>
<thead>
<tr>
<th>LED</th>
<th>Indication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWER</td>
<td>Green</td>
<td>Power is connected to the UBC Adapter.</td>
</tr>
<tr>
<td>READY or</td>
<td>Green</td>
<td>Charging complete.</td>
</tr>
<tr>
<td>STANDBY or</td>
<td>Flashing-Yellow</td>
<td>The battery was deeply discharged and is being trickle charged to bring the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>voltage up to the operating level. After operating level voltage is achieved the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>battery charges normally.</td>
</tr>
<tr>
<td>FAULT</td>
<td>Yellow</td>
<td>Charging error, check placement of RFID reader/spare battery.</td>
</tr>
<tr>
<td>CHARGING</td>
<td>Yellow</td>
<td>Normal charge.</td>
</tr>
</tbody>
</table>

Table 3-3  Power/Serial Connector Pin-Outs

<table>
<thead>
<tr>
<th>Pin*</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Gnd</td>
</tr>
<tr>
<td>2</td>
<td>+V</td>
</tr>
<tr>
<td>3</td>
<td>RS232 Tx</td>
</tr>
<tr>
<td>4</td>
<td>RS232 RX</td>
</tr>
</tbody>
</table>

The Pin numbers are on the connector.
Charging Cable With Serial Communications

The Charging Cable With Serial Communications is used to connect the power supply to the RD5000 and provide serial communications between the RD5000 and a local computer. The pin-outs for the Power/Serial Connector are provided in Table 3-3 on page 3-7 and the pin-outs for the Serial RS232 Connector are provided in Table 3-4.

![Charging Cable With Serial Communications](image)

**Figure 3-7  Charging Cable With Serial Communications**

**Table 3-4  Serial RS232 Connector Pin-Outs**

<table>
<thead>
<tr>
<th>Pin*</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>RS232 Tx</td>
</tr>
<tr>
<td>3</td>
<td>RS232 RX</td>
</tr>
<tr>
<td>5</td>
<td>Gnd</td>
</tr>
</tbody>
</table>

The Pin numbers are on the connector
USB Communications Cable

The USB Communications Cable is a standard USB to USB mini cable and may be purchased locally.

USB Connection Setup (Windows CE 5.0)

1. Ensure that ActiveSync was installed on the host computer and a partnership was created (see Chapter 4, ActiveSync).

2. Start ActiveSync if it is not running on the host computer. To start, select Start - Programs - Microsoft ActiveSync.

![ActiveSync - Not Connected](image)

3. In the ActiveSync window, select File > Connection Settings. The Connection Settings window displays.

![Serial Connection Settings](image)

4. For USB connection, select Allow USB connection with this desktop computer.

5. Click OK to save any changes made.

![NOTE](image)

Every RFID reader should have a unique device name. Never try to synchronize more than one RFID reader to the same name.

6. Connect the device to the host computer.
7. Upon connection, synchronization occurs automatically.

**USB Connection Setup (Windows CE 5.0)**

The RD5000 USB setup is controlled through the CTLPanel. The default setting is USB, to confirm or change the setting perform the following.

From the RD5000 main window (see Figure 3-10) click Start - Programs - Windows Explorer to access the Explorer application.

![Figure 3-10 Main Windows](image)

From main Explorer window (see Figure 3-10) click Application - CTLPanel to access the CTLPanel utility. The CTLPanel window appears (see Figure 3-11). Double-click on Comm Settings to access the USB settings window.

![Figure 3-11 Explorer Windows](image)

With Port highlighted, confirm that the Com port default value is set to USB Default. To change the value use the left and right arrow buttons to select USB Default.

**NOTE** The cradle requires a dedicated port. It cannot share a port with an internal modem or other device. Refer to the computer user manual supplied to locate the serial port(s).
Click **OK** to exit the *Comm Settings* window and click **Exit** to exit the *Control Panel* window.

### External Antenna

The external antenna provides a remotely mounted antenna location. The internal and the external antenna can operate independently from each other and can even have different power settings. Both antennas can be active at the same time.

> **Figure 3-13  External Antenna**

See *External Antenna Installation on page 2-12* for external antenna installation procedures.

See *Connect an External Antenna on page 1-11* for external antenna connection procedures.
Chapter 4 ActiveSync

Introduction

To communicate with various host devices, install Microsoft ActiveSync (version 4.1 or higher) on the host computer. Use ActiveSync to synchronize information on the reader with information on the host computer. Changes made on the reader or host computer appear in both places after synchronization.

NOTE When a reader with Windows Mobile 5.0 is connected to a host computer and an ActiveSync connection is made, the WLAN and WWAN radios (if applicable) are disabled. This is a Microsoft security feature to prevent connection to two networks at the same time.

ActiveSync software:

- Allows working with reader-compatible host applications on the host computer. ActiveSync replicates data from the reader so the host application can view, enter, and modify data on the reader.
- Synchronizes files between the reader and host computer, converting the files to the correct format.
- Backs up the data stored on the reader. Synchronization is a one-step procedure that ensures the data is always safe and up-to-date.
- Copies (rather than synchronizes) files between the reader and host computer.
- Controls when synchronization occurs by selecting a synchronization mode, e.g., set to synchronize continually while the reader is connected to the host computer, or set to only synchronize on command.
- Selects the types of information to synchronize and control how much data is synchronized.

Installing ActiveSync

To install ActiveSync on the host computer, download version 4.1 or higher from the Microsoft web site at http://www.microsoft.com. Refer to the installation included with the ActiveSync software.
Connect the RD5000 USB Communications Cable

Connect the RD5000 Communications cable to the RD5000 and the host computer, see *Serial Communications on page 1-8* and *Connect a USB Cable on page 1-10*.

Setting Up an ActiveSync Connection (with no Partnership) on the Host Computer

After ActiveSync installation is complete, the ActiveSync Setup Wizard sets up communications between the RFID reader and host computer. Before setting up communications between the RFID reader and host computer, refer to the *Chapter 3, Accessories* for a list of the accessories that can be used.

1. Connect the RFID reader to the host computer using the USB connection.
2. If the *Get Connected* window does not appear on the host computer, select *Start > Programs > Microsoft ActiveSync > File > Get Connected*.
3. Click **Next** to continue.

![Get Connected Window](image-url)
4. Select the No radio button in the Set up a Partnership window.

5. Click Next. If the ActiveSync Not Connected window (see Figure 4-3) displays, proceed to step 6. If the ActiveSync Connected window (see Figure 4-7) displays, proceed to step 11.

![Figure 4-2 Get Connected Window](image)

6. In the ActiveSync Not Connected window, select File > Connection Settings. The ActiveSync Connection Settings window appears.

![Figure 4-3 ActiveSync Not Connected Window](image)
7. Select the *Allow USB connections*, check box.

![ActiveSync Connection Settings Window](image)

**Figure 4-4** ActiveSync Connection Settings Window

8. Click on **OK**. The *ActiveSync Add/Remove Programs Window* displays.

9. Select any required programs to be added and click **OK**. The *ActiveSync Connecting Window* displays.

![ActiveSync Add/Remove Programs Window](image)

**Figure 4-5** ActiveSync Add/Remove Programs Window
10. The ActiveSync Connecting Window displays until ActiveSync connects.

![ActiveSync Connecting Window](image)

**Figure 4-6** ActiveSync Connecting Window

11. When Active Sync has connected, the ActiveSync Connected window displays.

![ActiveSync Connected Window](image)

**Figure 4-7** ActiveSync Connected Window

12. The ActiveSync Connected window indicated that ActiveSync has successfully connected.
Setting up a Partnership

After ActiveSync installation is complete, the ActiveSync Setup Wizard sets up a partnership to synchronize information between the RFID reader and host computer and customize synchronization settings.

Before setting up a partnership between the RFID reader and host computer, refer to the Chapter 3, Accessories for a list of the accessories that can be used.

To set up a partnership:

1. Connect the RFID reader to the host computer using the USB connection.
2. If the Get Connected window does not appear on the host computer, select Start > Programs > Microsoft ActiveSync > File > Get Connected.
3. Click Next to continue.

4. Select the Yes radio button to proceed with the partnership setup.
5. Select Next and the Add/Remove Programs window appears.
6. Select any required programs to be added and click on OK. The Select Number of Partnerships Window displays.

![Add/Remove Programs Window](image)

Figure 4-10  Add/Remove Programs Window

7. Select the appropriate radio button for the number of computers to be included in the partnership. Click Next, the Select Synchronization Settings window displays.

![Select Number of Partnerships Window](image)

Figure 4-11  Select Number of Partnerships Window
8. To synchronize a particular type of information, select its check box. To stop synchronization of that information, clear its check box. Select any required synchronization items and click Next. The Connecting window displays (may be very brief).

![Select Synchronization Settings Window](image)

**Figure 4-12** Select Synchronization Settings Window

9. The host computer and the RFID reader attempt to synchronize. When the synchronization is complete the Setup Complete window (see Figure 4-16) appears.

![Connecting Window](image)

**Figure 4-13** Connecting Window

10. If the ActiveSync Not Connected window (see Figure 4-14) displays, proceed to step 11. If the Setup Complete window (see Figure 4-16) displays, proceed to step 12.
11. In the ActiveSync Connection Settings window, select the *Allow USB Connections* check box and click **Connect**. The ActiveSync Connecting window (see Figure 4-13) displays (may be very brief).

![ActiveSync Not Connected Window](image)

**Figure 4-14  ActiveSync Not Connected Window**

12. When the synchronization is complete the Setup Complete window (see Figure 4-16) appears.

![ActiveSync Connection Settings Window](image)

**Figure 4-15  ActiveSync Connection Settings Window**

![Setup Complete Window](image)

**Figure 4-16  Setup Complete Window**
13. Select Finish the ActiveSync Connected and Synchronized window displays.

![ActiveSync Connected and Synchronized Window](image)

**Figure 4-17** ActiveSync Connected and Synchronized Window

The ActiveSync Connection and Synchronization are complete.

During the first synchronization, information stored on the host computer is copied to the RFID reader. When the copy is complete and all data is synchronized, the RFID reader can be disconnect from the host computer.

![Checkmark](image)

**NOTE** The first ActiveSync operation must be performed with a local, direct connection. To retain partnerships after a cold boot, capture partnership registry information in a .reg file and save it in the Flash File System, detailed information is provided in the SMDK Windows CE Help File for Zebra RFID readers, see Deployment on page 6-7 for the SMDK information.

For more information about using ActiveSync, start ActiveSync on the host computer, then see ActiveSync Help.
RFID Reader Setup

The RFID reader can be set up to communicate with a USB connection. Chapter 3, Accessories provides the accessory setup and cable connection information for use with the RFID reader. The RFID reader communication settings must be set to match the communication settings used with ActiveSync.

USB Connection Setup (Windows CE 5.0)

The RD5000 USB setup is controlled through the CTLPanel. The default setting is USB, to confirm or change the setting perform the following.

From the RD5000 main window (see Figure 4-18) click Start - Programs - Windows Explorer to access the Explorer application.

From main Explorer window (see Figure 4-18) click Application - CTLPanel to access the CTLPanel utility. The CTLPanel window appears (see Figure 4-19). Double-click on Comm Settings to access the USB settings window.
1. On the RFID reader double-click the Ctl Panel icon and double-click Comm Settings to display the Comm Settings window.

![Figure 4-20 Comm Settings Window](image)

2. With Port highlighted, use the left `<` and right arrow `>` buttons to select the value. The default value is USB.

3. Click OK to exit the Comm Settings window.

4. Proceed with installing ActiveSync on the host computer and setting up a partnership.
Chapter 5 Wireless Applications

Introduction

Wireless Local Area Networks (WLANs) allow readers to communicate wirelessly and send captured data to a host device in real time. The RD5000 RFID reader supports the IEEE 802.11a, 802.11b and 802.11g standards. Before using the reader on a WLAN, the facility must be set up with the required hardware to run the wireless LAN and the reader must be configured. Refer to the documentation provided with the access points (APs) for instructions on setting up the hardware.

NOTE The screens and windows are provided for illustration purposes only and may differ from actual screens. The applications described may not be available on (or applicable to) all devices. Procedures are not device specific and are intended to provide a functional overview.

To configure the reader, a set of wireless applications provide the tools to configure and test the wireless radio in the reader. The Wireless Application menu on the task tray provides the following wireless applications:

- Wireless Status
- Wireless Diagnostics
- Find WLANs
- Manage Profiles
- Options
- Enable/Disable Radio (not available on Windows CE 5.0 devices with Fusion 2.3 and lower)
- Log On/Off.

Click the Signal Strength icon to display the Wireless Applications menu.
The **Signal Strength** icon in the task tray indicates the wireless signal strength as follows:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>Excellent signal strength</td>
<td>Wireless LAN network is ready to use.</td>
</tr>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>Very good signal strength</td>
<td>Wireless LAN network is ready to use.</td>
</tr>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>Good signal strength</td>
<td>Wireless LAN network is ready to use.</td>
</tr>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>Fair signal strength</td>
<td>Wireless LAN network is ready to use. Notify the network administrator that the signal strength is only “Fair”.</td>
</tr>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>Poor signal strength</td>
<td>Wireless LAN network is ready to use. Performance may not be optimum. Notify the network administrator that the signal strength is “Poor”.</td>
</tr>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>Out-of-network range (not associated)</td>
<td>No wireless LAN network connection. Notify the network administrator.</td>
</tr>
<tr>
<td><img src="signal_strength_icon.png" alt="Signal Strength Icon" /></td>
<td>No wireless LAN network card detected</td>
<td>No wireless LAN network card detected or radio disabled. Notify the network administrator.</td>
</tr>
</tbody>
</table>
Turning the WLAN Radio On and Off

Windows CE 5.0 with Fusion 2.4 and Higher

To turn the WLAN radio off click the **Signal Strength** icon and select **Disable Radio**.

To turn the WLAN radio on click the **Signal Strength** icon and select **Enable Radio**.

![Disable Radio](image1.png) ![Enable Radio](image2.png)

**Figure 5-2** Disable and Enable Radio

To turn the WLAN radio on click the **Signal Strength** icon and select **Enable Radio**.
Find WLANs Application

Use the Find WLANs application to discover available networks in the vicinity of the user and reader. To open the Find WLANs application, click the Signal Strength icon > Find WLANs. The Find WLANs window displays.

![Find WLANs Window](image)

**NOTE** The Find WLANs display is limited to 32 items (ESSIDs or MAC addresses). A combination of up to 32 ESSIDs/APs may be displayed.

Manually enter valid ESSIDs not displayed in the Find WLANs window. See Figure 5-3 on page 5-4.

The Find WLANs list displays:

- WLAN Networks - Available wireless networks with icons that indicate signal strength and encryption type. The signal strength and encryption icons are described in Table 5-2 and Table 5-3.
- Network Type - Type of network.
- Channel - Channel on which the AP is transmitting.
- Signal Strength - The signal strength of the signal from the AP.

### Table 5-2  Signal Strength Icon

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Excellent signal</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Very good signal</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Good signal</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Fair signal</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Poor signal</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Out of range or no signal</td>
</tr>
</tbody>
</table>
Click-and-hold on a WLAN network to open a pop-up menu which provides two options: Connect and Refresh. Select Refresh to refresh the WLAN list. Select Connect to create a wireless profile from that network. This starts the Profile Editor Wizard which allows the values for the selected network to be set. After editing the profile, the RFID reader automatically connects to this new profile.

### Profile Editor Wizard

Use the Profile Editor Wizard to create a new profile or edit an existing profile. If editing a profile, the fields reflect the current settings for that profile. If creating a new profile, the known information for that WLAN network appears in the fields.

Navigate through the wizard using the Next and Back buttons. Click X to quit. On the confirmation dialog box, click No to return to the wizard or click Yes to quit and return to the Manage Profiles window. See Manage Profiles Application on page 5-22 for instructions on navigating the Profile Editor Wizard.

### Profile ID

In the Profile ID dialog box in the Profile Editor Wizard, enter the profile name and the ESSID.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN is an infrastructure network, with no encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN is an Ad-Hoc network, with no encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN access is encrypted and requires a password.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN is an Ad-Hoc network, with encrypted access and requires a password.</td>
</tr>
</tbody>
</table>

Click-and-hold on a WLAN network to open a pop-up menu which provides two options: Connect and Refresh. Select Refresh to refresh the WLAN list. Select Connect to create a wireless profile from that network. This starts the Profile Editor Wizard which allows the values for the selected network to be set. After editing the profile, the RFID reader automatically connects to this new profile.

### Profile Editor Wizard

Use the Profile Editor Wizard to create a new profile or edit an existing profile. If editing a profile, the fields reflect the current settings for that profile. If creating a new profile, the known information for that WLAN network appears in the fields.

Navigate through the wizard using the Next and Back buttons. Click X to quit. On the confirmation dialog box, click No to return to the wizard or click Yes to quit and return to the Manage Profiles window. See Manage Profiles Application on page 5-22 for instructions on navigating the Profile Editor Wizard.

### Profile ID

In the Profile ID dialog box in the Profile Editor Wizard, enter the profile name and the ESSID.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN is an infrastructure network, with no encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN is an Ad-Hoc network, with no encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN access is encrypted and requires a password.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>WLAN is an Ad-Hoc network, with encrypted access and requires a password.</td>
</tr>
</tbody>
</table>

Click-and-hold on a WLAN network to open a pop-up menu which provides two options: Connect and Refresh. Select Refresh to refresh the WLAN list. Select Connect to create a wireless profile from that network. This starts the Profile Editor Wizard which allows the values for the selected network to be set. After editing the profile, the RFID reader automatically connects to this new profile.

### Profile Editor Wizard

Use the Profile Editor Wizard to create a new profile or edit an existing profile. If editing a profile, the fields reflect the current settings for that profile. If creating a new profile, the known information for that WLAN network appears in the fields.

Navigate through the wizard using the Next and Back buttons. Click X to quit. On the confirmation dialog box, click No to return to the wizard or click Yes to quit and return to the Manage Profiles window. See Manage Profiles Application on page 5-22 for instructions on navigating the Profile Editor Wizard.

### Profile ID

In the Profile ID dialog box in the Profile Editor Wizard, enter the profile name and the ESSID.
Table 5-4  Profile ID Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name and (WLAN) identifier of the network connection. Enter a user friendly name for the reader profile used to connect to either an AP or another networked computer. Example: The Public LAN.</td>
</tr>
<tr>
<td>ESSID</td>
<td>The name and (WLAN) identifier of the network connection. Alternatively, enter the name and (WLAN) identifier of a WLAN network connection not listed on the Find WLANs window. The ESSID is the 802.11 extended service set identifier. The ESSID is 32-character (maximum) string identifying the WLAN, and must match the AP ESSID for the RFID reader to communicate with the AP.</td>
</tr>
</tbody>
</table>

✓ NOTE  Two profiles with the same user friendly name are acceptable but not recommended.

Click Next. The Operating Mode dialog box displays.

Operating Mode

Use the Operating Mode dialog box to select the operating mode (Infrastructure or Ad-Hoc) and the country location.
Click Next. If Ad-Hoc mode was selected the Ad-Hoc dialog box displays. If Infrastructure mode was selected the Authentication dialog box displays. See Authentication on page 5-9 for instruction on setting up authentication.

### Table 5-5  Operating Mode Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Mode</td>
<td>Select <strong>Infrastructure</strong> to enable the reader to transmit and receive data with an AP. <strong>Infrastructure</strong> is the default mode. Select <strong>Ad Hoc</strong> to enable the reader to form its own local network where readers communicate peer-to-peer without APs using a shared ESSID.</td>
</tr>
<tr>
<td>Country</td>
<td><strong>Country</strong> determines if the profile is valid for the country of operation. The profile country must match the country in the options page or it must match the acquired country if 802.11d is enabled. <strong>Single Country Use:</strong> When the device is only used in a single country, set every profile country to <strong>Allow Any Country</strong>. In the <strong>Options &gt; Regulatory</strong> dialog box (see Figure 4-46 on page 4-37), select the specific country the device is used in, and deselect the <strong>Enable 802.11d</strong> option. This is the most common and efficient configuration, eliminating the initialization overhead associated with acquiring a country via 802.11d. <strong>Multiple Country Use:</strong> When the device is used in more than one country, select the <strong>Enable 802.11d</strong> option in the <strong>Options &gt; Regulatory</strong> dialog box (see Figure 4-46 on page 4-37). This eliminates the need for reprogramming the country (in <strong>Options &gt; Regulatory</strong>) each time a new country is entered. However, this only works if the infrastructure (i.e., APs) supports 802.11d (some infrastructures do not support 802.11d, including some Cisco APs). When the Enable 802.11d option is selected, the <strong>Options &gt; Regulatory &gt; Country</strong> setting is not used. For a single profile that can be used in multiple countries, with infrastructure that supports 802.11d (including Zebra infrastructure), set the Profile Country to <strong>Allow Any Country</strong>. Under <strong>Options &gt; Regulatory</strong>, select <strong>Enable 802.11d</strong>. The <strong>Options &gt; Regulatory &gt; Country</strong> setting is not used. For a single profile that can be used in multiple countries, but with infrastructure that does not support 802.11d, set the profile country to <strong>Allow Any Country</strong>, and de-select (uncheck) <strong>Enable 802.11d</strong>. In this case, the <strong>Options &gt; Regulatory &gt; Country</strong> setting must always be set to the country the device is currently in. This configuration option is the most efficient and may be chosen for use with any infrastructure. However, the <strong>Options &gt; Regulatory &gt; Country</strong> setting must be manually changed when a new country is entered. Note that using a single profile in multiple countries implies that there is a common ESSID to connect to in each country. This is less likely than having unique ESSIDs in each country, this requires unique profiles for each country. For additional efficiency when using multiple profiles that can be used in multiple countries, the country setting for each profile can be set to a specific country. If the current country (found via 802.11d or set by <strong>Options &gt; Regulatory &gt; Country</strong> when 802.11d is disabled) does not match the country set in a given profile, then that profile is disabled. This can make profile roaming occur faster. For example, if two profiles are created and configured for Japan, and two more profiles are created and configured for USA, then when in Japan only the first two profiles are active, and when in USA only the last two are active. If they had all been configured for <strong>Allow Any Country</strong>, then all four would always be active, making profile roaming less efficient.</td>
</tr>
</tbody>
</table>
Ad-Hoc

Use the Ad-Hoc dialog box to select the required information to control Ad-Hoc mode. This dialog box does not appear if Infrastructure mode is selected. To select Ad-Hoc mode:

1. Select a channel number from the Channel drop-down list.

Table 5-6  Ad-Hoc Channels

<table>
<thead>
<tr>
<th>Band</th>
<th>Channel</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 GHz</td>
<td>1</td>
<td>2412 MHz</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2417 MHz</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2422 MHz</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2427 MHz</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2432 MHz</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2437 MHz</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2442 MHz</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2447 MHz</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>2452 MHz</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>2457 MHz</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>2462 MHz</td>
</tr>
<tr>
<td>5 GHz</td>
<td>36</td>
<td>5180 MHz</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>5200 MHz</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>5220 MHz</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>5240 MHz</td>
</tr>
</tbody>
</table>

Figure 5-6  Ad-Hoc Settings Dialog Box

2. Click Next. The Encryption dialog box displays. See Encryption on page 5-16 for encryption options.
Authentication

Use the Authentication dialog box to configure authentication. If Ad-Hoc mode is selected, this dialog box is not available and authentication is set to None by default.

Select an authentication type from the drop-down list and click Next. Selecting PEAP or TTLS displays the Tunneled dialog box. Selecting None, TLS, or LEAP displays the Encryption dialog box. See Encryption on page 5-16 for encryption options. Table 5-7 lists the available authentication options.

Table 5-7  Authentication Options

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Default setting when authentication is not required on the network.</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Select this option to enable EAP-TLS authentication. EAP-TLS is an authentication scheme through IEEE 802.1x. It authenticates users and ensures only valid users can connect to the network. It also restricts unauthorized users from accessing transmitted information by using secure authentication certificates.</td>
</tr>
<tr>
<td>PEAP</td>
<td>Select this option to enable PEAP authentication. This method uses a digital certificate to verify and authenticate a user's identity.</td>
</tr>
<tr>
<td>LEAP</td>
<td>Select this option to enable LEAP authentication, which is based on mutual authentication. The AP and the connecting reader require authentication before gaining access to the network.</td>
</tr>
<tr>
<td>TTLS</td>
<td>Select this option to enable TTLS authentication.</td>
</tr>
</tbody>
</table>

Tunneled Authentication

Use the Tunneled Authentication dialog box to select the tunneled authentication options. There are different selections available for PEAP or TTLS authentication.

To select a tunneled authentication type:
1. Select a tunneled authentication type from the drop-down list. See Table 5-8 and Table 5-9.

2. Select the User Certificate check box if a certificate is required. If the TLS tunnel type selected requires a user certificate, the check box is already selected.

3. Click Next. The Installed User Certificates dialog box appears.

Table 5-8 lists the PEAP tunneled authentication options.

Table 5-8  PEAP Tunneled Authentication Options

<table>
<thead>
<tr>
<th>PEAP Tunneled Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS CHAP v2</td>
<td>Microsoft Challenge Handshake Authentication Protocol version 2 (MS CHAP v2) is a password-based, challenge-response, mutual authentication protocol that uses the industry-standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.</td>
</tr>
<tr>
<td>TLS</td>
<td>EAP TLS is used during phase 2 of the authentication process. This method uses a user certificate to authenticate.</td>
</tr>
</tbody>
</table>

Table 5-9 lists the TTLS tunneled authentication options.

Table 5-9  TTLS Tunneled Authentication Options

<table>
<thead>
<tr>
<th>TTLS Tunneled Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol (CHAP) is one of the two main authentication protocols used to verify the user name and password for PPP Internet connections. CHAP is more secure than PAP because it performs a three way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link is established.</td>
</tr>
<tr>
<td>MS CHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol (MS CHAP) is an implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. MS CHAP is identical to CHAP, except that MS CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.</td>
</tr>
</tbody>
</table>
User Certificate Selection

If the User Certificate check box on the Tunneled Authentication dialog box was checked or if TLS is the selected authentication type, the Installed User Certificates dialog box displays. Select a certificate from the drop-down list of currently installed certificates before proceeding. The selected certificate name appears in the drop-down list. If the required certificate is not in the list, install it.

Table 5-9  TTLS Tunneled Authentication Options (Continued)

<table>
<thead>
<tr>
<th>TTLS Tunneled Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS CHAP v2</td>
<td>MS CHAP v2 is a password based, challenge response, mutual authentication protocol that uses the industry standard Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. The authenticating server challenges the access client and the access client challenges the authenticating server. If either challenge is not correctly answered, the connection is rejected. MS CHAP v2 was originally designed by Microsoft as a PPP authentication protocol to provide better protection for dial-up and virtual private network (VPN) connections. With Windows XP SP1, Windows XP SP2, Windows Server 2003, and Windows 2000 SP4, MS CHAP v2 is also an EAP type.</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol (PAP) has two variations: PAP and CHAP PAP. It verifies a user name and password for PPP Internet connections, but it is not as secure as CHAP, since it works only to establish the initial link. PAP is also more vulnerable to attack because it sends authentication packets throughout the network. Nevertheless, PAP is more commonly used than CHAP to log in to a remote host like an Internet service provider.</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest-5 (MD5) is an authentication algorithm developed by RSA. MD5 generates a 128-bit message digest using a 128-bit key, IPSec truncates the message digest to 96 bits.</td>
</tr>
</tbody>
</table>

User Certificate Installation

To install a user certificate (EAP TLS only) and a server certificate for EAP TLS and PEAP authentication:

1. Click Install Certificate. The Credentials dialog box appears.
2. Enter the User:, Pwd: (password), and Server: information in their respective text boxes.

3. Click Retrieve. A Progress dialog indicates the status of the certificate retrieval.

4. Click ok to exit.

After the installation completes, the Installed User Certs dialog box displays and the certificate is available in the drop-down for selection.

![Credentials Dialog Box](image)

Figure 5-10  Credentials Dialog Box

NOTE To successfully install a user certificate, the reader must already be connected to a network from which the server is accessible.

Server Certificate Selection

If the Validate Server Certificate check box is selected, a server certificate is required. Select a certificate on the Installed Server Certificates dialog box. An hour glass may appear as the wizard populates the existing certificate list. If the required certificate is not listed, install it:

1. Click the Install Certificate button.

![Installed Server Certificates Dialog Box](image)

Figure 5-11  Installed Server Certificates Dialog Box

A dialog box appears that lists the currently loaded certificate files found in the default directory (Application directory for Windows CE and all folders for Windows Mobile) with the default extension.
2. Locate a certificate:
   a. For Windows Mobile, select a different folder, if applicable, using the **Folder** drop-down list. Click the certificate filename. The certificate installs automatically.
   b. For Windows CE, navigate to the folder where the certificate is stored. Click the certificate filename and then click **ok**.

3. A confirmation dialog verifies the installation. If the information in this dialog is correct, click the **Yes** button. If the information in this dialog is not correct click the **No** button. The wizard returns to the **Installed Server Certs** dialog box.

![Image](image1.png)

**Figure 5-12** *Browse Server Certificates*

**Credential Cache Options**

If any of the password-based authentication types were selected, select the different credential caching options. These options specify when the network credential prompts appear: at connection, on each resume, or at a specified time.

Entering the credentials directly into the profile permanently caches the credentials. In this case, the reader does not require user login. If a profile does not contain credentials entered through the configuration editor, log in to the reader before connecting.

Caching options only apply on credentials entered through the login dialog box.
If the reader does not have the credentials, it prompts the user to enter a username and password. If the reader has the credentials (previous entered via a login dialog box), it uses these credentials unless the caching options require the reader to prompt for new credentials. If the credentials were entered via the profile, the reader does not prompt for new credentials. Table 5-10 lists the caching options.

**Table 5-10 Cache Options**

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>At Connect</strong></td>
<td>Select this option to prompt for credentials whenever the WCS tries to connect to a new profile. Deselect this to use the cached credentials to authenticate. If the credentials are not cached, a prompt appears to enter credentials. This option only applies when logged in.</td>
</tr>
<tr>
<td><strong>On Resume</strong></td>
<td>Selecting this reauthenticates an authenticated user when a suspend/resume occurs. Once reauthenticated, the user is prompted for credentials. If the user does not enter the same credentials that were entered prior to the suspend/resume within three attempts, the user is disconnected from the network. This option only applies when logged in.</td>
</tr>
<tr>
<td><strong>At Time</strong></td>
<td>Select this option to perform a local verification on an authenticated user at a specified time. The time can be an absolute time or a relative time from the authentication, and should be in at least 5 minute intervals. Once the time has passed, the user is prompted for credentials. If the user does not enter the correct credentials within three attempts, the user is disconnected from the network. This option only applies when logged in.</td>
</tr>
</tbody>
</table>

Entering credentials applies these credentials to a particular profile. Logging out clears all cached credentials. Editing a profile clears all cached credentials for that profile.

The following authentication types have credential caching:

- EAP TLS
- PEAP
- LEAP
- TTLS.

Selecting the **At Time** check box displays the **Time Cache Options** dialog box.
1. Click the Interval radio button to check credentials at a set time interval.

2. Enter the value in minutes in the Min box.

3. Click the At (hh:mm) radio button to check credentials at a set time.

4. Click Next. The At Time dialog box appears.

5. Enter the time using the 24 hour clock format in the (hh:mm) box.

6. Click > to move the time to the right. Repeat for additional time periods.

7. Click Next. The User Name dialog box displays.

**User Name**

The user name and password can be entered (but is not required) when the profile is created. When a profile authenticates with credentials that were entered in the profile, caching rules do not apply. Caching rules only apply on credentials that are entered through the login dialog box.

**Password**

Use the Password dialog box to enter a password. If EAP/TLS is the selected authentication type, the password is not required and the field is disabled.

1. Enter a password in the Password field.

2. Select the Advanced ID check box, if advanced identification is required.
3. Click Next. The Encryption dialog box displays. See Encryption on page 4-17.

Advanced Identity

Use the Advanced ID dialog box to enter the 802.1X identity to supply to the authenticator. This value can be 63 characters long and is case sensitive. In TTLS and PEAP, it is recommended entering the identity anonymous (rather than a true identity) plus any desired realm (e.g., anonymous@myrealm). A user ID is required before proceeding.

NOTE When authenticating with a Microsoft IAS server, do not use advanced identity.

![Advanced Identity Dialog Box](image)

Figure 5-19 Advanced Identity Dialog Box

Click Next. The Encryption dialog box displays.

Encryption

Use the Encryption dialog box to select an encryption type. The drop-down list includes encryption types available for the selected authentication type. See Table 5-12 for these encryption types.

![Encryption Dialog Box](image)

Figure 5-20 Encryption Dialog Box
### Table 5-11  Encryption Options

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Select <em>Open</em> (the default) when no data packet encryption is needed over the network. Selecting this option provides no security for data transmitting over the network.</td>
</tr>
<tr>
<td>40-Bit WEP</td>
<td>Select 40-Bit WEP to use 40-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (10 Hex digit value for 40-bit keys). Use the <em>Key Index</em> drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields. If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 40-bit (10 character) Hex digit string.</td>
</tr>
<tr>
<td>128-Bit WEP</td>
<td>Select 128-Bit WEP to use 128-bit key length WEP encryption. WEP keys are manually entered in the edit boxes. Only the required number of edit boxes for a key length is displayed (26 Hex digit value for 128-bit keys). Use the <em>Key Index</em> drop-down list to configure the four WEP keys. The adapter uses the selected key. Note: The default Hex digit keys are visible any time they are used. As a security precaution after setting the key values for the network, the digits are replaced with asterisks * in the encryption key fields. If the associated AP uses an optional passkey, the active adapter WLAN profile must use one as well. The passkey is a plain text representation of the WEP keys displayed in the encryption dialog box. The passkey provides an easy way to enter WEP key data without having to remember the entire 128-bit (26 character) Hex digit string.</td>
</tr>
<tr>
<td>TKIP</td>
<td>Select this option to use Wireless Protected Access (WPA) via TKIP. Manually enter the shared keys in the passkey field. Click <em>Next</em> to display the passkey dialog box. Enter an 8 to 63 character string.</td>
</tr>
<tr>
<td>AES (Fusion 2.5 only)</td>
<td>Select this option to use Advanced Encryption Standard (AES). Manually enter the shared keys in the passkey field. Click <em>Next</em> to display the passkey dialog box. Enter an 8 to 63 character string.</td>
</tr>
</tbody>
</table>

### Table 5-12  Encryption / Authentication Matrix

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Encryption</th>
<th>WEP</th>
<th>TKIP</th>
<th>AES (Fusion 2.5 only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP TLS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PEAP</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LEAP</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>TTLS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Key Entry Page

If either 40-Bit WEP or 128-Bit WEP is selected the wizard proceeds to the key entry dialog box unless the Use Passkey check box was selected in the Encryption dialog box (see Figure 5-20 on page 5-16). The Key Entry dialog box will be shown only if the authentication is set to None. To enter the key information:

1. Enter the 40-bit or 128-bit keys into the fields.
2. Click Next.

Passkey Dialog

When None is selected as an authentication and WEP as an encryption, choose to enter a passkey by checking the Use PassKey check box. The user is prompted to enter the passkey. For WEP, the Use PassKey checkbox is only available if the authentication is None.

When None is selected as an authentication and TKIP as an encryption, passkey entry is required. The user cannot enter a passkey if the encryption is TKIP and the authentication is anything other than None.

When None is selected as an authentication and AES as an encryption, passkey entry is required. The user cannot enter a passkey if the encryption is AES and the authentication is anything other than None.

Click Next. The IP Address Entry dialog box displays.
**IP Address Entry**

Use the **IP Address Entry** dialog box to configure network address parameters: IP address, subnet, gateway, DNS, and WINS.

![Figure 5-23 IP Address Entry Dialog Box](image)

**Table 5-13 IP Address Entry**

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Select Dynamic Host Configuration Protocol (DHCP) from the <strong>IP Address Entry</strong> drop-down list to obtain a leased IP address and network configuration information from a remote server. DHCP is the default setting for the reader profile. When DHCP is selected, the IP address fields are read-only.</td>
</tr>
<tr>
<td>Static</td>
<td>Select <strong>Static</strong> to manually assign the IP, subnet mask, default gateway, DNS, and WINS addresses the reader profile uses.</td>
</tr>
</tbody>
</table>

Select either **DHCP** or **Static** from the drop-down list and click **Next**. Selecting **Static** displays the **IP Address Entry** dialog box. Selecting **DHCP** displays the **Transmit Power** dialog box.

Use the **IP Address Entry** dialog box to enter the IP address and subnet information.

![Figure 5-24 Static IP Address Entry Dialog Box](image)

**Table 5-14 Static IP Address Entry Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>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 (Internet Protocol 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. Enter the IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.</td>
</tr>
</tbody>
</table>
Select the Advanced check box, then click NEXT to display the Advanced Address Entry dialog box. Enter the Gateway, DNS, and WINS address. Click NEXT without selecting the Advanced check box to display the Transmit Power dialog box.

![Advanced Address Entry Dialog Box](image)

**Figure 5-25  Advanced Address Entry Dialog Box**

The IP information entered in the profile is only used if the Enable IP Mgmt check box is selected in the Options > System Options dialog box (System Options on page 5-36). If this select was not selected, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G/W</td>
<td>The default gateway forwards IP packets to and from a remote destination.</td>
</tr>
<tr>
<td>DNS</td>
<td>The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet email delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located and/or email delivery fails.</td>
</tr>
<tr>
<td>WINS</td>
<td>WINS is a Microsoft® Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.</td>
</tr>
</tbody>
</table>

Click Next. The Transmit Power dialog box displays.
Transmit Power

The Transmit Power drop-down list contains different options for Ad-Hoc and Infrastructure mode. Automatic (i.e., use the current AP settings) and Power Plus (use higher than the current AP settings) are available for Infrastructure mode.

Adjusting the radio transmission power level enables the user to expand or confine the transmission area with respect to other wireless devices that could be operating nearby. Reducing coverage in high traffic areas improves transmission quality by reducing the amount of interference in that coverage area.

![Transmit Power Dialog Box (Infrastructure Mode)](image)

**Figure 5-26  Transmit Power Dialog Box (Infrastructure Mode)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic</td>
<td>Select <strong>Automatic</strong> (the default) to use the AP power level.</td>
</tr>
<tr>
<td>Power Plus</td>
<td>Select <strong>Power Plus</strong> to set the reader transmission power one level higher than the level set for the AP.</td>
</tr>
</tbody>
</table>

![Transmit Power Dialog Box (Ad-Hoc Mode)](image)

**Figure 5-27  Transmit Power Dialog Box (Ad-Hoc Mode)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Select <strong>Full</strong> power for the highest transmission power level. Select <strong>Full</strong> power when operating in highly reflective environments and areas where other devices could be operating nearby, or when attempting to communicate with devices at the outer edge of a coverage area.</td>
</tr>
<tr>
<td>30 mW</td>
<td>Select <strong>30 mW</strong> to set the transmit power level to 30 mW.</td>
</tr>
<tr>
<td>15 mW</td>
<td>Select <strong>15 mW</strong> to set the transmit power level to 15 mW.</td>
</tr>
<tr>
<td>5 mW</td>
<td>Select <strong>5 mW</strong> to set the transmit power level to 5 mW.</td>
</tr>
<tr>
<td>1 mW</td>
<td>Select <strong>1 mW</strong> for the lowest transmission power level. Use this level when communicating with other devices in very close proximity, or in instances where little or no radio interference is expected from other devices.</td>
</tr>
</tbody>
</table>

Click **Next** to display the **Battery Usage** dialog box.
Battery Usage

Use the Battery Usage dialog box to select power consumption of the wireless LAN. There are three settings available: CAM, Fast Power Save, and MAX Power Save. Battery usage cannot be configured in Ad-Hoc profiles.

![Battery Usage Dialog Box](image)

**NOTE** Power consumption is also related to the transmit power settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAM</td>
<td>Continuous Aware Mode (CAM) provides the best network performance, but yields the shortest battery life.</td>
</tr>
<tr>
<td>Fast Power Save</td>
<td>Fast Power Save (the default) performs in the middle of CAM and MAX Power Save with respect to network performance and battery life.</td>
</tr>
<tr>
<td>MAX Power Save</td>
<td>Max Power Save yields the longest battery life while potentially reducing network performance. In networks with minimal latency, Max Power Save performs as well as Fast Power Save, but with increased battery conservation.</td>
</tr>
</tbody>
</table>

Manage Profiles Application

The Manage Profiles window provides a list of user-configured wireless profiles. Define up to 32 profiles at any one time. To open the Manage Profiles window, click the Signal Strength icon > Manage Profiles.

![Manage Profiles Window](image)

Icons next to each profile identify the profile’s current state.
The profiles are listed in priority order for use by the automatic roaming feature. Change the order by moving profiles up or down. To edit existing profiles, click and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the Disable menu item changes to Enable if the profile is already disabled.)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="no-icon.png" alt="Icon" /></td>
<td>Profile is not selected, but enabled.</td>
</tr>
<tr>
<td><img src="disabled.png" alt="Icon" /></td>
<td>Profile is disabled.</td>
</tr>
<tr>
<td><img src="cancelled.png" alt="Icon" /></td>
<td>Profile is cancelled. A cancelled profile is disabled until a connect or login function is performed through the configuration editor.</td>
</tr>
<tr>
<td><img src="infrastructure-not-encrypted.png" alt="Icon" /></td>
<td>Profile is in use and describes an infrastructure profile not using encryption.</td>
</tr>
<tr>
<td><img src="infrastructure-encrypted.png" alt="Icon" /></td>
<td>Profile is in use and describes an infrastructure profile using encryption.</td>
</tr>
<tr>
<td><img src="ad-hoc-not-encrypted.png" alt="Icon" /></td>
<td>Profile is in use and describes an ad-hoc profile not using encryption.</td>
</tr>
<tr>
<td><img src="ad-hoc-encrypted.png" alt="Icon" /></td>
<td>Profile is in use and describes an ad-hoc profile using encryption.</td>
</tr>
<tr>
<td><img src="invalid-regulatory.png" alt="Icon" /></td>
<td>Profile is not valid in the device current operating regulatory domain.</td>
</tr>
</tbody>
</table>

The profiles are listed in priority order for use by the automatic roaming feature. Change the order by moving profiles up or down. To edit existing profiles, click and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the Disable menu item changes to Enable if the profile is already disabled.)

**Table 5-19 Profile Icons**

**Figure 5-30 Manage Profiles Context Menu**

**Changing Profiles**

A completed profile is a set of configuration settings that can be used in different locations to connect to a wireless network. Create different profiles to have pre-defined operating parameters available for use in various network environments. When the WLAN Profiles window displays, existing profiles appear in the list.
Figure 5-31  Manage Profiles

Click and hold a profile and select **Connect** from the pop-up menu to set this as the active profile. Once selected, the reader uses the authentication, encryption, ESSID, IP Config, and power consumption settings configured for that profile.

**Editing a Profile**

Click and hold a profile and select **Edit** from the pop-up menu to display the **Profile Wizard** where the ESSID and operating mode for the profile can be set. Use the **Profile Wizard** to edit the profile power consumption and security parameters. See **Profile Editor Wizard on page 5-5**.

**Creating a New Profile**

To create new profiles from the **Manage Profiles** window, click-and-hold anywhere in this window.

Select **Add** to display the **Profile Wizard** wherein the profile name and ESSID can be set. Set security, network address information, and power consumption level for the new profile.

**Deleting a Profile**

To delete a profile from the list, click and hold and select **Delete** from the pop-up menu. A confirmation dialog box appears.
Ordering Profiles

Click and hold a profile from the list and select **Move Up** or **Move Down** to order the profile. If the current profile association is lost, the reader attempts to associate with the first profile in the list, then the next, until it achieves a new association.

*NOTE*  Profile Roaming must be enabled.

Export a Profile

To export a profile to a registry file, click and hold a profile from the list and select **Export** from the pop-up menu. The **Save As** dialog box displays with the **Application** folder and a default name of WCS_PROFILE{profile GUID}.reg (Globally Unique Identifier).

If required, change the name in the **Name** field and click **Save**. A confirmation dialog box appears after the export completes.

Wireless Status Application

To open the **Wireless Status** window, click the **Signal Strength** icon > **Wireless Status**. The **Wireless Status** window displays information about the wireless connection.
The **Wireless Status** window contains the following options. Click 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 reader.
- **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.

Option windows contain 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, missed beacons, and transmit retry statistics. 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 2 seconds.

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

![Figure 5-35 Signal Strength Window](image)

After viewing the **Signal Strength** window, click the back button to return to the **Wireless Status** window.
The **Current Profile** window displays basic information about the current profile and connection settings. This window updates every two seconds.

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

### Table 5-20  *Signal Strength Status*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal</td>
<td>Displays the Relative Signal Strength Indicator (RSSI) of the signal transmitted between the AP and reader. 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Excellent Signal</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Very Good Signal</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Good Signal</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Fair Signal</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Poor Signal</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Out of Range (no signal)</strong></td>
</tr>
<tr>
<td>Status</td>
<td>Indicates if the reader is associated with the AP.</td>
</tr>
<tr>
<td>Signal Quality</td>
<td>Displays a text format of the Signal icon.</td>
</tr>
<tr>
<td>Tx Retries</td>
<td>Displays a percentage of the number of data packets the reader retransmits. The fewer transmit retries, the more efficient the wireless network is.</td>
</tr>
<tr>
<td>Missed Beacons</td>
<td>Displays a percentage of the amount of beacons the reader missed. The fewer transmit retries, the more efficient the wireless network is. Beacons are uniform system packets broadcast by the AP to keep the network synchronized.</td>
</tr>
<tr>
<td>Signal Level</td>
<td>The AP signal level in decibels per milliwatt (dBm).</td>
</tr>
<tr>
<td>Noise Level</td>
<td>The background interference (noise) level in decibels per milliwatt (dBm).</td>
</tr>
<tr>
<td>SNR</td>
<td>The access point/reader Signal to Noise Ratio (SNR) of signal strength to noise (interference) in decibels per milliwatt (dBm).</td>
</tr>
<tr>
<td>Association Count</td>
<td>Displays the number of APs the reader connects to while roaming.</td>
</tr>
<tr>
<td>AP MAC Address</td>
<td>Displays the MAC address of the AP to which the reader is connected.</td>
</tr>
<tr>
<td>Transmit Rate</td>
<td>Displays the current rate of the data transmission.</td>
</tr>
</tbody>
</table>
The IPv4 Status window displays the current IP address, subnet, and other IP related information assigned to the reader. It also allows renewing the address if the profile is using DHCP to obtain the IP information. Click Renew to initiate a full DHCP discover. The IPv4 Status window updates automatically when the IP address changes.

To open the IPv4 Status window, click IPv4 Status in the Wireless Status window.
### Figure 5-37  IPv4 Status Window

### Table 5-22  IPv4 Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Type</td>
<td>Displays the IP type for the current profile: <strong>DHCP</strong> or <strong>Static</strong>. If the IP type is DHCP, leased IP address and network address data appear for the reader. If the IP type is Static, the values displayed were input manually in the IP Config tab on page 4-19.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the reader’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 as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.</td>
</tr>
<tr>
<td>Subnet</td>
<td>Displays the subnet address. Most TCP/IP networks use subnets to manage routed IP addresses. Dividing an organization's network into subnets allows it to connect to the Internet with a single shared network address, for example, 255.255.255.0.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Displays the gateway address. A gateway forwards IP packets to and from a remote destination.</td>
</tr>
<tr>
<td>DCHP Server</td>
<td>The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet e-mail delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located or e-mail delivery fails.</td>
</tr>
<tr>
<td>Lease Obtained</td>
<td>Displays the date that the IP address was obtained.</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Displays the date that the IP address expires and a new IP address is requested.</td>
</tr>
<tr>
<td>DNS</td>
<td>Displays the IP address of the DNS server.</td>
</tr>
<tr>
<td>WINS</td>
<td>WINS is a Microsoft Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.</td>
</tr>
<tr>
<td>MAC</td>
<td>An IEEE 48-bit address is assigned to the reader at the factory to uniquely identify the adapter at the physical layer.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Displays the name of the reader.</td>
</tr>
</tbody>
</table>
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 (within this instance of the application only). Click the auto-scroll feature to automatically scroll down when a new items is added to the log.

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

![Wireless Log Window](image)

Figure 5-38 Wireless Log Window

Saving a Log

To save a Wireless Log:

1. Click the Save button. The Save As dialog box displays.
2. Navigate to the desired folder.
3. In the Name filed, enter a file name and then click OK. A text file is saved in the selected folder.

Clearing the Log

To clear the log, click Clear.

Versions Window

The Versions window displays software, firmware, and hardware version numbers. This window only updates when it is displayed. There is no need to update constantly. The content of the window is determined at runtime, along with the actual hardware and software to display in the list. Executable paths of the software components on the list are defined in registry, so that the application can retrieve version information from the executable. “File not found” appears if the executable cannot be found at the specified path.

To open the Versions window, click Versions in the Wireless Status window.
The window displays software version numbers for the following:

- Configuration Editor (Fusion 2.4 and lower only)
- Fusion Build
- LoginService
- PublicAPI (Fusion 2.5 and higher only)
- Photon10
- WCConfigED
- WCDiag
- WCLaunch
- WCSAPI
- WCSRV
- WCStatus.

**Wireless Diagnostics Application**

The **Wireless Diagnostics** application window provides links to perform ICMP Ping, Trace Routing, and Known APs. To open the **Wireless Diagnostics** window, click the **Signal Strength** icon > **Wireless Diagnostics**.
Figure 5-40  Wireless Diagnostics Window

The Wireless Diagnostics window contains the following options. Click 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 reader and any place on the network.
- Known APs - displays the APs in range using the same ESSID as the reader.
- 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 a connection at the network layer (part of the IP protocol) between the reader and an AP. Ping tests only stop when the Stop Test button is clicked, close the Wireless Diagnostics application, or if the reader switches between infrastructure and ad-hoc modes.

To open the ICMP Ping window, click ICMP Ping in the Wireless Diagnostics window.

Figure 5-41  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. Click Start Test. The ICMP Ping test starts. Information of the ping test displays in the appropriate fields.
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 reader and any place on the network.

To open the Trace Route window, click Trace Route in the Wireless Diagnostics window.

![Trace Route Window](image)

Figure 5-42 Trace Route Window

Enter an IP address or a DNS Name in the IP combo box, and click Start Test. The IP combo box should match the information shown in the ICMP Ping window’s IP combo box. When starting a test, the trace route attempts to find all routers between the reader and the destination. The Round Trip Time (RTT) between the reader and each router appears, along with the total test time. The total test time may be longer than all RTTs added together because it does not only include time on the network.

Known APs Window

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

![Known APs Window](image)

Figure 5-43 Known APs Window
See Table 5-23 for the definitions of the icons next to the AP.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon 1" /></td>
<td>The AP is the associated access point, and is set to mandatory.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon 2" /></td>
<td>The AP is the associated access point, but is not set to mandatory.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon 3" /></td>
<td>The reader is not associated to this AP, but the AP is set as mandatory.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon 4" /></td>
<td>The reader is not associated to this AP, and AP is not set as mandatory.</td>
</tr>
</tbody>
</table>

Click and hold on an AP to display a pop-up menu with the following options: Set Mandatory and Set Roaming. Select Set Mandatory to prohibit the reader from associating with a different AP. The letter M displays on top of the icon. The reader connects to the selected AP and never roams until:

- Select Set Roaming
- The reader roams to a new profile
- The reader suspends
- The reader resets (warm or cold).

Select Set Roaming to allow the reader to roam to any AP with a better signal. These settings are temporary and never saved to the registry.

Click Refresh to update the list of the APs with the same ESSID. The highest signal strength value is 32.

### Options

Use the wireless Option dialog box to select one of the following operation options from the drop-down list:

- Operating Mode Filtering
- Regulatory
- Band Selection
- System Options
- Change Password
- Export

### Operating Mode Filtering

The Operating Mode Filtering options cause the Find WLANs application to filter the available networks found.

![Figure 5-44](image5) OP Mode Filtering Dialog Box
The **AP Networks** and **Ad-Hoc Networks** check boxes are selected by default.

### Table 5-24  OP Mode Filtering Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Networks</td>
<td>Select the <strong>AP Networks</strong> check box to display available AP networks and their signal strength within the <strong>Available WLAN Networks</strong> (see <em>Find WLANs Application on page 5-4</em>). These are the APs available to the reader profile for association. If this option was previously disabled, refresh the <strong>Available WLAN Networks</strong> window to display the AP networks available to the reader.</td>
</tr>
<tr>
<td>AD-Hoc Networks</td>
<td>Select the <strong>Ad-Hoc Networks</strong> check box to display available peer (adapter) networks and their signal strength within the <strong>Available WLAN Networks</strong>. These are peer networks available to the reader profile for association. If this option was previously disabled, refresh the <strong>Available WLAN Networks</strong> window to display the Ad Hoc networks available to the reader.</td>
</tr>
</tbody>
</table>

Click **Save** to save the settings or click **X** to discard any changes.

### Regulatory Options

Use the **Regulatory** settings to configure the country the reader is in. Due to regulatory requirements (within a country) a reader is only allowed to use certain channels.

![Regulatory Options Dialog Box](image)

### Table 5-25  Regulatory Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Select the country from the drop-down list. To connect to a profile, the profile country must match this setting, or the AP country setting (if the <strong>Enable 802.11d</strong> check box is selected).</td>
</tr>
<tr>
<td>Enable 802.11d</td>
<td>The WLAN adapter attempts to retrieve the country from APs. Profiles which use <strong>Infrastructure</strong> mode can only connect if the country set is the same as the AP country settings or if the profile country setting is <strong>Allow Any Country</strong>. All APs must be configured to transmit the country information.</td>
</tr>
</tbody>
</table>
Band Selection

The Band Selection settings identify the frequency bands to scan when finding WLANs. These values refer to the 802.11 standard networks.

\[NOTE\] Select one band for faster access when scanning for WLANs.

![Band Selection Dialog Box](image)

**Table 5-26 Band Selection Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz Band</td>
<td>The Find WLANs application list includes all networks found in the 2.4 GHz band (802.11b and 802.11g).</td>
</tr>
<tr>
<td>5GHz Band</td>
<td>The Find WLANs application list includes all networks found in the 5 GHz band (802.11a).</td>
</tr>
</tbody>
</table>

Click Save to save the settings or click X to discard any changes.

System Options

Use System Options to set miscellaneous system setting.

![System Options Dialog Box](image)

**Table 5-27 System Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Roaming</td>
<td>Configures the reader to roam to the next available WLAN profile when it moves out of range of the current WLAN profile.</td>
</tr>
<tr>
<td>Enable IP Mgmt</td>
<td>Enables the Wireless Companion Services to handle IP address management. The Wireless Companion Service configures the IP based on what is configured in the network profile. Deselect this to manually configure the IP in the standard Windows IP window. Enabled by default.</td>
</tr>
<tr>
<td>Auto Time Config</td>
<td>Enables automatic update of the system time. Network association updates the device time based on the time set in the AP. This proprietary feature is only supported with Zebra infrastructure. Enabled by default.</td>
</tr>
</tbody>
</table>
Change Password

Use Change Password to require a password before editing a profile. This allows pre-configuring profiles and prevents users from changing the network settings. The user can use this feature to protect settings from a guest user. By default, the password is not set.

![Change Password Window](image)

**Figure 5-48 Change Password Window**

To create a password for the first time, leave the **Current**: text box empty and enter the new password in the **New**: and **Confirm**: text boxes. Click **Save**.

To change an existing password, enter the current password in the **Current**: text box and enter the new password in the **New**: and **Confirm**: text boxes. Click **Save**.

To delete the password, enter the current password in the **Current**: text box and leave the **New**: and **Confirm**: text boxes empty. Click **Save**.

✓ **NOTE** Passwords are case sensitive and can not exceed 160 characters.
Export

**NOTE** For Windows CE 5.0 devices, exporting options enables settings to persists after cold boot. For Mobile 5.0 devices, exporting options enables settings to persists after clean boot. See Persistence on page 5-39 for more information.

Use Export to export all profiles to a registry file, and to export the options to a registry file.

![Options - Export Dialog Box](image)

Figure 5-49  Options - Export Dialog Box

To export options:

1. Click Export Options. The **Save As** dialog box displays.

![Save As Dialog Box](image)

Figure 5-50  Export Options Save As Dialog Box

2. Enter a filename in the **Name:** field. The default filename is WCS_OPTIONS.REG.

3. Click Save.

To export all profiles:

1. Click Export All Profiles. The **Save As** dialog box displays.

![Save As Dialog Box](image)

Figure 5-51  Export All Profiles Save As Dialog Box

2. Enter a filename in the **Name:** field. The default filename is WCS_PROFILES.REG.

3. In the **Folder:** drop-down list, select the desired folder.

4. Click Save.

Selecting Export All Profiles saves the current profile. This information is used to determine which profile to connect with after a warm boot or cold boot.
Persistence

Export options and profiles to provide cold boot persistence for Windows CE 5.0 devices and clean boot persistence for Mobile 5.0 devices. Save the exported registry files in the Application folder to use them on a cold boot or clean boot and restore previous profile and option settings.

Currently, only server certificates can be saved for persistence. To save server certificates for persistence, save the certificate files in the folder Application to install the certificates automatically on a cold or clean boot.

\NOTE User certificates cannot be saved for cold boot or clean boot persistence at this time.

Registry Settings

Use a registry key to modify some of the parameters. The registry path is:

HKLM\SOFTWARE\Symbol Technologies, Inc.\Configuration Editor

Table 5-28  Registry Parameter Settings

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CertificateDirectory</td>
<td>REG_SZ</td>
<td>\Applications</td>
<td>The default directory to find certificates.</td>
</tr>
</tbody>
</table>
| EncryptionMask    | REG_DWORD | 0x0000001F | Defines the supported encryption types. This is a bitwise mask with each bit corresponding to an encryption type.  
1 = Type is supported  
0 = Type is not supported  
  | Bit Number | Encryption Type |
  | 0         | None          |
  | 1         | 40-Bit WEP    |
  | 2         | 128-Bit WEP   |
  | 3         | TKIP          |
  | 4         | AES (Fusion 2.5 and higher only) |
Log On/Off Application

When the user launches the Log On/Off application, the reader may be in two states; the user may be logged onto the reader by already entering credentials through the login box, or there are no user logged on. Each of these states have a separate set of use cases and a different look to the dialog box.

User Already Logged In

If already logged into the reader, the user can launch the login dialog box for the following reasons:

• Connect to and re-enable a cancelled profile. To do this:
  • Launch the Log On/Off dialog.
  • Select the cancelled profile from the profile list.
  • Login to the profile.

✓ NOTE Re-enable cancelled profiles using the Profile Editor Wizard and choosing to connect to the cancelled profile. Cancelled profiles are also re-enabled when a new user logs on.

• Log off the reader to prevent another user from accessing the current users network privileges.
• Switch reader users to quickly logoff the reader and allow another user to log into the reader.

No User Logged In

If no user is logged into the reader, launch the login dialog box and log in to access user profiles.

The Login dialog box varies if it is:

• Launched by WCS, because the service is connecting to a new profile that needs credentials.
• Launched by WCS, because the service is trying to verify the credentials due to credential caching rules.
• Launched by a user, when a user is logged in.
• Launched by a user, when no user is logged in.

Table 5-29 Log On/Off Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Profile Field</td>
<td>When launching the login application, the Wireless Profile field has available all the wireless profiles that require credentials. This includes profiles that use EAP TLS, PEAP, LEAP, and EAP-TTLS.</td>
</tr>
<tr>
<td>Profile Status Icon</td>
<td>The profile status icon (next to the profile name) shows one of the following states: The selected profile is cancelled. The selected profile is enabled but is not the current profile. The profile is the current profile (always the case for WCS Launched).</td>
</tr>
</tbody>
</table>
Click **OK** to send the credentials through WCS API. If there are no credentials entered, a dialog box displays informing the user which field was not entered.

The **Log Off** button only displays when a user is already logged on. When the **Log Off** button is clicked, the user is prompted with three options: Log Off, Switch Users, and Cancel. Switching users logs off the current user and re-initialize the login dialog box to be displayed for when there is no user logged on. Logging off logs off the current user and close the login dialog box. Click **Cancel** to close the Log Off dialog box.

When the user is logged off, the reader only roams to profiles that do not require credentials or to profiles that were created with the credentials entered into the profile.

The **Cancel** button closes the dialog without logging into the network. If the login dialog was launched by the WCS and not by the user, clicking **Cancel** displays a message box to display a warning that the cancel disables the current profile. If the user still chooses to cancel the login at this point, the profile is cancelled.

Once a profile is cancelled, the profile is suppressed until a user actively re-enables it or a new user logs onto the reader.

---

### Table 5-29  Log On/Off Options (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Username and Password Fields</td>
<td>The Network Username and Network Password fields are used as credentials for the profile selected in the Wireless Profile field. Currently these fields are limited to 159 characters.</td>
</tr>
<tr>
<td>Mask Password Checkbox</td>
<td>The <em>Mask Password</em> checkbox determines whether the password field is masked (i.e., displays only the ‘*’ character) or unmasked (i.e., displays the entered text). Check the box to unmask the password. Uncheck the box to mask the password (the default).</td>
</tr>
<tr>
<td>Status Field</td>
<td>The status field displays status that is important to the login dialog. If the user opens the dialog and needs to prompt for credentials for a particular profile at this time, it can use the status field to let the user know that the network is held up by the password dialog being open.</td>
</tr>
</tbody>
</table>
Chapter 6 Application Deployment for WinCE 5.0

Software Installation on Development PC

The following applications can be used to develop applications to run on the Windows CE RFID reader:

- Microsoft Visual Studio 2005 (or) Microsoft eVC++
- Symbol Mobility Developer Kit (SMDK) for C
- Windows CE Platform SDK for 9090c50
- Device Configuration Package DCP for RD5000

✓ **NOTE** The RD5000 uses the Windows CE Platform SDK for 9090c50 and the DCP for RD5000.

The SMDK for C is a development tool used to create native C and C++ applications for all Zebra RFID readers. It includes documentation, header files (.H), and library files (.LIB) for native code application development that targets Zebra value-add APIs.

The Windows CE Platform SDK for the MC9090c50 is used in conjunction with the SMDK for C to create Windows CE applications for the RD5000 RFID reader. The SMDK for C Upgrade Patch for RFID, adds the latest API functionality to the application development platform (see the Support Central web site, [http://support.symbol.com](http://support.symbol.com) for the latest updates). The Platform SDK installs a new Windows CE device type and its associated libraries onto the development PC. This new device is added to the Active WCE Configuration field of Microsoft eMbedded Visual C++ 4.0.

The Device Configuration Package (DCP) is required to create and download hex images that represent flash partitions to the RFID reader. The DCP includes the user documentation, flash partitions, Terminal Configuration Manager (TCM) and the associated TCM scripts.
**Required System Configurations**

The minimum system configuration required to use the SMDK for C and DCP for RD5000 is:

- IBM-compatible host computer with Pentium 450 MHz processor or higher
- Microsoft Windows XP or Microsoft Windows 2000 operating system
- 128 MB RAM and 200 MB available hard disk space
- CD-ROM drive
- One available serial port and one available USB port
- Mouse
- Adobe® Acrobat® Reader® 3.0 or higher, available at the Microsoft web site: [http://www.microsoft.com](http://www.microsoft.com)
- Microsoft ActiveSync version 4.0 or higher, available at the Microsoft web site: [http://www.microsoft.com](http://www.microsoft.com)
- Microsoft Embedded Visual C++ v4.0 with SP2
- Microsoft Windows Mobile 2005 SDK

**DCP for RD5000**

There are two ways to download the *DCP for RD5000*, the Top-down method and the Search method:

**The Top-down method, DCP for RD5000 download:**

1. Go to the Support Central web site, [http://support.symbol.com](http://support.symbol.com):
2. On the *Welcome to Support Central* web page, select: **Software Downloads**.
3. On the **Software Downloads** web page select: **RFID**.
4. On the **RFID** web page select: **RD5000**.
5. On the **RD5000** web page, under **Software Downloads**: select **RD5000 RFID Reader DCP Software**.

**The Search method, for the DCP for RD5000 download (see Figure 6-1):**

1. Go to the Support Central website, [http://support.symbol.com](http://support.symbol.com):
2. On the *Welcome to Support Central* web page, enter the following information into the search box:
3. Search: Device Configuration Package for RD5000
4. Product Line: RFID
5. Product: RD5000
6. Document Type: Software Downloads

**Figure 6-1  Support Central Web Site DCP Search Window**

7. Select: **RD5000 RFID Reader DCP Software**
To install the DCP for RD5000:

1. Save the .exe file to the development computer.
2. Locate the .exe file on the development computer, double-click the file, and follow the install screen prompts.

Components

*Table 6-1* lists the DCP components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Directory Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files that make up the flash partitions</td>
<td>Used to configure the terminal.</td>
<td>\Program Files\Symbol Device Configuration Packages\RD5000c50\v1.1\Flash Folders</td>
</tr>
<tr>
<td>Hex image - default location</td>
<td>Loads onto the RFID reader for configuration.</td>
<td>\Program Files\Symbol Device Configuration Packages\RD5000c50\v1.1\Hex Images</td>
</tr>
<tr>
<td>User Documentation</td>
<td>User manuals that provide guidance on using and integrating the RD5000.</td>
<td>\Program Files\Symbol Device Configuration Packages\RD5000c50\v1.1</td>
</tr>
<tr>
<td>Readme</td>
<td>Contains important information for the DCP.</td>
<td>\Program Files\Symbol Device Configuration Packages\RD5000c50\v1.1</td>
</tr>
<tr>
<td>Scripts</td>
<td>Used to customize flash partitions.</td>
<td>\Program Files\Symbol Device Configuration Packages\RD5000c50\v1.1\TCM Scripts</td>
</tr>
<tr>
<td>Terminal Configuration Manager (TCM)</td>
<td>An application used to customize flash file system partitions for the RFID reader.</td>
<td>\Program Files\Symbol\TCM2</td>
</tr>
<tr>
<td>Tools (ex Keyboard remap, if any)</td>
<td>Used in developing applications for the RFID reader.</td>
<td>\Program Files\Symbol Device Configurations package\RD5000c50\v1.1\Tools\kbtool</td>
</tr>
<tr>
<td>Start Menu: Readme User Documentation TCM WEB Updates</td>
<td>Specifies items to appear in the Start menu.</td>
<td>\Documents and Settings\All Users\Start Menu\Programs</td>
</tr>
</tbody>
</table>
Platform SDK

There are two ways to download the Platform SDKs that are required for the Microsoft® Windows CE 5.0 Professional and Microsoft® Windows CE 5.0 Core platforms, the Top-down method and the Search method:

The Top-down method, SDK download:

1. Go to the Support Central web site, http://support.symbol.com:
3. On the Software Downloads web page select: RFID.
5. On the RD5000 web page, under Software Downloads select: Platform SDK for 9090c50.

The Search method, for the SDK download (see Figure 6-2):

1. Go to the Support Central website, http://support.symbol.com:
2. On the Welcome to Support Central web page, enter the following information into the search box:
   - Search: SDK
   - Product Line: RFID
   - Product: RD5000
   - Document Type: Software Downloads
3. Select: Platform SDK for 9090c50

Figure 6-2  Support Central Web Site SDK Search Window
Symbol Mobility Developer Kits

There are two ways to download the SMDK, the Top-down method and the Search method:

The Top-down SMDK download method:

1. Go to the Support Central web site, http://support.symbol.com:
3. On the Software Downloads web page select: RFID.
5. On the RD5000 web page, under Software Downloads select: Symbol Mobility Developer Kit.
6. Select the latest version, then download the .exe file to the development computer.

The Search for the SMDK download method (see Figure 6-3):

1. Go to the Support Central website, http://support.symbol.com:
2. On the Welcome to Support Central web page, enter the following information into the search box:
   Search: Symbol Mobility Developer Kit
3. Product Line: RFID
4. Product: RD5000
5. Document Type: Software Downloads

   Figure 6-3   Support Central Web Site SMDK Search Window

6. Select: Symbol Mobility Developer Kit

To Install The SMDK:

1. Double-click the executable file and follow the install screen prompts.
2. Once installed, access the major components of the SMDK for C or .NET from the Symbol Mobility Developer Kit for C or .NET program group of the Windows Start Menu. The components include: Help, Platform Integrator, Readme, Samples, and Web Updates.
3. The sample applications provide examples of how to interface with the Symbol API functions. To build a sample application, open the Samples folder from the Windows Start menu. Open the folder for the desired sample and then open the project file. The project file has an extension of VCP. Microsoft Visual C++ v4.0 automatically launches. Select device as MC9090c50, select WinCE as the Active WCE Configuration. Select Win32 (WCE ARMv4I) debug or release as the Active Configuration.
**SMDK for C Contents and Locations**

*Table 6-2* lists the components of the SMDK for C.

<table>
<thead>
<tr>
<th>Components</th>
<th>Directory Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Help file and Readme file</td>
<td>\Program Files\Symbol Mobility Developer Kit v.x.x for C\</td>
</tr>
<tr>
<td>Sample applications for quick-start development</td>
<td>\Program Files\Symbol Mobility Developer Kit v.x.x for C\Samples\C\Standard</td>
</tr>
<tr>
<td>Header files with API prototypes and structures*</td>
<td>\Program Files\Windows CE Tools\wce420\WinCE\Include\armv4 and \Program Files\Windows CE Tools\wce500\MC9090c50\Include\Armv4i</td>
</tr>
<tr>
<td>Import Library files</td>
<td>\Program Files\Windows CE Tools\wce500\MC9090c50\Lib\ARMV4I</td>
</tr>
<tr>
<td>Start Menu Readme Help Platform Integrator Samples WEB Updates</td>
<td>\Documents and Settings\All Users\Start Menu\Programs</td>
</tr>
</tbody>
</table>

**SMDK Patch for RD5000**

The latest RFID SMDK updates and the latest RFID patch for SMDK updates are currently available on the Support Central website, [http://support.symbol.com](http://support.symbol.com). Instructions on how to use the patch are available with patch download.

**Installing Other Development Software**

Developing applications for the RFID reader may require installing other development software such as application development environments on the development PC. Follow the installation instructions provided with this software.

**Software Updates**

Download updates to the SMDK for C from the Support Central website, [http://support.symbol.com](http://support.symbol.com). Check this site periodically for important updates and new software versions.
Deployment

With the appropriate accessory, software, and connection, the RFID reader can share information with the host device. This chapter provides information about installing software and files on the RFID reader.

Download/Install software using:

- ActiveSync
- AirBEAM

ActiveSync

Use ActiveSync to copy files from a host computer to the RFID reader.

1. Ensure that ActiveSync is installed and that a partnership has been created, see Chapter 4, ActiveSync.
2. Connect the RFID reader to the host computer using a USB cradle or an appropriate cable, see Chapter 3, Accessories for connection information.
3. On the host computer, select Start > Programs > ActiveSync. On the host computer, select Start - Programs - ActiveSync.

4. Select Explore.
5. Double-click the folder to expand the contents of the folder.

6. Use Explorer to locate the host computer directory that contains the file to download. Tap that directory in the left pane to display its contents in the right pane.

7. Drag the desired file(s) from the host computer to the desired mobile device folder.
   - *Program Files* folder: files stored in this folder are discarded after a cold boot.
   - *Application* folder: files stored in this folder are retained after a cold boot.
Adding Programs

Install the appropriate software on the host computer before installing it on the RFID reader:

1. Download the program to the host computer (or insert the CD or disk that contains the program into the host computer). The program may consist of a single *.exe file, a *.zip file, or a Setup.exe file.

2. Read any installation instructions, Read Me files, or documentation that comes with the program. Many programs provide special installation instructions.

3. Connect the RFID reader to the host computer.

4. Double-click the executable file on the host computer.
   - If the file is an installer, the installation wizard begins. Follow the directions on the window. Once the software is installed on the host computer, the installer transfers the software to the RFID reader.
   - If the file is not an installer, an error message states that the program is valid but is designed for a different type of computer. Move this file to the RFID reader. Follow the installation instructions for the program in the Read Me file or documentation, or use ActiveSync Explore to copy the program file to the Program Files folder on the terminal as described in Deployment on page 6-7. For more information on copying files using ActiveSync, see ActiveSync Help.

5. When installation is complete, click Start - Programs on the terminal, then click the program icon.

Adding a Program from the Internet

1. Download the program to the RFID reader from the Internet using Internet Explorer.

2. Read any installation instructions, Read Me files, or documentation that comes with the program. Many programs provide special installation instructions.

3. Click the file, such as a *.zip or *.exe file, to launch the installation wizard. Follow the directions on the window.
Creating Hex Images

Terminal Configuration Manager (TCM) is an application used to customize flash file system partitions for the RFID reader. The most common use is to create an application partition hex file that contains the customer’s application. TCM can also be used to load hex files to the flash memory of the RFID reader.

The customization of partitions is controlled by TCM scripts. The scripts contain all of the necessary information for building an image. The script is a list of copy commands specifying the files to copy from the development computer to the partition.

TCM works with a pair of directory windows, one displaying the script and the other displaying the source files resident on the development computer. Using standard windows drag and drop operations, files can be added and deleted from the script window.

The DCP for RD5000 includes scripts used by Zebra to build the standard factory installed Platform and Application partitions provided on the RFID reader. The standard Platform partition contains drivers while the Application partition contains demo applications and optional components. The standard TCM scripts can be found in the following folder: C:\Program Files\Symbol Device Configuration Packages\RD5000c50\V1.1\TCMScripts.

**NOTE** Before creating a script to build a hex image, identify the files required (system files, drivers, applications, etc.) and locate the files’ source directories to make the script building process easier.

The required processes for building a hex image in TCM include:

- Starting Terminal Configuration Manager
- Defining Script Properties
- Creating The Script For The Hex Image
- Building The Image
- Sending The Hex Image
- Software Upgrade Using The OSUpdate Utility
- Flash storage
Starting Terminal Configuration Manager

Click the Windows start menu TCM icon (Symbol Device Configuration Packages, RD5000) to start TCM. The TCM window appears displaying two child windows: Script1 and File Explorer. The Script1 window contains a newly created script and the File Explorer window contains a file explorer view used for selecting files to be placed in the script.

Figure 6-7  TCM Startup Window

The following table lists the components of the TCM window.

Table 6-3  TCM Components

<table>
<thead>
<tr>
<th>Icon</th>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Script1" /></td>
<td>Script Window</td>
<td>Displays the files to be used in the creation of the partition(s).</td>
</tr>
<tr>
<td><img src="image" alt="File Explorer" /></td>
<td>File Explorer Window</td>
<td>Used to select the files to be added to the script.</td>
</tr>
<tr>
<td><img src="image" alt="Create button" /></td>
<td>Create button</td>
<td>Create a new script file.</td>
</tr>
<tr>
<td><img src="image" alt="Open button" /></td>
<td>Open button</td>
<td>Open an existing script file.</td>
</tr>
</tbody>
</table>
Table 6-3  *TCM Components*  (Continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Save button</td>
<td>Save the current script file.</td>
</tr>
<tr>
<td></td>
<td>Large icons button</td>
<td>View the current script items as large icon.</td>
</tr>
<tr>
<td></td>
<td>Small icons button</td>
<td>View the current script items as small icon.</td>
</tr>
<tr>
<td></td>
<td>List button</td>
<td>View the current script items as a list.</td>
</tr>
<tr>
<td></td>
<td>Details button</td>
<td>View the current script items with more details.</td>
</tr>
<tr>
<td></td>
<td>About button</td>
<td>Display version information for TCM.</td>
</tr>
<tr>
<td></td>
<td>Properties button</td>
<td>View/change the current script properties.</td>
</tr>
<tr>
<td></td>
<td>Build button</td>
<td>Build the current script into a set of hex files.</td>
</tr>
<tr>
<td></td>
<td>Check button</td>
<td>Check the script for errors (files not found).</td>
</tr>
</tbody>
</table>
Defining Script Properties

Before a script is created, the script properties must be defined. This defines the type of RFID reader, flash type, number of disks being created and the memory configuration of each disk partition.

To define the script properties:

1. Select the Script window to make it active.

2. Click the Properties button. The Script Properties window > Partition Data tab appears.

3. In the Terminal drop-down list, select the terminal type.

4. Use the default Flash Type.

Table 6-3  TCM Components  (Continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Component</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Send button" /></td>
<td>Send button</td>
<td>Download the hex image to the RFID reader.</td>
</tr>
<tr>
<td><img src="image" alt="Tile button" /></td>
<td>Tile button</td>
<td>Arrange the sub-windows in a tiled orientation.</td>
</tr>
<tr>
<td><img src="image" alt="Build and Send" /></td>
<td>Build and Send</td>
<td>Build the current script into a set of hex images and send the hex images to the RFID reader.</td>
</tr>
<tr>
<td><img src="image" alt="Preferences button" /></td>
<td>Preferences button</td>
<td>View/change the global TCM options.</td>
</tr>
</tbody>
</table>

Figure 6-8  Script Properties Window - Partition Data Tab
5. In the **Disks** drop-down list, select the number of disk partitions to create.

6. Select the (**memory**) **Size** for each partition. Note that adding space to one disk partition subtracts it from another.

7. In the **Access** drop-down list for each disk partition, determine and select the Read/Write access option.

8. Click the **Options** tab. The **Script Properties window > Options** tab appears.

![Figure 6-9 Script Properties Window - Options Tab](image)


10. Click **OK**.

### Creating The Script For The Hex Image

On start-up, **TCM** displays the **TCM** window with the **Script1 window** and **File Explorer window** pointing to the following directory:

```
\Program Files\Symbol Device Configuration Packages\RD5000c50\v1.1\TCMScripts\
```

The **Script1 window** directory pane displays two partitions: **Platform** and **Application**. Depending on the type of flash chip, the number of partitions may change. Files can be added to each of the partitions. **TCM** functionality includes:

- Opening a new or existing script file
- Copying components to the script window
- Saving the script file.

### Opening a New or Existing Script

A script file can be created from scratch or based on an existing script file. Click **Create** to create a new script or click **Open** to open an existing script (for example, a script provided in the DCP for RD5000). If an existing script is opened and changes are made, saving the changes overwrites the original script. To use an original or Zebra supplied standard script as a base and save the changes in a new script, use the **Save As** function to save the script using a different file name.
Copying Components to the Script

Script contents are managed using standard file operations such as **New Folder**, **Delete** and **Rename**. Items can be added to the script by clicking files and folders in the **File Explorer** window and dragging them to the **Script** window. The **File Explorer** window supports standard windows; multiple files may be selected by clicking while holding the **SHIFT** or **CTRL** keys.

Saving the Script

Modifications to a script file can be saved using the **Save** or the **Save As** function. Saving changes to an existing script writes over the original script. To use a Zebra-supplied standard script as a base and save the changes in a new script, use the **Save As** function.

Building the Image

Once the script is created, the hex image defined by the script can be built.

As part of the build, TCM performs a check on the script which verifies that all files referenced in the script exist. This check is important for previously created scripts to ensure that files referenced in the script are still in the designated locations.

To build scripts:

1. Click **Build** on the TCM toolbar. The **Configure Build** window appears.

   ![Configure Build Window](image)

   **Figure 6-10  Configure Build Window**

2. Select the items (partitions) to build using the check box(es) to the left of each named partition.

3. The **Build Path** defines where to store all built partitions.

4. Select (hex image) **COMPRESSION** to reduce the size and speed up the download.

5. Click **OK** and follow the on-screen instructions.

   If one of the partitions being built is the ESSID, a prompt appears requesting the ESSID value. Deselect the **HR (High Rate)** check box when building ESSID images for a device with an FH radio.
If one of the partitions being built is the Splash Screen, a prompt appears requesting both the source Bitmap file and the destination HEX file.

1. A check is performed and if there are no errors, the partition hex files are created.

If the build fails, the hex files are not be created and TCM displays an error message. Two of the most common reasons for a build failure are:

- Files defined in the script can not be found. This error can occur when the files referenced by the script are no longer stored on the development computer or the folders where they are stored were renamed.

- The total amount of flash memory space required by the script exceeds the image size. To correct this, reduce the number of files in the partition or increase the size of the partition. See Defining Script Properties on page 6-13 for more information about setting the image size appropriately.

### Downloading Partitions to the RFID Reader

The two methods for downloading partitions to the RD5000 are using the OSUpdate Utility (see Software Upgrade Using The OSUpdate Utility on page 6-16) and using AirBEAM Smart (see AirBEAM Smart on page 6-19).

### Software Upgrade Using The OSUpdate Utility

Use the Software Upgrade Using the OSUpdate Utility to copy the OSUpdate folder from DCP installation v1.1 directory (C:\Program Files\Symbol Device Configuration Packages\RD5000c50\V1.1) in to temp folder of the RD5000 device. To copy entire folder, set the memory allocation to 31MB for each program and storage memory.

1. Run OSUpdate utility by double clicking on RD5kc50BenColor_TEMP file on RD5000. A remote control tool like pocket controller can be used. The file is in the path \temp\OSUpdate on device.

2. Installation takes few minutes and device cold boots after completing the installation.

3. The firmware has to be flashed to appropriate devices using appropriate applications.

**Example:**

Latest MPS firmware - Mega16_Serial_x_xx.hex needs to be downloaded through AtmelFlasher.exe. Both the files would be available in \Application Folder.
Flash Storage

In addition to the RAM-based storage standard on Windows CE RFID readers, the RFID reader is also equipped with a non-volatile Flash-based storage area which can store data (partitions) that can not be corrupted by a cold boot. This Flash area is divided into two categories: Flash File System (FFS) Partitions and Non-FFS Partitions.

FFS Partitions

The RFID reader includes two FFS partitions. These partitions appear to the RFID reader as a hard drive that the OS file system can write files to and read files from. Data is retained even if power is removed.

The two FFS partitions appear as two separate folders in the Windows CE file system and are as follows:

- **Platform**: The Platform FFS partition contains Zebra-supplied programs and Dynamic Link Libraries (DLLs). This FFS is configured to include DLLs that control system operation. Since these drivers are required for basic RFID reader operation, only experienced users should modify the content of this partition.

- **Application**: The Application FFS partition is used to store application programs needed to operate the RFID reader.

Working with FFS Partitions

Because the FFS partitions appear as folders under the Windows CE file system, they can be written to and read like any other folder. For example, an application program can write data to a file located in the Application folder just as it would to the Windows folder. However, the file in the Application folder is in non-volatile storage and is not lost on a cold boot (see *Performing a Cold Boot on page 1-16*).

Standard tools such as ActiveSync can be used to copy files to and from the FFS partitions. They appear as the “Application” and “Platform” folders to the ActiveSync explorer. This is useful when installing applications on the RFID reader. Applications stored in the Application folder are retained even when the RFID reader is cold booted, just as the Demo 9000 program is retained in memory.

There are two device drivers included in the Windows CE image to assist developers in configuring the RFID reader following a cold boot: RegMerge and CopyFiles.

RegMerge.dll

RegMerge.dll is a built-in driver that allows registry edits to be made to the Windows CE Registry. Regmerge.dll runs very early in the boot process and looks for registry files (.reg files) in certain Flash File System folders during a cold boot. It then merges the registry changes into the system registry located in RAM.

Since the registry is re-created on every cold boot from the default ROM image, the RegMerge driver is necessary to make registry modifications persistent over cold boots.

RegMerge is configured to look in the root of two specific folders for .reg files in the following order:

```
\Platform
\Application
```

Regmerge continues to look for .reg files in these folders until all folders are checked. This allows folders later in the list to override folders earlier in the list. This way, it is possible to override Registry changes made by the Platforms partitions folders. Take care when using Regmerge to make Registry changes. The DCP for RD5000 contains examples of .reg files.

**NOTE** Regmerge only merges the .reg files on cold boots. The merge process is skipped during a warm boot.
Typically, do not make modifications to registry values for drivers loaded before RegMerge. However, these values may require modification during software development. Since these early loading drivers read these keys before RegMerge gets a chance to change them, the RFID reader must be cold booted. The warm boot does not re-initialize the registry and the early loading driver reads the new registry values.

Do not use Regmerge to modify built-in driver registry values, or merge the same Registry value to two files in the same folder, as the results are undefined.

**CopyFiles**

Windows CE expects certain files to be in the Windows folder, residing in volatile storage. Windows CE maintains the System Registry in volatile storage. CopyFiles copies files from one folder to another on a cold boot. Files can be copied from a non-volatile partition (Application or Platform) to the Windows or other volatile partition during a cold boot. During a cold boot CopyFiles looks for files with a .CPY extension in the root of the Platform and Application FFS partitions (Platform first and then Application). These files are text files containing the source and destination for the desired files to be copied separated by “>”. The following example from the file application.cpy is contained on the demo application partition included in the DCP for RD5000. It can also be obtained from the Support Central web site at [http://support.symbol.com/](http://support.symbol.com/).

Files are copied to the Windows folder from the Flash File System using copy files (*.cpy) in the following order:

- \Platform
- \Application

Example:

\Application\ScanSamp2.exe>\Windows\ScanSamp2.exe

This line directs CopyFiles to copy the ScanSamp2.exe application from the \Application folder to the \Windows folder.

**Non-FFS Partitions**

Non-FFS Partitions include additional software and data pre-loaded on the RFID reader that can be upgraded. Unlike FFS Partitions, these partitions are not visible when the operating system is running. They also contain system information. Non-FFS partitions include the following:

- **Windows CE**: The complete Windows CE operating system is stored on Flash devices. If necessary, the entire OS image may be downloaded to the RFID reader using files provided by Zebra. The current OS partition on the RFID reader is included as part of the TCM installation package. Any upgrades must be obtained from Zebra. This partition is mandatory for the RFID reader.

- **Partition Table**: Identifies where each partition is loaded in the RFID reader.
AirBEAM Smart

The AirBEAM Smart product allows specially designed software packages to be transferred between a host server and Zebra wireless handheld devices. Before transfer, AirBEAM Smart checks and compares package versions, so that only updated packages are loaded.

AirBEAM Smart resides on radio-equipped client devices and allows them to request, download, and install software, as well as to upload files and status data. A single communications session performs both file download and upload. The ability to transfer software over a radio network can greatly reduce the logistical efforts of client software management.

In an AirBEAM Smart system, a network-accessible host server acts as the storage point for the software transfer. The AirBEAM Smart Client uses the industry standard FTP or TFTP file transfer protocols to check the host system for updates and, if necessary, to transfer updated software.

**NOTE** For more information about AirBEAM Smart, refer to the *AirBEAM® Smart Windows® CE Client Product Reference Guide* (p/n 72-63060-xx).

AirBEAM Package Builder

In a typical distributed AirBEAM system, software to be transferred is organized into packages. In general, an AirBEAM package is a set of files that are assigned attributes both as an entire package and as individual component files. The package is assigned a version number and the transfer occurs when an updated version is available.

An AirBEAM package can optionally contain developer-specified logic to be used to install the package. Installation logic is typically used to update client device flash images or radio firmware. Examples of common AirBEAM packages would include packages for custom client application software, radio firmware, and AirBEAM Smart Client software.

Once these packages are built, they are installed on the host server for retrieval by the handheld device. Use the AirBEAM Package Builder utility to define, generate, and install AirBEAM packages to a server. The packages are then loaded from the server onto a client device equipped with an AirBEAM Smart Client executable.

For instructions on how to define, generate, and install AirBEAM packages to the server, refer to the *AirBEAM Package Builder Product Reference Guide*, p/n 72-55769-xx.

AirBEAM Smart Client

The AirBEAM Smart Client resides on the handheld mobile computer. It is configured with the server access information, the names of the packages to be downloaded and other controlling parameters. When the AirBEAM Smart Client is launched, the device connects to the specified FTP server and checks the packages it is configured to look for. If the package version was updated, the client requests the transfer.
**AirBEAM License**

The AirBEAM Smart Client is a licensed software product. A license key file stored on the client device enables the AirBEAM Smart Client's version synchronization functionality. Build the license key file into AirBEAM Smart Client's image, or download it in a special AirBEAM package.

The AirBEAM license key file contains a unique key and a customer specific banner that appears when the AirBEAM Smart Client version synchronization logic is invoked.

**Configuring the AirBEAM Smart Client**

1. Click Start > Programs > AirBEAM Smart Client. The AirBEAM Smart CE window appears.
2. Click File > Configure. The AirBEAM configuration window appears.

![AirBEAM Configuration Window](image)

Use the configuration window to view and edit AirBEAM Smart Client configurations. This dialog box has six tabs that can be modified - Packages(1), Packages(2), Server, Misc(1), Misc(2) and Misc(3).

**Packages(1) Tab**

Use this tab to specify the package name of the first four of eight packages to load during the AirBEAM synchronization process. The specified package name must correspond to a package available on the specified package server.

![Package (1) Tab](image)

**Table 6-4 Package (1) Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package 1</td>
<td>Package name of the first of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Package 2</td>
<td>Package name of the second of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Package 3</td>
<td>Package name of the third of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Package 4</td>
<td>Package name of the fourth of eight packages. This is an optional field.</td>
</tr>
</tbody>
</table>
Do not enter inadvertent trailing spaces on the Packages(1) tab. Information entered in these fields are case and space sensitive.

**Packages(2) Tab**

Use this tab to specify the package name of the last four of eight packages to load during the AirBEAM synchronization process. The specified package name must correspond to a package available on the specified package server.

![Figure 6-14 Package (2) Tab](image)

**Table 6-5 Package (2) Tab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package 5</td>
<td>Package name of the fifth of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Package 6</td>
<td>Package name of the sixth of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Package 7</td>
<td>Package name of the seventh of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Package 8</td>
<td>Package name of the eighth of eight packages. This is an optional field.</td>
</tr>
<tr>
<td>Upload Pkg</td>
<td>Package name of a package to be processed for “upload files” during the AirBEAM synchronization process. The specified package name must correspond to a package available on the specified package server. This is an optional field.</td>
</tr>
</tbody>
</table>

Do not enter inadvertent trailing spaces on the Packages(2) tab. Information entered in these fields are case and space sensitive.

**Server Tab**

Use this tab to specify the configurations of the server to which the client connects during the package synchronization process.

![Figure 6-15 Server Tab](image)
Use this tab to configure various miscellaneous features.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP Address of the server. It may be a host name or a dot notation format.</td>
</tr>
<tr>
<td>Directory</td>
<td>The directory on the server that contains the AirBEAM package definition files. All AirBEAM</td>
</tr>
<tr>
<td></td>
<td>package definition files are retrieved from this directory during the package synchronization</td>
</tr>
<tr>
<td></td>
<td>process.</td>
</tr>
<tr>
<td>User</td>
<td>The FTP user name that is used during the login phase of the package synchronization process.</td>
</tr>
<tr>
<td>Password</td>
<td>The FTP password that corresponds to the FTP user specified in the User field. The specified</td>
</tr>
<tr>
<td></td>
<td>password is used during the login phase of the package synchronization process.</td>
</tr>
</tbody>
</table>

**NOTE** Do not enter inadvertent trailing spaces on the Server tab. Information entered in these fields are case and space sensitive.

**Misc(1) Tab**

Use this tab to configure various miscellaneous features.

![Misc(1) Tab Diagram](image)
Table 6-7  Misc(1) Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-load</td>
<td>Use this drop-down list to specify how to invoke the AirBEAM Smart Client when the client device is rebooted. Options are: Disable: the AirBEAM Smart Client is not invoked automatically during the boot sequence. Interactive: the AirBEAM Smart Client is invoked during the boot sequence and begins package synchronization. The Synchronization Dialog box appears, click OK when the process completes. Non-interactive: the AirBEAM Smart Client is invoked during the boot sequence and begins package synchronization. The Synchronization Dialog box appears and closes automatically. Clicking OK is not required. Background: the AirBEAM Smart Client is invoked automatically during the boot sequence. The package synchronization process starts automatically. Nothing is displayed while the synchronization process is occurring.</td>
</tr>
<tr>
<td>RAM Management</td>
<td>This check box specifies whether the automatic RAM management is enabled during package synchronization. Enable this to invoke RAM management logic when there is not enough free disk space to download a package. The RAM management logic attempts to remove any discardable AirBEAM packages resident on the client.</td>
</tr>
<tr>
<td>Suppress Separator</td>
<td>This check box specifies whether to suppress the automatic insertion of a file path separator character when the client generated server package definition file names. When enabled, the parameter also disables appending .apd to the package. This feature is useful for AS/400 systems, in which the file path separator character is a period. Enabling this feature appends the server directory (Directory) and package name (Package 1, Package 2, Package 3, and Package 4) &quot;as is&quot; when building the name for the server package definition file. When this feature is disabled, a standard file path separator is used to separate the server directory (Directory) and package name (Package 1, Package 2, Package 3, and Package 4) when building the name for the server package definition file. In addition, an .apd extension is appended automatically.</td>
</tr>
<tr>
<td>TFTP</td>
<td>This check box specifies whether to use the TFTP protocol to download files. By default, the AirBEAM Smart Client uses the FTP protocol.</td>
</tr>
<tr>
<td>WNMS</td>
<td>This check box specifies whether the AirBEAM Smart Client uploads a WNMS information file at the end of each version synchronization.</td>
</tr>
</tbody>
</table>

Misc(2) Tab

Use this tab to configure various miscellaneous features.
Table 6-8  Misc(2) Tab

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto-retry | Use this field to specify whether the AirBEAM Smart Client automatically retries if synchronization fails.  
If this feature is enabled, the AirBEAM Smart Client displays a pop-up dialog indicating the retry attempt. The pop-up dialog appears for the number of seconds specified in the Retry Delay field.  
Values for this field are:  
-1: the AirBEAM Smart Client automatically retries indefinitely.  
0: the AirBEAM Smart Client does not automatically retry.  
-0: the AirBEAM Smart Client automatically retries up to the number of times specified. |
| Retry Delay | This field specifies the amount of time, in seconds, that the AirBEAM Smart Client delays before automatically retrying after a synchronization failure. |
| In-use Test | This check box specifies whether the AirBEAM Smart Client tests to determine if a file is in use before downloading. If the In-use Test feature is enabled, the AirBEAM Smart Client downloads a temporary copy of any files that are in use. If any temporary in-use files are downloaded the AirBEAM Smart Client automatically resets the client to complete copying the in-use files. If the In-use Test feature is disabled, the synchronization process fails (-813) if any download files are in use. |
| Wait Welcome | This check box specifies whether the AirBEAM Smart Client waits for the WELCOME windows to complete before automatically launching the synchronization process after a reset. |
| Close Apps | This check box specifies whether the AirBEAM Smart Client automatically attempts to close non-system applications prior to resetting the mobile unit. If enabled the AirBEAM Smart Client sends a WM_CLOSE message to all non-system applications before resetting the mobile unit. This feature offers applications the opportunity to prepare (i.e., close open files) for the pending reset. |

Misc(3) Tab
Use this tab to configure various miscellaneous features.
Synchronizing with the Server

When synchronization begins, the AirBEAM Smart Client attempts to open an FTP session using the AirBEAM Smart Client configuration. Once connected, the client processes the specified packages. Packages are loaded only if the server version of a given package is different from the version loaded on the client. When upload completes, the AirBEAM Smart Client closes the FTP session with the server.

The AirBEAM Smart Client can launch an FTP session with the server either manually, when initiated by the user, or automatically.

**Manual Synchronization**

1. Configure the AirBEAM Smart Client. See *Configuring the AirBEAM Smart Client on page 6-20*.
2. From the main *AirBEAM CE* window, click **File > Synchronize**. Once connected, the *AirBEAM Synchronize* window appears.

   ![Figure 6-19 AirBEAM Synchronize Window](image)

   - The Status List displays messages that indicate the synchronization progress.
   - Click **OK** to return to the Main Menu. This button remains inactive until synchronization completes.
   - Click **Retry** to restart synchronization. This button is active only if there is an error during synchronization.

**Automatic Synchronization**

To configure the AirBEAM Smart Client to launch automatically, use the **Misc(1)** preference tab (see *Misc(1) Tab on page 6-22*). When setting automatic synchronization, use the **Auto-load** drop-down list to specify how to invoke the AirBEAM Smart Client when the client device reboots. See *Misc(1) Tab on page 6-22* for instructions on enabling Auto Sync.
AirBEAM Staging

The AirBEAM Smart staging support simplifies the process of staging custom or updated operating software onto mobile devices directly from manufacturing. The staging support is part of the AirBEAM Smart CE Client integrated in the mobile computer.

The AirBEAM Smart support defaults the AirBEAM Client configuration to a known set of values and launches the AirBEAM Smart package download logic. A staging environment, including an RF network, FTP server, and AirBEAM packages must be set up. Ideally, set up a staging network and server to match the default AirBEAM Staging client configuration.

Invoke the AirBEAM Smart staging utility from the Application directory (click Start > Programs > File Explorer > Windows).

The AirBEAM Staging support provides several benefits:

- Loading many devices simultaneously over the RF network.
- A simple single dialog user interface used to quickly start the software installation process.
Chapter 7 RFID Applications

Introduction

Application developers can use these examples for an overview of how an application works and to assist in custom application development. Samples are provided in the SMDK for C.

Integrators can also use the Test Applications and Utilities on page 7-22 for product settings and as an aid in the product integration. Use the utilities to change and/or set the device parameters and to test applications.

NOTE The screens and windows are provided for illustration purposes only and may differ from actual screens. The applications described may not be available on (or applicable to) all devices.

Procedures are not device specific and are intended to provide a functional overview.

The RD5000 does not have a display. To view the system menus use an application such as Microsoft's Remote Display Control for Pocket PC. For more information see Host Computer Display Setup on page 1-13.
RFIDSocketBridge

From the desktop window double click the icon in the toolbar to display the SocketBridge window. The SocketBridge can be turned off from the SocketBridge window by selecting File - Exit.

![Figure 7-1 RFIDSocketBridge Window](image)

The RFIDSocketbridge application is responsible for managing the reader systems, including:

- Manages incoming wireless connections to the RFID reading subsystem. Offers support for TCP/IP, or Bluetooth connections.
- Monitors battery life, controls battery LEDs, and beeps on low battery.

The RFIDSocketbridge can be configured using the registry in 2 ways.

- Use a registry editor, or other equivalent tool to change settings directly.
- Edit rfidsocketbridge.reg using a text editor. Copy to device, cold boot device.

RFIDSocketBridge Registry File

The RFIDSocketBridge registry file restores the demo settings after a cold boot. If this file is edited, the settings will not be implemented until a cold boot occurs. Alternatively, on some Zebra devices, the registry file can be launched. When this is done, a prompt appears asking the user to choose whether to merge these settings into the registry. The next time the demo is launched, it will use the settings in this file. Table 7-1 on page 7-2 provides the SocketBridge registry file example.

**NOTE** All DWORD values must be in hex notation.

Table 7-1 RFIDSocketBridge Registry File Example

```plaintext
; *****************************************************************************************************
[HKEY_LOCAL_MACHINE\SOFTWARE\SYMBOL\RFIDSocketBridge]
; How many seconds without any activity on connection before connection is dropped. (5 second minimum)
"InactivityTimeout"=dword:3C
; If battery power less than 20 percent, then beep if 1, otherwise do not beep.
"BeepOnLowBattery"=dword:1
; If 1, then allow incoming socket connections. If 0, do not.
"SocketConnectionEnabled"=dword:1
; If 1, then allow incoming bluetooth connections. If 0, do not.
"BluetoothConnectionEnabled"=dword:0
; If NULL, then no Bluetooth Pin required to connect. Otherwise, this pin is required for all connections.
"BluetoothPin"="999"
```
RFIDDemo Application

Application developers can use the RFIDDemo Application on page 7-3 for an overview of how the application works and to assist in application development. A sample is provided in the SMDK for C.

The RFIDDemo application is provided as a demo application to be used by developers in developing customized production applications. The application is viewed on a host computer using a remote viewing application (not provided). The RFIDSocketbridge application is responsible for managing the reader systems (see RFIDSocketBridge on page 7-2). The RFIDDemo application is provided for the purpose of demonstration and is intended to be used as-is.

Gen2 tags can be read, programmed, erased, written locked and killed. Each tag contains the EPC number (64 or 96 bits), CRC and kill code. In addition, data can be collected by decoding in-range EPC Gen2 RFID tags.

NOTE    The reader is optimized to read only Gen 2 tags and the default setting on the RFIDDemo application are set to read and write only Gen2 tags.

The reader has the capability to read, program, erase, write lock and kill; Gen2 tags. The current RFIDDemo application only provides an example for programming tags.

When the read command is initiated, the reader interrogates all of the RFID tags within the radio frequency (RF) field of view. The reader captures data from each new tag found and adds it to the list box in the main Tags window. When the read command is stopped, the reader stops interrogating tags.

Perform the following procedures to setup and use the RFIDDemo application:

• Setup the local host computer display.
  The RD5000 does not have a display, a host computer must be setup to use the RD5000 menus.

• Setup the LAN host.
  The LAN host computer must be setup to receive the tag data.

• Setup the wireless connection.
  See Chapter 5, Wireless Applications for information on setting up the wireless connection.

• Launch the RFIDDemo application.

Using RFIDDemo to Read Tags From a Remote Reader

The RFIDDemo can reside on many CE4.2/CE5.0 based devices including Zebra's RD5000, MC90xx readers, WIN CE based VRCs, and XR Series products.

On devices that have integrated RFID reading, the RFIDDemo automatically finds and connects to the integrated RFID reader. These readers include RD5000, MC90xx, and XR Series.

On devices that do not have an integrated RFID reading capability, the RFIDDemo must be configured to connect to the remote RFID reader using the reader IP address and port number 3000.

The settings screen is described in Device Settings on page 7-7.
Using RFIDDemo to Forward/Log Tags to Remote Device

By default, the RFIDDemo does not display or log tags. The RFIDDemo beeps each time a tag is read. The RFIDDemo can be configured to log tags:

- Log tag reads to a file:
  - Writes tags to TagLog.txt
  - Data format:
    10-04-2006, 07:29:51.63646 (000141ms), [A0] 0220064806042978260000A5
  
- Log tag reads to the screen

- Log tag reads to a either a TCP/IP address/port or serial port:
  - TCP/IP logging
    
    Data format:
    
    <TAG>[A0] 0220064806042978260000A5</TAG>

    Buffers up to 1024 tags when no connection available

    Works with sample win32 application RFIDServer.exe on port 3535

  - Serial port logging. (Local, or Bluetooth)
    
    Data format:
    
    [A0] 0220064806042978260000A5
Launching the RFIDDemo Application

Set up the remote display software to display the reader menus on the host computer. From the Main Window (see Figure 7-2) double-click the RFIDDemo application icon to start the RFIDDemo application. It also displays battery status and the air protocols supported by the device.

![Main Window](image)

Figure 7-2  Main Window

When the RFIDDemo application is launched, the RFIDDemo Load window displays. It displays version of RFID API, reader firmware, the air protocols and the RFID demo application (see Status Icons (Windows CE 5.0) on page 1-14 for a full description of the icons displayed).

![RFIDDemo Load Window](image)

Figure 7-3  RFIDDemo Load Window

Click on the Settings button to modify the RFIDDemo application settings. See Device Settings on page 7-7 for detailed settings information.

Click on the Start Reading button to initiate the tag read. See Read Tags on page 7-21 for more information.

![NOTE](image)

×  NOTE  The Logging to File setting is enabled by default, so the tag reads will not be immediately displayed on the screen. Go to Device Settings on page 7-7 and deselect the Log to file option to see tags on the screen.
File Menu Options

The RFIDDemo File Menu Options include:

- About
- Device Settings
- MPS Settings
- Tag Access Parameters
- Program Tag
- Exit

![File Menu Options Window](image)

**Figure 7-4  File Menu Options Window**

About

The About window displays the demo application version information

![About Window](image)

**Figure 7-5  About Window**
Device Settings

The RFIDDemo behavior is configurable. Click on Settings from the RFIDDemo Load Window on page 7-5 or from File->Device Settings, RFID- Settings window appears. These settings are persistent and will be restored on a device cold boot. Once the settings have been modified, exit and relaunch application to enable new settings.

![Figure 7-6 DeviceSettings Window](image)

**Reader Device Settings:**

- **IP Address:**
  By default, the demo attempts to find a reader on the local COM ports. If the RFIDDemo application needs to find a reader at a specific IP Address, enter the address in the text box. It can be an IP address by name, or number (i.e. 192.168.1.1, or www.deviceaddress.com).

- **Port:**
  If the IP address is configured, configure the port as well. The default port setting is 3000.

- **Start On Boot:**
  Check to launch the RFIDDemo application on a warm or cold boot. When used with Read At Startup, the application will start on boot and read.

- **Read At Startup:**
  Check this box to have the application start reading as soon as the application is launched.

- **Beep On Read:**
  Check this box to have the device beep on every tag read.

- **Read On Time / OffTime:**
  When reading starts, it will read for On Time (in seconds), then pause reading for Off Time (in seconds).

**Tag Logging**

If Tag Logging is configured, all tags will be forwarded to the serial port, or to an IP address/port.

- **Address:**
  This can be an IP address, or COM port. If it is a COMPORT, enter "COM1:“, etc… (a Bluetooth COM port can be configured here as well).

- **Port:**
  The IP Port number or the COMPORT (i.e. if Address is COM1:, put 1 here).

- **Speed:**
  This is only used for the COM port. Can be up to 115200.

- **Log To File:**
  Check this box to save all logging to a file. If an external location is not specified the log file is saved in a file named Taglog.txt on the reader root directory.
Registry Settings Description

The RFIDDemo registry file restores the demo settings after a cold boot. If this file is edited, the settings will not be implemented until a cold boot occurs. Alternatively, on some Zebra devices, the registry file can be launched. When this is done, a prompt appears asking the user to choose whether to merge these settings into the registry. The next time the demo is launched, it will use the settings in this file. Do not perform this function while the demo is running. The Gemini_RFID.exe demo also uses many of these registry settings and can be used to registry settings. Do not launch the Gemini_RFID.exe demo while the RFIDDemo is running. Table 7-2 on page 7-9 provides the RFIDDemo registry file example.

NOTE All DWORD values must be in hex notation.
Table 7-2 Registry File Example

; RFIDDemo Registry File. This file will restore the demo settings after a cold boot.
; If you edit this file, the settings will not take affect until a cold boot occurs. Alternatively,
; on some Symbol Terminals, the registry file can be launched. When this is done, you will be
; prompted whether or not you want to merge these settings into the registry. The next time the demo is
; launched, it will use the settings in this file. (Make sure you are not running the demo when you do this!!!)
; The Gemini_RFID.exe demo also uses many of these registry settings, and in fact, can be used to registry settings
; (Also, make sure RFIDDemo is not running when launching the Gemini_RFID.exe demo.)
;
; NOTE: ALL DWORD VALUES NEED TO BE IN HEX NOTATION.

; HKEY_LOCAL_MACHINE\SOFTWARE\SYMBOL\RFIDDemo

; If 1, then beep on all tag reads. If 0, do not beep.
"RFIDDEMO_BEEPER_ENABLED"=dword:1

; If 0, the demo will read continuously.
"RFIDDEMO_AUTONOMOUS_MODE_ONTIME"=dword:000061A8

; If 0, the demo will read continuously. Otherwise, it will stop for this many ms.
"RFIDDEMO_AUTONOMOUS_MODE_OFFTIME"=dword:00000000

; If 1, the demo will start reading automatically after finding a RFID reader.
"RFIDDEMO_READ_TAGS_ON_LAUNCH"=dword:0

; If 1, the demo will start automatically upon the next warm or cold boot of the device.
"RFIDDEMO_START_APP_ON_BOOT"=dword:0

; Any number less than 16 is a com port number. Greater than 16 is a TCP/IP port number.
"RFIDDEMO_LOGGING_PORT_NUMBER"=dword:00000000

; Com Port baud rate for logging tags. Not used for TCP/IP connections.
; Common baud rates are:(USE HEX) (9600 = hex 2580) (38400 = hex 9600) (115200 = hex 1C200).
"RFIDDEMO_LOGGING_PORT_BAUDRATE"=dword:00000000

; Name of port where logging will occur. For COM ports, use COM1:  COM2:, etc...
; For TCP/IP Ports, use valid IP address, i.e. 192.168.1.1  localhost  www.mysitename.com ...
"RFIDDEMO_LOGGING_PORT_NAME"=""
"RFIDDEMO_LOGGING_TO_FILE"="1"

; If this is set, then the demo will attempt to contact an RFID reader at this port. (3000 is BB8 in hex)
"RFIDDEMO_READER_IP_PORT"=dword:00000000

; RF OnTime
"RFIDDEMO_READER_RF_ONTIME"=dword:0000003C
Table 7-2 Registry File Example (Continued)

; If this is set, then the demo will attempt to contact an RFID reader at this address.
"RFIDDEMO_READER_IP_ADDRESS"=""

; Attenuation level for reading tags. 0 is full power, 255 is low power. (Use hex values 00 - FF)
"RFID_READCAP_RF_ATTENUATION"=dword:00000000
"RFID_READCAP_RF_ATTENUATION2"=dword:00000000

; Order in which to issue read commands. Antenna 0, Antenna 1, etc ...
"RFID_DEVCAP_ANTENNA_SEQUENCE"=hex:00

; Enabled types of tag to read: a 0 means disabled, 1 means enabled.
; Each byte is as follows: C0 C1 G2
"RFID_TAGCAP_ENABLED_TYPES"=hex:00,00,00,00,00,01,00

; The RFIDAPI allows duty cycle control on a micro level during tag reading.
; The on time is in ms. The off time is as a percent of the total on time.
"RFID_READCAP_DUTYCYCLE_ONTIME"=dword:00000000
"RFID_READCAP_DUTYCYCLE_OFFTIME_PCNT"=dword:00000000
"RFIDDEMO_MPS_MOTION_ENABLED"=dword:00000000
"RFIDDEMO_MPS_MOTION_X_THRESHOLD"=dword:0000015E
"RFIDDEMO_MPS_MOTION_Y_THRESHOLD"=dword:0000015E
"RFIDDEMO_MPS_MOTION_Z_THRESHOLD"=dword:0000015E
"RFIDDEMO_MPS_PROX_ENABLED"=dword:00000001
"RFIDDEMO_MPS_PROX_EVENT_MASK"=dword:0000FE7F
"RFIDDEMO_MPS_PROX_POLL_TIME_MS"=dword:00000064
"RFIDDEMO_MPS_PROX_READ_THRESHOLD"=dword:00000000
"RFIDDEMO_MPS_VEL_MIN_DET_X_THRESHOLD"=dword:00000014
"RFIDDEMO_MPS_VEL_MIN_DET_Y_THRESHOLD"=dword:00000014
"RFIDDEMO_MPS_VEL_MIN_DET_Z_THRESHOLD"=dword:00000014
"RFIDDEMO_MPS_VEL_MIN_START_X_THRESHOLD"=dword:0000004B
"RFIDDEMO_MPS_VEL_MIN_START_Y_THRESHOLD"=dword:00000032
"RFIDDEMO_MPS_VEL_MIN_START_Z_THRESHOLD"=dword:00000064
"RFIDDEMO_MPS_VEL_RECAL_X_THRESHOLD"=dword:0000012C
"RFIDDEMO_MPS_VEL_RECAL_Y_THRESHOLD"=dword:0000012C
"RFIDDEMO_MPS_VEL_RECAL_Z_THRESHOLD"=dword:00000BB8
"RFIDDEMO_MPS_VEL_MISC_X_THRESHOLD"=dword:000000FA
"RFIDDEMO_MPS_VEL_MISC_Y_THRESHOLD"=dword:000007D0
"RFIDDEMO_MPS_VEL_MISC_Z_THRESHOLD"=dword:00000005

; Word Length of the tag to be read
"RFID_READCAP_WORD_LENGTH"=dword:2

; Mem Bank of the tag to be read
"RFID_DEVCAP_MEM_BANK"=dword:1

; Word offset from where to start reading.
"RFID_DEVCAP_WORD_OFFSET"=dword:1

; Attenuation level for writing tags. 0 is full power, 255 is low power. (Use hex values 00 - FF)
"RFID_WRITECAP_RF_ATTENUATION"=dword:00000000

; Order in which to issue write commands. Antenna 0, Antenna 1, etc ...
"RFID_WRITECAP_ANTENNA_SEQUENCE"=hex:00
Table 7-2 Registry File Example (Continued)

; SL bit of the tag to be accessed
"RFID_DEVCAP_SEL"=dword:00000000

; Session to be used for tag access
"RFID_DEVCAP_SESSION"=dword:00000000

; Starting Q for tag access operation
"RFID_DEVCAP_STARTING_Q"=dword:00000006

; Target Inventory for tag access operation
"RFID_DEVCAP_TARGET_INVENTORY"=dword:00000000

; Write options
"RFID_DEVCAP_WRITE_OPTIONS"=dword:00000001

; Action to be performed on add select record
"RFID_DEVCAP_SEL_ACTION"=dword:00000000

; Select Session to change inventory bit
"RFID_DEVCAP_SEL_TARGET"=dword:00000004

; Select index of Select record to be removed
"RFID_DEVCAP_SEL_INDEX"=dword:00000000

; Mem bank to be locked
"RFID_DEVCAP_LOCK_MEM_BANK"=dword:00000001

; Lock options
"RFID_DEVCAP_LOCK_OPTIONS"=dword:00000003

; Tag Mask Memory
"RFID_DEVCAP_TAG_MASK_MEM"=dword:00000001

; Tag Mask
"RFID_DEVCAP_TAG_MASK"=dword:0002CD10

; Tag Mask header nInit
"RFID_DEVCAP_TAG_MASK_HEADER_NINIT"=dword:00000417

; Tag Mask header StructureFormat
"RFID_DEVCAP_TAG_MASK_HEADER_STRUCTURE_FORMAT"=dword:00000000

; Tag Mask header StructureSize
"RFID_DEVCAP_TAG_MASK_HEADER_STRUCTURE_SIZE"=dword:000000A4

; EPC Mask Bit Length
"RFID_DEVCAP_EPC_MASK_BIT_LEN"=dword:00000000

; Tag Mask Bit Len
"RFID_DEVCAP_TAG_MASK_BIT_LEN"=dword:00000000

; Tag Mask Offset
"RFID_DEVCAP_TAG_MASK_OFFSET"=dword:00000010
MPS Settings

The RFIDDemo behavior is configurable. Click on Settings from the RFIDDemo Load Window on page 7-5 or from File->Device Settings, RFID- Settings window appears. These settings are persistent and will be restored on a device cold boot. Once the settings have been modified, exit and relaunch application to enable new settings.

![Figure 7-7 MPS Settings Window](image)

Reader MPS Settings:

- **Proximity On:**
  Selects the proximity sensor enable/disable and proximity events. Check box to enable the sensor. Sensor is enabled and proximity raw values are reported along with proximity events (detect and clear) based the detection level set using the *Events at* drop down list.

- **Events at:**
  This input sets the range for generating proximity detection (PROX_DET) and clear (PROX_CLR) events. When set to 1.5ft, device generates a PROX_DET event when an object moves to within 1.5ft of the device. A PROX_CLR event is generated if the object moves more than 1.5 ft away from the device.
  The maximum range setting is 8ft. There are different detection levels possible in the range 1.5ft to 8ft. The detection range can be set to these values: 1.5ft, 2ft, 3ft, 4ft, 5ft, 6ft, 7ft, 8ft.
  Automating the RFID tag reading can be used as an example of maximizing the power usage efficiency. For Example: Setting the proximity detection range at 2.5ft generates a PROX_DET event when an object appears within the 2.5ft setting. The PROX_DET event triggers RFID reader in the demo application to turn on and read tags. If the object moves away (beyond 2.5ft from the reader) the PROX_CLR event is generated and the PROX_CLR event stops the RFID reader module. The reader automatically stops reading the tags and conserves power, by not keeping the RFID reader module on.

- **Motion on:**
  Selects the motion sensor enable/disable and motion events. Check box to enable the sensor. The motion events are based on velocity changes and are depending on values set in the *Velocity Thresholds* parameters.
  The motion events can also be used to trigger the RFID reader ON and OFF. There are different motion events; FWD_START, BKWD_START with a FWDBKWD_STOP and UPSD_START, DNSD_START with a UP_DN_STOP event. The start events are set to turn the RFID reader module ON and the stop events turn the reader module OFF.
  For detailed information on setting thresholds refer to Appendix B, Motion Sensor Parameters.

- **Read Back:**
  The *Read Back* button displays the current threshold values in the corresponding parameter text boxes. The current parameters values are read back from the Atmel controller (that controls the motion sensor).

- **OK**
  *OK*, updates the Atmel with the displayed values, if motion sensor is enabled.

- **Cancel:**
  *Cancel* exits the MPS Settings and returns to the RFIDDemo Load Window, *Figure 7-3 on page 7-5.*
Proximity Initiated Tag Read

With the Proximity On (see MPS Settings on page 7-12) the reader automatically turns on and reads tags and turns off (to conserve power) based on the proximity events (detect and clear).

The proximity value is displayed in the Proximity and Motion Initiated Tag Read window (see Figure 7-8) and a blue bar represents the relative value.

✓ **NOTE** Once the proximity settings have been modified, exit and relaunch application to enable new settings.

![Proximity and Motion Initiated Tag Read Window](image)

**Figure 7-8** Proximity and Motion Initiated Tag Read Window

Raw proximity values are represented in an accelerator bar, P, from 0 to 255, 0 being closest and 255 representing object beyond reach. The different raw values displayed with respect to proximity measured in distance are as given in the table below.

<table>
<thead>
<tr>
<th>Proximity Raw Value</th>
<th>0</th>
<th>8</th>
<th>22</th>
<th>51</th>
<th>81</th>
<th>110</th>
<th>139</th>
<th>168</th>
<th>198</th>
<th>198 to 255</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance in ft.</td>
<td>Less than 1.5ft</td>
<td>1.5ft</td>
<td>2ft</td>
<td>3ft</td>
<td>4ft</td>
<td>5ft</td>
<td>6ft</td>
<td>7ft</td>
<td>8ft</td>
<td>Beyond 8ft / out of range</td>
</tr>
</tbody>
</table>

**Table 7-3** Raw Values With Respect to Measured Proximity

Raw motion values are represented in accelerator bars X, Y and Z for Up/Down, Left/Right side and Forward/Backward motion respectively. The value 2048 is the baseline and motion is represented in terms of velocity as 30 increments for each 1ft/sec velocity. For example; for a forward motion of velocity 1ft/sec, then Z axis data would be 2048+30 = 2078. Similarly if there is a backward motion of velocity 1ft/sec, then Z axis data would be 2048-30 = 2018.

See Tag Logging on page 7-7 for information on logging the file tag values.

Motion Initiated Tag Read

With the Motion Detect On (see Reader Device Settings: on page 7-7) the reader automatically turns on and reads tags when motion is detected. It also stops reading when no motion is detected. The motion value is displayed in the Proximity and Motion Initiated Tag Read window (see Figure 7-8) with blue bars represents the relative X, Y, and Z axis values.

✓ **NOTE** Once the motion settings have been modified, exit and relaunch application to enable new settings.

See Tag Logging on page 7-7 for information on logging the file tag values.
Tag Access Parameters

Click on Tag Access Params from the *RFIDDemo Load Window on page 7-5* or from *File->Tag Access Params*, the Tag Access Parameters window appears.

![Tag Access Parameters Window](image)

**Figure 7-9  Tag Access Parameters Window**

**Reader Settings:**

- **Sel:**
  - *Ignore SL*: All tags can be inventoried; ignore SL.
  - *SL*: Only inventory tags with SL NOT set.
  - *No SL*: Only inventory tags with SL SET.

- **Session:**
  - S0: Use session S0 for inventory.
  - S1: Use session S1 for inventory.
  - S2: Use session S2 for inventory.
  - S3: Use session S3 for inventory.

- **Target:**
  - A: Only inventory Tags with inventoried bit set to A for Session.
  - B: Only inventory Tags with inventoried bit set to B for Session.

- **Stating Q(0-15):**
  Sets the number of slots (=2^Q) in the first Inventory Round of the Inventory Algorithm. The starting Q should be chosen higher for a larger expected number of tags in the field. Q = 4 is recommended for 8 to 50 tags.

**Table 7-4  Select Record Settings**

<table>
<thead>
<tr>
<th>Action</th>
<th>Matching</th>
<th>Non-Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>assert SL; inventoried-&gt;A</td>
<td>deassert SL; inventoried-&gt;B</td>
</tr>
<tr>
<td>0x01</td>
<td>assert SL; inventoried-&gt;A</td>
<td>do nothing</td>
</tr>
<tr>
<td>0x02</td>
<td>do nothing</td>
<td>deassert SL; inventoried-&gt;B</td>
</tr>
<tr>
<td>0x03</td>
<td>negate SL; A-&gt;B, B-&gt;A</td>
<td>assert SL; inventoried-&gt;A</td>
</tr>
<tr>
<td>0x04</td>
<td>deassert SL; inventoried-&gt;B</td>
<td>assert SL; inventoried-&gt;A</td>
</tr>
<tr>
<td>0x05</td>
<td>deassert SL; inventoried-&gt;B</td>
<td>do nothing</td>
</tr>
<tr>
<td>0x06</td>
<td>do nothing</td>
<td>assert SL; inventoried-&gt;A</td>
</tr>
<tr>
<td>0x07</td>
<td>do nothing</td>
<td>negate SL; A-&gt;B, B-&gt;A</td>
</tr>
</tbody>
</table>
• Target
  0x00: Modify Session S0 inventoried flag.
  0x01: Modify Session S1 inventoried flag.
  0x02: Modify Session S2 inventoried flag.
  0x03: Modify Session S3 inventoried flag.
  0x04: Modify SL flag.

• Remove Select Record Index
  Index of the record selected to be removed from the list. This value is used when the remove select record command is issued from the main page.

• RD PWR A0
  Antenna power for read operation.
  
  | 18 | 252 |
  | 19 | 231 |
  | 20 | 210 |
  | 21 | 189 |
  | 22 | 168 |
  | 23 | 147 |
  | 24 | 126 |
  | 25 | 105 |
  | 26 |  84 |
  | 27 |  63 |
  | 28 |  42 |
  | 29 |  21 |
  | 30 |   0 |

• WR PWR A
  Antenna power for write operation. Above table used for conversion.
Program Tag

Click on Program Tag from the RFIDDemo Load Window on page 7-5 or from File->Program Tag, RFID- Program Tag window appears.

Reader Program Tag Settings:

- **Reserved**: Reserved memory bank access operation
- **EPC**: EPC memory bank access operation
- **TID**: TID memory bank access operation
- **User**: User memory bank access operation
- **User Offset**: A 16-bit word address at which to start reading/writing. Does not hold good for EPC read as EPC read always returns contents of the complete memory bank.
- **Length**: Number of 16-bit words to read.
- **Data**: Tag Write data is provided.
- **Lock**: Click **Lock** to send the lock command to the tag. If a valid (non zeros) access password is stored in the tag, then the access password is required to lock the tag.
- **Kill**: Click **Kill** to permanently kill the tag. To kill a tag, a valid kill code has to be stored in the tag and kill code is required to kill the tag.
- **Read**: Click **Read** to send the read command to the tag. If the tag is locked with valid (non zeros) access password stored in the tag, then password access is required to read the reserved memory bank. Other memory banks can be read without supplying access password.
- **Write button**: Click Write to send the write command to the tag. If the tag is locked with valid (non zeros) access password, then password access is required to write to the tag.
- **EPC Mask**: If bits of EPC ID are given in this field and Mask bank is selected as 1 i.e EPC, then select record is added for the tag with EPC ID given in the Mask field with the Select Record Settings given in Tag Access Params Dialog.
  
  **Note**: By selecting the read tag in the list box, it automatically comes in the Mask field.
• **Tag Mask**
  
  If select record is to be added to a memory bank other than EPC, then the memory bank bits for which select record is being added are provided here.

• **Mask bank**
  
  Sets the mask bank where the selected record is to be added:
  
  0x01: EPC  
  0x02: TID  
  0x03: User

✓ **NOTE**  

Select Records added remains valid if the user goes from this window to the main window. After that if the Select record settings are changed from the "Tag Access Params", select record command is sent with the new settings before any access command. If the user gives "Start Reading" command from the main page before coming to the program page or tag access page, add select record command is sent with the previous values of Action and Target and tag mask length as 0, where 0 implies all tags match.

• **Mask Offset**
  
  The Mask Offset is the memory word address used for adding select record.
**Lock Options**

Click on Lock Options from the *RFIDDemo Load Window on page 7-5* or from *File->Lock Options*, RFID- Lock Options window appears.

![Lock Options](image)

**Figure 7-11  Lock Options Window**

The Lock Options provide the option of locking/unlocking all or individual memory banks. In the reserved memory bank, access password and kill password can be locked or unlocked separately.

In lock command there are various options which can be selected in this dialog box.

**Reader Lock Option Settings:**

- **Lock**
  Tag is locked and tag access requires a valid access password.

- **Unlock**
  Tag is unlocked and tag access requires a valid access password. A tag locked by the Lock option can be unlocked by this unlock command.

- **Permanent Unlock**
  The tag is permanently unlocked. It can never be locked again. All other access operations are possible.

- **Permanent Lock**
  The tag is permanently locked. It can never be unlocked again. Tag write is not possible on this tag.
Tag Locking

Tag locking is a two step process:

- Write the tag access password (see Figure 7-10 on page 7-16)
- Lock the tag (see Figure 7-11 on page 7-18)

To write the access password first enter the access password of the tag:

1. Read the tag.
2. Click on the tag, it appear in the EPC Mask field. The tag is now selected for operations.
3. Write the access password for the tag:
   - Select the Reserved memory bank as the target memory bank.
   - In the Data field write 32 bits of access password (e.g.: 22222222 in the Data field.)
   - Select User Offset as 2 (this is in words) of access password. To program kill password use User Offset 1.
4. The following entries should be on the screen:
   - Reserved memory bank should be selected
   - User Offset field
   - Data field, this is the access password
   - EPC Mask field, the tag to write to
5. Click on Write.
6. Once the user has been successfully able write Access password on the tag, the tag can be locked.

To Lock the tag

1. Read the tag.
2. Click on the tag, it appear in the EPC Mask field. The tag is now selected for operations.
3. Enter the access password values as programmed (in the case of this example 22222222) in the field next to Lock.
4. Select the EPC memory bank as the target memory bank to lock the EPC ID field.
5. Select the Lock options, e.g.: EPC bank and Lock or permanently lock.
6. The following entries should be on the screen:
   - EPC memory bank should be selected
   - EPC Mask field, has the tag to write to
   - Lock, this has the Lock password
   - Lock Options have been configured
7. Click on Lock
8. Tag is now locked.
To write to a locked tag

1. Read the tag.

2. Click on the tag, it appears in *EPC Mask* field. The tag is now selected for operations.

3. Select the *EPC* memory bank as the target memory bank (since the EPC ID field is locked in this example).

4. In the *Data* field write the new 96 bit EPC ID.

5. Select *User Offset* as 2 (in words) *EPC* memory bank.

6. Enter the access password (in the case of this example 22222222) in the field next to *Lock*.

7. The following should be entered on the screen:
   - *EPC* memory bank is selected.
   - *EPC Mask* field, the tag to write to
   - *Lock*, this has the Lock password
   - *User Offset* field
   - *Data field*, this is the new tag ID

8. Click on *Write*
Read Tags

Click the **Start Reading** button, the unit starts to read tags. As the tags are read the values are displayed on the **RFID - Read Window**.

![RFID - Read Window](image1)

Figure 7-12  **RFID - Read Window**

Click the **Remove SR** button and the selected record is removed from the list. This command is not accepted when read is going on. If command is given while read is in progress the following message appears in the **RFID - Read Window**. or the record is removed, success is displayed in the **RFID - Read Window**.

![RFID - Read Window](image2)

Figure 7-13  **RFID - Read Window**

If no select record is found at the given index, then following error message is displayed in the **RFID - Read Window**. The Index to remove select record is provided in the tag access page.

![RFID - Read Window](image3)

Figure 7-14  **RFID - Read Window**

See **Tag Logging on page 7-7** for information on logging the file tag values.
Test Applications and Utilities

Integrators can use the RFID Test applications and Utilities for product settings and as an aid in the product integration. Use the utilities to change and/or set the device parameters and to test applications.

**NOTE** The screens and windows are provided for illustration purposes only and may differ from actual screens. The applications described may not be available on (or applicable to) all devices.

Procedures are not device specific and are intended to provide a functional overview.

Host Computer Display Setup

Use ActiveSync (see Chapter 4, ActiveSync) to connect to the reader and use an application such as Microsoft's Remote Display Control for Pocket PC to display the reader menus on a host computer. For more information and the Remote Display Control for Pocket PC download go to [http://www.microsoft.com/downloads/](http://www.microsoft.com/downloads/) and search for Remote Display Control for Pocket PC. Download the application and follow the provided installation and setup procedures.

Launching the RFID Test Utilities

Set up the remote display software to display the reader menus on the host computer. From the Main Window (see Figure 7-2) click Start - Programs - Windows Explorer to access the Explorer application.

![Main Windows](image)
From main Explorer window (see Figure 7-16) click Application - OTL to access the Demo window.

![Explorer Windows](image)

**Figure 7-16** Explorer Windows

From main Demo window (see Figure 7-16) click SelfTest to access the Test Applications window.

![Demo and Test Applications Windows](image)

**Figure 7-17** Demo and Test Applications Windows

> **NOTE** Only the Applications that are applicable to the reader can be launched. The remaining Zebra applications are not applicable to the reader.

The RFIDDemo application and utilities are described in the Symbol Application Guide for Symbol Devices, p/n 72E-68901-xx.
RFIDFlash Utility

The *RFIDFlash* utility is used to update the RFID module firmware. To access the *RFIDFlash* utility set up the remote display software to display the reader menus on the host computer. From the *Main Window* (see Figure 7-2) click *Start - Programs - Windows Explorer* to access the Explorer application. See *Flash Storage on page 6-17* for detailed flash storage information.

![Figure 7-18  Main Windows](image)

From main Explorer window (see *Figure 7-18*) click *Application - RFIDFLASH* to access the *RFIDFlash* utility. The *RFIDFlash* Loader window appears (see *Figure 7-20*).

![Figure 7-19  Explorer Windows](image)
Click **Browse for Flash File** and the Select Files window appears.

![RFID Flash Loader Windows](image1)

**Figure 7-20**  **RFIDFlash Loader Windows**

Scroll to the flash file and click to select, click **OK**.

The Select Files window appears.

![RFID Flash Loader Windows](image2)

**Figure 7-21**  **RFIDFlash Loader Windows**

Click **Start Flash** to download the flash update file.
AtmelFlasher Utility

The AtmelFlasher utility is used to update the Atmel micro controller. To access the AtmelFlasher utility set up the remote display software to display the menus on the host computer. From the Main Window (see Figure 7-2) click Start - Programs - Windows Explorer to access the Explorer application.

![Main Windows](image)

**Figure 7-22**  Main Windows

From main Explorer window (see Figure 7-22) click Application - AtmelFlasher to access the AtmelFlasher utility. The AtmelFlasher window appears (see Figure 7-24).

![Explorer Windows](image)

**Figure 7-23**  Explorer Windows
Click **Start**, the *AtmelFlasher* performs the flash and the message *Success* displays for the status.

![AtmelFlasher Window](image)

**Figure 7-24**  *AtmelFlasher Window*
Launching the GeminiRFID Demo Application

Set up the remote display software to display the reader menus on the host computer. From the reader main window double-click the RFIDDemo application icon to start the RFIDDemo application.

To launch the Gemini RFID sample application, click Start - File Explorer - Application - Gemini_RFID icon. When the Gemini RFID sample application is launched, the main Tags window displays.

![Figure 7-25 RFID - Main Tags Window](image)

Table 7-5 Main Tags Window and Settings Window, Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Locate Tag" /></td>
<td>Launches the Locate Tag window (see Locate Tag on page 7-35).</td>
</tr>
<tr>
<td><img src="image" alt="Program Tag" /></td>
<td>Launches the Program Tag window (see Program Tag on page 7-36).</td>
</tr>
<tr>
<td><img src="image" alt="Clear" /></td>
<td>Clears the tag list (see Clearing the Display on page 7-30).</td>
</tr>
<tr>
<td><img src="image" alt="Save" /></td>
<td>Saves the complete list of tags (see Saving Tag Data on page 7-31).</td>
</tr>
<tr>
<td><img src="image" alt="Previous" /></td>
<td>Previous and Next buttons appear on the menu when read tags exceed the amount of tags that can fit in the tag list display. Click <img src="image" alt="Previous" /> to display the previous page.</td>
</tr>
<tr>
<td><img src="image" alt="Next" /></td>
<td>Click <img src="image" alt="Next" /> to display the next page.</td>
</tr>
<tr>
<td><img src="image" alt="File Mode" /></td>
<td>File and Mode menus (see File Menu on page 7-31 and Mode Menu on page 7-35).</td>
</tr>
<tr>
<td><img src="image" alt="Sound" /></td>
<td>Click to disable/enable the sound when a tag is read.</td>
</tr>
<tr>
<td><img src="image" alt="RFID Module Power On" /></td>
<td>The RFID Module Power On icon (displayed next to the Speaker icon) indicates that the RFID radio module is powered on and attempting to read tags.</td>
</tr>
<tr>
<td><img src="image" alt="Attenuation" /></td>
<td>Use the Attenuation Slide Bar (see Figure 7-29 on page 7-33) to set the power range from 0 (full power) to 255 (low power). Drag the Attenuation Slide Bar to optimize tag reading and to minimize interference. For closer tag use a lower setting and for further away tag use a higher setting.</td>
</tr>
</tbody>
</table>
**Reading Tags**

When the mobile computer trigger is pressed, the mobile computer interrogates all of the tags within the radio frequency (RF) field of view. For each new tag found, the mobile computer beeps once and displays a tag icon in the main RFID Tag window. If the same tag is found again, the mobile computer does not beep and it does not display an additional tag icon.

When the trigger is released, the mobile computer stops interrogating tags. The total number of unique tags found displays in the Tag window.

To read tags:

1. Click *Start - RFIDDemo - RFID icon.*
2. Ensure that the mobile computer is within the RF field of view.
3. Set the RFID signal power. Use the *Attenuation* slide bar (see *Figure 7-29 on page 7-33*) to set a value in a range between 0 (full power) and 255 (low power).
4. Press and hold the mobile computer’s trigger.
5. For each new tag found, a beep sounds one time, the Indicator LED flashes green, and a tag icon displays in the Tag window.
   
   Each tag is identified by class. For example, a Gen2 tag displays in the window labeled G2.
6. Release the trigger.
Selecting Tags

The Tag window can display up to 20 tags. If more than 20 tags are found, the application allows the user to page forward and backward through the list of icons representing the tags found.

To select a tag to view the tag data:

1. Click Start - File Explorer - Application - Gemini_RFID icon.
2. Read a tag (see Reading Tags on page 7-29).
3. Select a tag icon in the Tags window.
4. The data contained in the tag, along with a count of how many times the selected tag was read, displays in the Tags window.

Figure 7-26 RFID - Main Tags Window / Selected Tag

Clearing the Display

To clear the tag list in the mobile computer’s display, click .
Saving Tag Data

A list of read tags can be saved on the mobile computer. The application saves the tag list to the "My Documents" folder and names the file RFIDTaglist.csv.

The file is a .csv format (comma separated text file). This file format can be read by MS Excel, or other applications that support .csv. The sample file contains the following information.

**Time Stamp, Tag ID, Tag Type, Read Count:**

- 2005-04-17T15:34:53-05:00,H22EEDDAEBFCCEDEE,C1,10
- 2005-04-17T15:34:53-05:00,H8000800428254006,C1,10
- 2005-04-17T15:34:57-05:00,H8000800428254124,C1,15

**The Time Stamp format is:**

Year-month-dateTHour:Minute:seconds-TimezoneHourDifferential(GMT):TimezoneMinutesDifferential

**The Tag ID format is:**

HTagData (H indicates the data is in hex)

**The Tag Type format is:**

CX, where X is the tag class. Currently the application supports Gen2, tags.

The file can not be displayed on the mobile computer (with the factory supplied software). The file is intended to be downloaded to a host and displayed using an application that can read comma delimited fields, such as an Excel spreadsheet.

The file contains a one line header and one line for each unique tag found. The header line contains a comma separated list of field text descriptions. The tag lines contain the Tag ID starting with 'H' for hex, and a number indicating how many times the tag was read.

To save tag data:

1. Click **Start** - 9000 Demo - **RFID** icon.
2. Read a tag(s). See **Reading Tags on page 7-29**.
3. Click **Save**.
4. Click **OK** to save using the default name and directory, or enter a custom name /directory and then click **OK**.

**File Menu**

Click the **File** menu on the **Main Tags** window to view version information about RFID, log information, reboot, adjust settings, or exit the application.
About
Click *File - About* to view the application version number, the RFID DLL version number, the RFID reader module firmware version number, date code, and serial and port information.

![RFID - About Window](image)

Figure 7-27  RFID - About Window

Log
Click *File - Log* to display the *Log* menu.

![RFID - Log Menu](image)

Figure 7-28  RFID - Log Menu

From the *Log* menu, click:

- *Clear Log* to clear logged data.
- *Log On* turns on the log feature. With this feature is turned on, the display splits into two sections: upper and lower. The lower section displays all communication to the RFID radio module, including tag data.
- *Log Off* to turn off the log feature. *Log Off* is the default.
- *Log File* to create and save a log file. The log file is saved in the root directory on the mobile computer to a file named RXTXLog.txt. This file can be used to track errors reading RFID tags.

Reboot
Click *File - Reboot* to issue a (warm) reboot command to the RFID radio module.

✓ **NOTE**  Reboot the RFID radio module only if tags are not being read.
**Settings**

The Settings window is used to set the number of iterations to read tags. To set the class type(s) to read (Gen2 is on by default). The settings window is also used to set and test read/write power. Click File - Settings to display the Settings window.

![Image of Settings Window](image)

**Figure 7-29  RFID - Settings Window**

To establish settings:

- Enter a number in the *Read Tag Outer Loop:* text box to set the number of outer inventory loops (iterations to read tags). Up to 255 loops are allowed. The default *Read Tag Outer Loop* setting is 5.

- Enter a number in the *Read Tag Inner Loop / Dwell* text box to set the number of inner inventory loops (iterations to read tags). Up to 255 loops are allowed. The default *Read Tag Inner Loop* setting is 3.

  **NOTE** *Read Tag Outer Loop* and *Read Tag Inner Loop* settings attempt to read a tag for a period of time based on the parameters entered in these fields. For more information, refer to the SMDK Help file.

- Select the *Enable Gen2 Tag Reads* (default setting is to read Gen2 tags) check box to enable the mobile computer to read Gen2 tags.

- In the Attenuation area:
  - Set the read strength by moving the *Read* attenuation slide bar to a value in a range between 0 (full read power) and 255 (low read power/off).
  - Set the write strength by moving the *Write* attenuation slide bar to a value in a range between 0 (full write power) and 255 (low write power/off).

- Click OK to exit Settings.

- Click Read Toggle to test the attenuation settings. When clicked, Read Toggle acts like the mobile computer’s trigger and can be used to test tag read and write strength.
Gen2 Operational Settings

The Gen2 Operational Settings window is used to configure the Gen2 tag operational parameters. Click File - Gen2 Settings to display the Gen2 Operational Settings window.

![Gen2 Operational Settings Window](image)

**Figure 7-30  Gen2 Operational Settings Window**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection</td>
<td></td>
<td>Specifies the expected selected flag setting in the target tag population.</td>
</tr>
<tr>
<td></td>
<td>Ignore SL</td>
<td>Ignore the selected flag.</td>
</tr>
<tr>
<td></td>
<td>SL not set</td>
<td>Select tags without the selected flag set.</td>
</tr>
<tr>
<td></td>
<td>SL set</td>
<td>Select tags with the selected flag set.</td>
</tr>
<tr>
<td>Session</td>
<td></td>
<td>Specify the session used in the communication with the target tag population.</td>
</tr>
<tr>
<td></td>
<td>S0</td>
<td>Use session S0</td>
</tr>
<tr>
<td></td>
<td>S1</td>
<td>Use session S1</td>
</tr>
<tr>
<td></td>
<td>S2</td>
<td>Use session S2</td>
</tr>
<tr>
<td></td>
<td>S3</td>
<td>Use session S3</td>
</tr>
<tr>
<td>Target</td>
<td></td>
<td>Specify the expected inventoried flag setting in the target tag population.</td>
</tr>
<tr>
<td></td>
<td>A</td>
<td>Select tags with the inventoried flag set to A.</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>Select tags with the inventoried flag set to B.</td>
</tr>
<tr>
<td>Starting</td>
<td></td>
<td>Sets the number of slots in the first inventory round of the inventory algorithm.</td>
</tr>
<tr>
<td></td>
<td>0 - 15</td>
<td>Set the number of slots in the first inventory round of the inventory algorithm from 1 to 15.</td>
</tr>
</tbody>
</table>

**Exit**

Click File - Exit to exit the Gemini RFID sample application.
Mode Menu

Click the Mode menu to use the Inventory method to read tags, locate a tag, program a tag, scan a bar code, or write a tag. Mode menu options offer all of the operations available by clicking an icon on the main Tags window menu bar.

Inventory

Click Mode - Inventory to start reading tags using the Inventory method. Using this method, the application performs as if the trigger is pulled. Tag read attempts continue until the Inventory menu option is clicked again.

Locate Tag

This option is used to find a specific tag.

1. Click in the main Tags window or click Mode - Locate Tag.

![RFID - Locate Tag Window](image)

2. Enter a valid Tag ID in the text box below the magnifying glass:
   - An 8-byte hex string for 64 bits
   - A 12-byte hex string for 96 bits.

   ![NOTE](image) To pre-fill the text box with a valid Tag ID, select a tag in the main Tags window and click .

3. Pull the trigger to locate the tag. The mobile computer beeps when the tag is found. The faster the beep, the closer the mobile computer is to the located tag. Figure 7-31 shows tag ID 80 00 80 04 23 23 84 33 was read 83 times.

4. Click Back to Global Scroll to return to the main Tags window.
Program Tag

This option can be used to program Gen2 RFID tags.

Gen2 tags can be programmed, erased, locked and killed. Each tag contains 88 or 120 bits, which includes the EPC number (64 or 96 bits), CRC, and Kill Code. Locking, and killing tags requires a Kill Code which is 1 byte (8 bits) long. Since a tag has a very small Kill Code and can be thwarted with many lock/kill attempts, it shuts down after a failed attempt for an extended amount of time (possibly up to 10 hours). In addition, data can be collected by decoding in-range EPC RFID tags that beam back to the mobile computer the information they contain.

![Figure 7-32 RFID - Tag Programming Window](image)

**NOTE** For detailed information about programming tags, refer to the SMDK Help file.

To program RFID tags:

1. Click in the main Tags window or click Mode - Program Tag.
2. Select the Class: 1 radio button to program tags.
3. In the Tag ID (Hex string) text box below Class:, enter an 8-byte (64 bits) or 12-byte (96 bits) hex string to be programmed into the tag. This string can contain any number from 0-9, and a letter from A-F. Each byte must consist of 2 characters. Each byte should be separated by a space character.

   For example, if the tag should contain 80012390AAFD3617, type 80 01 23 90 AA FD 36 17 as shown in Figure 7-32.

4. Set the write strength by moving the Write Att: (attenuation) slide bar to a value in a range between 0 (full write power) and 255 (low write power/off).
5. A password is required to lock a tag and kill a tag. In the 0x: Lock/Kill Code text box, enter a hex lock/kill password code.

   **NOTE** Remember the lock/kill code. Once a tag is locked, it cannot be killed without the lock/kill code.

6. Click Program Tags. It might take more than one attempt to program the tag.
7. When a tag is successfully programmed, a status message displays in the Status Message text box.
8. Click Read to read a newly programmed tag.
9. Click **Erase** to erase an unlocked tag.

10. Click **Lock** to lock a tag so that it cannot be changed. A lock/kill code is required to lock a tag. See *Program Tag on page 7-36*.

11. Click **Kill** to make a tag unreadable. A lock/kill code is required to kill a tag. (See *Program Tag on page 7-36*.)

12. Click **Back to Global Scroll** to return to the main *Tags* window.

*NOTE* For a successful tag read, the allowable read distance from the front of the mobile computer scan exit window to the tag is 0.2 ft - 10 ft (0.061 m to 3.1 m).

*NOTE* To successfully write data to a tag, the tag must be no less than 1 ft (.31 m) from the antenna and no greater than 2 ft (.61 m) from the antenna.
Chapter 8 Bluetooth Setup

Introduction

Bluetooth-equipped devices can communicate without wires, using frequency-hopping spread spectrum (FHSS) RF to transmit and receive data in the 2.4 GHz Industry Scientific and Medical (ISM) band (802.15.1). Bluetooth wireless technology is specifically designed for short-range (30 feet/10 meters) communications and low power consumption. Readers with Bluetooth capabilities can exchange information (e.g., files, appointments and tasks) with other Bluetooth enabled devices such as phones, printers, access points and RFID readers. Zebra readers with Bluetooth technology use the StoneStreet One Bluetooth stack. To program Bluetooth within the reader refer to the StoneStreet One SDK.

This chapter provides an overview of the Bluetooth functions and the RD5000 Bluetooth connection procedures. The following topics are provided:

- Adaptive Frequency Hopping on page 8-2
- Security on page 8-2
- Turning the Bluetooth Radio Mode On and Off on page 8-3
- Bluetooth Profiles on page 8-5
- Modes on page 8-6
- Discovering Bluetooth Device(s) on page 8-10
- Discovering Services on page 8-15
- Bluetooth Settings on page 8-21
- Tag Logging Setup Using RFID Demo Example on page 8-30
Adaptive Frequency Hopping

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

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

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

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

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

Security

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

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

It is recommended:

- Perform pairing in a secure environment
- Keep PIN codes private and do not store the PIN codes in the reader
- Implement application-level security
Turning the Bluetooth Radio Mode On and Off

Turn off the Bluetooth radio to save power or if entering an area with radio restrictions (e.g., an airplane). When the radio is off, the reader can not be seen or connected to by other Bluetooth devices. Turn on the Bluetooth radio to exchange information with other Bluetooth devices (within range). Communicate only with Bluetooth radios in close proximity.

✓ NOTE To achieve the best battery life in readers with multiple radios, turn off the radios that are not being used.

Disable Bluetooth

To disable Bluetooth, click Bluetooth icon > Disable Bluetooth. The Bluetooth icon changes to indicate that Bluetooth is disabled. An exclamation point appears with the icon.

![Disable Bluetooth](image)

Figure 8-1 Disable Bluetooth

Enable Bluetooth

To enable Bluetooth, click Bluetooth icon > Enable Bluetooth. The Bluetooth icon changes to indicate that Bluetooth is enabled.

![Enable Bluetooth](image)

Figure 8-2 Enable Bluetooth
Bluetooth Power States

Cold Boot
When a cold boot is performed on the reader, Bluetooth turns off. It is normal to see the Bluetooth icon appear and disappear, as well as a wait cursor, when initialization proceeds in all modes.

Warm Boot
When a warm boot is performed on the reader, Bluetooth returns to the disabled state (off).

Suspend
When the reader suspends, Bluetooth turns off.

Resume
When the reader resumes, Bluetooth turns on if it was on prior to suspend. Note that any Bluetooth connection that was dropped during a suspend needs to be reconnected after a resume.

NOTE  By default from BT stack, BT will not turn on after boot.

NOTE  It is now possible to make a connection with BT explorer, this was not possible in earlier versions.
Bluetooth Profiles

The reader is loaded with a number of Bluetooth services profiles. These profiles can be loaded or removed from memory. If a profile is not used, it can be removed to save memory. To load or remove profiles:

1. On Windows CE 5.0 devices only, if BTExplorer is running, click > Disable Bluetooth.

2. Click > Programs > BTProfileSelector. The ProfileSelector window appears.

3. Click a check box next to the profile to load (activate). The Serial Port profile is always active and cannot be removed.

4. Click Select All to select all profiles or click Deselect All to deselect all profiles.

5. Click Apply to activate the profiles and then Close to exit the application.

6. On Windows CE 5.0 devices only, click > Enable Bluetooth to enable BTExplorer application.

See Services Tab on page 8-22 for more information on selecting services.
Modes

The BTExplorer application has two modes for managing Bluetooth connections: Wizard Mode and Explorer Mode. The Wizard Mode is for novice Bluetooth users and the Explorer Mode is for experienced Bluetooth users.

Wizard Mode

Wizard Mode provides a simple step by step process for discovering and connecting to Bluetooth devices. The wizard steps through the entire process.

NOTE When switching between Wizard Mode and Explorer Mode, all active connections are closed.

The following steps provide an example for using the Wizard to services for remote devices.

1. Click the Bluetooth icon and select Show BTExplorer. The BTExplorer window appears.
2. Click File > New Connection. The New Connection Wizard window appears.

![New Connection Wizard Window](image)

3. Select an action from the drop-down list. In this example, Explore Services on Remote Device is selected.
4. Click Next. The BTExplorer searches for Bluetooth devices in the area and displays the devices in the Select Remote Device window.
5. Select a device from the list and then click **Next**. The **Connection Favorite Options** window appears.

![Select Remote Device Window]

**Figure 8-5**  Select Remote Device Window

![Connection Favorite Options Window]

**Figure 8-6**  Connection Favorite Options Window

6. Select **Save As Favorite** check box to save this service in the **Favorite** view.

7. In the **Favorite Name** text box, enter a name for this service that will appear in the **Favorite** list.

8. Click **Next**. The **Connection Summary** window appears.

**NOTE**  Devices discovered previously are listed to save time. To start a new device discovery, click and hold and select **Discover Devices** from the menu.
9. Click **Connect** to connect to the service.

The following actions are available in the drop-down list (actions may vary depending upon configurations):

- Explore Services on Remote Device
- Pair with a Remote Device
- Active Sync via Bluetooth
- Browse Files on Remote Device
- Connect to Internet Using Access Point
- Connect to Internet Using Phone/Modem
- Connect to a Personal Area Network
- Send or Exchange Objects
- Associate Serial Port.
Explorer Mode

The **BTExplorer** window is streamlined and easy to navigate and provides greater control to users familiar with Bluetooth functionality. The menu bar provides quick access to the options and tools used to connect to devices.

![Explorer Mode Window](image)

**Figure 8-8**  Explorer Mode Window

Use the "click and hold" technique to view available options. Scroll bars and view options are similar to the ones used on the Windows desktop. The tree structure lists the following sub-items:

- Local Device - MC909X
- Remote Device - Other Bluetooth devices
  - Trusted Devices - Bonded (paired) Bluetooth devices
  - Untrusted Devices - Discovered devices that are not bonded
- Favorites - Selected services that are set as being *Favorite* for quick access.

**NOTE**  Switching between Wizard Mode and Explorer Mode closes all active connections.
Discovering Bluetooth Device(s)

Follow the steps below to discover Bluetooth devices. The reader can receive information from discovered devices, without bonding. However, once bonded, an exchange of information between the reader and a bonded device occurs automatically when the Bluetooth radio is turned on.

![NOTE]
The RFIDDemo application supports only sending out tag data on Bluetooth port. It does not support accepting incoming connections for Bluetooth devices.

To find Bluetooth devices in the area:

1. Ensure that the Bluetooth device being looked for is in discoverable mode.

2. Ensure that the two devices are within 30 feet (10 meters) of one another.

3. Click the Bluetooth icon and select Show BTExplorer. The BTExplorer window appears.

![Figure 8-9] BTExplorer Window

4. Click and hold Remote Devices and select Discover Devices from the pop-up menu. The reader searches for Bluetooth devices in the area.

![Figure 8-10] Discover Devices

5. The discovered devices display in the Untrusted Devices folder.
Bonding with Discovered Device(s)

A bond is a relationship created between the reader and another Bluetooth device in order to exchange information in a secure manner. Creating a bond involves entering the same PIN on the two devices to bond. Once a bond is created, and the Bluetooth radios are turned on, the devices recognize the bond and are able to exchange information without re-entering a PIN.

To bond with a discovered Bluetooth device:

1. Discover remote devices. See Discovering Bluetooth Device(s) on page 8-10.

2. In the Untrusted Devices folder, click and hold on a device to pair with.

3. Select Pair from the pop-up menu.

4. On the reader, the PIN Code Request window appears.
5. In the PIN Code: text box, enter the PIN number (between 1 and 16 characters) and then click OK.

6. On the remote device, enter the same PIN number.

7. The devices are successfully paired. The device name moves to the Trusted Devices folder.

Renaming a Bonded Device

If it is necessary to rename a bonded device, it can be done from the BTExplorer window.

1. Launch BTExplorer.

2. Click and hold the device to rename and select Rename in the pop-up menu.
3. The **Change Device Name** window appears.

4. Enter a new name for the bonded device in the text box. Click **OK**.

**Deleting a Bonded Device**

If it is no longer necessary to connect with a device, delete it from the **Bluetooth Bonded Devices** window.

1. Launch **BTExplorer**.

2. Click and hold the device to delete and select **Delete** in the pop-up menu.
3. A confirmation dialog appears. Click Yes.

**Accepting a Bond**

When a remote device wants to bond with a reader, give permission by entering a PIN when requested.

1. Ensure that the reader is set to discoverable and connectable. See *Bluetooth Settings on page 8-21*.

2. When prompted to bond with the remote device the **PIN Code Request** window appears.

   ![PIN Code Request Window](image)

   **Figure 8-18**  *PIN Code Request Window*

   - **NOTE** Connections to untrusted devices are a security risk.

3. In the **PIN Code**: text box, enter the same PIN that was entered on the device requesting the bond. The PIN must be between 1 and 16 characters.

4. In the **Device Name**: text box, edit the name of the device requesting the bond, if desired.

5. Click **OK**.

6. The bond is created and the reader can now exchange information with the other device.
Discovering Services

Before services can be used, discover the available remote devices and then bond to those devices.

To determine what services are available on a bonded remote device:

1. Click the Bluetooth icon and select Show BTEexplorer.

2. In BTEexplorer window, click and hold on the remote device and select Explore from the pop-up menu.

3. The reader communicates with the remote device and then lists the services under the device name.

Some examples of available services are:

- File Transfer Services
- Dial-Up Networking Services
- Headset or Hands-Free Services
- OBEX Object Push Services
- Serial Port Services
- IrMA Synchronization Services.

These services are discussed in the following paragraphs.
File Transfer Services

To transfer files between the reader and another Bluetooth enabled device:

1. Ensure the reader is discoverable and connectable. See Bluetooth Settings on page 8-21.
2. Discover and bond (pair) with the remote access point. See Bonding with Discovered Device(s) on page 8-11.
3. In BTExplorer, select the Remote Devices folder.
4. Select the Trusted Devices folder.
5. Click the remote device folder.
6. Click and hold on the remote device and select Explore from the pop-up menu.
7. Click and hold on File Transfer and select Connect. The remote device’s accessible folders appear.
8. Select a folder. The contents of the folder appear in the sub-window.

![Remote Device Folders](image)

**Figure 8-21 Remote Device Folders**

9. Click and hold on the file. A pop-up menu appears.
10. Select the action to perform:
    a. New - create a new file or folder on the remote device
    b. Delete - delete the selected file on the remote device.
    c. Get File - copy the file from the remote device to the reader.
    d. Put File - copies a file from the reader to the remote device.

**Create New File or Folder**

To create a new folder or file on the remote device:

1. Click and hold on the file and select New > Folder or New > File. The Create New Folder or Create New File window appears.
2. Enter the name for the new folder or file. Click OK.
3. A new folder or file is created on the remote device.

**NOTE** Shared folders are a security risk.
Delete File
To delete a file from the remote device:
1. Click and hold on the file and select Delete.
2. In the Delete Remote Device File dialog box click OK.

Get File
To copy a file from a remote device:
1. Click and hold on the file and select Get. The Save Remote File window appears.
2. Navigate to the directory to save the file.
3. Click Save. The file is transferred from the remote device to the reader.

Put File
To copy a file to a remote device:
1. Click and hold on the file and select Put. The Send Local File window appears.
2. Navigate to the directory to save the file and select a file.
3. Click Open. The file is transferred from the reader to the remote device.

Connect to Internet Using Access Point
This section explains how to access a Bluetooth-enabled LAN access point (AP) for a network connection. With this method of communication the Internet Explorer can be used to connect to a server.

1. Ensure the reader is discoverable and connectable. See Bluetooth Settings on page 8-21.
2. Discover and bond (pair) with the remote access point. See Bonding with Discovered Device(s) on page 8-11.
3. In BTExplorer, select the Remote Devices folder.
4. Select the Trusted Devices folder.
5. Click the remote device folder.
6. Click and hold the remote device and select Explore from the pop-up menu.
7. Click and hold LAN Access using PPP service and select Connect from the pop-up menu.
8. The reader connects with the Access Point.
9. Click Start > Internet Explorer. The Internet Explorer window appears.
10. In the address field, enter an internet address and click the Enter button. The web page loads.
OBEX Object Push Services

Object Exchange (OBEX) is a set of protocols allowing objects such as Contacts or pictures to be shared using Bluetooth.

To exchange contact information with another Bluetooth enabled device:

1. Ensure the reader is discoverable and connectable. See Bluetooth Settings on page 8-21.
2. Discover and bond (pair) with the remote device. See Bonding with Discovered Device(s) on page 8-11.
3. In BTExplorer, select the Remote Devices folder.
4. Select the Trusted Devices folder.
5. Click the remote device folder.
6. Click and hold on OBEX Object Push and select Connect. The OBEX Object Push window appears.
7. In the Action drop-down list, select one of the options: Send Contact Information, Swap Contact Information, Fetch Contact Information or Send a Picture.

Send a Picture

To send a picture to another device:

1. Ensure the reader is discoverable and connectable. See Bluetooth Settings on page 8-21.
2. Discover and bond (pair) with the remote device. See Bonding with Discovered Device(s) on page 8-11.
3. In BTExplorer, select the Remote Devices folder.
4. Select the Trusted Devices folder.
5. Click the remote device folder.
6. Click and hold on OBEX Object Push and select Connect. The OBEX Object Push window appears.
7. In the Action drop-down list, select Send A Picture.
8. Click . The Send Local Picture window appears.
10. Navigate to the picture to be send to the other device.

11. Click **Open**.

12. Click **OK**. The picture is sent to the other device and a confirmation dialog box appears on the other device to accept the picture. A **Send Picture** dialog appears.

13. Click **Ok**.

**Headset Services**

Headset services are not enabled on the RD5000.
Serial Port Services

**NOTE** By default, COM ports COM4, COM5 and COM9 are Bluetooth virtual ports. If an application opens one of these ports, the Bluetooth driver activates and steps through a Bluetooth connection setup.

Use the wireless Bluetooth serial port connection like a physical serial cable connection. The application that will use the connection to the correct serial port must be configured.

To establish a serial port connection:

1. Ensure the reader is discoverable and connectable. See Bluetooth Settings on page 8-21.
2. Discover and bond (pair) with the remote device. See Bonding with Discovered Device(s) on page 8-11.
3. In BTExplorer, select the Remote Devices folder.
4. Select the Trusted Devices folder.
5. Click the remote device folder.
6. Click and hold Serial Port and select Connect in the pop-up menu. The Remote Service Connection window appears.

![Remote Service Connection Window](image)

7. In the Local COM Port drop-down list select a COM port.
8. Click OK.

Personal Area Network Services

Connect two or more Bluetooth devices to share files, collaborate or play multi player games.

To establish a Personal Area Network connection:

1. Ensure the reader is discoverable and connectable. See Bluetooth Settings on page 8-21.
2. Discover and bond (pair) with the remote device. See Bonding with Discovered Device(s) on page 8-11.
3. In BTExplorer, select the Remote Devices folder.
4. Select the Trusted Devices folder.
5. Click the remote device folder.
6. Click and hold Personal Area Network and select Connect in the pop-up menu.
Bluetooth Settings

Use the BTExplorer Settings window to configure the operation of the BTExplorer application. Click Tools > Settings. The BTExplorer Settings window appears.

Device Info Tab

Use the Device Info tab to configure the Bluetooth connection modes.

![BTExplorer Settings - Device Info Tab](image)

**Device Info Tab**

- **Device Name**
  - Displays the name of the reader.

- **Discoverable Mode**
  - Allows the reader to be set to discoverable by other Bluetooth devices or to be set to not discoverable.
  - **Note:** For security reasons, the default is set to Non Discoverable.

- **Connectable Mode**
  - Allows the reader to be set to connectable by other Bluetooth devices or set to not connectable.
  - **Note:** For security reasons, the default is set to Non Connectable.
Services Tab

NOTE  For security reason, by default services are not enabled.

Use the Services tab to add or delete Bluetooth services.

![BTExplorer Settings - Services Tab](image)

**Figure 8-26  BTExplorer Settings - Services Tab**

To add a service:

1. Click Add. The Add Local Service window displays.

![Add Local Service Window](image)

**Figure 8-27  Add Local Service Window**

2. In the list, select a service to add.

3. Click OK. The Edit Local Service window displays for the selected service.

4. Select the appropriate information and then click OK. See the following paragraphs for detailed information on the available services.

Dial-Up Networking Service

Dial-up Networking Services are not enabled on the RD5000.
**File Transfer Service**

File transfer allows files to be browsed by other Bluetooth devices.

![File Transfer Information Window](image)

**Figure 8-28  File Transfer Information Window**

- **Service Name**: Displays the name of the service.
- **Service Security**: Select the security type from the drop-down list; *None, Authenticate* or *Authenticate/Encrypt*.
- **Root Directory**: Select the directory that other Bluetooth devices can access.
- **File Permissions**: Select the file permissions for the selected directory. Check the appropriate box to grant Read access, write access and delete access.
**OBEX Object Push Service**

OBEX Object Push allows contacts, business cards, pictures, appointments, and tasks to be pushed to the device by other Bluetooth devices.

![OBEX Exchange Information Window](image)

**Figure 8-29  **OBEX Exchange Information Window

- **Service Name** Displays the name of the service.
- **Service Security** Select the security type from the drop-down list; *None, Authenticate* or *Authenticate/Encrypt*.
- **Business Card** Select a contact information to another mobile device.
- **Do not allow clients to push objects** Disables clients from pushing objects to the reader.
- **Inbox Directory** Select a directory where another Bluetooth device can store files.

**Personal Area Networking Service**

Personal Area Networking hosts a network which allows communication with other Bluetooth devices.

![Personal Area Networking Window](image)

**Figure 8-30  **Personal Area Networking Window

- **Service Name** Displays the name of the service.
- **Service Security** Select the security type from the drop-down list; *None, Authenticate* or *Authenticate/Encrypt*.
- **Support Group Ad-Hoc Networking** Select to enable Ad-Hoc networking.
Serial Port Service

Serial port allows COM ports to be accessed by other Bluetooth devices.

![Serial Port Service Window](image)

**Figure 8-31 Serial Port Service Window**

- **Service Name**: Displays the name of the service.
- **Service Security**: Select the security type from the drop-down list; *None, Authenticate* or *Authenticate/Encrypt*.
- **Local COM Port**: Select the COM port. Select COM1 to use a modem or other device that is connected to the connector on the bottom of the reader.
- **Local Baud Rate**: Select the communication baud rate.
- **Local Port Options**: Select the port option.

Headset Service

Headset services are not enabled on the RD5000.
Security Tab

To adjust the security settings for an individual service, select the Services tab first, then select the individual service, then Properties.

![BTExplorer Settings - Security Tab](image)

**Figure 8-32  BTExplorer Settings - Security Tab**

- **Use PIN Code (Incoming Connecting)**: Automatic use of the PIN code entered in the PIN Code text box. It is recommended not to use this automatic PIN code feature. See Security on page 8-2 for more information.
- **PIN Code**: Enter the PIN code.
- **Encrypt Link On All Outgoing Connections**: Select to enable or disable encryption. Use encryption whenever possible.
Discovery Tab

Use the **Discovery** tab to set and modify discovered devices.

![BTExplorer Settings - Discovery Tab](image)

**Figure 8-33**  *BTExplorer Settings - Discovery Tab*

- **Inquiry Length**: Sets the amount of time that the reader takes to discover Bluetooth devices in the area.
- **Name Discovery Mode**: Select either **Automatic** or **manual**.
- **Discovered Devices**: Deletes all discovered devices and link keys.
Virtual COM Port Tab

Use the Virtual COM Port tab to select the COM ports for Bluetooth communication.

![Virtual COM Port Tab](image)

**Figure 8-34** BTExplorer Settings - Virtual COM Port Tab

- COM4: Bluetooth Enable or disable COM Port 4.
- COM5: Bluetooth Enable or disable COM Port 5
- COM9: Bluetooth Enable or disable COM Port 9

![COM Port Connection](image)

**Figure 8-35** COM Port Connection

**NOTE** If an application uses one of the COM ports assigned to Bluetooth, opening this port causes the Bluetooth stack to activate and step through the connection process.
Miscellaneous Tab

Highlight Connections

Select the connection type to highlight when connected. In the Wizard Mode, the only option is Favorites or None. In the Explorer Mode the options are None, Tree View Only, List View Only or Tree and List View.

Apply Text Style

Select the text style to be applied to the connection text.

Apply Text Color

Select the text color to be applied to the connection text.
Tag Logging Setup Using RFID Demo Example

The purpose of tag logging demo here is to show RFID data being captured to remote device via bluetooth. The example provides setup information for both the RD5000 and for the VRC (the example other terminal):

On the RD5000:

Active sync the RD5000 and use a tool like SOTI Pocket Controller tool to display of RD5000 windows on a local PC.

1. Go to Start menu->Settings->Control Panel->System and click the Device name tab. Enter RD5000 as the device name and click OK, and then click X to get on default device screen.

2. Click on BT icon in right corner of screen and select Enable Bluetooth.

3. Click again on BT icon and select Show BTExplorer.

4. Go to View and select Explorer Mode.

5. Go to Local Device->RD5000 (Windows CE will be displayed if the RD5000 reader was not renamed). Right click on it.

6. Change the Set Discoverability option to Discoverable.
7. Change the Set Connectibility option to Connectable.

8. Right click on RD5000; again and go to Settings->Services tab.

9. Click Add and Add Serial Port service. Set Service name as Serial Port5 and select COM5:

![Figure 8-39 Physical Device Settings Window]

10. Click OK to exit and minimize BT Explorer. Do not click the X button this discards the new settings.

11. Run the RFIDDemo application.

12. Click the Settings button, in the Tag logging option:
   Enter:
   Address: COM5:
   Port: 5
   Speed: 115200
   Imp: Uncheck the Log to File option.
   Use COM5 as the example port to connect to.

13. Click OK and exit the RFIDDemo application.

On VRC (or any other terminal):

Use a third party application (such as mobileterminalev_pc_install.exe) to capture data. This is a third party application from internet (used in this example). Any similar application can be actually used.

1. Pre-requisite: Install the demo application mobileterminalev_pc_install.exe on remote device (VRC is being used as an example, where the tag data is to be received). Active sync to VRC and run the mobileterminalev_pc_install.exe application on the PC. Complete installation steps on your device. The application will appear on your device in Start->Programs->Mobile Terminal EV.

2. From BT Explorer icon in right bottom corner of the screen, click Enable Bluetooth.

3. Run the Mobile Terminal EV application on VRC device from Start->Programs.

   √ NOTE If the app has already been configured accordingly for BT, Go to menu Comm->Open port and proceed directly to step 8

4. Go to Comm->Properties. Select port as COM5 and baud rate as 115200. Click OK.
   Go to Comm->Open port.
Go to menu Comm->Properties and set Port to COM5
(This is local port on VRC, by default COM4,5,9 are BT ports).

Figure 8-40 Communications Window

5. The Select Remote Device Window displays the BT discovered devices. Select the RD5000 and click Next.

Figure 8-41 Select Remote Device Window

6. A serial port selection screen displays. Set the local port (on VRC) to connect to COM5: and click Next.

Figure 8-42 Connection Favorite Options Window
7. Click Connect in the Connection summary window.

![Connection Summary Window](image)

**Figure 8-43  Connection Summary Window**

8. The Bluetooth Connection window confirms that the Bluetooth connection is now established and the Bluetooth icon (in right corner of screen) has a green bar on it.

![Bluetooth Connection Window](image)

**Figure 8-44  Bluetooth Connection Window**

9. Return to the RD5000, run the RFIDDemo application and Start Reading tags.

![Remote Tag Data Window](image)

**Figure 8-45  Remote Tag Data Window**

10. On VRC, the same tag data is displayed.

    **NOTE** Confirm that the host application on remote device is opened and listening before RFID Demo is started and check BT Explorer version.
Chapter 9 Maintenance & Troubleshooting

Introduction

This chapter includes instructions on cleaning and storing the RFID reader, and provides troubleshooting solutions for potential problems during RFID reader operating.

Maintaining the RFID reader

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

- Although the RFID reader is water and dust resistant, it is good practice not to expose it to rain or moisture for an extended period of time.
- The battery must be changed in a clean dry area.
- Protect the RFID reader from temperature extremes. Keep it away from heat sources.
- Do not store or use the RFID reader in any location that is extremely dusty, damp or wet.
- Use a soft cloth to clean the RFID reader. If the surface of the RFID reader becomes soiled, clean it with a soft cloth moistened with a diluted window-cleaning solution.

Battery Safety Guidelines

- The area in which the units are charged should be clear of debris and combustible materials or chemicals. Particular care should be taken where the device is charged in a non-commercial environment.
- Do not use incompatible batteries and chargers. For any questions about the compatibility of a battery or a charger, contact Zebra support. See Service Information on page i-xiv for contact information.
- Do not crush, puncture, or place a high degree of pressure on the battery.
- Severe impact from dropping any battery-operated device on a hard surface could cause the battery to overheat.
- 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.
• Do not dispose of batteries in fire.
• If battery or equipment is suspected, call Zebra support to arrange for inspection. See Service Information on page xiv for contact information.

## Troubleshooting

### RFID Reader

<table>
<thead>
<tr>
<th>Problem</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID reader does not turn on.</td>
<td>Lithium-ion battery not charged.</td>
<td>Charge or replace the lithium-ion battery in the RFID reader.</td>
</tr>
<tr>
<td></td>
<td>Lithium-ion battery not installed properly.</td>
<td>Ensure battery is installed properly. See Installing and Removing the Battery on page 1-5.</td>
</tr>
<tr>
<td></td>
<td>System crash.</td>
<td>Perform a warm boot. If the RFID reader still does not turn on, perform a cold boot. See Resetting the Reader on page 1-15.</td>
</tr>
<tr>
<td>Rechargeable lithium-ion battery did not charge.</td>
<td>Battery failed.</td>
<td>Replace battery. If the RFID reader still does not operate, try a warm boot, then a cold boot. See Resetting the Reader on page 1-15.</td>
</tr>
<tr>
<td></td>
<td>RFID reader removed from cradle while battery was charging.</td>
<td>Insert RFID reader in cradle and begin charging. The lithium-ion battery requires less than four hours to recharge fully.</td>
</tr>
<tr>
<td>During data communication, no data was transmitted, or transmitted data was incomplete.</td>
<td>RFID reader unplugged from host computer during communication.</td>
<td>Reattach the Synchronization cable and re-transmit.</td>
</tr>
<tr>
<td></td>
<td>Incorrect cable configuration.</td>
<td>See the System Administrator.</td>
</tr>
<tr>
<td></td>
<td>Communication software was incorrectly installed or configured.</td>
<td>Perform setup. See Chapter 3, Accessories for details.</td>
</tr>
<tr>
<td></td>
<td>Ensure that Microsoft ActiveSync 4.1 or greater is installed on the host computer.</td>
<td></td>
</tr>
<tr>
<td>No sound is audible.</td>
<td>Volume setting is low or turned off.</td>
<td>Unit may be a beeper only unit or incorrect Config Block is programmed into device.</td>
</tr>
</tbody>
</table>
### Table 9-1  Troubleshooting the RFID reader (Continued)

<table>
<thead>
<tr>
<th>Problem</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID reader turns itself off.</td>
<td>RFID reader is inactive.</td>
<td>The RFID reader turns off after a period of inactivity. If the RFID reader is running on battery power, this period can be set to 30 sec., 1, 2, 3, 4, 5 or 6 minutes. If the RFID reader is running on external power, this period can be set to 1, 2, 3, 5, 10, 15 and 30 minutes. For WinCE 5.0 devices, Check the power settings by tapping <strong>Start &gt; Settings &gt; Control Panel &gt; Power</strong> icon &gt; <strong>Power Off</strong> tab. Change the setting if a longer delay is required before the automatic shutoff feature activates.</td>
</tr>
<tr>
<td>Battery is depleted.</td>
<td>Replace the battery.</td>
<td></td>
</tr>
<tr>
<td>Battery is not inserted properly.</td>
<td>Insert the battery properly (see <em>Installing and Removing the Battery on page 1-5</em>).</td>
<td></td>
</tr>
<tr>
<td>Error LED is on, the RFID reader memory is full.</td>
<td>Too many files stored on the RFID reader.</td>
<td>Delete unused memos and records. Save these records on the host computer.</td>
</tr>
<tr>
<td></td>
<td>Too many applications installed on the RFID reader.</td>
<td>If additional applications have been installed on the RFID reader, remove them to recover memory. For Windows Mobile 5.0 devices, tap <strong>Start &gt; Settings &gt; System tab &gt; Remove Programs</strong> icon. For WinCE 5.0 devices, tap <strong>Start &gt; Settings &gt; Control Panel &gt; Remove Programs</strong> icon. Select the unused program and tap <strong>Remove</strong>.</td>
</tr>
<tr>
<td>The RFID reader does not read a tag.</td>
<td>Read application is not loaded.</td>
<td>Verify that the unit is loaded with a read application. See the System Administrator.</td>
</tr>
<tr>
<td></td>
<td>Unreadable tag.</td>
<td>Ensure the tag is not defective.</td>
</tr>
<tr>
<td></td>
<td>Distance between the reader and the tag is incorrect.</td>
<td>Ensure RFID reader is within proper read range.</td>
</tr>
<tr>
<td></td>
<td>RFID reader is not programmed for the tag type.</td>
<td>Ensure the RFID reader is programmed to accept the tag type being read.</td>
</tr>
<tr>
<td></td>
<td>Battery is low.</td>
<td>If the reader stops reading check the battery level. When the battery is low, the reader shuts off. Note: If the reader is still not reading, contact the distributor or Zebra.</td>
</tr>
</tbody>
</table>
Bluetooth Connection

Table 9-2  Troubleshooting Bluetooth Connection

<table>
<thead>
<tr>
<th>Problem</th>
<th>Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID reader cannot find any Bluetooth devices nearby.</td>
<td>Too far from other Bluetooth devices.</td>
<td>Move closer to the other Bluetooth device(s), within a range of 10 meters.</td>
</tr>
<tr>
<td></td>
<td>The Bluetooth device(s) nearby are not turned on.</td>
<td>Turn on the Bluetooth device(s).</td>
</tr>
<tr>
<td></td>
<td>The Bluetooth device(s) are not in discoverable mode.</td>
<td>Set the Bluetooth device(s) to discoverable mode. If needed, refer to the device’s user documentation for help.</td>
</tr>
<tr>
<td>RFID reader keeps powering down to protect memory contents.</td>
<td>The RFID reader’s battery is low.</td>
<td>Recharge the battery.</td>
</tr>
<tr>
<td>There is a delay in the Bluetooth stack re-initializing during a resume from suspend.</td>
<td>This is the normal behavior.</td>
<td>No solution required.</td>
</tr>
</tbody>
</table>

Four Slot Spare Battery Charger

Table 9-3  Troubleshooting The Four Slot Spare Battery Charger

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batteries not charging.</td>
<td>Battery was removed from the charger or charger was unplugged from AC power too soon.</td>
</tr>
<tr>
<td></td>
<td>Ensure MSR is receiving power. Ensure RFID reader is attached correctly. Confirm main battery is charging. If a RFID reader battery is fully depleted, it can take up to four hours to fully recharge a battery (if the RFID reader is off and longer if the RFID reader is operating). For WinCE 5.0 devices, view battery status by tapping Start &gt; Settings &gt; Control Panel &gt; Power icon.</td>
</tr>
<tr>
<td>Battery is faulty.</td>
<td>Verify that other batteries charge properly. If so, replace the faulty battery.</td>
</tr>
<tr>
<td>Battery contacts not connected to charger.</td>
<td>Verify that the battery is seated in the battery well correctly with the contacts facing down.</td>
</tr>
</tbody>
</table>
Appendix A  Technical Specifications

Technical Specifications

The following tables summarize the RFID reader intended operating environment and general technical hardware specifications.

RFID Reader

The following table summarizes the reader’s technical specifications.

Table A-1  RD5000 Technical Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>RD5000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical and Environmental Characteristics</strong></td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td>7 in. L x 9 in. W x 2 in. H 17.78 cm L x 22.86 cm W x 5.08 cm H</td>
</tr>
<tr>
<td>Weight</td>
<td>3 lbs 10 oz./1.64 kg (includes battery)</td>
</tr>
<tr>
<td>Battery</td>
<td>Removable, rechargeable 7.2 volt Lithium Ion 2200 mAh battery pack, 15.8 watt hours</td>
</tr>
<tr>
<td><strong>Performance Characteristics</strong></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Intel® XScale® Bulverde PXA270 processor at 624MHz</td>
</tr>
<tr>
<td>Operating System</td>
<td>Microsoft Windows CE 5.0</td>
</tr>
<tr>
<td>Memory (RAM/ROM)</td>
<td>64MB/64MB</td>
</tr>
<tr>
<td>Application Development</td>
<td>PSDK, DCP and SMDK available through the Support Web Site</td>
</tr>
<tr>
<td>Data Capture Options</td>
<td>Gen2 tags (default)</td>
</tr>
<tr>
<td></td>
<td>Configurable for Class 0 and Class 1 tags</td>
</tr>
</tbody>
</table>
### RD5000 Technical Specifications (Continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>RD5000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Environment</strong></td>
<td></td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-4°F to 122°F (-20°C to 50°C)</td>
</tr>
<tr>
<td>Battery Charging Temperature</td>
<td>32°F to 104°F / 0°C to 40°C ambient temperature range</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40°F to 158°F / -40° to 70°C</td>
</tr>
<tr>
<td>Humidity</td>
<td>5% to 95% non condensing</td>
</tr>
<tr>
<td>Drop Specification</td>
<td>30 in. / 76.2 cm to concrete</td>
</tr>
<tr>
<td>Repetitive Shock</td>
<td>Over 3,500 70-g shocks and 21,600 60-g shocks</td>
</tr>
<tr>
<td>Environmental Sealing</td>
<td>IP66</td>
</tr>
<tr>
<td>ESD</td>
<td>+/-15kVdc air discharge</td>
</tr>
<tr>
<td></td>
<td>+/-8kVdc direct discharge</td>
</tr>
<tr>
<td></td>
<td>+/-8kVdc indirect discharge</td>
</tr>
<tr>
<td><strong>RFID</strong></td>
<td></td>
</tr>
<tr>
<td>Standards Supported</td>
<td>EPC Generation 2 UHF</td>
</tr>
<tr>
<td>Nominal read range(^1)</td>
<td>10 ft./3.04 m with the RFX6000 4x4 tag optimally oriented.</td>
</tr>
<tr>
<td>Field</td>
<td>Half read range beam width: +/- 80 degrees (with tags optimally oriented).</td>
</tr>
<tr>
<td>Antenna</td>
<td>Integrated, circularly polarized, 1.5 dB effective linear gain per axis (nominal); Antenna port for future support of optional external antenna.</td>
</tr>
<tr>
<td>Frequency Range</td>
<td>902-928 MHz</td>
</tr>
<tr>
<td>Output power</td>
<td>1W conducted (1.4W EIRP with integrated antenna)</td>
</tr>
<tr>
<td><strong>Wireless Data Communications</strong></td>
<td></td>
</tr>
<tr>
<td>WLAN</td>
<td>802.11a/b/g</td>
</tr>
<tr>
<td>Output Power</td>
<td>100mW U.S. and International</td>
</tr>
<tr>
<td>Data Rate</td>
<td>802.11a: 54Mb per second</td>
</tr>
<tr>
<td></td>
<td>802.11b: 11Mb per second</td>
</tr>
<tr>
<td></td>
<td>802.11g: 54Mb per second</td>
</tr>
<tr>
<td>Antenna</td>
<td>Internal</td>
</tr>
<tr>
<td>Frequency Range:</td>
<td>802.11a: 5 GHz; country-dependent</td>
</tr>
<tr>
<td></td>
<td>802.11b: 2.4 GHz; country-dependent</td>
</tr>
<tr>
<td></td>
<td>802.11g: 2.4 GHz; country-dependent</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>Bluetooth® Version 1.2 with BTExplorer™ (manager) included</td>
</tr>
<tr>
<td>Item</td>
<td>RD5000</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Peripherals and Accessories</strong></td>
<td></td>
</tr>
<tr>
<td>Charging</td>
<td>Four Slot Spare Battery Charger, Universal Battery Charger Adapter, Charging Cable, Charging Cable with Serial Communications.</td>
</tr>
<tr>
<td>Power Supply</td>
<td>12 Vdc and a minimum of 3.33 A, certified to EN60950-1 with SELV outputs.</td>
</tr>
<tr>
<td>Other Accessories</td>
<td>USB Communications Cable.</td>
</tr>
<tr>
<td><strong>Regulatory</strong></td>
<td></td>
</tr>
<tr>
<td>Electrical Safety</td>
<td>Certified to UL60950-1, CSA C22.2 No. 60950-1, EN60950-1, IEC 60950-1.</td>
</tr>
<tr>
<td>EMI/RFI</td>
<td>USA — FCC Part 15; Canada — ICES 0003 Class B.</td>
</tr>
</tbody>
</table>
Appendix B Motion Sensor Parameters

Introduction

The Motion/Proximity sensor API for the RD5000 includes a MPS_CMD_MOTION_SET_THRESHOLD command that allowed the setting of an acceleration threshold used to determine whether a motion event had occurred. Modifications to the motion sensing algorithm have made it desirable to allow the reconfiguration of several parameters to optimize the code for different environments and this has been implemented using an extension of this single API call.

API Calls

The API call has been extended using an indexing scheme that dedicates the 3 most significant bits of the 1st 16-bit data word as a parameter identifier. There are currently four parameter sets that may be set using this call. All parameter values default to values specified in motion.h, an include file that forms part of the program source code. Table B-1 to Table B-5 show the programming values required in each case and the defaults that apply. Since in each case only 13 bits remain for specification of a numeric value, values are restricted to unsigned values in the range 0-8191. D is used to designate the do not care bits.

Table B-1 Set Minimum Detectable Velocity Change

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wd1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X</td>
<td>value expressed as 100 * value in ft/sec. (Default is 0.2 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd2</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Y</td>
<td>value expressed as 100 * value in ft/sec. (Default is 0.2 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd3</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Z</td>
<td>value expressed as 100 * value in ft/sec. (Default is 0.2 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Possible Extensions

The design allows for a further four sets of parameters to be configured, this may occur in future code versions. The parameters from the old MPS_CMD_MOTION_GET_THRESHOLD API call cannot be read.

### Table B-2  Set Minimum Velocity for Motion Start Event

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wd1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>X value expressed as 100 * value in ft/sec. (Default is 0.5 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd2</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>Y value expressed as 100 * value in ft/sec. (Default is 0.5 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd3</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>Z value expressed as 100 * value in ft/sec. (Default is 1.0 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table B-3  Set Recalibration Velocity

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wd1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>X value expressed as 100 * value in ft/sec. (Default is 3.0 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd2</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>Y value expressed as 100 * value in ft/sec. (Default is 3.0 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd3</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>Z value expressed as 100 * value in ft/sec. (Default is 3.0 ft/sec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table B-4  Set Miscellaneous Thresholds

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wd1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>Total noise energy in all axes for quiet threshold (Default is 250)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd2</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>Total energy in all axes for shock threshold (Default is 2000)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd3</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>Threshold count of consecutive vel. updates for recal. (Dflt is 10)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table B-5  Reserved for Future Use

<table>
<thead>
<tr>
<th>Bit</th>
<th>15</th>
<th>14</th>
<th>13</th>
<th>12</th>
<th>11</th>
<th>10</th>
<th>9</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wd1</td>
<td>1</td>
<td>X</td>
<td>X</td>
<td>DDDD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd2</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>DDDD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wd3</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>DDDD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Parameter Details**

There are three sets of parameters that govern the basic operation of the motion sensing subsystem. Within each set, there is a parameter that applies to each of the three axes, X, Y and Z. Alignment of the axes in reference to the RD5000 unit is as shown in *Figure B-1*.

![RD5000 Axes Alignment](image)

*Figure B-1  RD5000 Axes Alignment*

The optimum values for a forklift truck for a reliable motion detection displayed in *Figure B-2*.

![MPS Settings Window](image)

*Figure B-2  MPS Settings Window*
Min Detection Parameters:

These parameters govern minimum change in velocity to be detected by the device for calculation of resultant velocity in respective axes. Refer to Set Minimum Detectable Velocity Change (Table B-1 on page B-1) to set values through the API.

Example: The value 20 means, if the velocity change is more than 0.2ft/sec then only device detects the velocity and updates the resultant velocity value. Refer the Set Minimum Detectable Velocity Change table above to set different values through API.

Min Start Parameters:

These parameters govern minimum change in resultant velocity to declare a motion start in respective axes. Refer to Set Minimum Velocity for Motion Start Event (Table B-2 on page B-2) to set values through the API.

Example: The value 100 indicates, the resultant velocity should be at-least 1ft/sec to declare a motion START event in the corresponding axis. If the resultant velocity falls below 1ft/sec, a motion STOPevent is reported for corresponding axis.

Recalibration Parameters:

These parameters set a limit on the estimated velocities in each of the three axes. Refer to Set Recalibration Velocity (Table B-3 on page B-2) to set values through the API.

Example: The value 3000 indicates, a RECALIBRATION event is reported if the resultant velocity exceeds the limit 30ft/sec in the respective axis.

NOTE  The motion sensor is sensitive to orientation. Even a slight orientation change affects the measured baseline and results in continuous velocity updates, triggering a recalibration. In when this happens the previously reported START events may not be valid.

Misc Parameters:

There are three different parameters in the Misc. parameters. These parameters affect all the three axes and enhances the reliability of motion events reported and RECALIBRATION.

Total noise energy Threshold:

This parameter is used with the estimated resultant velocities to set the noise energy threshold of all the three axes. The motion event velocities must exceed this threshold or the estimated resultant velocity is considered noise and the motion START events are not reported.

Total Shock Energy Threshold:

This parameter minimizes spurious responses when the device is subject to violent shocks. If the measured energy value exceeds this limit, then the measured velocity change is discarded and will not be used for estimating resultant velocity.

Total Consecutive Velocity Updates Threshold:

This parameter restricts the total number of consecutive velocity updates. If the total number of uninterrupted velocity updates in all axes exceeds this threshold, then a recalibration is performed and a RECALIBRATION event is flagged, even though the recalibration threshold may not have been reached for any axis.

NOTE  Care should be taken to choose parameter values to avoid unwanted RECALIBRATION events.

Refer the Set Miscellaneous Thresholds (Table B-4 on page B-2) to set different values through the API.
Index

Numerics

802.11 ESSID ........................................ 5-6

A

accessories ........................................... 1-4
  four slot spare battery charger ........... 1-4, 2-1, 2-12, 3-1, A-3
MSR
  battery charging ............................... 3-6
  power connection .............................. 3-6
single slot serial/USB cradle
  LED indicators ..................................... 3-4
SMDK ..................................................... 1-4
spare battery ....................................... 1-4, 3-1
spare battery charger ............................ 3-3
  power connection .................................. 3-4
UBC
  battery insertion .................................. 3-5
  UBC adapter ....................................... 1-4, 3-1, A-3
ActiveSync .......................................... 4-1
downloading files ................................. 6-7
installing ........................................... 4-1
setting up a connection .......................... 4-2
Adaptive Frequency Hopping ...................... 8-2
adding programs ..................................... 6-9
  from Internet ..................................... 6-9
ad-hoc ............................................... 5-7
ad-hoc networks .................................... 5-35
Advanced Encryption Standard .................. 5-17
AES ...................................................... 5-17
AFH ...................................................... 8-2
AirBEAM
  AirBEAM Smart .................................... 6-19
  Client .............................................. 6-19
  configuring ....................................... 6-20
  license ............................................. 6-20
  package builder .................................. 6-19
  staging ........................................... 6-26
  synchronization with server .................... 6-25
  antenna, external ............................... 1-3, 1-4, 1-11, 2-12, 3-11
AP networks ......................................... 5-35
authentication
  EAP-TLS ........................................... 5-9
  LEAP ............................................... 5-9
  none ............................................... 5-9
  PEAP ............................................... 5-9
  battery ............................................ 1-7
  backup charging .................................. 1-7
battery
  charging ........................................... 1-7
  check status ...................................... 1-13
  installing ........................................ 1-5
  removing ......................................... 1-6
battery charging temperature..................... A-2
battery icon ......................................... 1-14
battery LED ......................................... 1-8
battery status ...................................... 1-14
Bluetooth
  adaptive frequency hopping ..................... 8-2
  ad-hoc mode ....................................... 5-7
  bonding .......................................... 8-11
  communicating icon .............................. 1-14
  deleting bonded device ........................... 8-13
  disabled icon ...................................... 1-14
  discovering devices .............................. 8-10
  enabled icon ...................................... 1-14
  renaming bonded device .......................... 8-12
  turning off ....................................... 8-3
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cable, charging</td>
<td>1-4, 1-8, 3-1, A-3</td>
</tr>
<tr>
<td>charging</td>
<td></td>
</tr>
<tr>
<td>spare batteries</td>
<td>1-9</td>
</tr>
<tr>
<td>charging batteries</td>
<td>1-7</td>
</tr>
<tr>
<td>charging cable</td>
<td>1-4, 1-8, 3-1, A-3</td>
</tr>
<tr>
<td>charging spare batteries</td>
<td>1-9</td>
</tr>
<tr>
<td>charging the main battery</td>
<td>1-7, 1-8</td>
</tr>
<tr>
<td>cleaning RFID reader</td>
<td>9-1</td>
</tr>
<tr>
<td>clearing RFID tags</td>
<td>7-30</td>
</tr>
<tr>
<td>cold boot</td>
<td>1-13, 1-15, 1-16, 6-17, 8-4</td>
</tr>
<tr>
<td>communications, serial</td>
<td>1-8</td>
</tr>
<tr>
<td>communications, USB</td>
<td>1-10</td>
</tr>
<tr>
<td>configuration</td>
<td>xii, 1-4</td>
</tr>
<tr>
<td>conventions</td>
<td></td>
</tr>
<tr>
<td>notational</td>
<td>xiii</td>
</tr>
<tr>
<td>country code</td>
<td>5-7</td>
</tr>
<tr>
<td>CPU</td>
<td>A-1</td>
</tr>
<tr>
<td>cradles</td>
<td></td>
</tr>
<tr>
<td>single slot</td>
<td></td>
</tr>
<tr>
<td>LED indicators</td>
<td>3-4</td>
</tr>
<tr>
<td>spare battery charger</td>
<td>3-3</td>
</tr>
<tr>
<td>power connection</td>
<td>3-4</td>
</tr>
<tr>
<td>data capture</td>
<td>xii</td>
</tr>
<tr>
<td>DCP</td>
<td>6-1</td>
</tr>
<tr>
<td>components</td>
<td>6-3</td>
</tr>
<tr>
<td>DCP for RD5000</td>
<td>xiv, 4, 6-14, 6-17, 6-18</td>
</tr>
<tr>
<td>default gateway</td>
<td>5-19</td>
</tr>
<tr>
<td>deleting Bluetooth bond</td>
<td>8-13</td>
</tr>
<tr>
<td>Device Configuration Package</td>
<td></td>
</tr>
<tr>
<td>components</td>
<td>6-3</td>
</tr>
<tr>
<td>Device Configuration Package for RD5000</td>
<td>xiv, 4, 6-10, 6-14, 6-17, 6-18</td>
</tr>
<tr>
<td>DHCP</td>
<td>5-19</td>
</tr>
<tr>
<td>DNS</td>
<td>5-19, 5-20</td>
</tr>
<tr>
<td>downloading files</td>
<td>6-7</td>
</tr>
<tr>
<td>drop specification</td>
<td>A-2</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>5-9</td>
</tr>
<tr>
<td>electrical safety</td>
<td>A-3</td>
</tr>
<tr>
<td>encryption</td>
<td></td>
</tr>
<tr>
<td>open system</td>
<td>5-17, 5-19</td>
</tr>
<tr>
<td>TKIP (WPA)</td>
<td>5-17</td>
</tr>
<tr>
<td>error LED</td>
<td>1-9</td>
</tr>
<tr>
<td>external antenna</td>
<td>1-3, 1-4, 1-11, 2-12, 3-11</td>
</tr>
<tr>
<td>file explorer</td>
<td>6-11</td>
</tr>
<tr>
<td>flash file system</td>
<td>6-17</td>
</tr>
<tr>
<td>downloading partitions</td>
<td>6-16</td>
</tr>
<tr>
<td>non-FFS partitions</td>
<td>6-18</td>
</tr>
<tr>
<td>partitions</td>
<td>6-17</td>
</tr>
<tr>
<td>copyfile</td>
<td>6-18</td>
</tr>
<tr>
<td>regmerge</td>
<td>6-17</td>
</tr>
<tr>
<td>flash storage</td>
<td>6-17</td>
</tr>
<tr>
<td>four slot spare battery charger</td>
<td>1-4, 2-1, 2-12, 3-1, A-3</td>
</tr>
<tr>
<td>gateway</td>
<td>5-20</td>
</tr>
<tr>
<td>hard reset</td>
<td>1-13, 1-15, 1-16, 8-4</td>
</tr>
<tr>
<td>humidity</td>
<td>A-2</td>
</tr>
<tr>
<td>icons</td>
<td></td>
</tr>
<tr>
<td>bluetooth communicating</td>
<td>1-14</td>
</tr>
<tr>
<td>bluetooth disabled</td>
<td>1-14</td>
</tr>
<tr>
<td>bluetooth enabled</td>
<td>1-14</td>
</tr>
<tr>
<td>information, service</td>
<td>xiv</td>
</tr>
<tr>
<td>infrastructure</td>
<td>5-7</td>
</tr>
<tr>
<td>installing development tools</td>
<td>6-6</td>
</tr>
<tr>
<td>installing main battery</td>
<td>1-5</td>
</tr>
<tr>
<td>IP address</td>
<td>5-19</td>
</tr>
<tr>
<td>IP config</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>5-20</td>
</tr>
<tr>
<td>gateway</td>
<td>5-20</td>
</tr>
<tr>
<td>IP address</td>
<td>5-19</td>
</tr>
<tr>
<td>subnet mask</td>
<td>5-19</td>
</tr>
<tr>
<td>WINS</td>
<td>5-20</td>
</tr>
<tr>
<td>keyboard input panel</td>
<td>1-14</td>
</tr>
<tr>
<td>LEAP</td>
<td>5-9</td>
</tr>
<tr>
<td>M</td>
<td>1-8, 1-7, 9-1, xii, A-1</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>main battery</td>
<td></td>
</tr>
<tr>
<td>charging</td>
<td>1-4, 1-7</td>
</tr>
<tr>
<td>installing</td>
<td>1-4</td>
</tr>
<tr>
<td>maintenance</td>
<td>9-1</td>
</tr>
<tr>
<td>memory</td>
<td>xii, A-1</td>
</tr>
<tr>
<td>mode</td>
<td></td>
</tr>
<tr>
<td>802.11 ESSID</td>
<td>5-6</td>
</tr>
<tr>
<td>ad-hoc</td>
<td>5-7</td>
</tr>
<tr>
<td>country</td>
<td>5-7</td>
</tr>
<tr>
<td>infrastructure</td>
<td>5-7</td>
</tr>
<tr>
<td>operating</td>
<td>5-7</td>
</tr>
<tr>
<td>profile name</td>
<td>5-6</td>
</tr>
<tr>
<td>MSR</td>
<td></td>
</tr>
<tr>
<td>battery charging</td>
<td>3-6</td>
</tr>
<tr>
<td>power connection</td>
<td>3-6</td>
</tr>
<tr>
<td>O</td>
<td></td>
</tr>
<tr>
<td>open system</td>
<td>5-17, 5-19</td>
</tr>
<tr>
<td>operating mode</td>
<td>5-7</td>
</tr>
<tr>
<td>operating system</td>
<td>xii, A-1</td>
</tr>
<tr>
<td>operating temperature</td>
<td>A-2</td>
</tr>
<tr>
<td>P</td>
<td></td>
</tr>
<tr>
<td>partitions</td>
<td></td>
</tr>
<tr>
<td>downloading</td>
<td>6-16</td>
</tr>
<tr>
<td>FFS</td>
<td>6-17</td>
</tr>
<tr>
<td>non-FFS</td>
<td>6-18</td>
</tr>
<tr>
<td>parts of the RFID Reader</td>
<td>1-2</td>
</tr>
<tr>
<td>PEAP</td>
<td>5-9</td>
</tr>
<tr>
<td>ports</td>
<td>1-3</td>
</tr>
<tr>
<td>power supply</td>
<td>1-4, 3-1, A-3</td>
</tr>
<tr>
<td>power/serial port</td>
<td>1-3</td>
</tr>
<tr>
<td>profile</td>
<td></td>
</tr>
<tr>
<td>create new</td>
<td>5-24</td>
</tr>
<tr>
<td>delete</td>
<td>5-24</td>
</tr>
<tr>
<td>edit</td>
<td>5-24</td>
</tr>
<tr>
<td>profile name</td>
<td>5-6</td>
</tr>
<tr>
<td>programming an RFID tag</td>
<td></td>
</tr>
<tr>
<td>programs</td>
<td></td>
</tr>
<tr>
<td>adding</td>
<td>6-9</td>
</tr>
<tr>
<td>adding from Internet</td>
<td>6-9</td>
</tr>
<tr>
<td>flash file system</td>
<td>6-17</td>
</tr>
<tr>
<td>R</td>
<td></td>
</tr>
<tr>
<td>radios</td>
<td>xii</td>
</tr>
<tr>
<td>reading RFID tags</td>
<td>7-29</td>
</tr>
<tr>
<td>saving RFID tag data</td>
<td>7-31</td>
</tr>
<tr>
<td>scanning</td>
<td>7-29</td>
</tr>
<tr>
<td>scripts</td>
<td></td>
</tr>
<tr>
<td>creating</td>
<td>6-14</td>
</tr>
<tr>
<td>saving</td>
<td>6-15</td>
</tr>
<tr>
<td>SDK</td>
<td>6-1</td>
</tr>
<tr>
<td>See SMDK for C</td>
<td>1-4</td>
</tr>
<tr>
<td>selecting RFID tags</td>
<td>7-30</td>
</tr>
<tr>
<td>serial comm cable</td>
<td>1-4, 1-8, 3-1, A-3</td>
</tr>
<tr>
<td>serial communications</td>
<td>1-8</td>
</tr>
<tr>
<td>serial port</td>
<td>1-3</td>
</tr>
<tr>
<td>setting up a partnership</td>
<td></td>
</tr>
<tr>
<td>partnership</td>
<td>4-6</td>
</tr>
<tr>
<td>signal strength</td>
<td>5-27</td>
</tr>
<tr>
<td>single slot serial/USB cradle</td>
<td></td>
</tr>
<tr>
<td>LED indicators</td>
<td></td>
</tr>
<tr>
<td>S</td>
<td></td>
</tr>
<tr>
<td>saving RFID tag data</td>
<td></td>
</tr>
<tr>
<td>scanning</td>
<td></td>
</tr>
<tr>
<td>scripts</td>
<td></td>
</tr>
<tr>
<td>creating</td>
<td></td>
</tr>
<tr>
<td>saving</td>
<td></td>
</tr>
<tr>
<td>SDK</td>
<td></td>
</tr>
<tr>
<td>See SMDK for C</td>
<td></td>
</tr>
<tr>
<td>selecting RFID tags</td>
<td></td>
</tr>
<tr>
<td>serial comm cable</td>
<td></td>
</tr>
<tr>
<td>serial communications</td>
<td></td>
</tr>
<tr>
<td>serial port</td>
<td></td>
</tr>
<tr>
<td>setting up a partnership</td>
<td></td>
</tr>
<tr>
<td>partnership</td>
<td></td>
</tr>
<tr>
<td>signal strength</td>
<td></td>
</tr>
<tr>
<td>single slot serial/USB cradle</td>
<td></td>
</tr>
<tr>
<td>LED indicators</td>
<td></td>
</tr>
<tr>
<td>SMDK</td>
<td></td>
</tr>
<tr>
<td>SMDK for C</td>
<td></td>
</tr>
<tr>
<td>SMDK for eVC4</td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Page(s)</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>components</td>
<td>6-6</td>
</tr>
<tr>
<td>system requirements</td>
<td>6-2</td>
</tr>
<tr>
<td>soft keyboard</td>
<td>1-14</td>
</tr>
<tr>
<td>soft reset</td>
<td>1-15, 7-32, 8-4</td>
</tr>
<tr>
<td>software</td>
<td>1-4</td>
</tr>
<tr>
<td>spare batteries</td>
<td></td>
</tr>
<tr>
<td>charging</td>
<td>1-9</td>
</tr>
<tr>
<td>spare battery</td>
<td>1-4, 3-1</td>
</tr>
<tr>
<td>charging</td>
<td>1-9</td>
</tr>
<tr>
<td>spare battery charger</td>
<td>3-3</td>
</tr>
<tr>
<td>power connection</td>
<td>3-4</td>
</tr>
<tr>
<td>starting the RFID reader</td>
<td>1-4, 1-13</td>
</tr>
<tr>
<td>static</td>
<td>5-19</td>
</tr>
<tr>
<td>status</td>
<td>1-14</td>
</tr>
<tr>
<td>status icon</td>
<td>1-14</td>
</tr>
<tr>
<td>status icons</td>
<td></td>
</tr>
<tr>
<td>Windows CE 5.0</td>
<td>1-14</td>
</tr>
<tr>
<td>storage temperature</td>
<td>A-2</td>
</tr>
<tr>
<td>stylus</td>
<td>1-1</td>
</tr>
<tr>
<td>subnet mask</td>
<td>5-19</td>
</tr>
<tr>
<td>suspend</td>
<td>1-6, 8-4</td>
</tr>
<tr>
<td>Symbol Mobility Developer Kit for C</td>
<td>1-4, 6-1</td>
</tr>
<tr>
<td>Symbol Mobility Developer Kit for eVC4</td>
<td>xiv</td>
</tr>
<tr>
<td>components</td>
<td>6-6</td>
</tr>
<tr>
<td>T</td>
<td></td>
</tr>
<tr>
<td>taskbar</td>
<td>1-14</td>
</tr>
<tr>
<td>TCM</td>
<td></td>
</tr>
<tr>
<td>building hex image</td>
<td>6-10, 6-15, 6-16</td>
</tr>
<tr>
<td>creating script</td>
<td>6-14</td>
</tr>
<tr>
<td>defining properties</td>
<td>6-13</td>
</tr>
<tr>
<td>saving script</td>
<td>6-15</td>
</tr>
<tr>
<td>starting</td>
<td>6-11</td>
</tr>
<tr>
<td>terminal</td>
<td></td>
</tr>
<tr>
<td>charging</td>
<td>1-14</td>
</tr>
<tr>
<td>terminal charging</td>
<td>1-14</td>
</tr>
<tr>
<td>TKIP (WPA)</td>
<td>5-17</td>
</tr>
<tr>
<td>troubleshooting</td>
<td>9-2</td>
</tr>
<tr>
<td>U</td>
<td></td>
</tr>
<tr>
<td>UBC</td>
<td>1-9, 3-5</td>
</tr>
<tr>
<td>UBC adapter</td>
<td>1-4, 3-1, A-3</td>
</tr>
<tr>
<td>universal battery charger</td>
<td>3-5</td>
</tr>
<tr>
<td>unpacking</td>
<td>1-1</td>
</tr>
<tr>
<td>USB cable</td>
<td>1-10</td>
</tr>
<tr>
<td>USB client port</td>
<td>1-3</td>
</tr>
<tr>
<td>USB comm cable</td>
<td>1-4, 3-1, A-3</td>
</tr>
<tr>
<td>USB communications</td>
<td>1-10</td>
</tr>
<tr>
<td>W</td>
<td></td>
</tr>
<tr>
<td>warm boot</td>
<td>1-15, 7-32, 8-4</td>
</tr>
</tbody>
</table>