FX7500
RFID READER
INTEGRATOR GUIDE

FX7500 RFID READER INTEGRATOR GUIDE

MN000026A04

Revision A

July 2016

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, sublicensed, 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.

Zebra and the Zebra head graphic are registered trademarks of ZIH Corp. The Symbol logo is a registered trademark of Symbol Technologies, Inc., a Zebra Technologies company.

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

Warranty

For the complete Zebra hardware product warranty statement, go to:
http://www.zebra.com/warranty.

Revision History

Changes to the original manual are listed below:

Change	Date	Description
-01 Rev A	1/2014	Initial release
-02 Rev	2/2015	Zebra Re-Branding
-03 Rev	4/2016	Updates for SNAP; updated screen shots.
-04 Rev	7/2016	Updates: - Changed the installing antenna separation distance to 13.4 in (34 cm). - Changed max antenna gain exceed to + 6.6dBiL. - Changed Max Conducted RF Power at Antenna Input for US in table 3-1. - Changed Max Antenna Gain Allowed for US in table 3-1.

TABLE OF CONTENTS

Warranty ii
Revision History iii

About This Guide

Introduction ix
Configurations ix
Chapter Descriptions x
Notational Conventions xi
Related Documents and Software xi
Service Information xii

Chapter 1: Quick Start

Introduction 1-1
Quick Start Demonstration 1-1
Step 1, Setup 1-1
Step 2, Connecting to the Reader 1-2
Step 3, First Time / Start-Up Login 1-3
Step 4, Set Region 1-4
Step 5, Read Tags 1-6

Chapter 2: Getting Started

Introduction 2-1
RFID Technology Overview 2-1
RFID Components 2-2
FX7500 RFID Readers 2-3
Versions and Kits 2-4
FX7500 RFID Reader 2-4
FX7500 RFID Reader Rear Panel 2-5
FX7500 RFID Readers LEDs 2-5
FX7500 RFID Reader Features 2-7
Configuration and Upgrading 2-7

Tag Management 2-7
Device Management 2-7
Logging 2-7
Connection Options 2-7

Chapter 3: Installation and Communication

Introduction 3-1
Unpacking the Reader 3-1
Mounting and Removing the Reader 3-2
Mounting Tips 3-2
Mounting Using the Mounting Plate 3-2
Direct Mounting (Without the Mounting Plate) 3-3
Connecting Antennas 3-4
Communications Connections 3-5
Ethernet Connection 3-5
USB Connection 3-6
GPIO Interface Connection 3-9
Powering the Reader 3-10
Powering the Reader via AC Power Supply 3-10
Powering the Reader via Power-over-Ethernet (POE) 3-10
LED Sequences 3-11
System Start-up/Boot LED Sequence 3-11
PWR LED Sequence to Indicate IPv4 Status after Booting 3-11
Reset to Factory Defaults LED Sequence 3-11
LED Sequence for Software Update Status 3-11
Reading Tags 3-12

Chapter 4: Administrator Console

Introduction 4-1
Profiles 4-2
Resetting the Reader 4-2
Connecting to the Reader 4-3
Connecting via Host Name 4-3
Auto Discovery 4-4
Connecting via IP Address 4-4
Using Zero-Configuration Networking when DHCP Server is Not Available 4-5
Obtaining the IP Address via Command Prompt 4-5
Administrator Console Login 4-6
First Time / Start-Up Login 4-6
Setting the Region 4-7
Reader Administrator Console 4-9
Administrator Console Option Selections 4-9
Status 4-10
Reader Statistics 4-11
Reader Gen2 Optional Operation Statistics 4-12
NXP Custom Command Operation Statistics 4-13
Event Statistics 4-14
Other Custom Command Operation Statistics 4-15
Configure Reader 4-16

Reader Parameters (General) 4-16
Read Points 4-17
Read Points - Advanced 4-18
Configure Region 4-19
Certificates 4-20
Read Tags 4-30
Communication Settings 4-31
Configure Network Settings - Ethernet Tab 4-31
Configure Network Settings - Wi-Fi Tab 4-32
Configure Network Settings - Bluetooth Tab 4-33
Configure LLRP Settings 4-34
SNMP Settings 4-35
Wireless Settings 4-36
Network Services Settings 4-37
System Time Management 4-38
IPV6 IP Sec 4-39
Change Password 4-40
FX7500 User Accounts 4-40
Managing User Login and Logout 4-41
GPIO 4-41
Applications 4-42
Reader Profiles 4-43
FIPS Support on FX7500 4-44
Firmware Version/Update 4-44
Firmware Update 4-45
Commit/Discard 4-45
System Log 4-46
Configure System Log 4-47
Reader Diagnostics........ 4-48
Shutdown 4-49

Chapter 5: Wi-Fi Configuration

Wireless Network Advanced Configuration........ 5-1
Sample Configuration Files 5-2
Preferred Configurations for Access Points 5-4
AP: Zebra AP 5131 5-4
AP: Android Device 5-7
iPhone 5-9
Copying Files to the Reader 5-9

Chapter 6: Application Development

Introduction 6-1
Reference Guides 6-1

Chapter 7: Firmware Upgrade

Introduction 7-1
Prerequisites 7-1
Failsafe Update 7-2
Update Phases 7-2
Updating FX7500 Reader Software 7-3
Verifying Firmware Version 7-3
Updating Methods 7-4
Verifying Firmware Version 7-9

Chapter 8: Troubleshooting

Appendix A: Technical Specifications

FX7500 Kits A-1
KT-FX75004US-01 4-Port US Reader Kit A-1
KT-FX75002US-01 2-Port US Reader Kit A-1
KT-FX75004WR-01 4-Port Global Reader Kit A-1
KT-FX75002WR-01 2-Port Global Reader Kit A-2
Technical Specifications A-2
Cable Pinouts A-4
10/100bT Ethernet / POE Connector A-4
USB Client Connector A-5
USB Host Connector A-5
GPIO Port Connections A-6

Appendix B: Static IP Configuration

Introduction B-1
Reader IP Address or Host Name is Known -
Set the Static IP Using the Web Console B-1
Reader IP is Not Known (DHCP Network Not Available) -
Set the Static IP Using the Web Console B-3

Appendix C: RF Air Link Configuration

Introduction C-1
Radio Modes C-1

Appendix D: Connecting Wi-Fi and Bluetooth Dongles

Introduction D-1
Connecting to a Wireless Network Using a Wi-Fi Dongle D-1
Connecting to a Peer Device over Bluetooth Using a Bluetooth Dongle D-5

Appendix E: Copying Files To and From the Reader

Introduction E-1
SCP E-1
FTP E-1
FTPS E-2

Appendix F: Data Protection

Introduction F-1

Index

ABOUT THIS GUIDE

Introduction

This Integrator Guide provides information about installing, configuring, and using the FX7500 RFID readers and is intended for use by professional installers and system integrators. The FX7500 readers provide real time, seamless tag processing for EPC Class1 Gen2 compliant tags.

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

Configurations

This guide includes the following FX7500 RFID reader configurations:

- FX7500-42320A50-US: 4-Port FCC
- FX7500-22320A50-US: 2-Port FCC
- FX7500-42325A50-WR: 4-Port Worldwide
- FX7500-22325A50-WR: 2-Port Worldwide

Chapter Descriptions

Topics covered in this guide are as follows:

- *Chapter 1, Quick Start* provides a Quick Start tag reading demonstration.
- *Chapter 2, Getting Started* provides an overview of RFID technology/components and a description of the FX7500 reader and features.
- *Chapter 3, Installation and Communication* provides information on installing and setting up the FX7500 readers.
- *Chapter 4, Administrator Console* describes how to connect to the reader and how to use the web-based Administrator Console to configure and manage FX7500 readers.
- *Chapter 5, Wi-Fi Configuration* details wireless network advanced configuration and preferred configurations for access points.
- *Chapter 6, Application Development* provides information on developing applications for the FX7500, and includes references to the appropriate guides.
- *Chapter 7, Firmware Upgrade* provides reader firmware upgrade information on using the web-based **Administrator Console** and an FTP or FTPS server running a host computer.
- *Chapter 8, Troubleshooting* describes FX7500 readers troubleshooting procedures.
- *Appendix A, Technical Specifications* includes the technical specifications for the reader.
- *Appendix B, Static IP Configuration* describes three methods of setting the static IP address on an FX7500 RFID Reader.
- *Appendix C, RF Air Link Configuration* describes how to select air link configuration from a set of available air link profiles.
- *Appendix D, Connecting Wi-Fi and Bluetooth Dongles* describes how to connect to a wireless network using a USB Wi-Fi dongle on the FX7500, and how to connect to a peer device over Bluetooth using a USB Bluetooth dongle.
- *Appendix E, Copying Files To and From the Reader* describes the SCP, FTP, and FTPS protocols for copying files.
- *Appendix F, Data Protection* describes how the FX7500 protects RFID data in transition.

Notational Conventions

The following conventions are used in this document:

- “RFID reader” or “reader” refers to the Zebra FX7500 RFID readers.
- *Italics* are used to highlight the following:
  - Chapters and sections in this and related documents
  - Dialog box, window, links, software names, and screen names
  - Drop-down list, columns and list box names
  - Check box and radio button names
  - Icons on a screen
- **Bold** text is used to highlight the following:
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - 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 reader.

- *FX7500 RFID Reader Quick Start Guide*, p/n MN000070A01
- *FX Series Reader Software Interface Control Guide,* p/n 72E-131718-xx. Describes Low Level Reader Protocol (LLRP) and Reader Management (RM) extensions for the FX7500 reader.
- *RFID Demo Applications User Guide*, p/n 72E-160038-01. Provides instructions for using sample applications which demonstrate how to use Zebra RFID readers.
- *FX7500 Embedded SDK Installation Guide*. Provides instructions for installing the embedded SDK for C and Java.
- *FX7500 Embedded SDK Sample Application Guide*. Explains how to use the embedded sample application with an integrated development environment.
- *FX7500 Embedded SDK Programmers Guide*. Provides instructions for creating new embedded applications.
- *RFID3 API*
- EPCglobal *Low Level Reader Protocol (LLRP) Standard*

For the latest version of these guides and software, visit: http://www.zebra.com/support.

Service Information

If you have a problem using the equipment, contact your facility's technical or systems support. If there is a problem with the equipment, they will contact the Zebra Global Customer Support Center at: http://www.zebra.com/support.

When contacting Zebra support, please have the following information available:

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

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

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

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

CHAPTER 1 QUICK START

Introduction

This chapter provides a Quick Start setup demonstration.

Quick Start Demonstration

The Quick Start demonstration offers a simple, temporary way to quickly set up the reader and read tags. The demonstration includes:

- *Step 1, Setup on page 1-1*
- *Step 2, Connecting to the Reader on page 1-2*
- *Step 3, First Time / Start-Up Login on page 1-3*
- *Step 4, Set Region on page 1-4*
- *Step 5, Read Tags on page 1-6*

Step 1, Setup

For information on complete component kits available from Zebra, see *Appendix A, Technical Specifications*.

1. Unpack the reader. See *Unpacking the Reader on page 3-1*.
2. Set up the reader and tags on a desktop.
3. Connect the antenna to antenna Port 1. See *Figure 1-1*.
4. Connect the Ethernet cable to the Ethernet port. See *Figure 1-1*.
   Connecting the reader to a subnet that supports DHCP is recommended. This Quick Start procedure is not guaranteed to work if DHCP is disabled in the reader and if the reader is connected directly to a PC.
5. Connect the AC power supply to a power outlet and connect to the power port. See *Figure 1-1.*

✓ ***NOTE*** This step is not required for networks supporting Power-over-Ethernet (POE).

6. Wait for the green power LED to stay lit. See *System Start-up/Boot LED Sequence on page 3-11* for boot-up details.

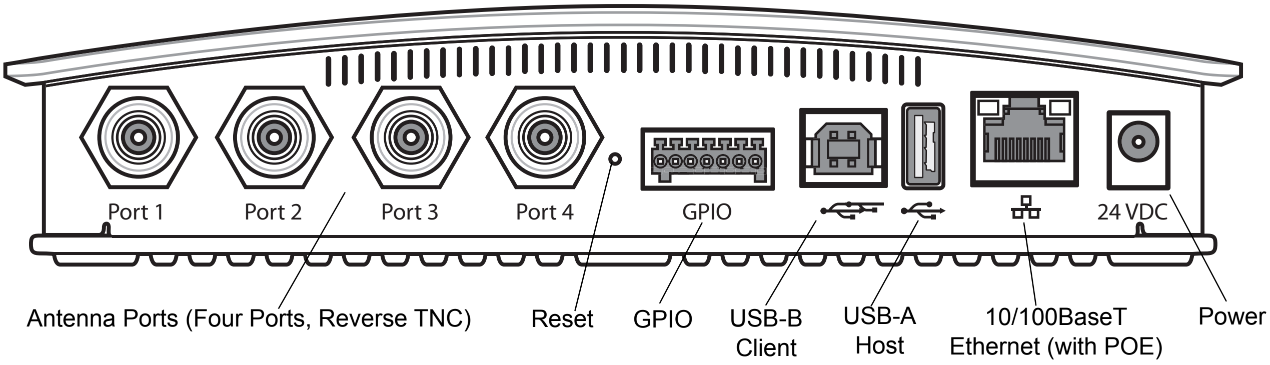

Port 1
Port 2
Port 3
Port 4
GPIO
24 VDC
Antenna Ports (Four Ports, Reverse TNC)
Reset
GPIO
USB-B Client
USB-A Host
10/100BaseT Ethernet (with POE)
Power

Figure 1-1 *FX7500 RFID Reader Rear Panel Connections*

Step 2, Connecting to the Reader

To connect via host name:

1. Open a browser. Recommended browsers are IE10 (disabling Compatibility View is recommended), Chrome v29, and FireFox 24.

2. Enter the host name, printed on the host name label on the reader, in the browser (e.g., http://fx7500cd3b0d) and press **Enter**. The **User Login** window appears and the reader is ready.

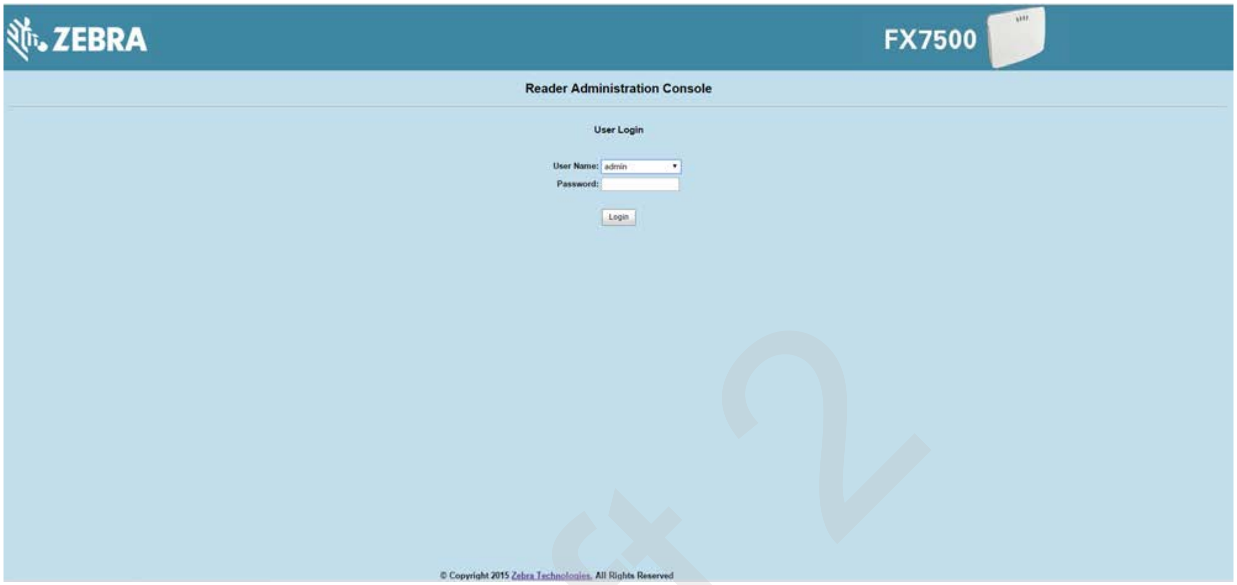
NOTE Connect the reader to a network that supports host name registration and lookup to ensure the network can access the reader using the host name. For instance, some networks can register hostnames through DHCP. When first connecting to the reader, it is recommended to keep DHCP enabled in both the PC and in the reader, although it is not guaranteed that hostname will work all the time. Use the host name printed on the reader label, or construct it using the reader MAC address on the bottom of the reader. The host name is a string with the prefix FX7500, followed by the last three MAC address octets. For example, for a MAC address of 00:15:70:CD:3B:0D, use the prefix FX7500, followed by CD, 3B, and 0D, to create the host name FX7500CD3B0D. Enter **http://FX7500CD3B0D** in the browser address bar to access the reader.

To connect using the USB port for network connection, see Wireless Intrusion Protection System. The default USB RNDIS IP address for the reader is 169.254.10.1

Step 3, First Time / Start-Up Login

When starting the reader for the first time:

1. In the **User Login** window, enter **admin** in the **User Name:** field and enter **change** in the **Password:** field.



Reader Administration Console

User Login

User Name: admin
Password:

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 1-2 *User Login Window*

> **NOTE** If you forget the user ID and/or password, see *Reset to Factory Defaults LED Sequence on page 3-11* to reset the reader to factory defaults, and then select **admin** for the user name and enter **change** in the password field to regain access.

2. Click **Login.** The **Region Configuration** window appears.

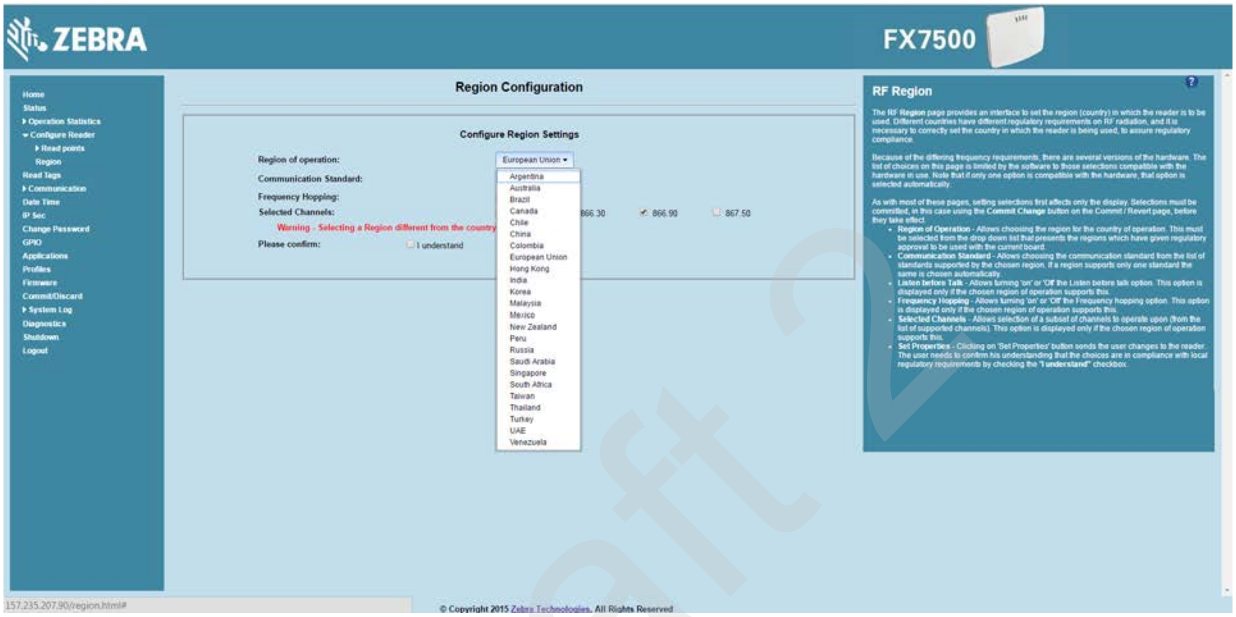
> **NOTE** The Region Configuration window does not appear for US reader configurations. For these models, the Administrator Console main window appears. See *Figure 4-1 on page 4-2*.

Step 4, Set Region

Set the region of operation. **Setting the unit to a different region is illegal**.

✓ ***NOTE*** Region configuration is not available for readers configured to operate in the United States region (under FCC rules). In this case, skip this step.

1. In the **Configure Region Settings** window, select the region from the drop-down menu.



Region Configuration

Configure Region Settings

Region of operation: European Union

Communication Standard:

Frequency Hopping:

Selected Channels: 866.30 ☑ 866.90 □ 867.50

Warning - Selecting a Region different from the country

Please confirm: □ I understand

RF Region

The **RF Region** page provides an interface to set the region (country) in which the reader is to be used. Different countries have different regulatory requirements on RF radiation, and it is necessary to correctly set the country in which the reader is being used, to assure regulatory compliance.

Because of the differing frequency requirements, there are several versions of the hardware. The list of choices on this page is limited by the software to those selections compatible with the hardware in use. Note that if only one option is compatible with the hardware, that option is selected automatically.

As with most of these pages, setting selections first affects only the display. Selections must be committed, in this case using the **Commit Change** button on the Commit / Revert page, before they take effect.

- **Region of Operation** - Allows choosing the region for the country of operation. This must be selected from the drop down list that presents the regions which have given regulatory approval to be used with the current board.
- **Communication Standard** - Allows choosing the communication standard from the list of standards supported by the chosen region. If a region supports only one standard the same is chosen automatically.
- **Listen before Talk** - Allows turning 'on' or 'Off' the Listen before talk option. This option is displayed only if the chosen region of operation supports this.
- **Frequency Hopping** - Allows turning 'on' or 'Off' the Frequency hopping option. This option is displayed only if the chosen region of operation supports this.
- **Selected Channels** - Allows selection of a subset of channels to operate upon (from the list of supported channels). This option is displayed only if the chosen region of operation supports this.
- **Set Properties** - Clicking on 'Set Properties' button sends the user changes to the reader. The user needs to confirm his understanding that the choices are in compliance with local regulatory requirements by checking the **"I understand"** checkbox.

Figure 1-3 *Selecting the Region*

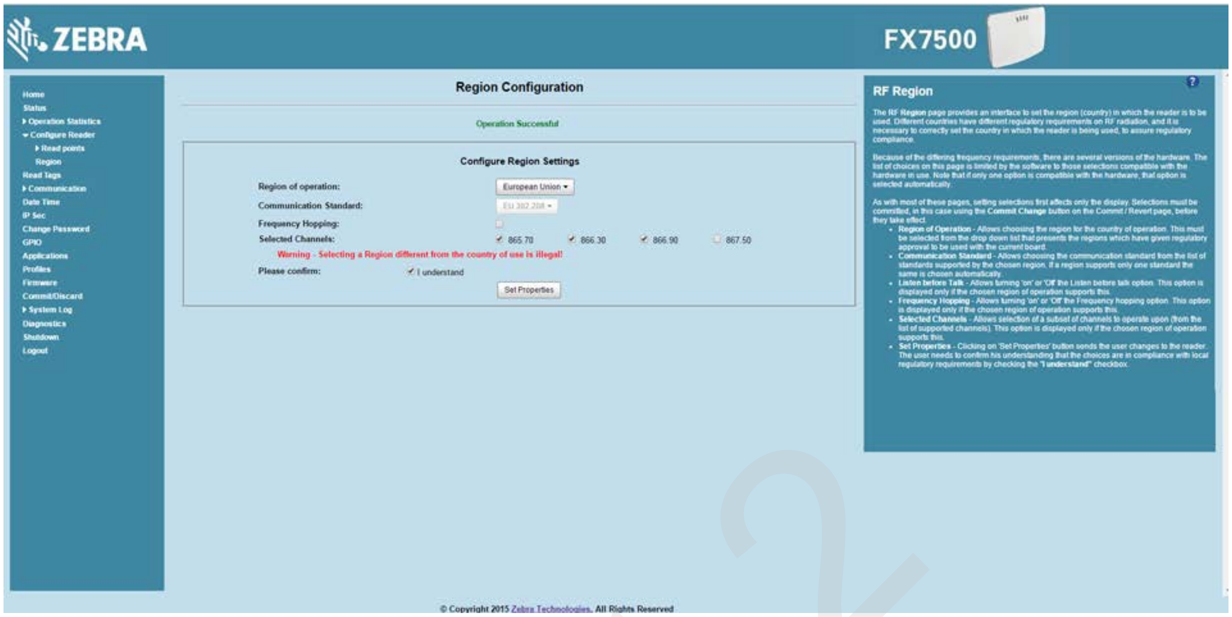
2. Select the **Communication Standard**, if applicable.

3. Select **Frequency Wireless IPSy Hopping**, if applicable.

4. Select the appropriate channel(s), if applicable.

5. Select the **I understand** check box.

6. Select **Set Properties** to complete the region selection. The **Operation Successful** window appears.



Region Configuration

Operation Successful

Configure Region Settings

Region of operation: European Union

Communication Standard: EU 302 208

Frequency Hopping: □

Selected Channels: ☑ 865.70 ☑ 866.30 ☑ 866.90 □ 867.50

Warning - Selecting a Region different from the country of use is illegal!

Please confirm: ☑ I understand

RF Region

The **RF Region** page provides an interface to set the region (country) in which the reader is to be used. Different countries have different regulatory requirements on RF radiation, and it is necessary to correctly set the country in which the reader is being used, to assure regulatory compliance.

Because of the differing frequency requirements, there are several versions of the hardware. The list of choices on this page is limited by the software to those selections compatible with the hardware in use. Note that if only one option is compatible with the hardware, that option is selected automatically.

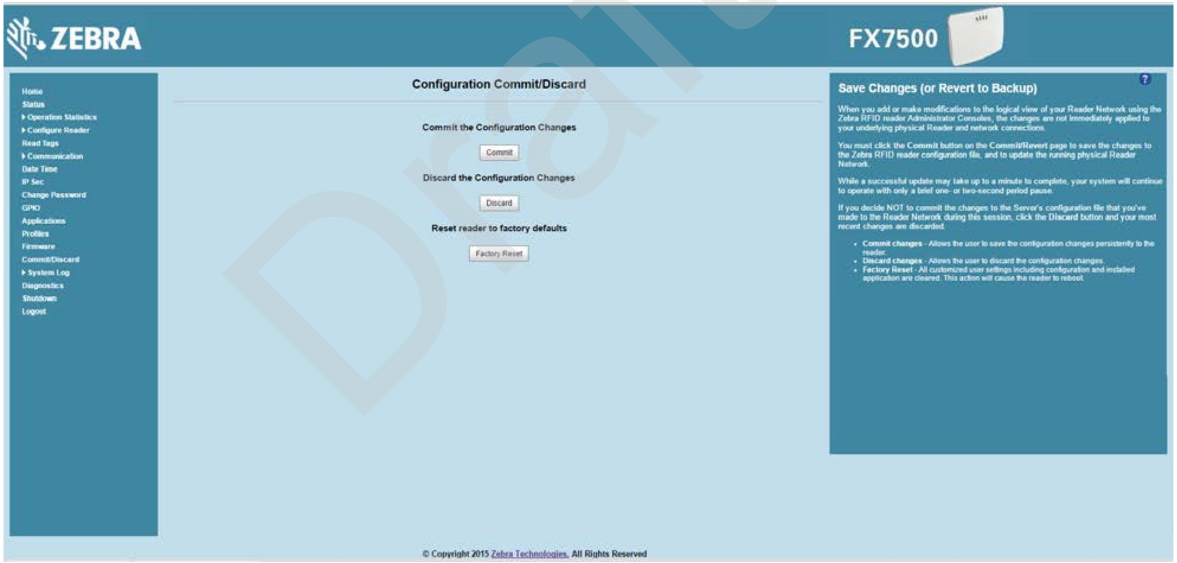
As with most of these pages, setting selections first affects only the display. Selections must be committed, in this case using the **Commit Change** button on the Commit / Revert page, before they take effect.

- **Region of Operation** - Allows choosing the region for the country of operation. This must be selected from the drop down list that presents the regions which have given regulatory approval to be used with the current board.
- **Communication Standard** - Allows choosing the communication standard from the list of standards supported by the chosen region. If a region supports only one standard the same is chosen automatically.
- **Listen before Talk** - Allows turning 'on' or 'Off' the Listen before talk option. This option is displayed only if the chosen region of operation supports this.
- **Frequency Hopping** - Allows turning 'on' or 'Off' the Frequency hopping option. This option is displayed only if the chosen region of operation supports this.
- **Selected Channels** - Allows selection of a subset of channels to operate upon (from the list of supported channels). This option is displayed only if the chosen region of operation supports this.
- **Set Properties** - Clicking on 'Set Properties' button sends the user changes to the reader. The user needs to confirm his understanding that the choices are in compliance with local regulatory requirements by checking the "**I understand**" checkbox.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 1-4 *Region Configuration, Operation Successful Window*

7. Select **Commit/Discard**.



Configuration Commit/Discard

Commit the Configuration Changes

Discard the Configuration Changes

Reset reader to factory defaults

Save Changes (or Revert to Backup)

When you add or make modifications to the logical view of your Reader Network using the Zebra RFID reader Administrator Consoles, the changes are not immediately applied to your underlying physical Reader and network connections.

You must click the Commit button on the Commit/Revert page to save the changes to the Zebra RFID reader configuration file, and to update the running physical Reader Network.

While a successful update may take up to a minute to complete, your system will continue to operate with only a brief one- or two-second period pause.

If you decide NOT to commit the changes to the Server's configuration file that you've made to the Reader Network during this session, click the Discard button and your most recent changes are discarded.

- **Commit changes** - Allows the user to save the configuration changes persistently to the reader.
- **Discard changes** - Allows the user to discard the configuration changes.
- **Factory Reset** - All customized user settings including configuration and installed application are cleared. This action will cause the reader to reboot.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 1-5 *Commit/Discard Window*

8. Click **Commit** to save the new region configuration and apply these changes to the reader configuration file, or click **Discard** to discard the region configuration changes. When the commit completes, the **Commit Successful** window appears.

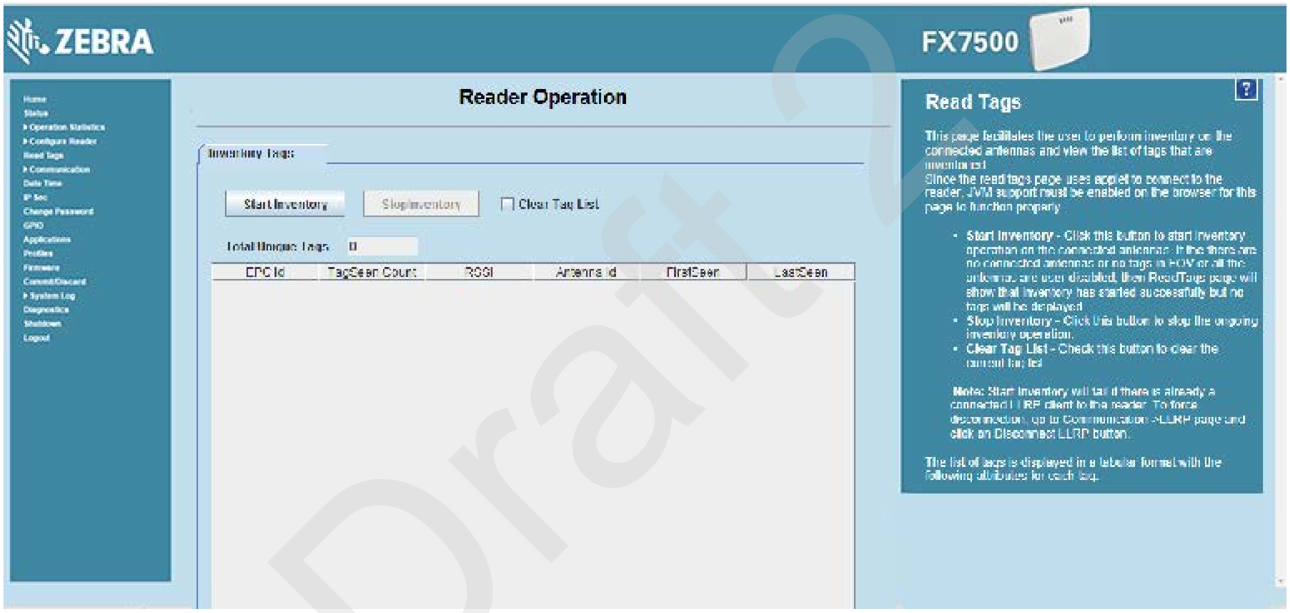
Step 5, Read Tags

Select **Read Tags** to view the **Reader Operation** window.

NOTE Enable Java JRE support on the browser for this page to function properly.

NOTE For security reasons browsers may block the **Read Tags** page. Look for a pop window that can be hidden behind the browser or at the bottom of the screen (the taskbar in Windows) and allow the applet to run.

NOTE With older browsers, when upgrading/downgrading the FX7500, close the browser and re-open it to clear the old version of files cached. If the java cache for applets is on, clear the cached applet before starting the browser to use the **Read Tags** page.



Reader Operation

□ Clear Tag List

Total Unique Tags 0

EPC Id	TagSeen Count	RSSI	Antenna Id	FirstSeen	LastSeen

Read Tags

This page facilitates the user to perform inventory on the connected antennas and view the list of tags that are inventoried.
Since the read tags page uses applet to connect to the reader, JVM support must be enabled on the browser for this page to function properly.

- **Start Inventory** - Click this button to start inventory operation on the connected antennas. If the there are no connected antennas or no tags in FOV or all the antennas are user disabled, then ReadTags page will show that inventory has started successfully but no tags will be displayed
- **Stop Inventory** - Click this button to stop the ongoing inventory operation.
- **Clear Tag List** - Check this button to clear the current tag list

Note: Start Inventory will fail if there is already a connected LLRP client to the reader. To force disconnection, go to Communication->LLRP page and click on Disconnect LLRP button.

The list of tags is displayed in a tabular format with the following attributes for each tag.

Figure 1-6 *Read Tags Window*

- Click **Start Inventory** to initiate an on-demand scan on the connected antennas that are enabled.
- Click **Stop Inventory** to stop the inventory operation.
- Select the **Clear Tag List** check box to clear the current tag list.

The list of tags appears in a table with the following attributes for each tag:

- **EPC Id***:* Unique tag EPC ID.
- **TagSeen Count***:* Number of times the tag is identified on the specific antenna.
- **RSSI**: Received Signal Strength Indication.
- **Antenna Id***:* Antenna ID on which the tag is seen.
- **FirstSeen** time stamp: UTC time (in microseconds) when the tag was first seen.
- **LastSeen** time stamp: UTC time (in microseconds) when the tag was last seen.

CHAPTER 2 GETTING STARTED

Introduction

This chapter provides an overview of RFID technology and components, and describes the FX7500 reader and its features.

RFID Technology Overview

RFID (Radio Frequency Identification) is an advanced automatic identification (Auto ID) technology that uses radio frequency signals to identify *tagged* items. An RFID tag contains a circuit that can store data. This data may be pre-encoded or can be encoded in the field. The tags come in a variety of shapes and sizes.

A typical RFID system consists of transponders (called tags), readers, and antennas. To read a tag the reader sends out radio frequency waves (using attached antennas). This RF field powers and charges the tags, which are tuned to receive radio waves. The tags use this power to modulate the carrier signal. The reader interprets the modulated signal and converts the data to a format for computer storage. The computer application translates the data into an understandable format.

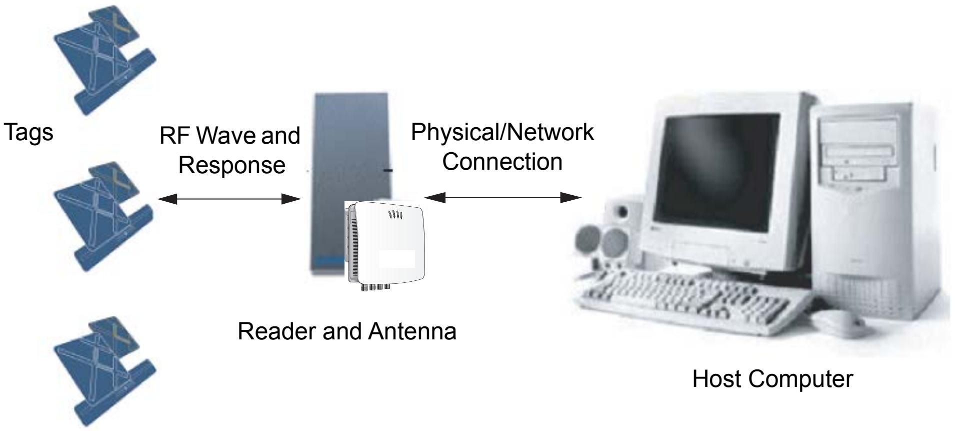


Figure 2-1 *RFID System Elements*

RFID Components

Zebra RFID offer low cost, long read range, and a high read rate. These features provide real time, end-to-end visibility of products and assets in the factory, distribution center, retail outlet, or other facility. A typical Zebra RFID system consists of the following components:

- Silicon based RFID tags that attach to retail products, vehicles, trailers, containers, pallets, boxes, etc.
- Different antenna types to support applications such as dock door (area antennas) and conveyor.
- Readers power and communicate with the tags for data capture and provide host connectivity for data migration.

Tags

Tags contain embedded chips that store unique information. Available in various shapes and sizes, tags, often called **transponders**, receive and respond to data requests. Tags require power to send data, and are available with two power options:

- Active Tags: typically powered by light-weight batteries and have limited life.
- Passive Tags: the RFID reader generates an RF field that powers the tag. Passive tags are much lighter, less expensive, and have a much longer life than active tags.

Antennas

Antennas transmit and receive radio frequency signals. A **read point** is the RF range of an antenna.

Readers

Readers communicate with the tags and can transfer the data to a host computer. Readers also provide features such as filtering and tag writing. FX7500 readers read Gen2 (dense reader mode) RFID tags.

FX7500 RFID Readers

The Zebra FX7500 RFID readers are intelligent, C1G2 UHF RFID readers with RFID read performance that provides real-time, seamless EPC-compliant tags processing. FX7500 RFID readers are designed for indoor inventory management and asset tracking applications in large scale deployments. The readers can host third-party customer-driven embedded applications.

FX7500 RFID readers are based on Zebra's strategic FX7500 reader platform and are easy to use, deploy, and manage. The readers offer a variety of options for connecting to corporate networks using Ethernet or USB connections. Features include:

- ISO 18000-6C standard (EPC Class 1 Gen 2)
- Dense reader mode capability
- Enterprise-class performance
- Application-specific setup for ease of installation
- Power over Ethernet (POE) to eliminate the need for a power drop
- SSL/SSH based security for secure data transmission
- Linux operating system
- Support for custom or third-party applications
- Feature set for event and tag management
- Support for NXP custom commands over LLRP
- Radio mode support via LLRP v1.0.1

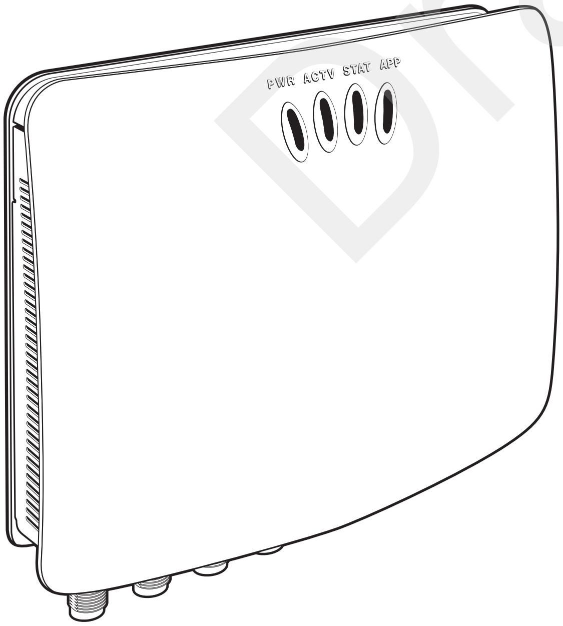


Figure 2-2 *FX RFID Reader*

The reader provides a wide range of features that enable implementation of complete, high-performance, intelligent RFID solutions.

FX7500 RFID reader configurations include either two or four monostatic antenna ports. The monostatic ports are used only with monostatic antennas.

Versions and Kits

FX7500 RFID readers are available in a 2-port or 4-port version, individually (reader and mounting bracket) or in a kit that includes the reader, mounting bracket, an antenna, and a power supply. For detailed kit information, see *FX7500 Kits on page A-1*.

WARNING! **For Mounting in Environmental Air Handling Space (EAHS): Do not install the Mounting Bracket, Antenna, Cables, PSU, and PoE (Power Injector) in the EAHS unless they are suitable for use in EAHS per UL 2043.**

FX7500 RFID Reader

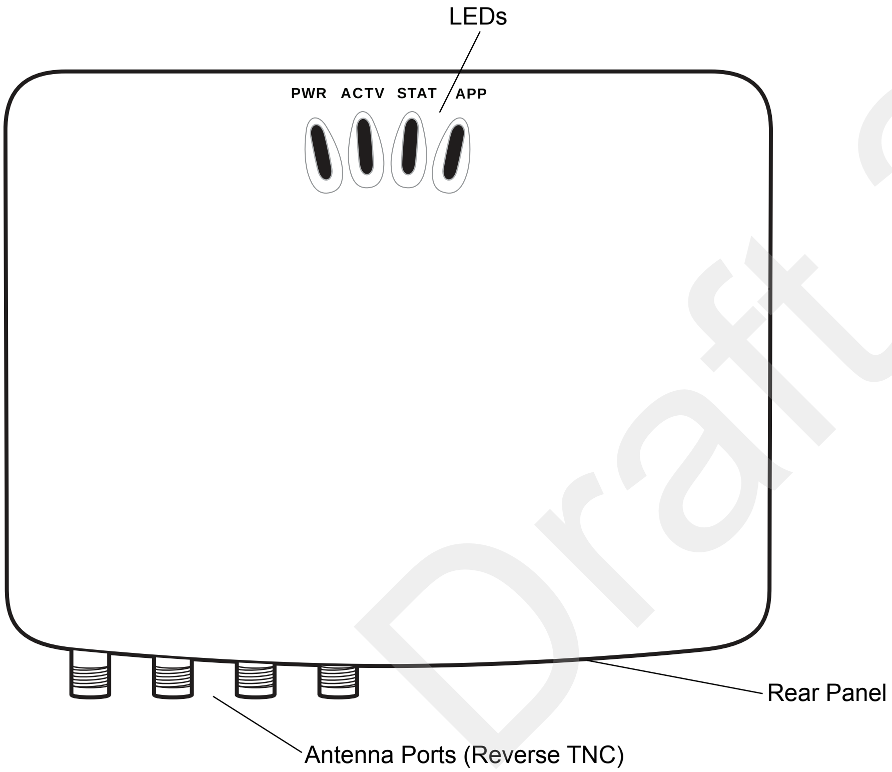


Figure 2-3 *FX7500 RFID Reader*

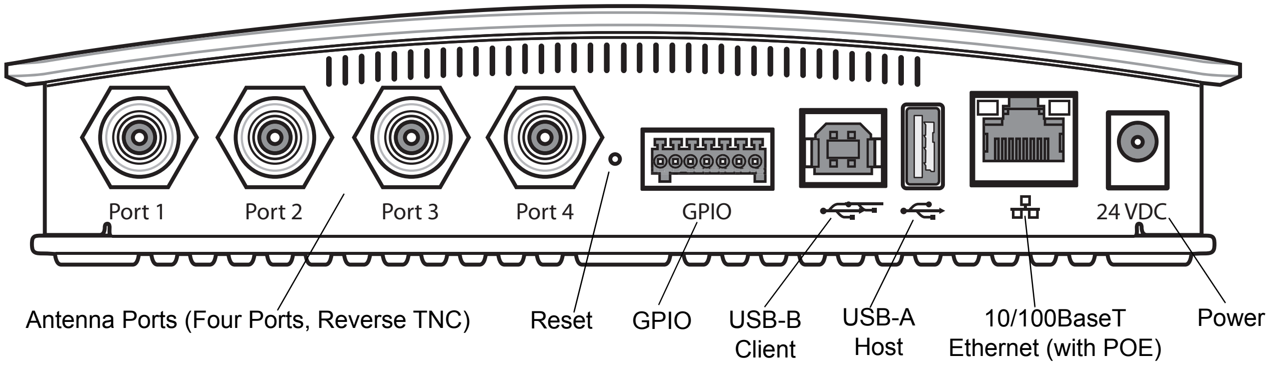

Port 1
Port 2
Port 3
Port 4
GPIO
24 VDC
Antenna Ports (Four Ports, Reverse TNC)
Reset
GPIO
USB-B Client
USB-A Host
10/100BaseT Ethernet (with POE)
Power

Figure 2-4 *FX7500 RFID Reader Rear Panel Connections*

CAUTION Use only parts provided with the FX7500 RFID readers, or Zebra approved/recommended parts. Substituting other cables or parts can degrade system performance, damage the reader, and/or void the warranty.

FX7500 RFID Reader Rear Panel

Table 2-1 *Rear Panel Descriptions*

Port	Description
Antenna Ports (Reverse TNC)	Two port version: Connect up to two antennas. Four port version: Connect up to four antennas. See *Table A-1 on page A-2* for the maximum antenna gains and RF output powers for both US/Canada and EU. See *Connecting Antennas on page 3-4* for connection information.
Reset	To reset the reader insert a paper clip into the reset hole, press and hold the reset button for not more than 2 seconds. This resets the reader, but retains the user ID and password.
GPIO	See *GPIO Interface Connection on page 3-9* for more information.
USB Client	The USB client port supports (by default) a network mode of operation. This enables a secondary network interface as a virtual adapter over USB. Advanced users can create a custom communication protocol on the USB port. See *USB Connection on page 3-6* for connection information.
USB Host	Use the USB host port to connect USB devices such as WiFi / Bluetooth over USB dongles and flash memory drives.
10/100BaseT Ethernet	Insert a standard RJ45 Ethernet cable to connect to an Ethernet network with or without POE capability, or to a local computer. See *Ethernet Connection on page 3-5* for connection information.
Power	DC connector connects to a Zebra approved power supply AC adapter (varies depending on the country). Maximum power 24 VDC, 1.2 A. See *Powering the Reader on page 3-10* for connection information.

FX7500 RFID Readers LEDs

The reader LEDs indicate reader status as described in *Table 2-2*. For the LED boot up sequence see *System Start-up/Boot LED Sequence on page 3-11*.

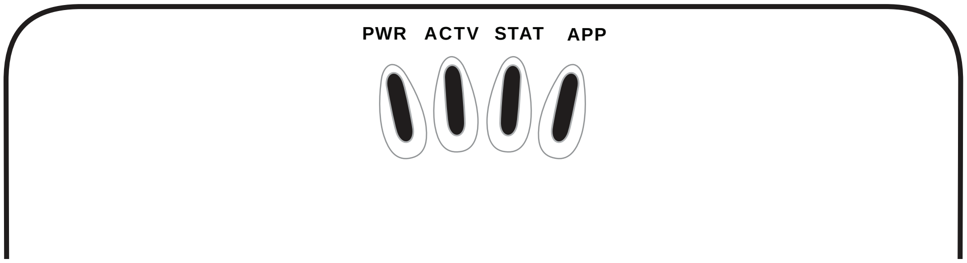


Figure 2-5 *FX7500 RFID Readers LEDs*

Table 2-2 *LED Indications*

LED	Function	Color/Status	Description
PWR	Power	Off Amber Solid Red Flashing Amber Solid Green Solid	Reader is powered off Booting Firmware upgrade Application initialization after booting Reader is powered on and operational
ACTV	Activity	Off Amber Flashing Green Flashing	No RF operations On for 500 mSec indicates another tag operation On for 500 mSec indicates a tag is inventoried or read
STAT	Status	Off Red Solid Red Flashing Green Flashing	No errors or GPIO events Firmware update failure On for 500 mSec indicates an error in RF operation On for 500 mSec indicates a GPI event
APP	Application	Green/Red/Amber	Controlled through RM

FX7500 RFID Reader Features

Configuration and Upgrading

Use the **Administrator Console** to reconfigure the reader. See *Chapter 4, Administrator Console*. The reader can also accept new firmware and configuration updates.

Tag Management

The **Administrator Console** provides the **Read** tags feature. See *Read Tags on page 4-30*. Use client applications based on Zebra EMDK (Enterprise Mobility Development Kit) such as Power Session, or LLRP (EPCGlobal Low Level Reader Protocol) for additional tag management operations such as **Write**, **Lock**, **Filtering**, **Event Management** and **Kill**.

Device Management

Quick Backup and Recovery

Use a web browser to back up and restore reader configuration by downloading the configuration XML file. Use the **Administrator Console** to download the file to the reader.

SNMP Integration

The reader can send real time notification of specific events and failures to an SNMP server.

Logging

The reader keeps a log of all system-related activities for security and troubleshooting. The log includes time-stamped system activities such as login attempts and hardware failures. Use the log to pinpoint problems, to facilitate quick resolution, and to identify administrators who may require additional training to prevent future problems. See *System Log on page 4-46*.

Connection Options

The FX7500 provides flexibility for connecting to networks through an Ethernet connection or the USB client port. The reader’s primary network interface is Ethernet. The Ethernet interface accesses each reader from anywhere on the network using the unique host name or IP address.

Additionally, the USB client port supports (by default) a **Network** mode of operation. This enables a secondary network interface as a virtual adapter over USB. The interfaces co-exist and if the Ethernet connection fails, the application can switch to USB using a specific IP and can control the reader.

See *Communications Connections on page 3-5*. To use the USB port for network connection, see Wireless Intrusion Protection Systeml Wireless IPS.

CHAPTER 3 INSTALLATION AND COMMUNICATION

Introduction

This chapter includes the following FX7500 RFID reader installation and communication procedures:

- *Unpacking the Reader on page 3-1*
- *Mounting and Removing the Reader on page 3-2*
  - *Mounting Tips on page 3-2*
  - *Mounting Using the Mounting Plate on page 3-2*
  - *Direct Mounting (Without the Mounting Plate) on page 3-3*
- *Connecting Antennas on page 3-4*
- *Communications Connections on page 3-5*
  - *Ethernet Connection on page 3-5*
  - *USB Connection on page 3-6*
  - *GPIO Interface Connection on page 3-9*
- *Powering the Reader on page 3-10*
  - *Powering the Reader via AC Power Supply on page 3-10*
  - *Powering the Reader via Power-over-Ethernet (POE) on page 3-10*
- *System Start-up/Boot LED Sequence on page 3-11*

⚠ ***CAUTION*** FX7500 RFID readers must be professionally installed.

⚠ ***WARNING!*** **For Mounting in Environmental Air Handling Space (EAHS): Any cables used to interconnect to other equipment must be suitable for use in EAHS as per UL2043.**

Unpacking the Reader

Remove the reader from the shipping container and inspect it for damage. Keep the shipping container, it is the approved shipping container and should be used if the reader needs to be returned for servicing.

Mounting and Removing the Reader

WARNING! **When installing the antenna ensure a minimum separation distance of 13.4 in (34 cm) between the antennas and all persons.**

Mounting Tips

Mount the reader in any orientation. Consider the following before selecting a location for the FX7500 reader:

- Mount the reader indoors, in operating range and out of direct sunlight, high moisture, and/or extreme temperatures.
- Mount the reader in an area free from electromagnetic interference. Sources of interference include generators, pumps, converters, non-interruptible power supplies, AC switching relays, light dimmers, and computer CRT terminals.
- Mount the reader within 15 feet of the antennas.
- Ensure that power can reach the reader.
- The recommended minimum horizontal mounting surface width is 7 1/2 inches. However, the unit can mount on surfaces as narrow as 6 inches (in locations where unit overhang is not an issue). For vertical mounting the unit can mount on a surface as small as 6 inches by 6 inches.
- Mount the reader onto a permanent fixture, such as a wall or a shelf, where it is not disturbed, bumped, or damaged. The recommended minimum clearance on all sides of the reader is five inches.
- Use a level for precise vertical or horizontal mounting.

Mounting Using the Mounting Plate

WARNING! **For Mounting in Environmental Air Handling Space (EAHS): Do not install the Mounting Bracket in the EAHS.**

1. Position the mounting plate on a flat surface (wall or shelf). Position the release tab on the top. See *Figure 3-1*.
2. Mark the hole locations using the mounting plate as a guide. See *Figure 3-1*. Remove the mounting plate and drill holes (appropriate for the surface material) at the marked locations.

NOTE For wood surfaces, drill two 1/8" diameter by 7/8" deep holes. For drywall/masonry surfaces, drill two 3/16" diameter by 7/8" deep (min) holes and install using the provided anchors.

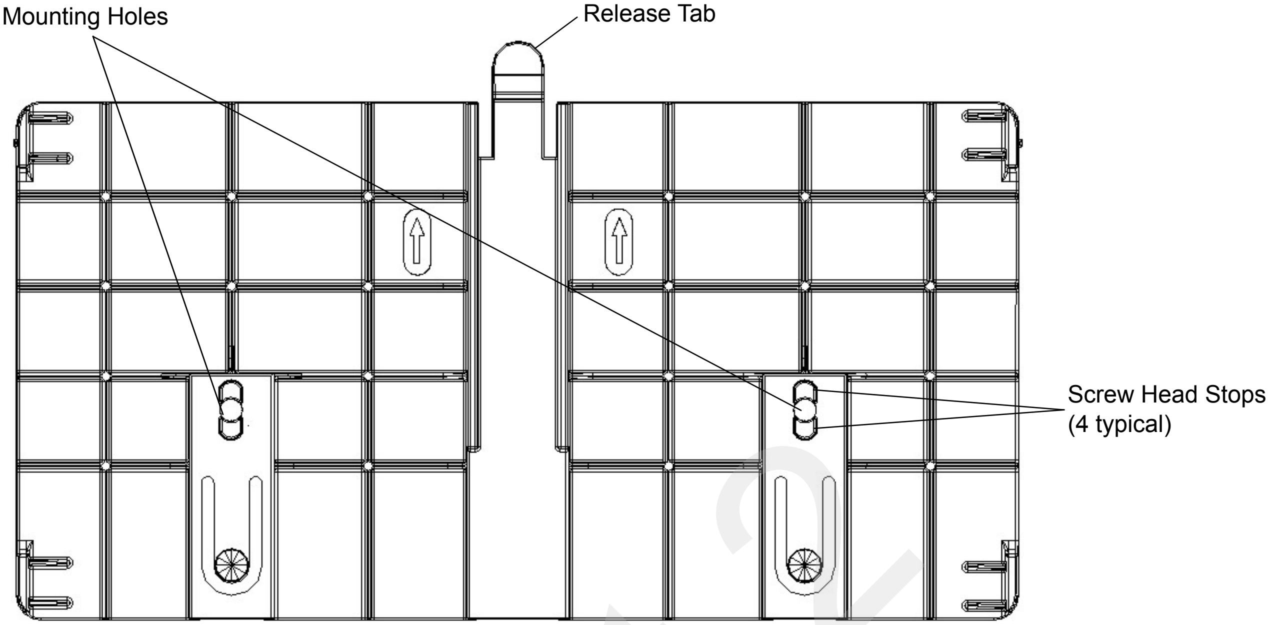


Figure 3-1 *Mounting Plate, Front*

3. Reposition the mounting plate over the mounting holes and secure using the supplied fasteners (as appropriate for the surface material).

✓ ***NOTE*** Mount the reader with the cable connections up or down, depending on the installation requirements.

⚠ ***CAUTION*** Use a hand screw driver to install the mounting plate (do not use a power driver). Do not use excessive torque, and tighten the screws so that they are just snug on the screw head stops (see *Figure 3-1*). If the reader does not engage the mounting plate, loosen the screw(s) 1/8 to 1/4 turn and try again.

4. Position the reader by aligning the markers on the metal base plate and the wall bracket, with the key-slot holes over the mounting screws. Gently slide the reader down to lock into place.
5. To remove the reader, press the release tab and slide the reader up while gently pulling out.

Direct Mounting (Without the Mounting Plate)

⚠ ***CAUTION*** Not using the mounting plate can affect read performance at elevated temperatures. Also, if not using the mounting plate, secure the reader to prevent it from coming off of the mounting screws.

To mount the unit without using the mounting bracket:

1. Use the mounting bracket as a template to locate the holes, or locate and mark the holes on 4 3/16” centers, +/- 1/32”.
2. For wood surfaces, drill two 1/8" diameter by 7/8" deep holes on 4.192" centers. For drywall/masonry surfaces, drill two 3/16" diameter by 7/8" deep (min) holes on 4.192" centers and install using the provided anchors.
3. Position the reader with the key-slot holes over the mounting screws and gently slide the reader down to lock into place.
4. Adjust the screw head height to assure a snug fit. Or if the screws are accessible from the back, use machine screws with a lock washer/nut and tighten the nut (from the back) to secure the reader.

Connecting Antennas

WARNING! **When installing the antenna ensure a minimum separation distance of 13.4 in (34 cm) between the antenna and all persons.**

CAUTION Power off the reader before connecting antennas. See *Powering the Reader on page 3-10*. Never disconnect the antennas while the reader is powered on or reading tags. This can damage the reader.

Do not turn on the antenna ports from a host when the antennas are not connected.

Maximum antenna gain (including any cable loss) cannot exceed + 6.6dBiL. See *Table 3-1* for corresponding maximum conducted RF power at antenna input.

When mounting the antennas outside the building, connect the screen of the coaxial cable to earth (ground) at the entrance to the building. Perform this in accordance with applicable national electrical installation codes. In the U.S., this is required by Section 820.93 of the National Electrical Code, ANSI/NFPA 70.

WARNING! **For Mounting in Environmental Air Handling Space (EAHS): Do not install Antennas and Antenna Cables in the EAHS unless they are suitable for use in EAHS as per UL 2043.**

Table 3-1 *Antenna Gain and Radiated Power*

FX7500	US and Canada	EU	Taiwan
Max Conducted RF Power at Antenna Input	+ 30.0dBm with + 6.0dBiL max gain antenna or + 29.36dBm with + 6.6dBiL max gain antenna	+29.2dBm	+ 29.79dBm with + 6.0dBiL max gain antenna or + 29.36dBm with + 6.6dBiL max gain antenna
Max Antenna Gain Allowed	+ 6.6dBiL	+ 5.5dBiL	+ 6.6dBiL
Max Radiated Power Allowed	4W EIRP	2W ERP	4W EIRP
Antenna Type	Circularly Polarized Plate	N/A	Circularly Polarized Plate

To connect the antennas to the reader (see *Figure 3-2*):

1. For each antenna, attach the antenna reverse TNC connector to an antenna port.
2. Secure the cable using wire ties. Do not bend the cable.

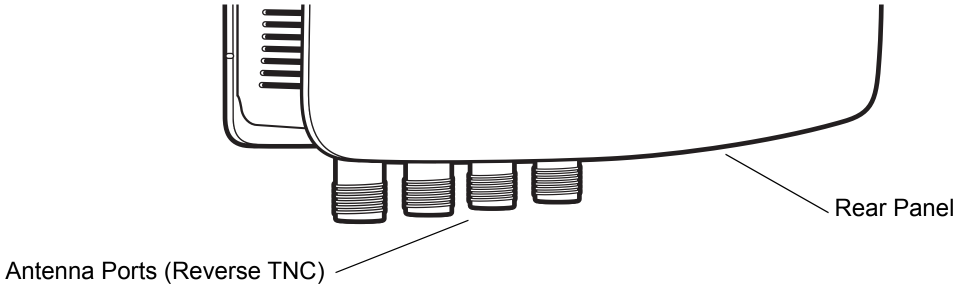


Figure 3-2 *FX7500 RFID Reader Antenna Connection*

Communications Connections

Use a standard Ethernet connection, a standard POE, or POE + Ethernet connection to connect the FX7500 reader to a host or network.

Ethernet Connection

The reader communicates with the host using an Ethernet connection (10/100Base-T Ethernet cable). This connection allows access to the **Administrator Console**, used to change reader settings and control the reader. With a wired Ethernet connection (10/100Base-T cable), power the FX7500 reader using either the reader Zebra AC power supply, or by Power-Over-Ethernet through the Ethernet cable.

Ethernet: Power through AC Outlet

The FX7500 reader communicates to the host through a 10/100Base-T Ethernet cable and receives power through a Zebra AC power supply.

1. Route the Ethernet cable.
2. Route the power cable.
3. Terminate the Ethernet cable according to *Table A-2 on page A-4*.
4. Connect the Ethernet cable to the LAN port on the FX7500 reader. See *Figure 2-4 on page 2-4*.
5. Connect the other end of the Ethernet cable to the host system LAN port.
6. Connect the Zebra AC power supply to a wall outlet.
7. Insert the power supply barrel connector into the FX7500 reader power port. See *Figure 2-4 on page 2-4*.
8. Verify that the unit booted properly and is operational. See *System Start-up/Boot LED Sequence on page 3-11*.
9. On a networked computer, open an internet browser and connect to the reader. See *Connecting to the Reader on page 4-3*.
10. Log in to the **Administrator Console**. See *Administrator Console Login on page 4-6*.

Ethernet: Power through Standard POE or POE+

The POE installation option allows the FX7500 reader to communicate and receive power on the same 10/100Base-T Ethernet cable.

1. Insert the POE Ethernet connector on the RJ45 Ethernet cable into the reader 10/100BaseT Ethernet port. See *Figure 2-4 on page 2-4*.
2. Connect the other end of the cable to an Ethernet network with POE capability.
3. Verify that the reader booted properly and is operational. See *System Start-up/Boot LED Sequence on page 3-11*.
4. On a networked computer, open an internet browser and connect to the reader. See *Connecting to the Reader on page 4-3*.
5. Log in to the **Administrator Console**. See *Administrator Console Login on page 4-6*.

⚠ ***CAUTION*** Do not connect to PoE networks outside the building.

To connect to a network that is not POE capable:

1. Terminate the Ethernet cable according to *Table A-2 on page A-4.*
2. Connect the Ethernet cable to the FX7500 reader 10/100BaseT Ethernet port. See *Figure 2-4 on page 2-4*.
3. Connect the other end of the Ethernet cable to a POE power injector.
4. Connect a patch cable from the POE power injector to the host system LAN port.
5. Verify that the unit booted properly and is operational. See *System Start-up/Boot LED Sequence on page 3-11*.
6. On a networked computer, open an internet browser and connect to the reader. See *Connecting to the Reader on page 4-3*.
7. Log in to the **Administrator Console***.* See *Administrator Console Login on page 4-6*.

USB Connection

The USB client port supports (by default) a **Network** mode of operation. This enables a secondary network interface as a virtual adapter over USB. The interfaces co-exist and if the Ethernet connection fails, the application can switch to USB using a specific IP and can control the reader. To use the USB port for network connection, install the *USB RNDIS Driver* on the Windows XP PC or follow the instructions to install the Microsoft RNDIS driver for Windows 7 below.

To connect the FX7500 to the host PC, insert a USB cable into the USB client port on the reader. See *Figure 2-4 on page 2-4*. Connect the other end of the cable to a USB port on the host PC.

Zebra USB RNDIS Driver

To use the USB port for network connection, install the Zebra USB Remote Network Device (RNDIS) driver and enable the driver on the FX7500. The Zebra RNDIS driver supports 32-bit version operating systems Windows XP, Windows Vista, Windows 7, and Windows Server 2008. For Windows 7 32-bit and 64-bit systems, it is recommend to use Microsoft RNDIS driver (see *Microsoft RNDIS Driver for Windows 7 on page 3-7*).

To install the RNDIS driver on the host.

1. Download the installer file **Zebra RNDIS.msi** from http://www.zebra.com/support to the host PC.
2. Select this file on the host PC to install the host side drivers for using the USB Remote Network Device Interface on the FX7500.
3. Connect a USB cable between the host and the reader. The **Welcome to the Found New Hardware Wizard** screen appears.
4. Select the **No, not this time** radio button and click **Next**.
5. Select the default option **Install Software Automatically (Recommended)**.
6. In the Hardware Installation pop-up window, select **Continue Anyway**.
7. Select **Finish** to complete the installation. This assigns the host an auto-configured IP address. The network is now ready to use and the reader's IP address is fixed to 169.254.10.1.

Microsoft RNDIS Driver for Windows 7

If using Windows 7:

1. After connecting a USB cable between the PC and reader, the RNDIS driver automatically installs. If it does not, right-click on **Computer** and select **Manage**. From **System Tools**, select **Device Manager**. Under **Other Devices**, look for an entry for RNDIS with an exclamation icon indicating that the driver was not installed.

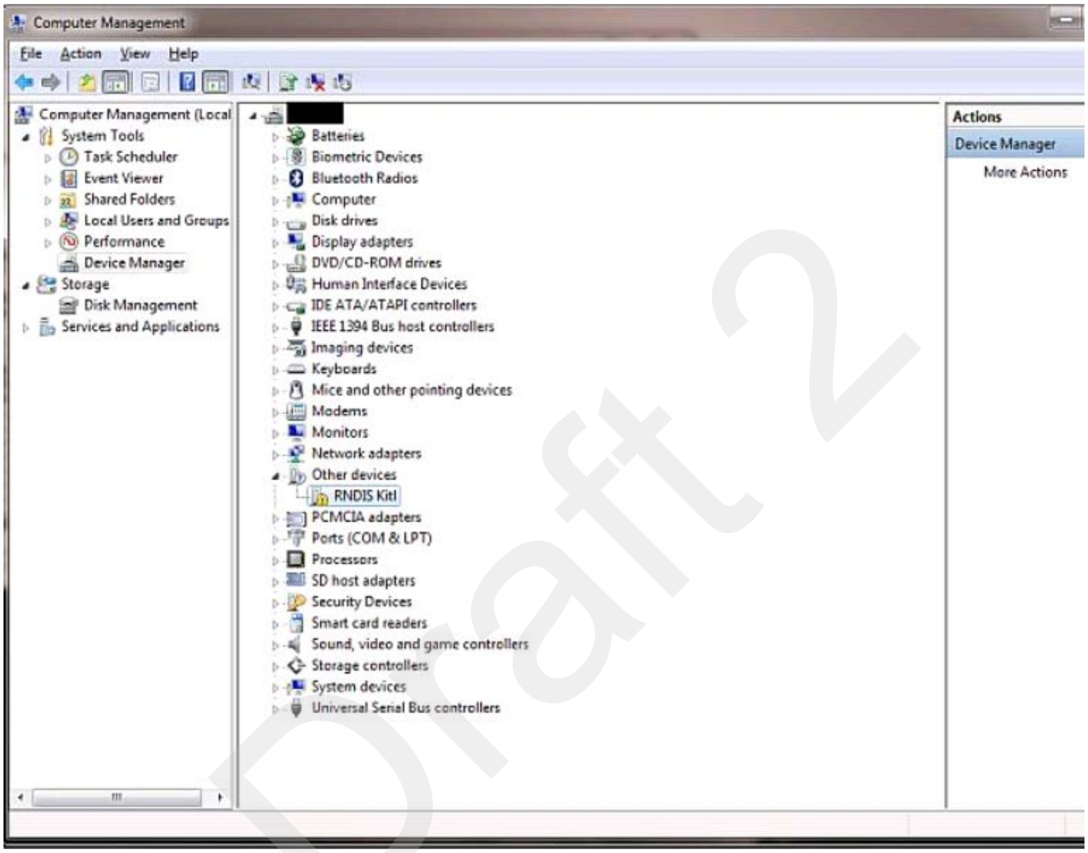
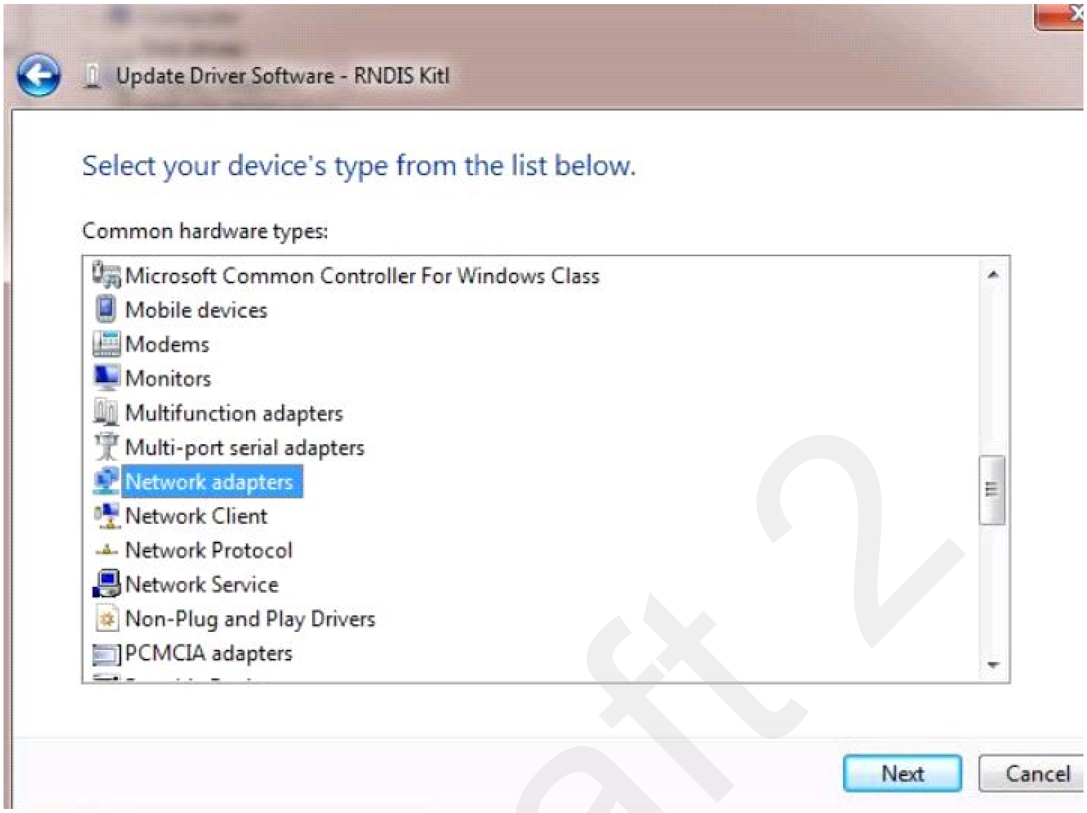


Figure 3-3 *Computer Management Window*

2. Right-click the icon and select **Update Driver Software**. Search for the device driver software by clicking on **Browse my computer for driver software**.

3. Select **Let me pick from a list of device drivers on my computer**.

4. Select **Network adapters**.



Update Driver Software - RNDIS Kitl

Select your device's type from the list below.

Common hardware types:

- Microsoft Common Controller For Windows Class
- Mobile devices
- Modems
- Monitors
- Multifunction adapters
- Multi-port serial adapters
- Network adapters
- Network Client
- Network Protocol
- Network Service
- Non-Plug and Play Drivers
- PCMCIA adapters

Figure 3-4 *Selecting Device Type*

5. Select **Microsoft Corporation** from the manufacturer list.

6. Under **Network Adapter**, select **Remote NDIS Compatible Device**, and click **Next**.

After installation, the PC recognizes the reader as an RNDIS device. The PC obtains the IP address 169.254.10.102, and the reader is reachable at the IP address 169.254.10.1.

Sample Implementation

This implementation assumes that only one FX7500 reader is connected to a host PC via USB. This feature does not function with multiple readers connected to the host. Zebra recommends disabling any other network interface on the PC.

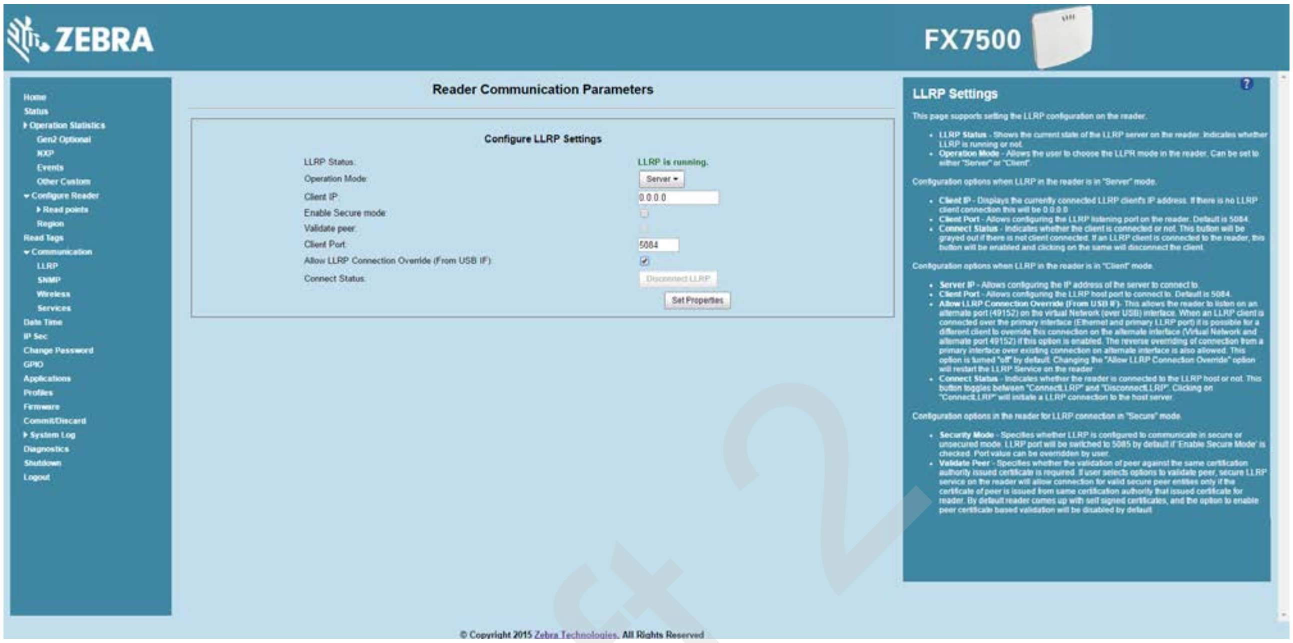
Use an application that uses RFID3 APIs such as Power Session, or use an LLRP application to connect to the reader to read tags.

1. The primary RFID server connects to the FX7500 via the Ethernet interface.

2. The host PC connects to the FX7500 via the USB port. An application on the host PC monitors communication between the primary RFID server and FX7500 reader.

3. When the application on the host PC detects a communication failure between the primary RFID server and the reader, it connects to and controls the reader using the USB virtual interface.

4. The FX7500 listens on the USB virtual interface on a fixed port (49152) as well as on the standard LLRP port (5084). To enable this, select the **Allow LLRP Connection Override** check box in **Configure LLRP Settings** console window.



Reader Communication Parameters

Configure LLRP Settings

LLRP Status:	LLRP is running.
Operation Mode:	Server
Client IP:	0.0.0.0
Enable Secure mode:	□
Validate peer:	□
Client Port:	5084
Allow LLRP Connection Override (From USB IF):	☑
Connect Status:	Disconnect LLRP

Set Properties

LLRP Settings

This page supports setting the LLRP configuration on the reader.

- **LLRP Status** - Shows the current state of the LLRP server on the reader. Indicates whether LLRP is running or not.
- **Operation Mode** - Allows the user to choose the LLPR mode in the reader. Can be set to either "Server" or "Client".

Configuration options when LLRP in the reader is in "Server" mode.

- **Client IP** - Displays the currently connected LLRP client's IP address. If there is no LLRP client connection this will be 0.0.0.0
- **Client Port** - Allows configuring the LLRP listening port on the reader. Default is 5084.
- **Connect Status** - Indicates whether the client is connected or not. This button will be grayed out if there is not client connected. If an LLRP client is connected to the reader, this button will be enabled and clicking on the same will disconnect the client.

Configuration options when LLRP in the reader is in "Client" mode.

- **Server IP** - Allows configuring the IP address of the server to connect to.
- **Client Port** - Allows configuring the LLRP host port to connect to. Default is 5084.
- **Allow LLRP Connection Override (From USB IF)**- This allows the reader to listen on an alternate port (49152) on the virtual Network (over USB) interface. When an LLRP client is connected over the primary interface (Ethernet and primary LLRP port) it is possible for a different client to override this connection on the alternate interface (Virtual Network and alternate port 49152) if this option is enabled. The reverse overriding of connection from a primary interface over existing connection on alternate interface is also allowed. This option is turned "off" by default. Changing the "Allow LLRP Connection Override" option will restart the LLRP Service on the reader.
- **Connect Status** - Indicates whether the reader is connected to the LLRP host or not. This button toggles between "ConnectLLRP" and "DisconnectLLRP". Clicking on "ConnectLLRP" will initiate a LLRP connection to the host server.

Configuration options in the reader for LLRP connection in "Secure" mode.

- **Security Mode** - Specifies whether LLRP is configured to communicate in secure or unsecured mode. LLRP port will be switched to 5085 by default if 'Enable Secure Mode' is checked. Port value can be overridden by user.
- **Validate Peer** - Specifies whether the validation of peer against the same certification authority issued certificate is required. If user selects options to validate peer, secure LLRP service on the reader will allow connection for valid secure peer entities only if the certificate of peer is issued from same certification authority that issued certificate for reader. By default reader comes up with self signed certificates, and the option to enable peer certificate based validation will be disabled by default.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 3-5 *Communication / Configure LLRP Settings Window*

Only one LLRP session can be active on the reader, either through the primary Ethernet interface or through the virtual network over USB interface.

If a connection is active on one interface, a subsequent connection attempt on a second interface disconnects the first. The second connection attempt always prevails and creates a new session.

GPIO Interface Connection

This pluggable terminal block type allows connecting individual wires independently. A single connector accommodates both inputs and outputs. See *Table A-5 on page A-6* for pinout information.

GPIO signals allow some flexibility. Inputs are pulled up within the reader to +5 VDC and can be shorted to ground to pull them low. This allows driving them directly via simple relay or switch contacts. Alternatively, 5V logic can drive inputs. In the logic low state, the current sourced from the reader is approximately 3 mA, so standard gates in most logic families can drive them. Current flow in the high state is negligible. When the equipment uses an external +24 VDC power supply, a +24 VDC connection is provided. This output is not available when an external 24 VDC supply is not present.

✓ ***NOTE*** Do not connect the +24 VDC output directly to either general purpose input that tolerates voltages in excess of 5V but is designed to operate optimally within the range of 0 to +5 VDC.

The general purpose outputs are open-drain drivers, pulled up to 5V. Each output can withstand voltages up to +30 VDC but should not be driven negative. For best results use the +24 VDC supply as a source of external current and use the outputs directly to drive 24V relays, indicator lamps, etc., wired between the 24V supply and individual general purpose outputs. Although each output can sink up to 1A, the maximum current that can be drawn from the internal 24V supply is 1A, so use an external power supply if the current requirement exceeds this. Note that the state of the general purpose outputs is inverted, e.g., driving a GPO line high at the processor pulls the corresponding output low.

Powering the Reader

CAUTION Connect the antennas before supplying power to the reader.

WARNING! **For Mounting in Environmental Air Handling Space (EAHS): Do not install Power Supplies and PoE (Power Injector) in the EAHS unless they are suitable for use in EAHS as per UL 2043.**

Powering the Reader via AC Power Supply

The approved AC power supply connects to the power port on the FX7500 reader using a locking connector (see *Figure 2-4 on page 2-4*). The power supply is compatible with:

- 120V 60 Hz (North America)
- 230V 50 Hz (International excluding Japan)
- 100V 50/60 Hz (Japan).

1. Insert the power supply barrel connector into the reader power port (see *Figure 2-4 on page 2-4*). Rotate the connector to lock it in place.
2. Apply power to the power supply. The green Power LED stays on to indicate the reader is powered and ready. See *System Start-up/Boot LED Sequence on page 3-11*.

To power down the reader, unplug the power supply from its power source. The green Power LED turns off to indicate that the device is off and the system is not operational. Remove the connector from the reader power port.

Powering the Reader via Power-over-Ethernet (POE)

Connect the reader to either a standard POE or POE+ injectors.

1. Insert the POE Ethernet connector on the RJ45 Ethernet cable into the reader 10/100BaseT Ethernet port. See *Figure 2-4 on page 2-4*.
2. Connect the other end of the cable to an Ethernet network with POE capability. See *System Start-up/Boot LED Sequence on page 3-11*.

To power down the reader, remove the Ethernet cable from the network. The green Power LED turns off to indicate that the device is off and the system is not operational. Remove the connector from the 10/100BaseT Ethernet port.

LED Sequences

System Start-up/Boot LED Sequence

See *Figure 2-5 on page 2-5* for LED locations. During system start-up:

1. All LEDs turn on for a few seconds when power is applied to the reader.
2. All LEDs turn off and the PWR LED turns amber.
3. The PWR LED turns green to indicate successful RFID application initialization.
4. When the sequence completes, the green PWR LED remains on and all other LEDs are off.

PWR LED Sequence to Indicate IPv4 Status after Booting

After the RFID application initializes:

1. The PWR LED turns green for 5 seconds to indicate success (following the sequence from *System Start-up/Boot LED Sequence*).
2. The reader checks the eth0 IPv4 address and indicates the IPv4 status using the LEDs:
   - If the reader has a DHCP address, the PWR LED blinks green for 3 seconds.
   - If the reader has static IP address, the PWR LED blinks amber 3 seconds.
   - If the reader has an IP address from zero-configuration networking algorithm, the PWR LED blinks red for 3 seconds.
   - If the reader doesn't have valid IP, the PWR LED blinks amber and green using a 90-second timeout to indicate that it is waiting to acquire an IP address.
     - If it obtains a valid IP within the timeout period, the reader indicates the status as described above.
     - If the timeout expires before the reader obtains an IP, the PWR LED stops blinking.
3. The PWR LED again turns solid green.

Reset to Factory Defaults LED Sequence

Holding the reset button for 8 seconds resets the reader to the factory default configuration.

1. All LEDs turn on as usual when you press and hold the reset button.
2. The PWR LED blinks amber when the reset button is held.
3. The PWR LED blinks green fast 5 times to indicate that the reader detects a reset operation.
4. Release the reset button to reset the reader to factory defaults.

LED Sequence for Software Update Status

1. The PWR LED blinks red during the software update process.
2. After reset, the STAT LED blinks red if the radio module requires a firmware update.

Reading Tags

After the reader powers up, test the reader. See *System Start-up/Boot LED Sequence on page 3-11*.

1. Enable tag reading using the web-based **Administrator Console** (see *Read Tags on page 4-30*) or control the reader through a real-time application such as Power Session.
2. Present a tag so it is facing the antenna and slowly approach the antenna until the activity LED turns green, indicating that the reader read the tag. See *Figure 2-5 on page 2-5*. The distance between the tag and the antenna is the approximate read range.

✓ ***NOTE*** For optimal read results, do not hold the tag at an angle or wave the tag, as this can cause the read distance to vary.

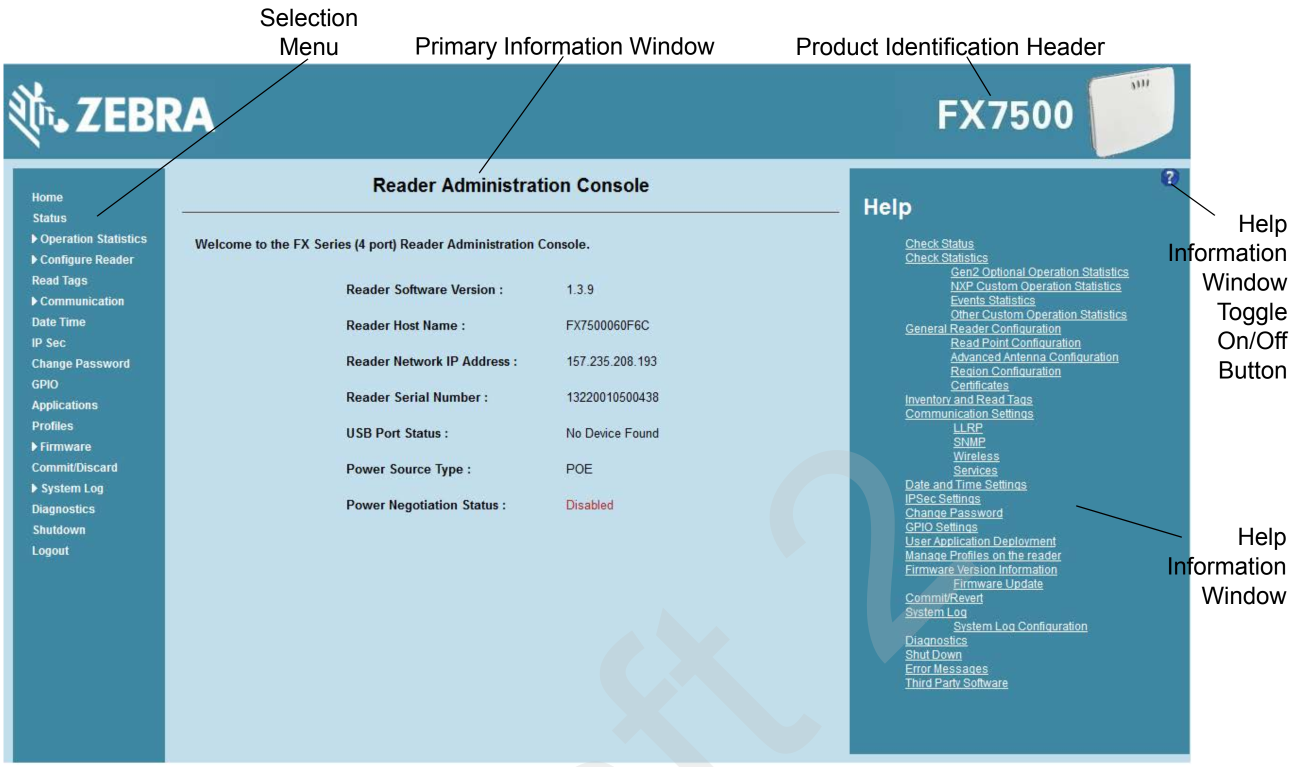
CHAPTER 4 ADMINISTRATOR CONSOLE

Introduction

✓ ***NOTE*** The screens and windows in this chapter may differ from actual screens and windows. 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.

This chapter describes the FX7500 **Reader Administrator Console** functions and procedures. Access the **Administrator Console** using a web browser from a host computer, and use this to manage and configure the readers. The **Administrator Console** main window and support windows have four areas, each containing unique information about the reader.

- **Selection Menu** - selects the function for the primary information window.
- **Primary Information Window** - provides the primary function information.
- **Product Identification Header** - identifies the product.
- **USB Port Status** - provides details on the USB device connected to the USB host port. Hover the mouse pointer over the blue link, available only when a device is detected.
- **Help Information Window**:
  - provides detailed information to support the primary information window
  - includes a scroll bar to scroll through information
  - includes a toggle button to turn on/off the help information window



Reader Administration Console

Welcome to the FX Series (4 port) Reader Administration Console.

Reader Software Version : 1.3.9

Reader Host Name : FX7500060F6C

Reader Network IP Address : 157.235.208.193

Reader Serial Number : 13220010500438

USB Port Status : No Device Found

Power Source Type : POE

Power Negotiation Status : Disabled

Figure 4-1 *Reader Administrator Console Main Menu*

Profiles

Use profiles for multiple reader deployments to save configuration time, as only a few APIs are needed to completely configure a reader. See *Reader Profiles on page 4-43*.

Resetting the Reader

To reset the reader, press and hold the reset button for not more than 2 seconds. See *Figure 2-4 on page 2-4* for the reset button location. The reader reboots but retains the user ID and password. See *System Start-up/Boot LED Sequence on page 3-11*.

✓ ***NOTE*** Hard rebooting the reader (disconnecting power) is not recommended as this discards all the tag events and system log information.

Connecting to the Reader

✓ ***NOTE*** This section describes procedures in a Windows environment.

To use the Administrator Console to manage the reader, first power up the reader and connect it to an accessible network. See *Powering the Reader on page 3-10* and *Ethernet Connection on page 3-5*. The green power LED indicates that the reader is ready. If the green power LED is not lit, reset the reader. See *Resetting the Reader on page 4-2*.

Connect to the reader in one of two ways:

1. *Connecting via Host Name on page 4-3*
2. *Connecting via IP Address on page 4-4*

There are three ways to assign an IP address to the reader:

1. Using DHCP on the network
2. *Using Zero-Configuration Networking when DHCP Server is Not Available on page 4-5*
3. Statically assigning an IP

Any method of assigning the IP supports connection using host name or IP address. Alternatively, connect the reader directly to a local computer using zero-configuration networking. See *Using Zero-Configuration Networking when DHCP Server is Not Available on page 4-5*.

✓ ***NOTE*** When using zero-configuration networking, the FX7500 reader cannot communicate with computers on different subnets, or with computers that do not use automatic private IP addressing.

Connecting via Host Name

To connect to the reader using the host name:

⚠ ***CAUTION*** Reader host name is not guaranteed to work at all times. Its recommended use is only in networks where the probability for IP collisions is low, such as a network in which a DNS server is configured to work together with DHCP to register host names. Host name usage is not recommended in a network where there is no strict control to prevent IP collisions, such as informal networks that use IP static configuration without strict control.

1. Open a browser. Recommended browsers are IE10 (disabling Compatibility View is recommended), Chrome v29, and FireFox 24.
2. Enter the host name provided on the reader label in the browser (e.g., http://fx7500cd3b0d) and press **Enter**. The **Console Login** window appears and the reader is ready.

3. Proceed to *Administrator Console Login on page 4-6* to log in to the reader.

✓ ***NOTE*** Connect the reader to a network that supports host name registration and lookup to ensure the network can access the reader using the host name. For instance, some networks can register host names through DHCP. When first connecting to the reader, it is recommended to keep DHCP enabled in both the PC and the reader, although it is not guaranteed that the host name will work all the time. Use the host name printed on the reader label, or construct it using the reader MAC address on the reader back label. The host name is a string with prefix FX7500, followed by the last three MAC address octets. For example, for a MAC address of 00:15:70:CD:3B:0D, use the prefix FX7500, followed by the last three MAC address octets (CD, 3B, and 0D), for the host name FX7500CD3B0D. Type http://FX7500CD3B0D in the browser address bar to access the reader.

For a network that does not support host name registration and lookup, use the Power Session auto discovery feature to obtain the IP address, and use the IP address connect method.

Auto Discovery

The FX7500 can automatically belong to a network. The reader implements WS-Discovery conforming to RFID Reader Management Profile (RDMP) specification in ISO 24791-3. RDMP is based on an extension for Device Profile for Web Services (DPWS). The discovery mechanism is limited to subnets and does not work across subnets. The Power Session application supports this feature, and it lists the discovered reader using reader hostnames. Because this feature is based on WS-Discovery, the readers can also be discovered in Windows Vista and Windows 7 computers by clicking on the **Network** icon in a file browser.

Connecting via IP Address

To use the IP address to connect to the reader:

1. Open a browser. Recommended browsers are IE10 (disabling Compatibility View is recommended), Chrome v29, and FireFox 24.

2. Enter the IP address in the browser (e.g., http://157.235.88.99) and press **Enter**. The **Console Login** window appears and the reader is ready.

3. Proceed to *Administrator Console Login on page 4-6* to login to the reader.

Using Zero-Configuration Networking when DHCP Server is Not Available

If a DHCP server is not available, the FX7500 reader can use zero-configuration networking to automatically provide a unique network IP address. The reader can then use TCP/IP to communicate with other computers also using a zero-configuration networking-generated IP address.

✓ ***NOTE*** When using zero-configuration networking, the FX7500 reader cannot communicate with computers on different subnets, or that do not use automatic private IP addressing. Automatic private IP addressing is enabled by default.

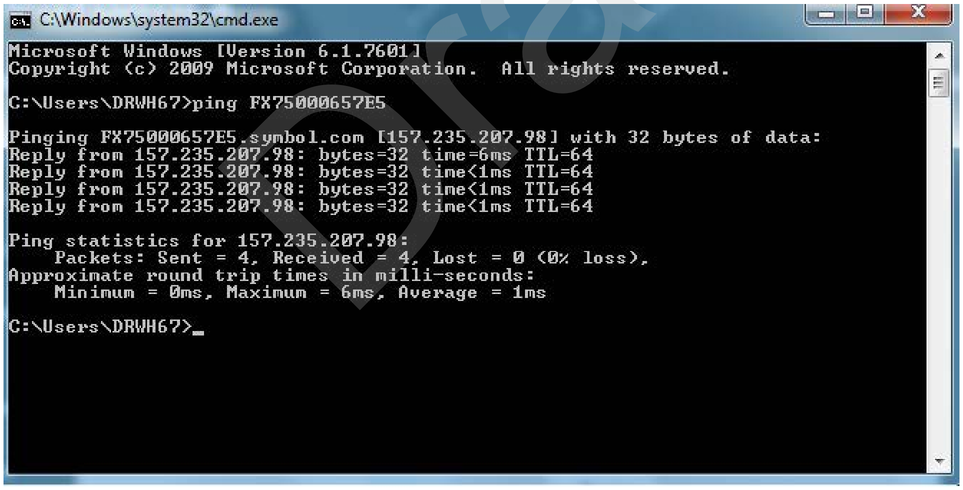
The zero-configuration networking procedure is recommended when the reader is connected directly to a PC. It reduces the overhead needed to configure the reader to a static IP address.

When zero-configuration networking executes after failing to detect a DHCP server, the reader automatically assigns an IPv4 IP address to the Ethernet interface in the form **169.254.xxx.xxx**. This IP address is predictable because it uses the last 2 bytes of the MAC address, usually represented as HEX values, to complete the IPv4 address. These values are converted to decimal format (e.g., if the MAC address ends with **55:9A**, the IPv4 address assigned by the zero-configuration algorithm is **169.254.85.148**.

Windows-based computers support APIPA/zero-configuration networking by default when DHCP fails. To enable APIPA for a Windows PC, visit http://support.microsoft.com/ and search for APIPA.

Obtaining the IP Address via Command Prompt

The **Administrator Console** provides the reader IP address. See *Figure 4-1 on page 4-2*. To obtain the reader IP address without logging into the reader, open a command window and ping the reader host name. See *Connecting via Host Name on page 4-3*.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\DRWH67>ping FX75000657E5

Pinging FX75000657E5.symbol.com [157.235.207.98] with 32 bytes of data:
Reply from 157.235.207.98: bytes=32 time=6ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64

Ping statistics for 157.235.207.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Users\DRWH67>_
```

Figure 4-2 *IP Ping Window*

Administrator Console Login

The reader has a unique first time startup sequence that requires setting a unique user ID and password and as well as the region (regulatory requirement).

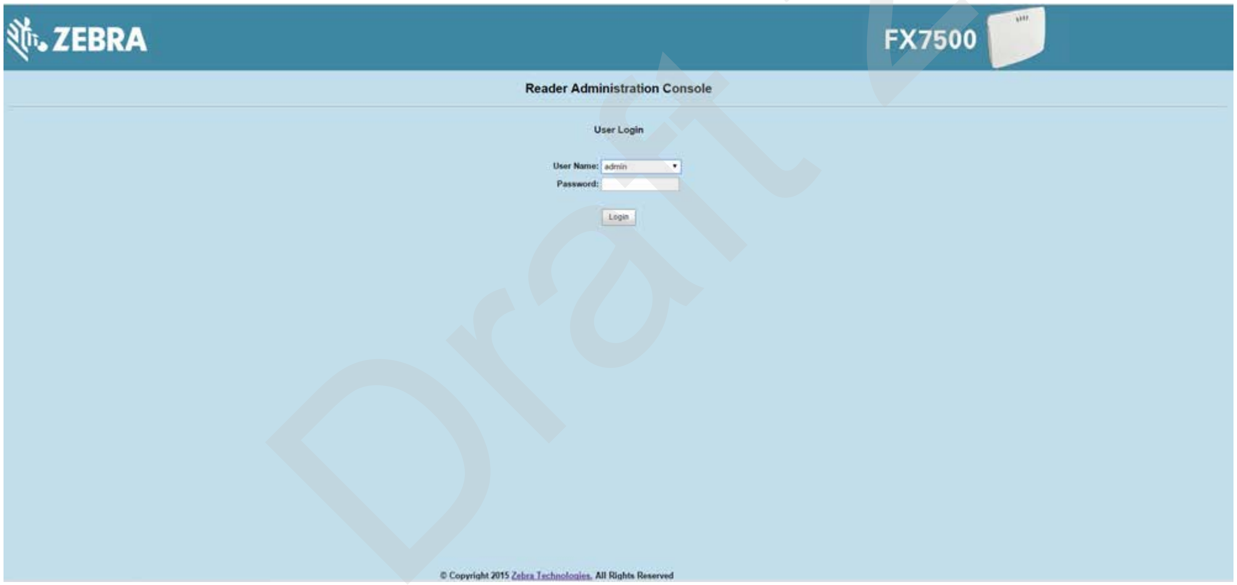
✓ ***NOTE*** The recommended browsers are IE10 (disabling Compatibility View is recommended), Chrome v29, and FireFox 24. These browsers were tested and validated to work properly. Other browsers may or may not work properly.

First Time / Start-Up Login

When starting the reader for the first time, set a unique user ID and password and set the region of reader operation. Setting the reader to a different region is illegal.

Logging In with Default User ID and Password

1. Upon connecting to the reader with a web browser, the **User Login** window appears.



Reader Administration Console

User Login

User Name: admin

Password:

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-3 *User Login Window*

2. Enter **admin** in the **User Name:** field and **change** in the **Password:** field and click **Login.**

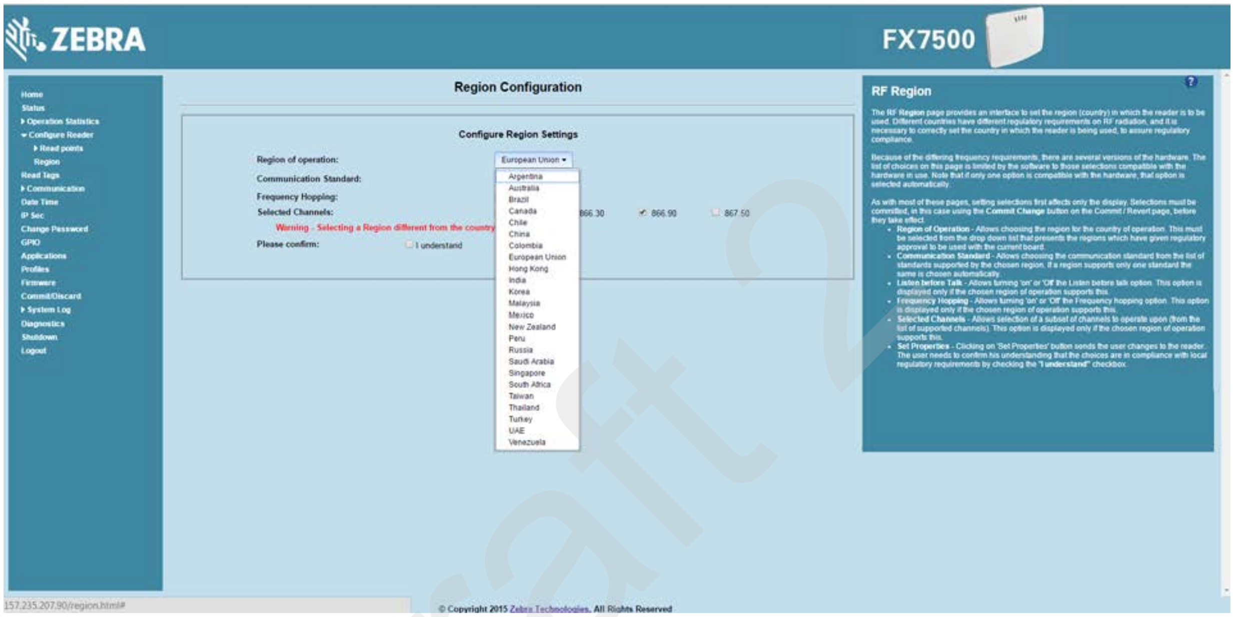
For global reader configurations, the **Region Configuration** window appears. For US reader configurations, the **Administrator Console** main window appears.

Setting the Region

For global reader configurations, set the region of operation. **Setting the unit to a different region is illegal**.

✓ ***NOTE*** Region configuration is not available for readers configured to operate in the United States region (under FCC rules). In this case, skip this step.

1. In the **Configure Region Settings** window, select the region from the drop-down menu.



Region Configuration

Configure Region Settings

Region of operation: European Union

Communication Standard:

Frequency Hopping:

Selected Channels: 866.30 ☑ 866.90 □ 867.50

Warning - Selecting a Region different from the country

Please confirm: □ I understand

RF Region

The RF Region page provides an interface to set the region (country) in which the reader is to be used. Different countries have different regulatory requirements on RF radiation, and it is necessary to correctly set the country in which the reader is being used, to assure regulatory compliance.

Because of the differing frequency requirements, there are several versions of the hardware. The list of choices on this page is limited by the software to those selections compatible with the hardware in use. Note that if only one option is compatible with the hardware, that option is selected automatically.

As with most of these pages, setting selections first affects only the display. Selections must be committed, in this case using the **Commit Change** button on the Commit / Revert page, before they take effect.

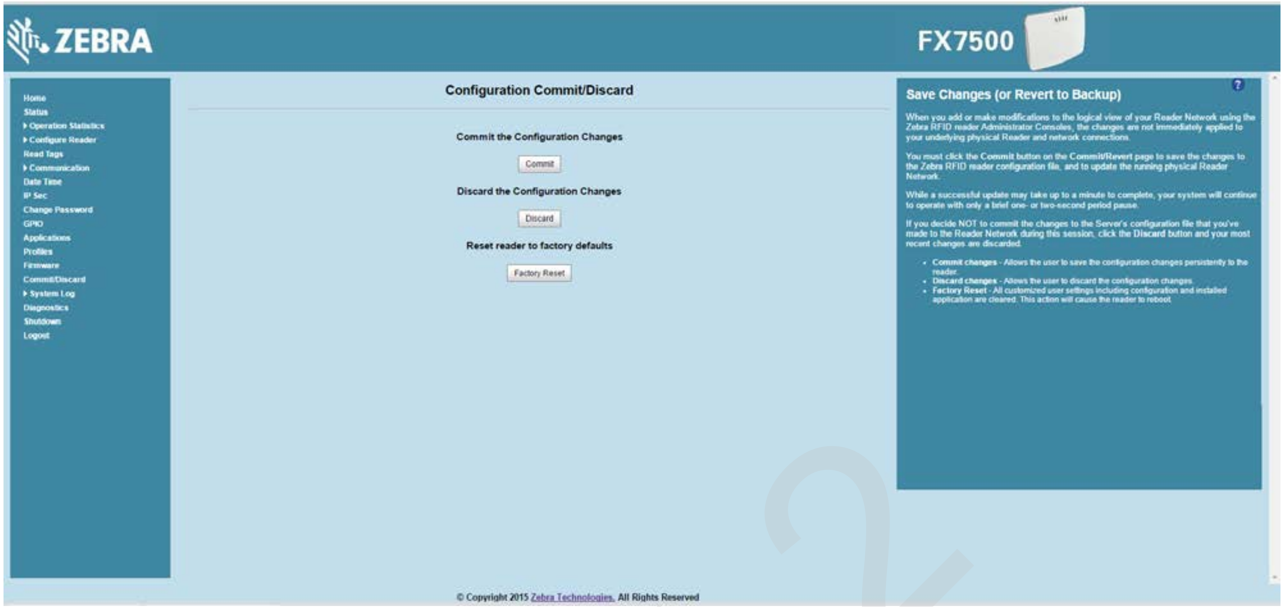
- **Region of Operation** - Allows choosing the region for the country of operation. This must be selected from the drop down list that presents the regions which have given regulatory approval to be used with the current board.
- **Communication Standard** - Allows choosing the communication standard from the list of standards supported by the chosen region. If a region supports only one standard the same is chosen automatically.
- **Listen before Talk** - Allows turning 'on' or 'Off' the Listen before talk option. This option is displayed only if the chosen region of operation supports this.
- **Frequency Hopping** - Allows turning 'on' or 'Off' the Frequency hopping option. This option is displayed only if the chosen region of operation supports this.
- **Selected Channels** - Allows selection of a subset of channels to operate upon (from the list of supported channels). This option is displayed only if the chosen region of operation supports this.
- **Set Properties** - Clicking on 'Set Properties' button sends the user changes to the reader. The user needs to confirm his understanding that the choices are in compliance with local regulatory requirements by checking the "I understand" checkbox.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-4 *Selecting the Region*

2. Select the **Communication Standard** if applicable.
3. Select **Frequency Hopping**, if applicable.
4. Select the appropriate channel(s), if applicable.
5. Click the **I understand** check box.
6. Click **Set Properties** to complete the region selection. The **Operation Successful** window appears.
7. Select **Commit/Discard** from the selection menu.

✓ ***NOTE*** Most changes to the reader require a commit to save them.



Configuration Commit/Discard

Commit the Configuration Changes

Discard the Configuration Changes

Reset reader to factory defaults

Save Changes (or Revert to Backup)

When you add or make modifications to the logical view of your Reader Network using the Zebra RFID reader Administrator Consoles, the changes are not immediately applied to your underlying physical Reader and network connections.

You must click the Commit button on the Commit/Revert page to save the changes to the Zebra RFID reader configuration file, and to update the running physical Reader Network.

While a successful update may take up to a minute to complete, your system will continue to operate with only a brief one- or two-second period pause.

If you decide NOT to commit the changes to the Server's configuration file that you've made to the Reader Network during this session, click the Discard button and your most recent changes are discarded.

- **Commit changes** - Allows the user to save the configuration changes persistently to the reader.
- **Discard changes** - Allows the user to discard the configuration changes.
- **Factory Reset** - All customized user settings including configuration and installed application are cleared. This action will cause the reader to reboot

© Copyright 2015 Zebra Technologies. All Rights Reserved

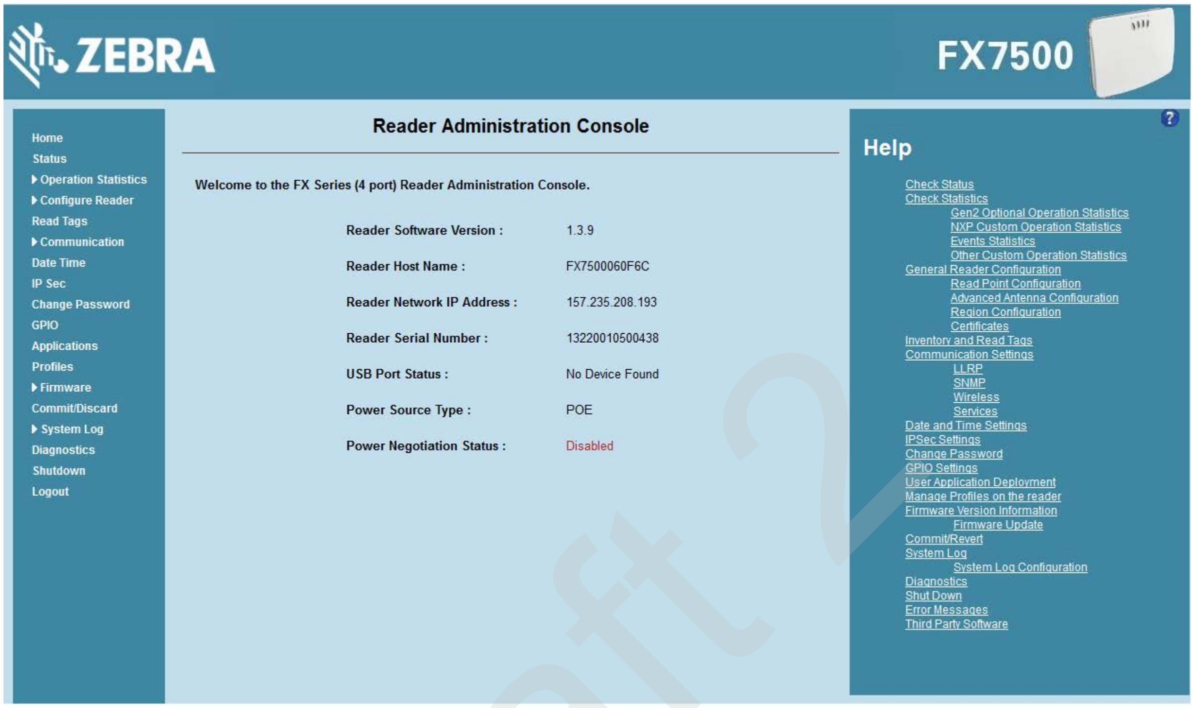
Figure 4-5 *Commit/Discard Window*

8. Click **Commit** to apply the changes to the reader configuration file, or **Discard** to discard the new region configuration changes.

When the commit completes, the **Commit Successful** window appears. The region is now set and stored in the reader.

Reader Administrator Console

The **Reader Administrator Console** main window appears after successfully logging into the reader.



Reader Administration Console

Welcome to the FX Series (4 port) Reader Administration Console.

Reader Software Version : 1.3.9

Reader Host Name : FX7500060F6C

Reader Network IP Address : 157.235.208.193

Reader Serial Number : 13220010500438

USB Port Status : No Device Found

Power Source Type : POE

Power Negotiation Status : Disabled

Figure 4-6 *Reader Administrator Console Main Window*

Administrator Console Option Selections

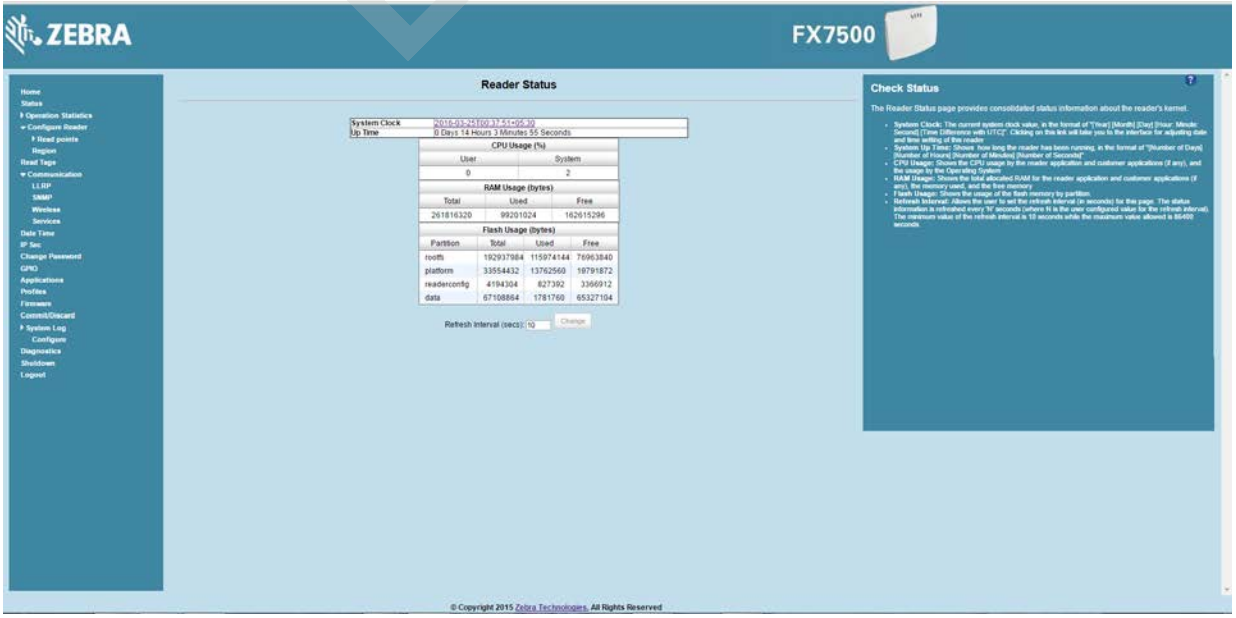
Click an item from the selection menu on the left to select:

- **Status** - see *Status on page 4-10*
- **Operation Statistics** - see *Reader Statistics on page 4-11*
  - **Gen2 Optional** - see *Reader Gen2 Optional Operation Statistics on page 4-12*
  - **NXP** - see *NXP Custom Command Operation Statistics on page 4-13*
  - **Events** - see *Event Statistics on page 4-14*
  - **Other Custom** - see *Other Custom Command Operation Statistics on page 4-15*
- **Configure Reader** - see *Configure Reader on page 4-16*
  - **Read Points** - see *Read Points on page 4-17*
    - **Advanced** - see *Read Points - Advanced on page 4-18*
  - **Region** - see *Configure Region on page 4-19*
  - **Certificates** - see *Certificates on page 4-20*
- **Read Tags** - see *Read Tags on page 4-30*

- **Communication** - see *Communication Settings on page 4-31*
  - **LLRP** - see *Configure LLRP Settings on page 4-34*
  - **SNMP** - see *SNMP Settings on page 4-35*
  - **Wireless** - see *Wireless Settings on page 4-36*
  - **Services** - see *Network Services Settings on page 4-37*
- **Date/Time** - see *System Time Management on page 4-38*
- **IP Sec** - see *IPV6 IP Sec on page 4-39*
- **Change Password** - see *Change Password on page 4-40*
- **GPIO** - see *GPIO on page 4-41*
- **Applications** - see *Applications on page 4-42*
- **Profiles** - see *Reader Profiles on page 4-43*
- **Firmware** - see *Firmware Version/Update on page 4-44*
  - **Update** - see *Firmware Update on page 4-45*
- **Commit/Discard** - see *Commit/Discard on page 4-45*
- **System Log** - see *System Log on page 4-46*
  - **Configure** - see *Configure System Log on page 4-47*
- **Diagnostics** - see *Reader Diagnostics on page 4-48*
- **Shutdown** - see *Shutdown on page 4-49*
- **Logout** - click **Logout** to immediately log out of the **Administrator Console.**

Status

Click **Status** on the selection menu to view the **Reader Status** window. This window displays information about the reader and read points (antennas).



Reader Status

System Clock	2016-03-25T00:37:51+05:30
Up Time	0 Days 14 Hours 3 Minutes 55 Seconds

CPU Usage (%)	
User	System
0	2

RAM Usage (bytes)		
Total	Used	Free
261816320	99201024	162615296

Flash Usage (bytes)			
Partition	Total	Used	Free
rootfs	192937984	115974144	76963840
platform	33554432	13762560	19791872
readerconfig	4194304	827392	3366912
data	67108864	1781760	65327104

Refresh Interval (secs): 10 Change

Check Status

The Reader Status page provides consolidated status information about the reader's kernel.

- System Clock: The current system clock value, in the format of "[Year] [Month] [Day] [Hour: Minute: Second] [Time Difference with UTC]". Clicking on this link will take you to the interface for adjusting date and time setting of this reader
- System Up Time: Shows how long the reader has been running, in the format of "[Number of Days] [Number of Hours] [Number of Minutes] [Number of Seconds]"
- CPU Usage: Shows the CPU usage by the reader application and customer applications (if any), and the usage by the Operating System
- RAM Usage: Shows the total allocated RAM for the reader application and customer applications (if any), the memory used, and the free memory
- Flash Usage: Shows the usage of the flash memory by partition.
- Refresh Interval: Allows the user to set the refresh interval (in seconds) for this page. The status information is refreshed every 'N' seconds (where N is the user configured value for the refresh interval). The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 seconds.

© Copyright 2015 Zebra Technologies. All Rights Reserved

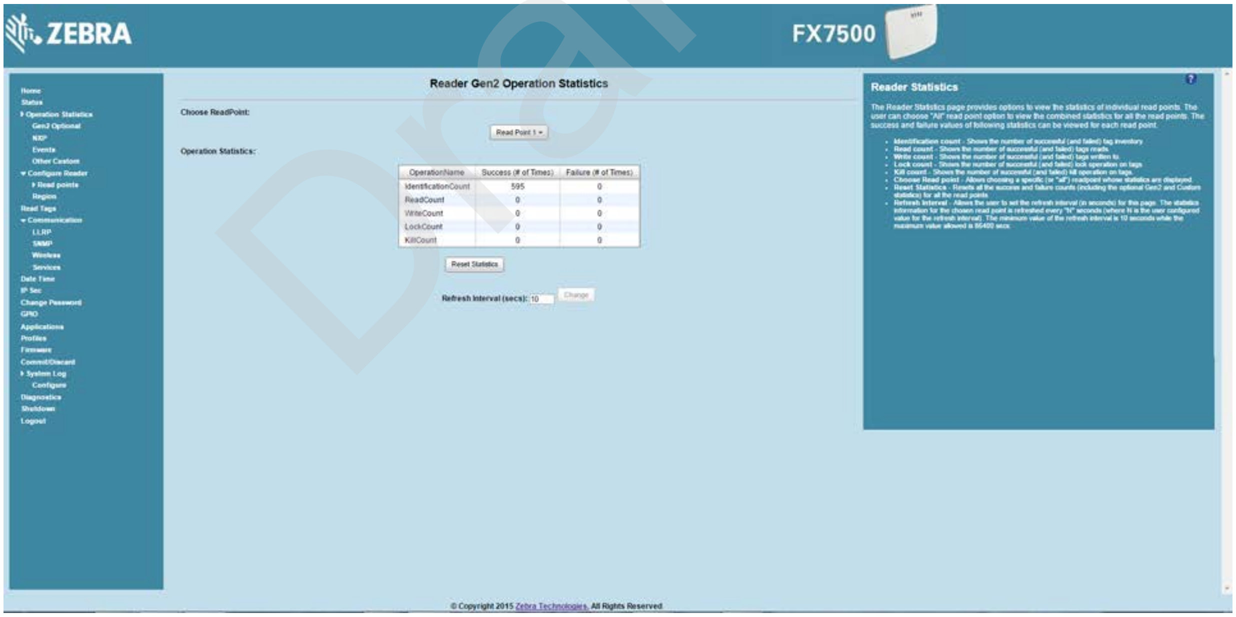
Figure 4-7 *Reader Status Window*

The **Reader Status** window provides consolidated reader status information:

- **System Clock:** The current system clock value, in the format of [Year] [Month] [Day] [Hour: Minute: Second] [Time Difference with UTC]. Click the link to adjust the reader date and time settings.
- **Up Time** - Displays how long the reader has been running, in the format [Number of Days] [Number of Hours] [Number of Minutes] [Number of Seconds].
- **CPU Usage:** Displays the CPU usage for the system and reader applications, including customer applications.
- **RAM Usage:** Displays the total allocated RAM for the reader application and customer applications (if any), the memory used, and the free memory.
- **Flash Usage:** Displays the flash memory usage by partition.
- **Refresh Interval** - Sets the refresh interval (in seconds) for the window. The status information refreshes every **N** seconds (where **N** is the user configured value for the refresh interval). The minimum refresh interval value is 10 seconds; the maximum allowed is 86,400 seconds.

Reader Statistics

Select **Operation Statistics** to view the **Reader Operation Statistics** window. This window provides options to view the statistics of individual read points or combined statistics for all read points, including the success and failure values of statistics for each read point. The statistic count is cumulative once the reader starts or the **Reset Statistics** button is selected.



Reader Gen2 Operation Statistics

Choose ReadPoint: Read Point 1

Operation Statistics:

OperationName	Success (# of Times)	Failure (# of Times)
IdentificationCount	595	0
ReadCount	0	0
WriteCount	0	0
LockCount	0	0
KillCount	0	0

Refresh Interval (secs): 10

Reader Statistics

The Reader Statistics page provides options to view the statistics of individual read points. The user can choose "All" read point option to view the combined statistics for all the read points. The success and failure values of following statistics can be viewed for each read point.

- Identification count - Shows the number of successful (and failed) tag inventory
- Read count - Shows the number of successful (and failed) tags reads.
- Write count - Shows the number of successful (and failed) tags written to.
- Lock count - Shows the number of successful (and failed) lock operation on tags
- Kill count - Shows the number of successful (and failed) kill operation on tags.
- Choose Read point - Allows choosing a specific (or "all") readpoint whose statistics are displayed.
- Reset Statistics - Resets all the success and failure counts (including the optional Gen2 and Custom statistics) for all the read points.
- Refresh Interval - Allows the user to set the refresh interval (in seconds) for this page. The statistics information for the chosen read point is refreshed every "N" seconds (where N is the user configured value for the refresh interval). The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 secs.

© Copyright 2015 Zebra Technologies. All Rights Reserved

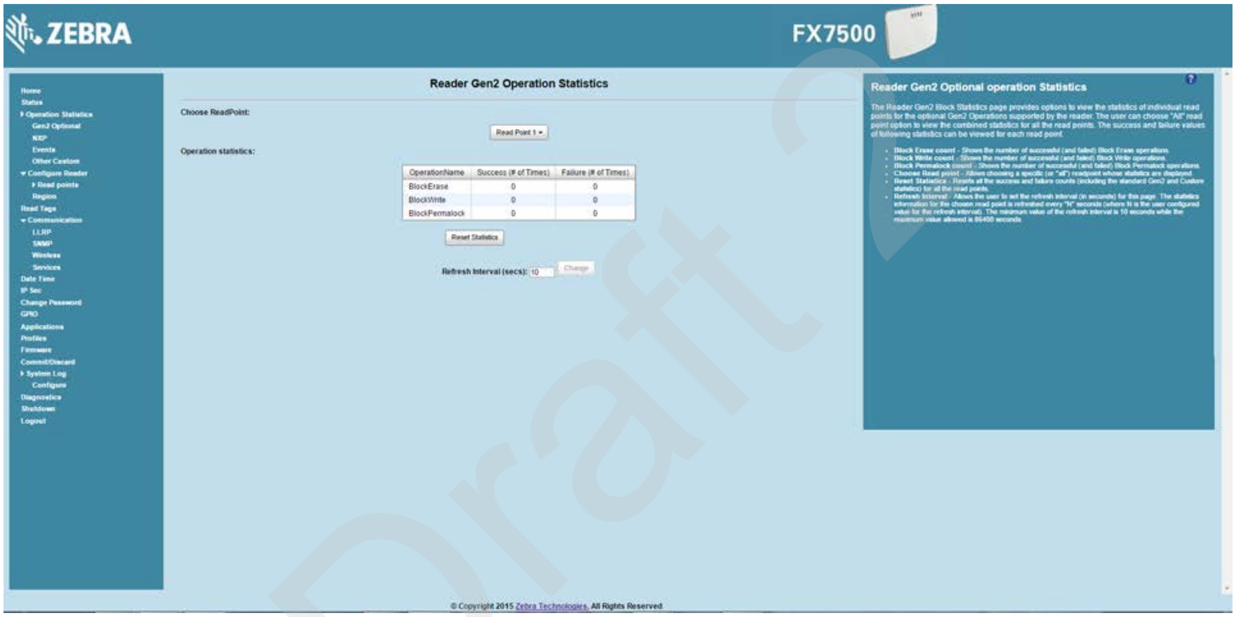
Figure 4-8 *Reader Operation Statistics Window*

- **Choose ReadPoint** - Select a specific read point or select **All** from the drop-down list to display the statistics.
- **IdentificationCount** - Displays the number of successful (and failed) tag inventories.
- **ReadCount** - Displays the number of successful (and failed) tag reads.
- **WriteCount** - Displays the number of successful (and failed) tag writes.
- **Lockcount** - Displays the number of successful (and failed) lock operations on tags.

- **KillCount** - Displays the number of successful (and failed) kill operations on tags.
- **Reset Statistics** - Resets all success and failure counts (including the optional Gen2 and Custom statistics) for all read points.
- **Refresh Interval** - Sets the refresh interval (in seconds) for this window. The statistics information for the chosen read point is refreshed every **N** seconds (where **N** is the set refresh interval). The minimum value is 10 seconds and the maximum value allowed is 86,400 seconds. Input a new value and click **Change** to set a new interval.

Reader Gen2 Optional Operation Statistics

Select **Gen2 Optional** to view the **Reader Gen2 Operation Statistics** window. This window provides options to view the statistics of read points for the optional Gen2 operations the reader supports.



Reader Gen2 Operation Statistics

Choose ReadPoint: Read Point 1

Operation statistics:

OperationName	Success (# of Times)	Failure (# of Times)
BlockErase	0	0
BlockWrite	0	0
BlockPermalock	0	0

Refresh Interval (secs): 10

Reader Gen2 Optional operation Statistics

The Reader Gen2 Block Statistics page provides options to view the statistics of individual read points for the optional Gen2 Operations supported by the reader. The user can choose "All" read point option to view the combined statistics for all the read points. The success and failure values of following statistics can be viewed for each read point.

- Block Erase count - Shows the number of successful (and failed) Block Erase operations.
- Block Write count - Shows the number of successful (and failed) Block Write operations.
- Block Permalock count - Shows the number of successful (and failed) Block Permalock operations.
- Choose Read point - Allows choosing a specific (or "all") readpoint whose statistics are displayed.
- Reset Statistics - Resets all the success and failure counts (including the standard Gen2 and Custom statistics) for all the read points.
- Refresh Interval - Allows the user to set the refresh interval (in seconds) for this page. The statistics information for the chosen read point is refreshed every "N" seconds (where N is the user configured value for the refresh interval). The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 seconds.

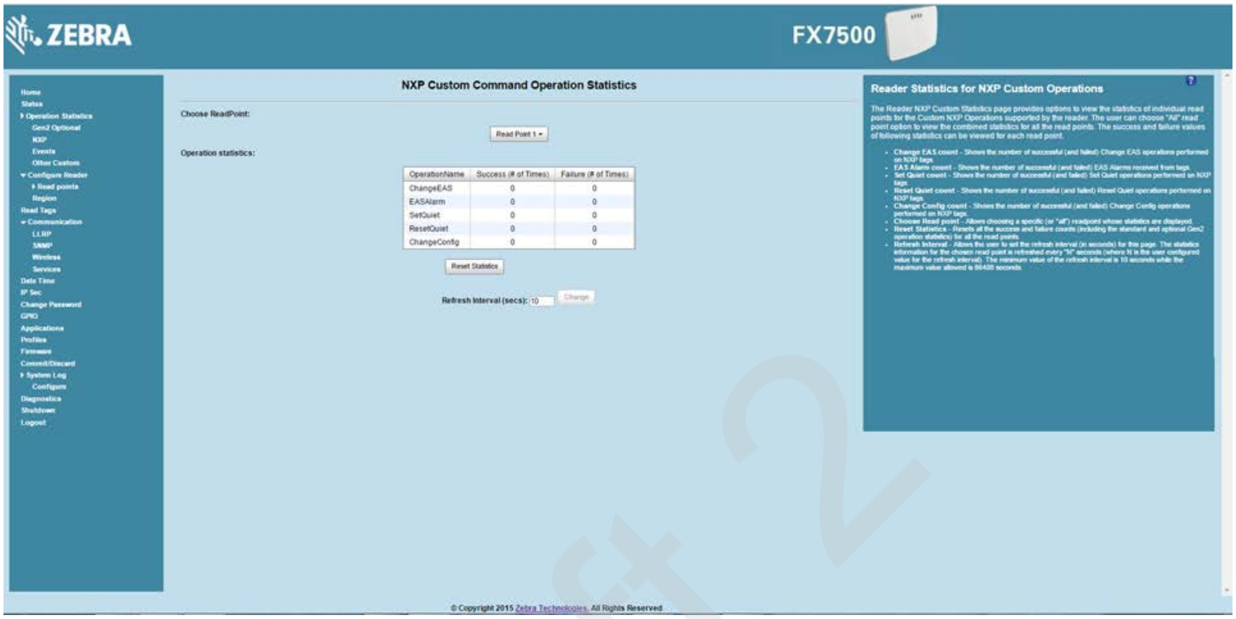
© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-9 *Reader Gen2 Operation Statistics Window*

- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **BlockErase** - Displays the number of successful (and failed) block erase operations.
- **BlockWrite** - Displays the number of successful (and failed) block write operations.
- **BlockPermalock** - Displays the number of successful (and failed) block permalock operations.
- **Reset Statistics** - Resets all success and failure counts (including the standard Gen2 and custom statistics) for all read points.
- **Refresh Interval** - Sets the refresh interval (in seconds) for this window. The statistics information for the chosen read point is refreshed every **N** seconds (where **N** is the set refresh interval). The minimum value is 10 seconds and the maximum value allowed is 86,400 seconds. Input a new value and click **Change** to set a new interval.

NXP Custom Command Operation Statistics

Select **NXP** to view the **NXP Custom Command Operation Statistics** window. This window provides options to view the statistics of read points for the custom NXP operations the reader supports.



NXP Custom Command Operation Statistics

Choose ReadPoint:

Operation statistics:

OperationName	Success (# of Times)	Failure (# of Times)
ChangeEAS	0	0
EASAlarm	0	0
SetQuiet	0	0
ResetQuiet	0	0
ChangeConfig	0	0

Refresh Interval (secs): 10

Reader Statistics for NXP Custom Operations

The Reader NXP Custom Statistics page provides options to view the statistics of individual read points for the Custom NXP Operations supported by the reader. The user can choose "All" read point option to view the combined statistics for all the read points. The success and failure values of following statistics can be viewed for each read point.

- Change EAS count - Shows the number of successful (and failed) Change EAS operations performed on NXP tags.
- EAS Alarm count - Shows the number of successful (and failed) EAS Alarms received from tags.
- Set Quiet count - Shows the number of successful (and failed) Set Quiet operations performed on NXP tags.
- Reset Quiet count - Shows the number of successful (and failed) Reset Quiet operations performed on NXP tags.
- Change Config count - Shows the number of successful (and failed) Change Config operations performed on NXP tags.
- Choose Read point - Allows choosing a specific (or "all") readpoint whose statistics are displayed.
- Reset Statistics - Resets all the success and failure counts (including the standard and optional Gen2 operation statistics) for all the read points.
- Refresh Interval - Allows the user to set the refresh interval (in seconds) for this page. The statistics information for the chosen read point is refreshed every "N" seconds (where N is the user configured value for the refresh interval). The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 seconds.

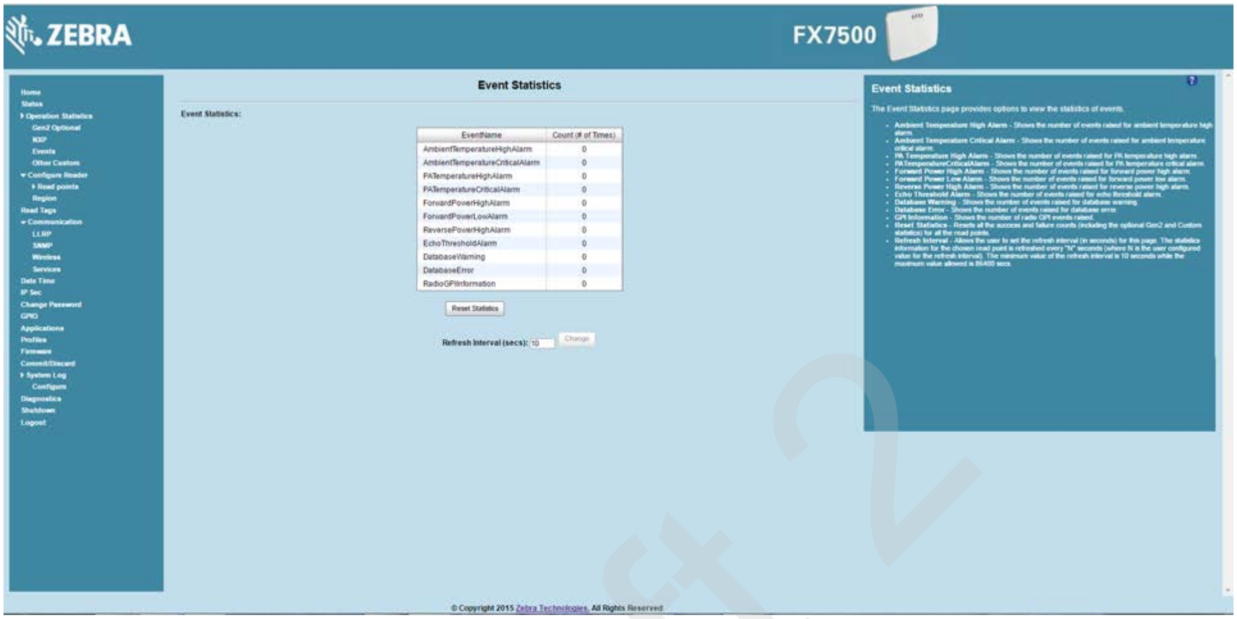
© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-10 *NXP Custom Command Operation Statistics Window*

- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **ChangeEAS** - Displays the number of successful (and failed) change EAS operations performed on NXP tags.
- **EASAlarm** - Displays the number of successful (and failed) EAS alarms received from tags.
- **SetQuiet** - Displays the number of successful (and failed) set quiet operations performed on NXP tags.
- **ResetQuiet** - Displays the number of successful (and failed) reset quiet operations performed on NXP tags.
- **ChangeConfig** - Displays the number of successful (and failed) change configuration operations performed on NXP tags.
- **Reset Statistics** - Resets all the success and failure counts (including the standard and optional Gen2 operation statistics) for all the read points.
- **Refresh Interval** - Sets the refresh interval (in seconds) for this window. The statistics information for the chosen read point is refreshed every **N** seconds (where **N** is the set refresh interval). The minimum value is 10 seconds and the maximum value allowed is 86,400 seconds. Input a new value and click **Change** to set a new interval.

Event Statistics

Select **Events** to view the **Events Statistics** window. This window provides options to view the statistics of events.



Event Statistics

Event Statistics:

EventName	Count (# of Times)
AmbientTemperatureHighAlarm	0
AmbientTemperatureCriticalAlarm	0
PATemperatureHighAlarm	0
PATemperatureCriticalAlarm	0
ForwardPowerHighAlarm	0
ForwardPowerLowAlarm	0
ReversePowerHighAlarm	0
EchoThresholdAlarm	0
DatabaseWarning	0
DatabaseError	0
RadioGPIInformation	0

Refresh Interval (secs): 10

Event Statistics

The Event Statistics page provides options to view the statistics of events.

- **Ambient Temperature High Alarm** - Shows the number of events raised for ambient temperature high alarm.
- **Ambient Temperature Critical Alarm** - Shows the number of events raised for ambient temperature critical alarm.
- **PA Temperature High Alarm** - Shows the number of events raised for PA temperature high alarm.
- **PATemperatureCriticalAlarm** - Shows the number of events raised for PA temperature critical alarm.
- **Forward Power High Alarm** - Shows the number of events raised for forward power high alarm.
- **Forward Power Low Alarm** - Shows the number of events raised for forward power low alarm.
- **Reverse Power High Alarm** - Shows the number of events raised for reverse power high alarm.
- **Echo Threshold Alarm** - Shows the number of events raised for echo threshold alarm.
- **Database Warning** - Shows the number of events raised for database warning.
- **Database Error** - Shows the number of events raised for database error.
- **GPI Information** - Shows the number of radio GPI events raised.
- **Reset Statistics** - Resets all the success and failure counts (including the optional Gen2 and Custom statistics) for all the read points.
- **Refresh Interval** - Allows the user to set the refresh interval (in seconds) for this page. The statistics information for the chosen read point is refreshed every "N" seconds (where N is the user configured value for the refresh interval). The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 secs.

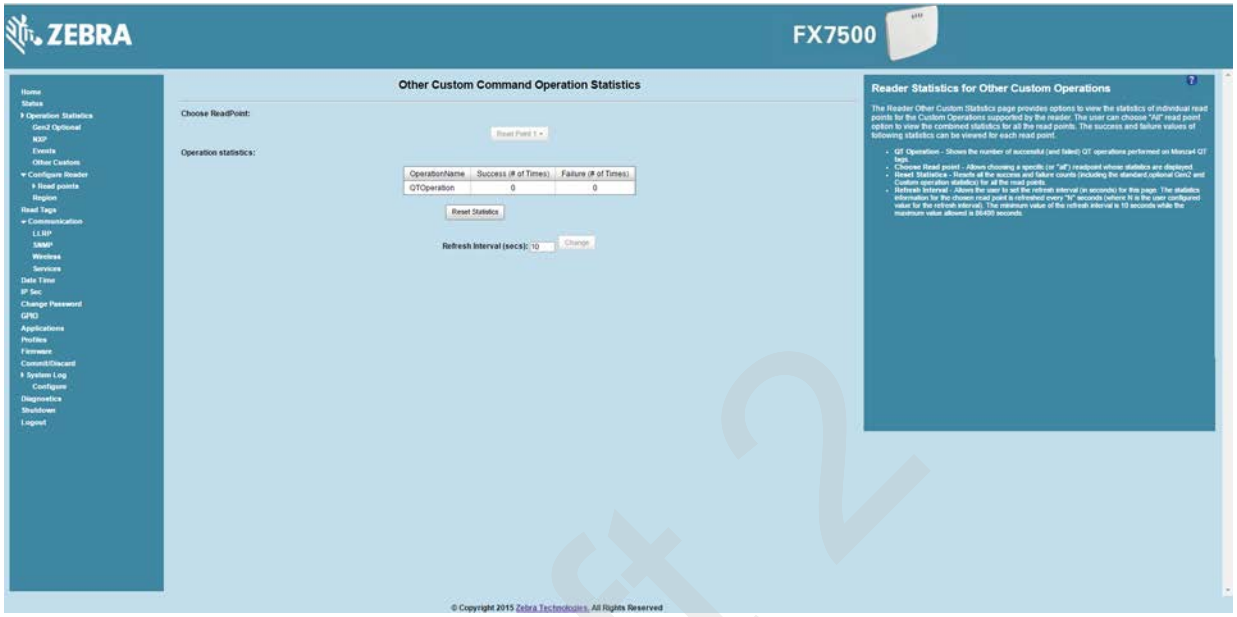
© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-11 *Event Statistics Window*

- **AmbientTemperatureHighAlarm** - Displays the number of events raised for ambient temperature high alarm.
- **AmbientTemperatureCriticalAlarm** - Displays the number of events raised for ambient temperature critical alarm.
- **PATemperatureHighAlarm** - Displays the number of events raised for PA temperature high alarm.
- **PATemperatureCriticalAlarm** - Displays the number of events raised for PA temperature critical alarm.
- **ForwardPowerHighAlarm** - Displays the number of events raised for forward power high alarm.
- **ForwardPowerLowAlarm** - Displays the number of events raised for forward power low alarm.
- **ReversePowerHighAlarm** - Displays the number of events raised for reverse power high alarm.
- **EchoThresholdAlarm** - Displays the number of events raised for echo threshold alarm.
- **DatabaseWarning** - Displays the number of warning events raised whenever the radio tag list buffer is almost full.
- **DatabaseError** - Displays the number of events raised when the radio tag list buffer is full.
- **GPIInformation** - Displays the number of events raised for radio GPI events.
- **Reset Statistics** - Resets all the success and failure counts for all the read points.
- **Refresh Interval** - Sets the refresh interval (in seconds) for this window. The statistics information for the chosen read point is refreshed every **N** seconds (where **N** is the set refresh interval). The minimum value is 10 seconds and the maximum value allowed is 86,400 seconds. Input a new value and click **Change** to set a new interval.

Other Custom Command Operation Statistics

Select **Other Custom** to view the **Other Custom Command Operation Statistics** window. This window provides options to view the statistics of read points for the custom operations the reader supports.



Other Custom Command Operation Statistics

Choose ReadPoint:

Operation statistics:

OperationName	Success (# of Times)	Failure (# of Times)
QTOperation	0	0

Refresh Interval (secs): 10

Reader Statistics for Other Custom Operations

The Reader Other Custom Statistics page provides options to view the statistics of individual read points for the Custom Operations supported by the reader. The user can choose "All" read point option to view the combined statistics for all the read points. The success and failure values of following statistics can be viewed for each read point.

- QT Operation - Shows the number of successful (and failed) QT operations performed on Monza4 QT tags.
- Choose Read point - Allows choosing a specific (or "all") readpoint whose statistics are displayed.
- Reset Statistics - Resets all the success and failure counts (including the standard,optional Gen2 and Custom operation statistics) for all the read points.
- Refresh Interval - Allows the user to set the refresh interval (in seconds) for this page. The statistics information for the chosen read point is refreshed every "N" seconds (where N is the user configured value for the refresh interval). The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 seconds.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-12 *NXP Custom Command Operation Statistics Window*

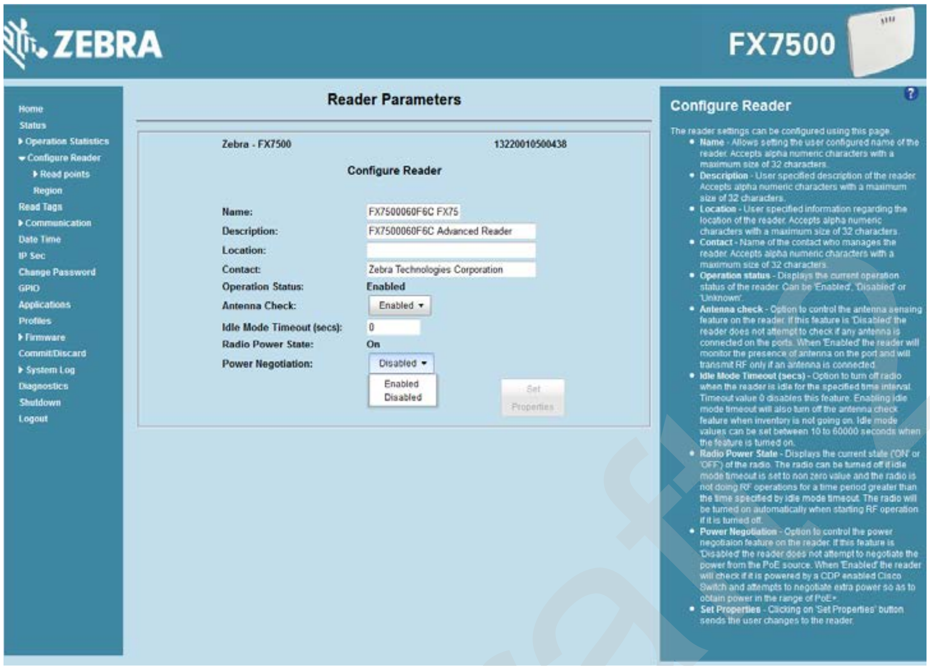
- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **QTOperation** - Displays the number of successful (and failed) QT operations performed on Monza4 QT tags.
- **Reset Statistics** - Resets all the success and failure counts for all the read points.
- **Refresh Interval** - Sets the refresh interval (in seconds) for this window. The statistics information for the chosen read point is refreshed every **N** seconds (where **N** is the set refresh interval). The minimum value is 10 seconds and the maximum value allowed is 86,400 seconds. Input a new value and click **Change** to set a new interval.

Configure Reader

Use the **Configure Reader** submenus to access the following functions.

Reader Parameters (General)

Select **Configure Reader** in the selection menu to configure reader settings using this window.



Reader Parameters

Zebra - FX7500 13220010500438

Configure Reader

Name: FX7500060F6C FX75
Description: FX7500060F6C Advanced Reader
Location:
Contact: Zebra Technologies Corporation
Operation Status: Enabled
Antenna Check: Enabled
Idle Mode Timeout (secs): 0
Radio Power State: On
Power Negotiation: Disabled

Configure Reader

The reader settings can be configured using this page.

- **Name** - Allows setting the user configured name of the reader. Accepts alpha numeric characters with a maximum size of 32 characters.
- **Description** - User specified description of the reader. Accepts alpha numeric characters with a maximum size of 32 characters.
- **Location** - User specified information regarding the location of the reader. Accepts alpha numeric characters with a maximum size of 32 characters.
- **Contact** - Name of the contact who manages the reader. Accepts alpha numeric characters with a maximum size of 32 characters.
- **Operation status** - Displays the current operation status of the reader. Can be 'Enabled', 'Disabled' or 'Unknown'.
- **Antenna check** - Option to control the antenna sensing feature on the reader. If this feature is 'Disabled' the reader does not attempt to check if any antenna is connected on the ports. When 'Enabled' the reader will monitor the presence of antenna on the port and will transmit RF only if an antenna is connected.
- **Idle Mode Timeout (secs)** - Option to turn off radio when the reader is idle for the specified time interval. Timeout value 0 disables this feature. Enabling idle mode timeout will also turn off the antenna check feature when inventory is not going on. Idle mode values can be set between 10 to 60000 seconds when the feature is turned on.
- **Radio Power State** - Displays the current state ('ON' or 'OFF') of the radio. The radio can be turned off if idle mode timeout is set to non zero value and the radio is not doing RF operations for a time period greater than the time specified by idle mode timeout. The radio will be turned on automatically when starting RF operation if it is turned off.
- **Power Negotiation** - Option to control the power negotaion feature on the reader. If this feature is 'Disabled' the reader does not attempt to negotiate the power from the PoE source. When 'Enabled' the reader will check if it is powered by a CDP enabled Cisco Switch and attempts to negotiate extra power so as to obtain power in the range of PoE+.
- **Set Properties** - Clicking on 'Set Properties' button sends the user changes to the reader.

Figure 4-13 *Reader Parameters*

- **Name** - Sets the user-configured reader name. Accepts up to 32 alphanumeric characters.
- **Description** - Sets a user-configured reader description. Accepts up to 32 alphanumeric characters.
- **Location** - Enter information on the reader location. Accepts up to 32 alphanumeric characters.
- **Contact** - Enter the name of the reader manager contact. Accepts up to 32 alphanumeric characters.
- **GPI Debounce Time** - Delays input events up to this time, and delivers these events only if the PIN states remains on the same level.
- **Operation Status** - Displays the current operation status of the reader (**Enabled**, **Disabled**, or **Unknown**).
- **Antenna Check** - Controls the antenna sensing feature on the reader. **Disabled** indicates that the reader does not attempt to check if an antenna is connected on the ports. When **Enabled**, the reader monitors the presence of an antenna on the port and only transmits RF if an antenna is connected.
- **Idle Mode Timeout (secs)** - Turns off the radio when the reader is idle for the specified time interval. A value of **0** disables this feature. Enabling this also turns off the antenna check feature when idle mode is entered after time out.
- **Radio Power State** - Displays the current state (**On** or **Off**) of the radio. The radio can be turned off if the **Idle Mode Timeout** is set to a non-zero value and the radio is not performing RF operations for a time period greater than the time specified by this timeout. The radio turns on automatically when RF operation starts.

- **Power Negotiation** - When the Power Negotiation option is set as enabled, and committed, the FX7500 reader starts power negotiation. Power negotiation occurs only if the reader is powered from a switch that is capable of LLDP based power negotiation. If the reader is powered from a source that does not support LLDP, power negotiation can still be enabled and disabled, but the reader does not carry out any power negotiation.

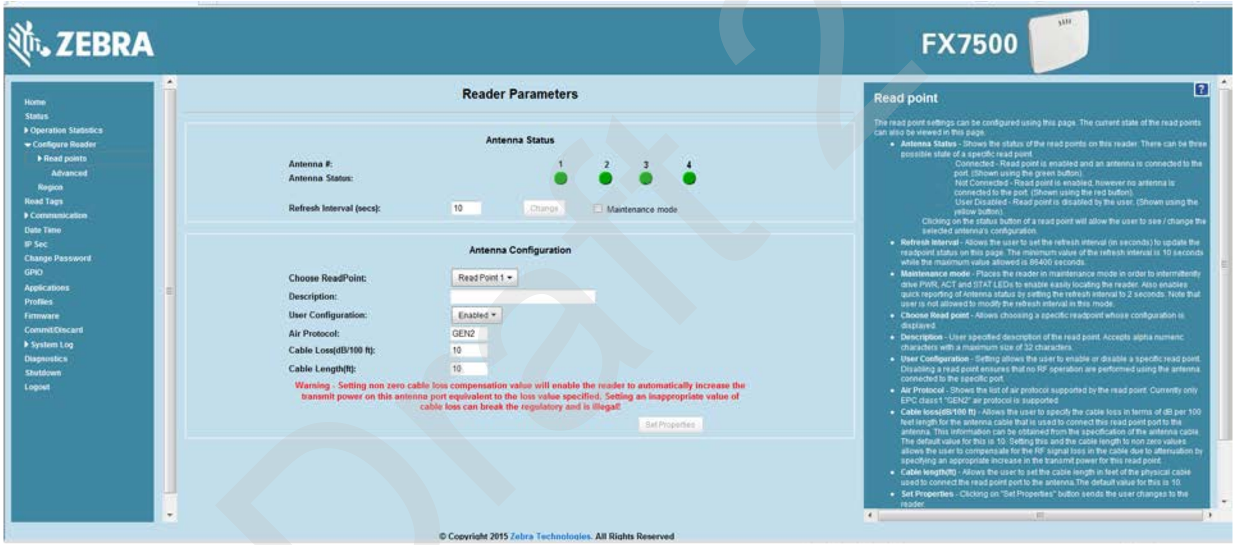
  The moment the power source is switched to an LLDP enabled switch, power negotiation occurs at startup if it was enabled from the UI previously.

  After power negotiation is enabled, and committed, it takes approximately 2 to 5 minutes to reach the PoE+ level. This is the time taken for LLDP packet exchange between the reader and the switch for power negotiation.

These settings only affect the display. Use *Commit/Discard on page 4-45* to save the changes.

Read Points

Click **Read points** in the selection menu to configure the read point settings and view the current read points state.



Reader Parameters

Antenna Status

Antenna #: 1 2 3 4
Antenna Status: ● ● ● ●

Refresh Interval (secs): 10 ☐ Maintenance mode

Antenna Configuration

Choose ReadPoint: Read Point 1
Description:
User Configuration: Enabled
Air Protocol: GEN2
Cable Loss(dB/100 ft): 10
Cable Length(ft): 10

Warning - Setting non zero cable loss compensation value will enable the reader to automatically increase the transmit power on this antenna port equivalent to the loss value specified. Setting an inappropriate value of cable loss can break the regulatory and is illegal!

Read point

The read point settings can be configured using this page. The current state of the read points can also be viewed in this page.

- **Antenna Status** - Shows the status of the read points on this reader. There can be three possible state of a specific read point.
  Connected - Read point is enabled and an antenna is connected to the port. (Shown using the green button).
  Not Connected - Read point is enabled, however no antenna is connected to the port. (Shown using the red button).
  User Disabled - Read point is disabled by the user. (Shown using the yellow button).
  Clicking on the status button of a read point will allow the user to see / change the selected antenna's configuration.
- **Refresh Interval** - Allows the user to set the refresh interval (in seconds) to update the readpoint status on this page. The minimum value of the refresh interval is 10 seconds while the maximum value allowed is 86400 seconds.
- **Maintenance mode** - Places the reader in maintenance mode in order to intermittently drive PWR, ACT and STAT LEDs to enable easily locating the reader. Also enables quick reporting of Antenna status by setting the refresh interval to 2 seconds. Note that user is not allowed to modify the refresh interval in this mode.
- **Choose Read point** - Allows choosing a specific readpoint whose configuration is displayed.
- **Description** - User specified description of the read point. Accepts alpha numeric characters with a maximum size of 32 characters.
- **User Configuration** - Setting allows the user to enable or disable a specific read point. Disabling a read point ensures that no RF operation are performed using the antenna connected to the specific port.
- **Air Protocol** - Shows the list of air protocol supported by the read point. Currently only EPC class1 "GEN2" air protocol is supported.
- **Cable loss(dB/100 ft)** - Allows the user to specify the cable loss in terms of dB per 100 feet length for the antenna cable that is used to connect this read point port to the antenna. This information can be obtained from the specification of the antenna cable. The default value for this is 10. Setting this and the cable length to non zero values allows the user to compensate for the RF signal loss in the cable due to attenuation by specifying an appropriate increase in the transmit power for this read point.
- **Cable length(ft)** - Allows the user to set the cable length in feet of the physical cable used to connect the read point port to the antenna.The default value for this is 10.
- **Set Properties** - Clicking on "Set Properties" button sends the user changes to the reader.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-14 *Configure Read Points*

Antenna Status

- Status buttons - indicate the status of the reader read points:
  - Green: Connected - Read point is enabled and an antenna is connected to the port.
  - Red: Not connected - Read point is enabled, but no antenna is connected to the port.
  - Yellow: User disabled - The user disabled the read point.

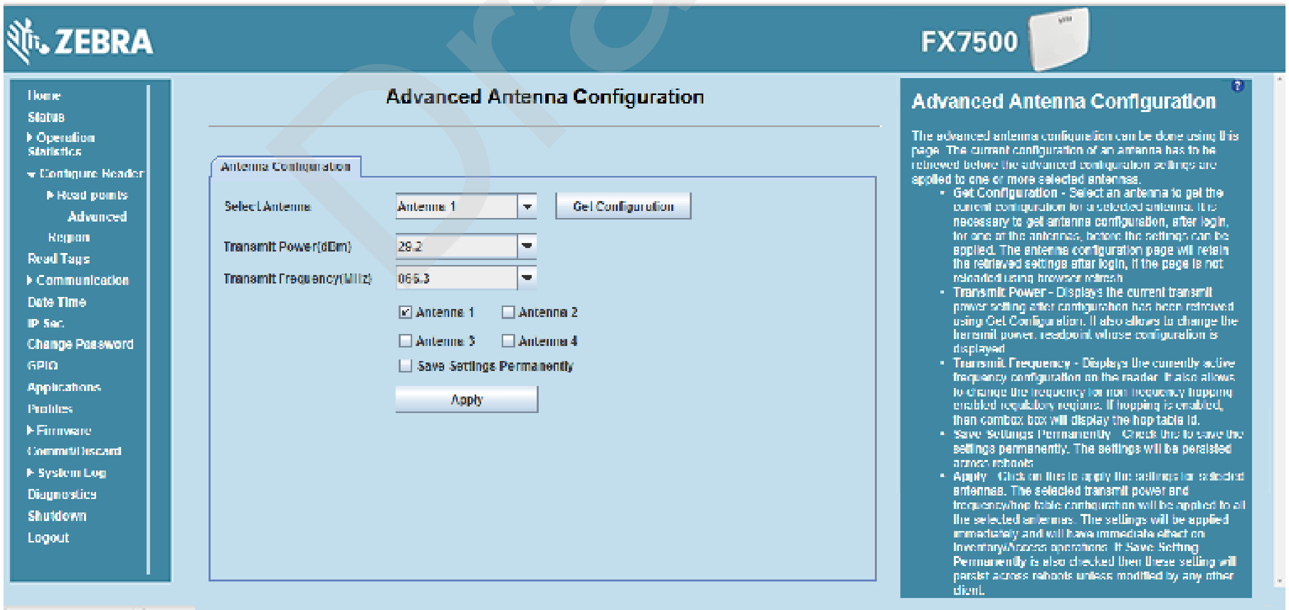
  Click a read point's status button to view and/or change the selected antenna configuration.
- **Refresh Interval** - Sets the refresh interval (in seconds) to update the readpoint status. The minimum value is 10 seconds and the maximum value allowed is 86,400 seconds. Input a new value and click **Change** to set a new interval.
- **Maintenance mode** - Places the reader in maintenance mode which intermittently drives PWR, ACT, and STAT LEDs to easily locate the reader. Also enables quick reporting of antenna status by setting the refresh interval to 2 seconds. Note that you can not modify the refresh interval in this mode.

Antenna Configuration

- **Choose Read Point** - Select a read point to display the configuration.
- **Description** - Enter a read point description of up to 32 alphanumeric characters.
- **User Configuration** - Enable or disable the read point. Disabling a read point blocks RF operation using the port/antenna.
- **Air Protocol** - Displays the air protocols the read point supports. The reader currently supports only EPC Class1 GEN2 air protocol.
- **Cable loss (dB/100 ft)** - Specifies the cable loss in terms of dB per 100 feet length for the antenna cable that is used to connect this read point port to the antenna. Refer to the specification of the antenna cable for this information. The default value is **0**. Setting this and the cable length to non-zero values allows the compensating for the RF signal loss in the cable due to attenuation by specifying an appropriate increase in the transmit power for this read point. The reader uses this and the cable length value to internally calculate the cable loss. The calculated cable loss is internally added to the power level configured on the read point.
- **Cable length (ft)** - Sets the cable length in feet of the physical cable that connects the read point port to the antenna.
- **Set Properties** - Select **Set Properties** to apply the changes. Select *Commit/Discard on page 4-45* to save the changes to the reader.

Read Points - Advanced

Click **Advanced** under **Read points** in the selection menu to view the **Advanced Antenna Configuration** window. Use this window to modify the transmission power and frequency configuration elements of the antenna.



Advanced Antenna Configuration

Select Antenna: Antenne 1

Transmit Power(dBm): 29.2

Transmit Frequency(MHz): 066.3

☑ Antenna 1 □ Antenna 2

□ Antenna 3 □ Antenna 4

□ Save Settings Permanently

Advanced Antenna Configuration

The advanced antenna configuration can be done using this page. The current configuration of an antenna has to be retrieved before the advanced configuration settings are applied to one or more selected antennas.

- Get Configuration - Select an antenna to get the current configuration for a selected antenna. It is necessary to get antenna configuration, after login, for one of the antennas, before the settings can be applied. The antenna configuration page will retain the retrieved settings after login, if the page is not reloaded using browser refresh
- Transmit Power - Displays the current transmit power setting after configuration has been retrieved using Get Configuration. It also allows to change the transmit power. readpoint whose configuration is displayed
- Transmit Frequency - Displays the currently active frequency configuration on the reader. It also allows to change the frequency for non frequency hopping enabled regulatory regions. If hopping is enabled, then combox box will display the hop table Id.
- Save Settings Permanently - Check this to save the settings permanently. The settings will be persisted across reboots
- Apply - Click on this to apply the settings for selected antennas. The selected transmit power and frequency/hop table configuration will be applied to all the selected antennas. The settings will be applied immediately and will have immediate effect on Inventory/Access operations. If Save Setting Permanently is also checked then these setting will persist across reboots unless modified by any other client.

Figure 4-15 *Advanced Antenna Configuration*

✓ ***NOTE*** This page is not supported when LLRP is configured in secure mode.

Retrieve the current configuration of an antenna before applying the advanced configuration settings.

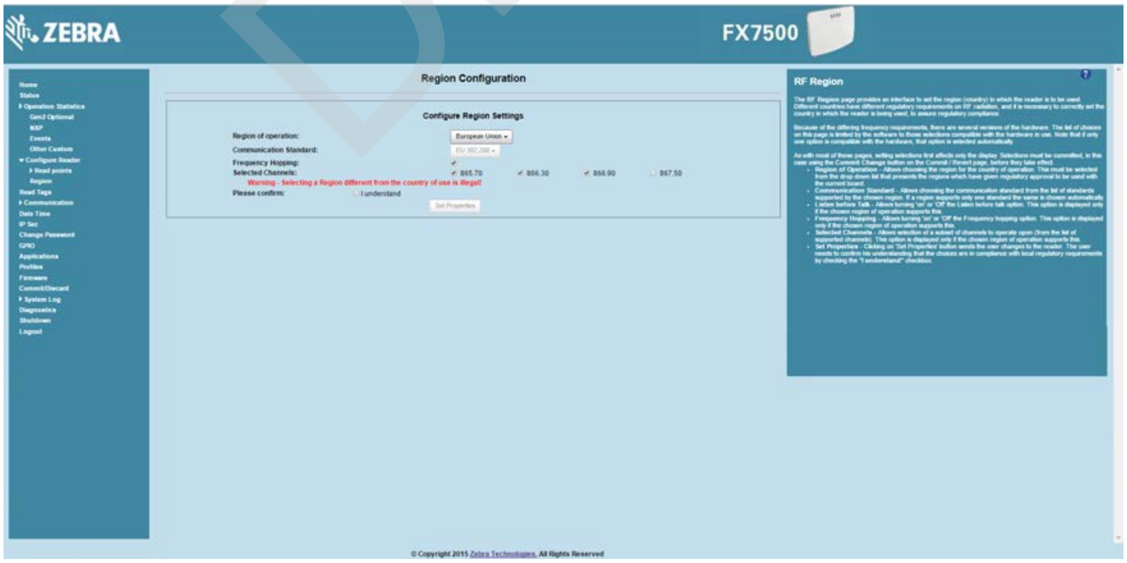
- **Get Configuration** - Select an antenna to get the current configuration for that antenna. After login, you must get the antenna configuration for an antenna before settings can be applied. The antenna configuration page retains the retrieved settings after login if you do not refresh the page using browser refresh.
- **Transmit Power** - Displays the current transmit power setting after selecting **Get Configuration**, and allows changing the transmit power for that antenna. This transmit power level does not include cable loss compensation.
- **Transmit Frequency** - Displays the active frequency configuration on the reader, and allows changing the frequency for non-frequency hopping enabled regulatory regions. If hopping is enabled, the combo box displays the hop table ID.
- **Save Settings Permanently** - Check this to save the settings permanently and persist them across reboots.
- **Apply** - Click to apply the settings for the selected antennas. This applies the selected transmit power and frequency/hop table configuration to all selected antennas. The settings are applied immediately and have immediate effect on Inventory/Access operations. Also check **Save Setting Permanently** to persist these settings across reboots unless modified by another client.

Configure Region

Different countries have different RF regulatory requirements. To assure regulatory compliance, select **Region** to set the reader for specific regulatory requirements in the country of reader operation using the **Configure Region Settings** window.

✓ ***NOTE*** Region configuration is not required for readers configured to operate in the United States region (under FCC rules).

Because of the differing frequency requirements, there are several versions of the hardware. The list of choices on this page is limited by the software to those selections compatible with the hardware in use. Note that if only one option is compatible with the hardware, that option is selected automatically.



Region Configuration

Configure Region Settings

Region of operation: European Union

Communication Standard: EU 302 208

Frequency Hopping: ✓

Selected Channels: ✓ 865.70 ✓ 866.30 ✓ 866.90 □ 867.50

Warning - Selecting a Region different from the country of use is illegal!

Please confirm: □ I understand

RF Region

The RF Region page provides an interface to set the region (country) in which the reader is to be used. Different countries have different regulatory requirements on RF radiation, and it is necessary to correctly set the country in which the reader is being used, to assure regulatory compliance.

Because of the differing frequency requirements, there are several versions of the hardware. The list of choices on this page is limited by the software to those selections compatible with the hardware in use. Note that if only one option is compatible with the hardware, that option is selected automatically.

As with most of these pages, setting selections first affects only the display. Selections must be committed, in this case using the Commit Change button on the Commit / Revert page, before they take effect.

- Region of Operation - Allows choosing the region for the country of operation. This must be selected from the drop down list that presents the regions which have given regulatory approval to be used with the current board.
- Communication Standard - Allows choosing the communication standard from the list of standards supported by the chosen region. If a region supports only one standard the same is chosen automatically.
- Listen before Talk - Allows turning 'on' or 'Off' the Listen before talk option. This option is displayed only if the chosen region of operation supports this.
- Frequency Hopping - Allows turning 'on' or 'Off' the Frequency hopping option. This option is displayed only if the chosen region of operation supports this.
- Selected Channels - Allows selection of a subset of channels to operate upon (from the list of supported channels). This option is displayed only if the chosen region of operation supports this.
- Set Properties - Clicking on 'Set Properties' button sends the user changes to the reader. The user needs to confirm his understanding that the choices are in compliance with local regulatory requirements by checking the "I understand" checkbox.

© Copyright 2015 Zebra Technologies, All Rights Reserved

Figure 4-16 *Configure Region Settings Window*

- **Region of Operation** - Select the region for the country of operation from the drop-down list. This list includes regions which have regulatory approval to use with the current board.

- **Communication Standard** - Select the communication standard from the list of standards that the chosen region supports. If a region supports only one standard, it is automatically selected.
- **Frequency Hopping** - Check to select frequency hopping. This option appears only if the chosen region of operation supports this.
- **Selected Channels** - Select a subset of channels on which to operate (from the list of supported channels). This option appears only if the chosen region of operation supports this.
- **Please confirm** - Check the **I understand** check box to confirm your understanding that the choices are in compliance with local regulatory requirements.
- **Set Properties** - Click to apply the changes. Select *Commit/Discard on page 4-45* to save the changes to the reader.

Certificates

You can protect network services on the reader using SSL/TLS to secure the communication channel against eavesdropping or tampering, and optionally authenticate peer networked nodes involved in the communication. SSL/TLS protocol uses Public Key Infrastructure digital certificates. The following services on the reader support SSL/TLS:

- Web **Administrator Console** service (HTTPS). See *Network Services Settings on page 4-37*.
- File Transfer Service (FTPS - explicit SSL/TLS over FTP). See *Network Services Settings on page 4-37*.
- Shell Service (SSH - by default always in secure mode).
- Secure LLRP Service (refer to the EPC Global LLRP Standard, **Security in TCP Transport**). See the **Enable Secure Mode** option in *Configure LLRP Settings on page 4-34*.

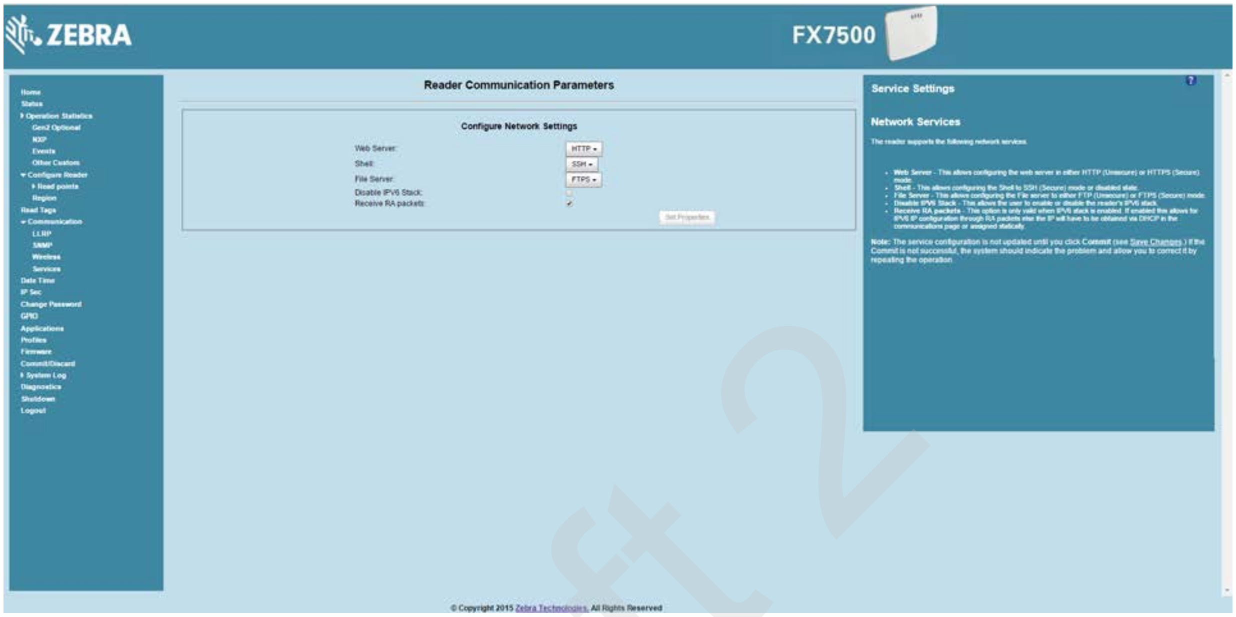
✓ ***NOTE*** The supported version of SSL/TLS varies between services. Different services support SSL v3 and TLS 1.0 and above.

✓ ***NOTE*** The **Validate Peer** option in Secure LLRP Service configuration enables authentication of reader and/or clients using digital certificates. You must import a custom certificate (instead of the default self-signed certificate) to the reader to enable this option. See *Configure LLRP Settings on page 4-34* for details. Services other than Secure LLRP rely on password-based authentication.

✓ ***NOTE*** The SNMP service on the reader supports SNMP v2c and does not support security.

Certificate Configuration

The **Certificate Configuration** page is available under the **Configure Reader** menu when the **Administrator Console** is in HTTPS mode only. To enable HTTPS mode, select **Communication** > **Services**, and on the **Reader Communication Parameters** page select **HTTPS** from the **Web Server** drop-down menu.



Reader Communication Parameters

Configure Network Settings

Web Server: HTTP ▾
Shell: SSH ▾
File Server: FTPS ▾
Disable IPV6 Stack: □
Receive RA packets: ☑

Service Settings

Network Services

The reader supports the following network services.

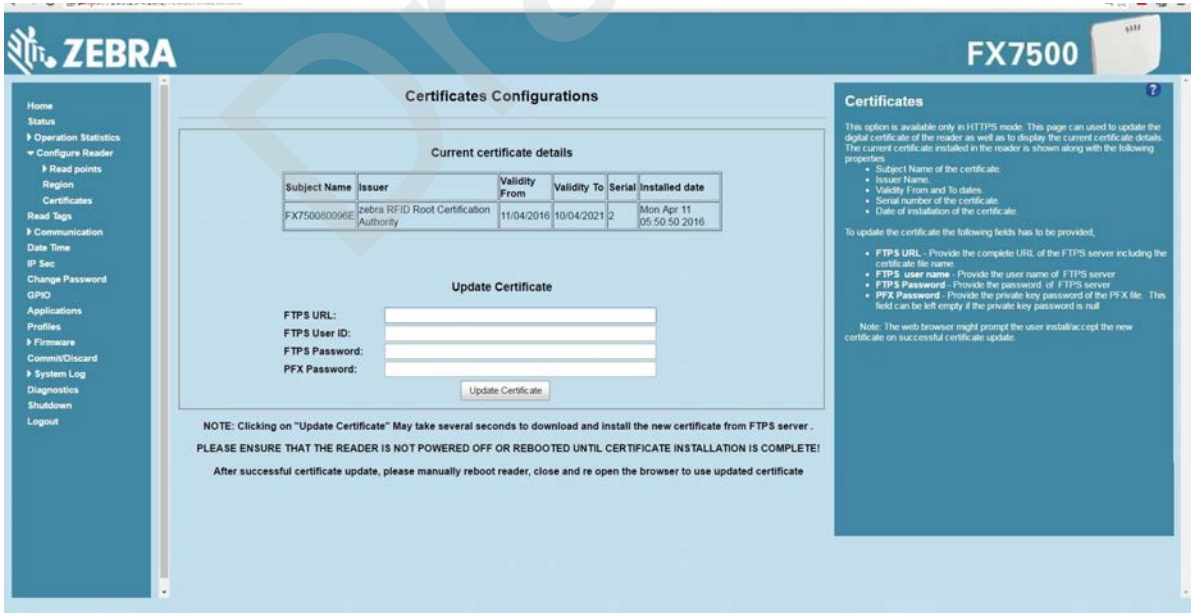
- **Web Server** - This allows configuring the web server in either HTTP (Unsecure) or HTTPS (Secure) mode.
- **Shell** - This allows configuring the Shell to SSH (Secure) mode or disabled state.
- **File Server** - This allows configuring the File server to either FTP (Unsecure) or FTPS (Secure) mode.
- **Disable IPV6 Stack** - This allows the user to enable or disable the reader's IPV6 stack.
- **Receive RA packets** - This option is only valid when IPV6 stack is enabled. If enabled this allows for IPV6 IP configuration through RA packets else the IP will have to be obtained via DHCP in the communications page or assigned statically.

Note: The service configuration is not updated until you click **Commit** (see Save Changes.) If the Commit is not successful, the system should indicate the problem and allow you to correct it by repeating the operation.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-17 *Setting HTTPS Mode*

Select **Configure Reader** > **Certificates.** The **Certificate Configuration** page provides the current certificate details and an option to update to a custom certificate.



Certificates Configurations

Current certificate details

Subject Name	Issuer	Validity From	Validity To	Serial	Installed date
FX750080096E	zebra RFID Root Certification Authority	11/04/2016	10/04/2021	2	Mon Apr 11 05:50:50 2016

Update Certificate

FTPS URL:
FTPS User ID:
FTPS Password:
PFX Password:

NOTE: Clicking on "Update Certificate" May take several seconds to download and install the new certificate from FTPS server .

PLEASE ENSURE THAT THE READER IS NOT POWERED OFF OR REBOOTED UNTIL CERTIFICATE INSTALLATION IS COMPLETE!

After successful certificate update, please manually reboot reader, close and re open the browser to use updated certificate

Certificates

This option is available only in HTTPS mode. This page can used to update the digital certificate of the reader as well as to display the current certificate details. The current certificate installed in the reader is shown along with the following properties

- Subject Name of the certificate.
- Issuer Name.
- Validity From and To dates.
- Serial number of the certificate.
- Date of installation of the certificate.

To update the certificate the following fields has to be provided,

- **FTPS URL** - Provide the complete URL of the FTPS server including the certificate file name.
- **FTPS user name** - Provide the user name of FTPS server
- **FTPS Password** - Provide the password of FTPS server
- **PFX Password** - Provide the private key password of the PFX file. This field can be left empty if the private key password is null

Note: The web browser might prompt the user install/accept the new certificate on successful certificate update.

Figure 4-18 *Certificate Configuration Page*

The **Current certificate details** section displays the installed certificate's details such as issuer, serial number, and validity information.

By default, the reader uses self-signed certificates (characterized by **Subject name** and **Issuer** in **Current certificate details**) for all secure interfaces using SSL/TLS.

Self-signed certificates have restrictions, such as by default clients do not trust them because they are not issued by a trusted Certification Authority (CA). Custom trusted certificates may be beneficial in certain use cases, for example:

- LLRP by default does not authenticate the client or reader. Security extensions to the standard allow client or reader authentication using digital certificates. The entities involved validate digital certificates by confirming the certificates were issued from a trusted source. Therefore a custom certificate is required to authenticate the client or reader. See the **Validate Peer** option in *Configure LLRP Settings on page 4-34*.
- By default web browsers display a warning or prevent connection to the **Administrator Console** when the console service is in HTTPS mode. See *Network Services Settings on page 4-37*. This can be an inconvenience for certain environments, particularly when browsers are configured to reject connection to servers that do not publish a trusted certificate.

FX7500 reader does not allow automatic certificate request and updating. The reader certificate must be issued externally and imported to the reader.

The **Update Certificate** section allows importing a custom certificate to the reader. You must use one of the digital certificate generation mechanisms to create the certificate (see *Creating a Custom Certificate*). The reader only supports certificates in PKCS#12 format (typically with a **.pfx** extension). This format uses a signed certificate, with a private key (optionally encrypted) bundled into a single file. The certificate must be hosted on a secure FTP server (running in **Explicit SSL/TLS over FTP mode**). The following options are used to perform the update:

- **FTPS URL**: Full path to server, including ftps:// prefix, where the **.pfx** file is hosted.
- **FTPS User ID**: User login ID to secure FTP server.
- **FTPS Password**: Password for specified user.
- **PFX Password**: Password for encrypted key in the **.pfx** file, if the key is encrypted.

✓ ***NOTE*** The FX7500 supports only a single digital certificate. If a custom certificate is installed, the issuer of the certificate is trusted by the reader, so any client attempting to connect to the reader over secure LLRP mode is trusted if the certificate issued to the client is from the same issuer.

✓ ***NOTE*** The FX7500 only supports certificates using the RSA public key algorithm. When obtaining a certificate issued from the reader or clients, ensure that RSA is the selected key algorithm.

✓ ***NOTE*** A manual reboot of the reader is required after updating the certificate for the services using SSL/TLS.

Creating a Custom Certificate

FX7500 reader requires that custom certificates are created externally and imported to the reader using a secure FTP, as described previously. The certificate and key used by the reader must be in PKCS#12 format (a single **.pfx** file), while the certificate and keys used by clients interfacing to the LLRP service on the reader must be in PEM format. If you obtain a certificate in a different format it must be converted to the appropriate format using a tools such as **OpenSSL** (www.openssl.org).

Digital certificates are typically requested and issued from a certification authority hosted internally in an enterprise environment or by a trusted third party certification authority. The process of requesting and creating certificates varies between platforms. For example, a Windows Server environment typically uses Microsoft Certification Server to process certificate requests and issue certificates. Unix-based systems typically use

OpenSSL. This guide can not document all options. The following example illustrates one method of creating custom certificates.

Custom Certificate Creation Example

The following example illustrates how to set up an OpenSSL-based certification authority to issue reader and client certificates. These scripts can be executed in a Unix operating system or on Windows with a Unix shell scripting environment such as Cygwin:

Create the following text files in a suitable folder:

- caconfig.cnf - OpenSSL configuration file for Certification Authority certificate creation and signing
- samplereader.cnf - OpenSSL configuration file for reader certificate creation
- samplehost.cnf - OpenSSL configuration file for reader certificate creation
- InitRootCA.sh - Script for initializing a new Root Certification Authority
- CreateReaderCert.sh - Script for creating reader certificate
- CreateClientCert.sh - Script for creating client certificate

File contents are as follows. Refer to **OpenSSL** (www.openssl.org) documentation for details on configuration options. Edit configuration options to accommodate the deployment environment.

caconfig.cnf

```
# Sample caconfig.cnf file for XYZ certification authority
#
# Default configuration to use when one is not provided on the command line.
#
[ ca ]
default_ca      = local_ca
#
#
# Default location of directories and files needed to generate certificates.
#
[ local_ca ]
dir             = .
certificate     = $dir/cacert.pem
database        = $dir/index.txt
new_certs_dir   = $dir/signedcerts
private_key     = $dir/private/cakey.pem
serial          = $dir/serial
#
#
# Default expiration and encryption policies for certificates.
#
default_crl_days        = 365
default_days            = 1825
default_md              = sha1
#
policy          = local_ca_policy

#
#
# Default policy to use when generating server certificates.  The following
# fields must be defined in the server certificate.
#
[ local_ca_policy ]
commonName              = supplied
stateOrProvinceName     = supplied
countryName             = supplied
emailAddress            = supplied
organizationName        = supplied
organizationalUnitName  = supplied
```

```
#
#
# The default root certificate generation policy.
#
[ req ]
default_bits    = 2048
default_keyfile = ./private/cakey.pem
default_md      = sha1
#
prompt                  = no
distinguished_name      = root_ca_distinguished_name
x509_extensions         = v3_ca
#
#
# Root Certificate Authority distinguished name.  Change these fields to match
# your local environment!
#
[ root_ca_distinguished_name ]
commonName              = XYZ Root Certification Authority
stateOrProvinceName     = IL
countryName             = US
emailAddress            = ca@xyz.com
organizationName        = XYZ
organizationalUnitName  = ABC Dept
#
[ root_ca_extensions ]
basicConstraints        = CA:true

[ v3_req ]
basicConstraints       = CA:FALSE
keyUsage               = nonRepudiation, digitalSignature, keyEncipherment

[ v3_ca ]
basicConstraints        = critical, CA:true, pathlen:0
nsCertType              = sslCA
keyUsage                = cRLSign, keyCertSign
extendedKeyUsage        = serverAuth, clientAuth
nsComment               = "CA Certificate"

[ ssl_client_server ]
basicConstraints        = CA:FALSE
nsCertType              = server, client
```

```
keyUsage             = digitalSignature, keyEncipherment
extendedKeyUsage       = serverAuth, clientAuth, nsSGC, msSGC
nsComment            = "SSL/TLS Certificate"
```

samplereader.cnf

```
#
# samplehost.cnf - customized for a reader. Edit last 4 octets after FX7500 to suit hostname of reader to
which certificate is issued
#

[ req ]
prompt               = no
distinguished_name      = FX7500123456.ds

[ FX75000657E5.ds ]
commonName             = FX7500123456
stateOrProvinceName     = IL
countryName            = US
emailAddress           = root@FX7500123456
organizationName        = Company Name
organizationalUnitName  = Department Name
```

samplehost.cnf

```
#
# samplehost.cnf - customized for a client that will connect to the reader's LLRP port. Edit hostname to
match FQDN of client.
#

[ req ]
prompt               = no
distinguished_name      = clienthostname.mycompany.com

[clienthostname.mycompany.com ]
commonName             = CLIENTHOSTNAME
stateOrProvinceName     = IL
countryName            = US
emailAddress           = root@clienthostname.mycompany.com
organizationName        = Company Name
organizationalUnitName  = Department Name
```

InitRootCA.sh

```
#Initialize from current directory
#Enable definition for environment variable OPENSSL_FIPS to execute in FIPS mode on system with FIPS compliant OpenSSL build
#export OPENSSL_FIPS=1
export WORKSPACE_DIR=$( cd "$( dirname "$0" )" && pwd )
#Make sure CA key password is unique and secret
export CA_KEY_PASSWORD=CA-abcd12345
#Cleanup Certificate Store folder
rm -rf $WORKSPACE_DIR/CA-Certs
#Change directory to CA-Certs and create folders for certificate and key storage in myCA
mkdir -p $WORKSPACE_DIR/CA-Certs
cd $WORKSPACE_DIR/CA-Certs
mkdir -p myCA/signedcerts
mkdir -p myCA/private
cd myCA
#Initialize serial number
echo '01' > serial  && touch index.txt
#Create CA private key and certificate
export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf
echo 'Creating CA key and certificate....'
openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 1825 -passout pass:$CA_KEY_PASSWORD
openssl x509 -in cacert.pem -out cacert.crt
echo 'Test Certificate Authority Initialized. CA certificate saved in cacert.crt. Install it to trusted CA certificate store'
```

CreateReaderCert.sh

```
#Initialize from current directory
#Enable definition for environment variable OPENSSL_FIPS to execute in FIPS mode on system with FIPS compliant OpenSSL build
#export OPENSSL_FIPS=1
export WORKSPACE_DIR=$( cd "$( dirname "$0" )" && pwd )
#Make sure passwords are unique and secret
export CA_KEY_PASSWORD=CA-abcd12345
export GENERATED_CERT_KEY_PASSWORD=abcd12345
cd $WORKSPACE_DIR/CA-Certs/myCA
#Create sample reader key and certificate
export OPENSSL_CONF=$WORKSPACE_DIR/samplereader.cnf
echo 'Creating reader key and certificate with its signing request ....'
openssl req -newkey rsa:1024 -keyout reader_key.pem -keyform PEM -out tempreq.pem -outform PEM -passout pass:$GENERATED_CERT_KEY_PASSWORD
#CA now signs client certificate by processing its certificate sigining request
echo 'CA Signing reader certificate....'
export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf
openssl ca -extensions ssl_client_server -in tempreq.pem -out reader_crt.pem -passin pass:$CA_KEY_PASSWORD -batch
rm -f tempreq.pem
echo 'Exporting reader certificate and key to PKCS#12 format....'
openssl pkcs12 -export -out reader.pfx -inkey reader_key.pem -in reader_crt.pem -certfile cacert.crt -passin pass:$GENERATED_CERT_KEY_PASSWORD -passout pass:$GENERATED_CERT_KEY_PASSWORD
echo 'Reader certificate, key and export to PKCS#12 format (.pfx) completed.'
echo 'Note: PFX protected with password: '$GENERATED_CERT_KEY_PASSWORD
```

CreateClientCert.sh

```
#Initialize from current directory
#Enable definition for environment variable OPENSSL_FIPS to execute in FIPS mode on system with FIPS compliant OpenSSL build
#export OPENSSL_FIPS=1
export WORKSPACE_DIR=$( cd "$( dirname "$0" )" && pwd )
#Make sure passwords are unique and secret
export CA_KEY_PASSWORD=CA-abcd12345
export GENERATED_CERT_KEY_PASSWORD=abcd12345
cd $WORKSPACE_DIR/CA-Certs/myCA
echo 'Current dir:'$( cd "$( dirname "$0" )" && pwd )
#Create sample client key and certificate
export OPENSSL_CONF=$WORKSPACE_DIR/samplehost.cnf
echo 'Creating client key and certificate with its signing request ....'
openssl req -newkey rsa:1024 -keyout client_key.pem -keyform PEM -out tempreq.pem -outform PEM -passout pass:$GENERATED_CERT_KEY_PASSWORD
#CA now signs client certificate by processing its certificate sigining request
echo 'CA Signing client certificate....'
export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf
openssl ca -in tempreq.pem -out client_crt.pem -extensions ssl_client_server -passin pass:$CA_KEY_PASSWORD -batch
rm -f tempreq.pem
echo 'Client key, certificate creation and signing completed. Use files client_key.pem and client_crt.pem'
```

Script Usage

The following section illustrates how to use the previous scripts.

Certification Authority Initialization

- Edit **caconfig.cnf** to change the configuration for CA if necessary.
- Execute CA initialization command sequence by invoking **./InitRootCA.sh.**

Issue Reader certificate:

- Edit **samplereader.cnf** to update any configuration such as **hostname** if necessary.
- Execute **CreateReaderCert.sh** by invoking **./CreateReaderCert.sh**.

Issue Client certificate:

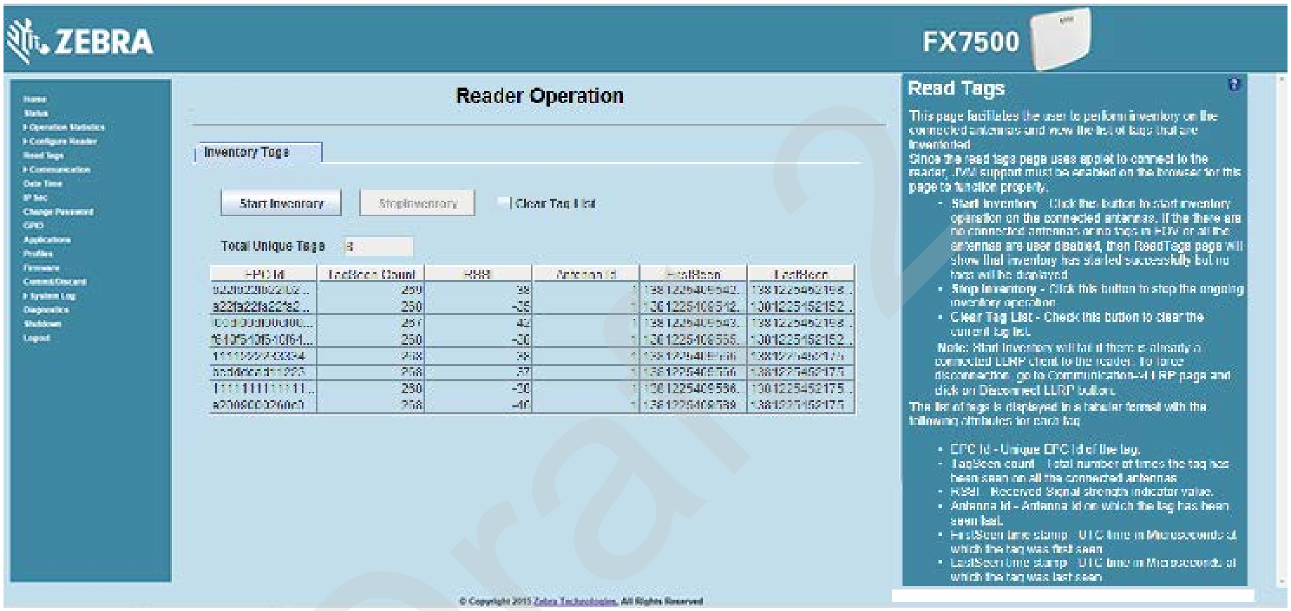
- Certificate and key issued using this method can be directly used with the LLRP client.
- Edit **samplehost.cnf** to update any configuration such as **hostname** for the client, if necessary.
- Execute **CreateClientCert.sh** by invoking **./CreateClientCert.sh**.

Read Tags

Select **Read Tags** to view the **Reader Operation** window. Use this window to perform inventory on the connected antennas and view the list of inventoried tags.

NOTE Enable Java JRE support on the browser in order for this window to function properly.

NOTE This page is not supported when LLRP is configured in secure mode.



Total Unique Tags 8

EPC Id	TagSeen Count	RSSI	Antenna Id	FirstSeen	LastSeen
b22fb22fb22fb2 ..	259	-38	1	1381225405542.	1381225452158 .
a22fa22fa22fa2 ..	250	-35	1	1381225405512.	1381225452152 .
100d100d100d100...	257	-42	1	1381225405543.	1381225452158 .
f6f0f5f0f5f0f64...	250	-30	1	1381225405555.	1381225452152 .
1111222233334	258	-38	1	1381225405556	1381225452175
bcddccaa111223	258	-37	1	1381225405556	1381225452175
111111111111...	250	-30	1	1381225405586.	1381225452175 .
a2008000320000	258	-40	1	1381225405589	1381225452175

Read Tags

This page facilitates the user to perform inventory on the connected antennas and view the list of tags that are inventoried.
Since the read tags page uses applet to connect to the reader, JVM support must be enabled on the browser for this page to function properly.

- **Start Inventory** - Click this button to start inventory operation on the connected antennas. If the there are no connected antennas or no tags in FOV or all the antennas are user disabled, then ReadTags page will show that inventory has started successfully but no tags will be displayed.
- **Stop Inventory** - Click this button to stop the ongoing inventory operation.
- **Clear Tag List** - Check this button to clear the current tag list.

Note: Start Inventory will fail if there is already a connected LLRP client to the reader. To force disconnection, go to Communication->LLRP page and click on Disconnect LLRP button.

The list of tags is displayed in a tabular format with the following attributes for each tag:

- EPC Id - Unique EPC Id of the tag.
- TagSeen count - Total number of times the tag has been seen on all the connected antennas.
- RSSI - Received Signal strength indicator value.
- Antenna Id - Antenna Id on which the tag has been seen last.
- FirstSeen time stamp - UTC time in Microseconds at which the tag was first seen.
- LastSeen time stamp - UTC time in Microseconds at which the tag was last seen.

© Copyright 2015 Zebra Technologies, All Rights Reserved

Figure 4-19 *Read Tags Window*

- **Start Inventory** - Click to starts inventory operation on the connected antennas. If the there are no connected antennas, no tags in the field of view, or all the antennas are user-disabled, the **Read Tags** window indicates that inventory successfully started but no tags display.
- **Stop Inventory** - Stops the ongoing inventory operation.
- **Clear Tag List** - Clears the current tag list.
- **Total Unique Tags** - Indicates the number of unique tags read.

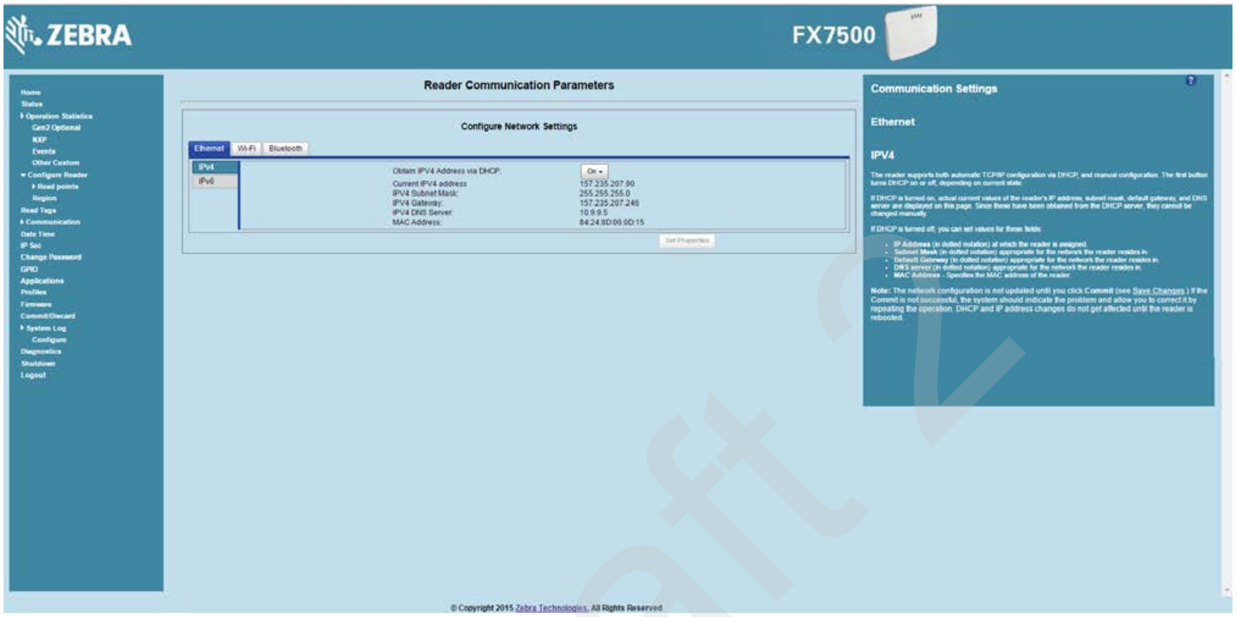
The list of tags appears in a table with the following attributes for each tag:

- **EPC Id** - Unique tag EPC ID.
- **TagSeen Count** - Number of times the tag was identified on the specific antenna.
- **RSSI** - Received Signal Strength Indication.
- **Antenna Id** - Antenna ID on which the tag is seen.
- **FirstSeen** time stamp - UTC time (in microseconds) when the tag was first seen.
- **LastSeen** time stamp - UTC time (in microseconds) when the tag was last seen.

Communication Settings

Select **Communication** to view the **Configure Network Settings** window. This window has tabs for Ethernet, WiFi, and Bluetooth. Each tab has options for IPV4 and IPV6.

Configure Network Settings - Ethernet Tab



Reader Communication Parameters

Configure Network Settings

Obtain IPV4 Address via DHCP: On

Current IPV4 address 157.235.207.90

IPV4 Subnet Mask: 255.255.255.0

IPV4 Gateway: 157.235.207.246

IPV4 DNS Server: 10.9.9.5

MAC Address: 84:24:8D:06:0D:15

Communication Settings

Ethernet

IPV4

The reader supports both automatic TCP/IP configuration via DHCP, and manual configuration. The first button turns DHCP on or off, depending on current state.

If DHCP is turned on, actual current values of the reader's IP address, subnet mask, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

If DHCP is turned off, you can set values for these fields:

- **IP Address** (in dotted notation) at which the reader is assigned.
- **Subnet Mask** (in dotted notation) appropriate for the network the reader resides in.
- **Default Gateway** (in dotted notation) appropriate for the network the reader resides in.
- **DNS server** (in dotted notation) appropriate for the network the reader resides in.
- **MAC Address** - Specifies the MAC address of the reader.

Note: The network configuration is not updated until you click **Commit** (see Save Changes.) If the Commit is not successful, the system should indicate the problem and allow you to correct it by repeating the operation. DHCP and IP address changes do not get affected until the reader is rebooted.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-20 *Configure Network Settings - Ethernet Tab*

IPV4

- **Obtain IPV4 Address via DHCP** - The reader supports both automatic TCP/IP configuration via DHCP and manual configuration. The DHCP button turns DHCP on and off.

  If DHCP is turned on, this window displays actual current values of the reader's IP address, subnet mask, default gateway, and DNS server. Because these are obtained from the DHCP server, they cannot be changed manually.

  If DHCP is turned off, you can set the following values for these fields.
- **Current IPV4 Address** - IP address (in dotted notation) at which the reader is assigned.
- **IPV4 Subnet Mask** - Subnet mask (in dotted notation) appropriate for the network in which the reader resides.
- **IPV4 Default Gateway** - Default gateway (in dotted notation) appropriate for the network in which the reader resides.
- **IPV4 DNS Server** - DNS server (in dotted notation) appropriate for the network in which the reader resides.
- **MAC Address** - The MAC address of the reader.

✓ ***NOTE*** You must click **Commit** to update the network configuration (see Save Changes.) If the Commit is not successful, the system indicates the problem and allows correcting it by repeating the operation. DHCP and IP address updates do apply until the reader is rebooted.

IPV6

- **Obtain IPV6 Address via DHCP** - The reader supports both automatic TCP/IPV6 configuration via DHCP and manual configuration. The DHCP button turns DHCP on and off.

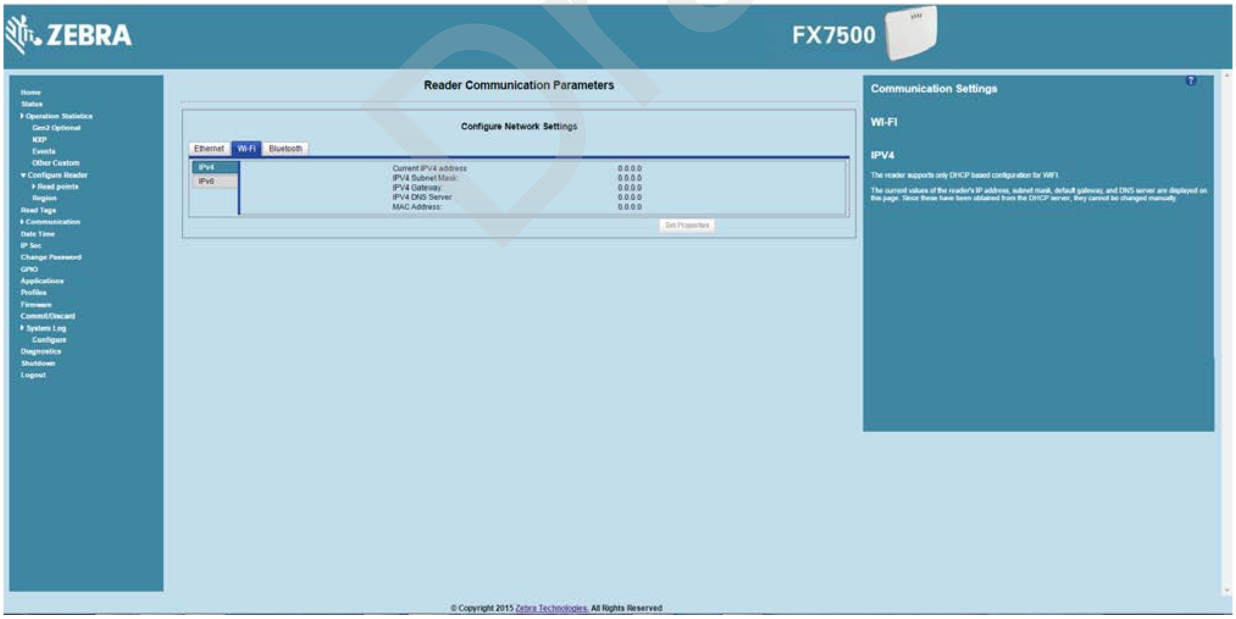
  If DHCP is turned on, this window displays actual current values of the reader's IPV6 address, prefix length, default gateway, and DNS server. Because these are obtained from the DHCP server, they cannot be changed manually.

  If DHCP is turned off, you can set the following values for these fields.
- **Current IPV6 Address** - IP address (in dotted notation) at which the reader is assigned.
- **Prefix Length** - Prefix length appropriate for the network in which the reader resides.
- **IPV6 Default Gateway** - Default gateway (in dotted notation) appropriate for the network in which the reader resides.
- **IPV6 DNS Server** - DNS server (in dotted notation) appropriate for the network in which the reader resides.
- **MAC Address** - The MAC address of the reader.

✓ ***NOTE*** You must click **Commit** to update the network configuration (see Save Changes.) If the Commit is not successful, the system indicates the problem and allows correcting it by repeating the operation. DHCP and IP address updates do apply until the reader is rebooted.

✓ ***NOTE*** Also enable automatic configuration for IPV6 through RA packets configuration. To enable or disable RA packet configuration go to the Services window (see Services).

Configure Network Settings - Wi-Fi Tab



Reader Communication Parameters

Configure Network Settings

Current IPV4 address	0.0.0.0
IPV4 Subnet Mask:	0.0.0.0
IPV4 Gateway:	0.0.0.0
IPV4 DNS Server:	0.0.0.0
MAC Address:	0.0.0.0

Communication Settings

WI-FI

IPV4

The reader supports only DHCP based configuration for WIFI.

The current values of the reader's IP address, subnet mask, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-21 *Configure Network Settings - Wi-Fi Tab*

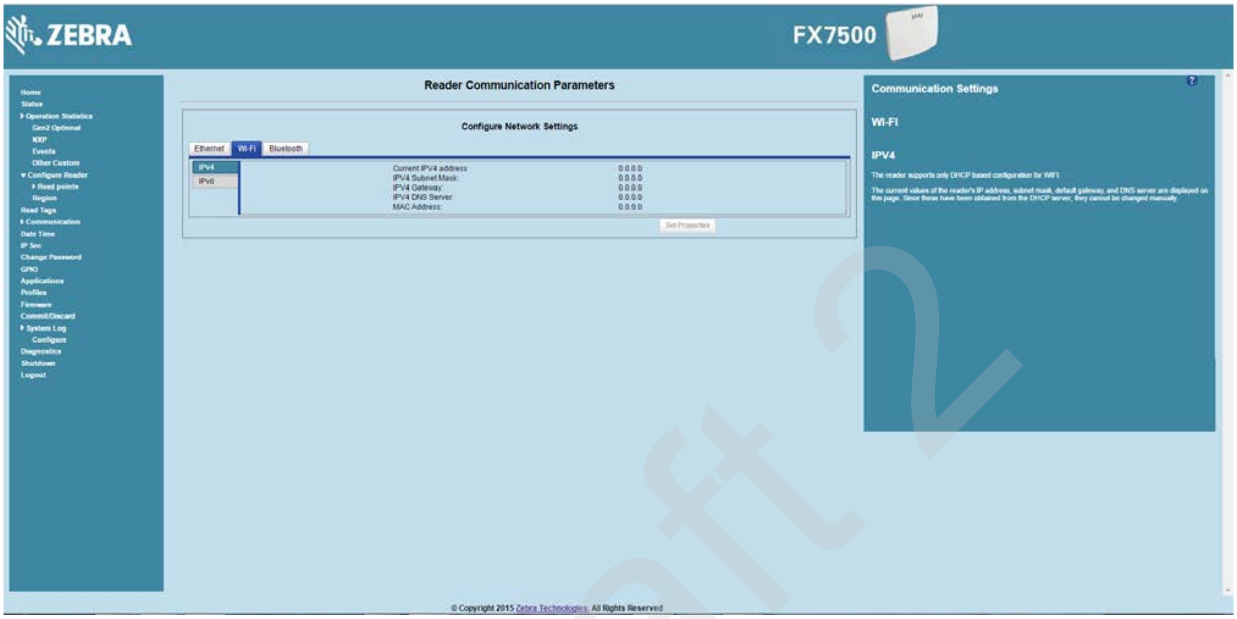
IPV4

The reader supports only DHCP-based configuration for WIFI. This window displays the current values of the reader's IP address, subnet mask, default gateway, and DNS server. Since these are obtained from the DHCP server, they cannot be changed manually.

IPV6

The reader supports only DHCP based configuration for WIFI. This window displays the current values of the reader's IPV6 address, prefix length, default gateway, and DNS server. Since these are obtained from the DHCP server, they cannot be changed manually.

Configure Network Settings - Bluetooth Tab



Reader Communication Parameters

Configure Network Settings

Current IPV4 address	0.0.0.0
IPV4 Subnet Mask:	0.0.0.0
IPV4 Gateway:	0.0.0.0
IPV4 DNS Server:	0.0.0.0
MAC Address:	0.0.0.0

Communication Settings

WI-FI

IPV4

The reader supports only DHCP based configuration for WIFI.

The current values of the reader's IP address, subnet mask, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

Figure 4-22 *Configure Network Settings - Bluetooth Tab*

The reader supports only automatic IP configuration of the Bluetooth interface.

If a Bluetooth client is connected to the reader, this window displays the current values of the reader's IPV4 address, Subnet mask, IPV6 address, and prefix length in the appropriate tabs. Because these are automatically configured for a reader, they cannot be changed manually.

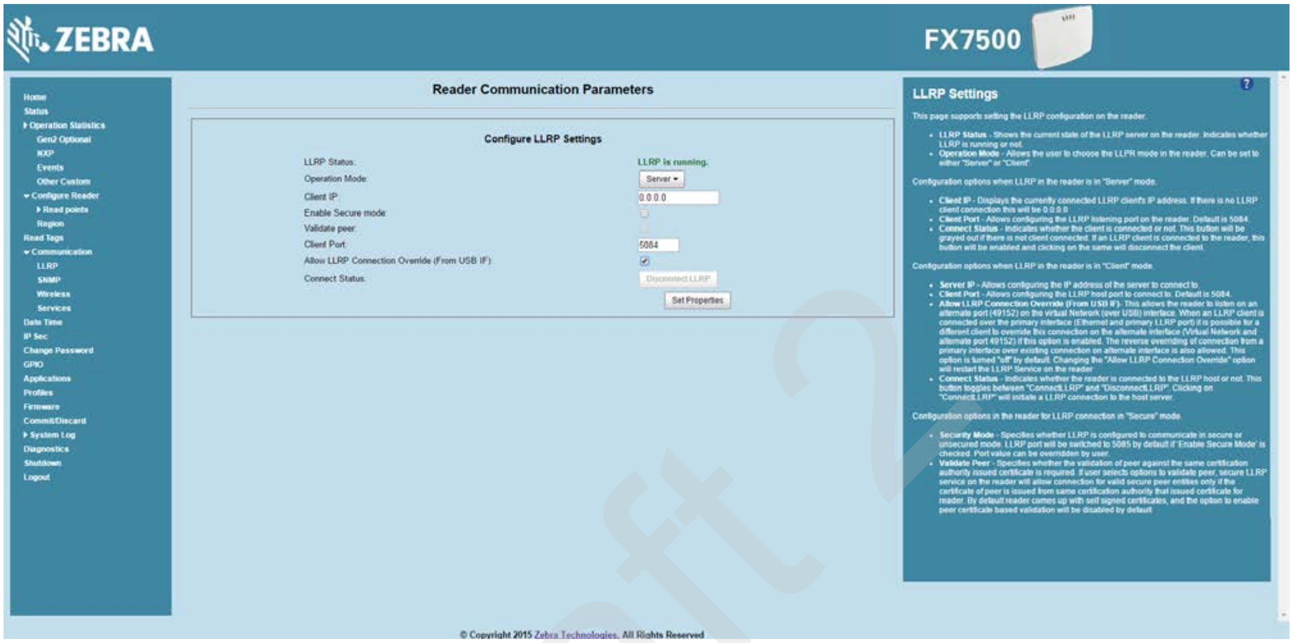
If a Bluetooth USB dongle is connected to the reader, you can set the following Bluetooth properties in this window:

- **Discoverable** - Select whether the reader is seen by other Bluetooth-enabled devices on discovery.
- **Pairable** - Select whether any Bluetooth-enabled device can pair with reader.
- **Use Passkey** - Enable this option to mandate the connecting device to supply a pre-determined passkey to use for authentication while pairing.
- **Passkey** - The passkey to use for authentication.
- **DHCP start address** - The starting address of the DHCP IP range out of which an IP is assigned to the connecting device.
- **DHCP end address** - The end address of the DHCP IP range out of which an IP is assigned to the connecting device.

✓ ***NOTE*** The DHCP IP range specified using the DHCP start address and DHCP end address options also determine the IP of the Bluetooth interface of the reader. The first two octets of the IP address of the reader Bluetooth interface are taken from the IP range specified and the last two octets use the reader BD address.

Configure LLRP Settings

Select **LLRP** to view and set the LLRP settings. By default, LLRP activates in server mode, where LLRP clients can connect to the reader using the port number specified in the **Client** port field. You can also configure the reader in LLRP client mode. In this case, configure the LLRP server address in this web page as well. LLRP cannot be disabled since it is the primary native protocol for RFID for the reader.



Reader Communication Parameters

Configure LLRP Settings

LLRP Status: LLRP is running.

Operation Mode: Server

Client IP: 0.0.0.0

Enable Secure mode: □

Validate peer: □

Client Port: 5084

Allow LLRP Connection Override (From USB IF): ☑

Connect Status:

LLRP Settings

This page supports setting the LLRP configuration on the reader.

- **LLRP Status** - Shows the current state of the LLRP server on the reader. Indicates whether LLRP is running or not.
- **Operation Mode** - Allows the user to choose the LLPR mode in the reader. Can be set to either "Server" or "Client".

Configuration options when LLRP in the reader is in "Server" mode.

- **Client IP** - Displays the currently connected LLRP client's IP address. If there is no LLRP client connection this will be 0.0.0.0
- **Client Port** - Allows configuring the LLRP listening port on the reader. Default is 5084.
- **Connect Status** - Indicates whether the client is connected or not. This button will be grayed out if there is not client connected. If an LLRP client is connected to the reader, this button will be enabled and clicking on the same will disconnect the client.

Configuration options when LLRP in the reader is in "Client" mode.

- **Server IP** - Allows configuring the IP address of the server to connect to.
- **Client Port** - Allows configuring the LLRP host port to connect to. Default is 5084.
- **Allow LLRP Connection Override (From USB IF)**- This allows the reader to listen on an alternate port (49152) on the virtual Network (over USB) interface. When an LLRP client is connected over the primary interface (Ethernet and primary LLRP port) it is possible for a different client to override this connection on the alternate interface (Virtual Network and alternate port 49152) if this option is enabled. The reverse overriding of connection from a primary interface over existing connection on alternate interface is also allowed. This option is turned "off" by default. Changing the "Allow LLRP Connection Override" option will restart the LLRP Service on the reader.
- **Connect Status** - Indicates whether the reader is connected to the LLRP host or not. This button toggles between "ConnectLLRP" and "DisconnectLLRP". Clicking on "ConnectLLRP" will initiate a LLRP connection to the host server.

Configuration options in the reader for LLRP connection in "Secure" mode.

- **Security Mode** - Specifies whether LLRP is configured to communicate in secure or unsecured mode. LLRP port will be switched to 5085 by default if 'Enable Secure Mode' is checked. Port value can be overridden by user.
- **Validate Peer** - Specifies whether the validation of peer against the same certification authority issued certificate is required. If user selects options to validate peer, secure LLRP service on the reader will allow connection for valid secure peer entities only if the certificate of peer is issued from same certification authority that issued certificate for reader. By default reader comes up with self signed certificates, and the option to enable peer certificate based validation will be disabled by default.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-23 *Configure LLRP Settings Window*

This window offers the following fields:

- **LLRP Status** - Displays the current state of the LLRP server on the reader. Indicates whether LLRP is running.
- **Operation Mode** - Sets the LLPR mode in the reader to either **Server** or **Client**.

LLRP configuration options when the reader is in **Server** mode:

- **Client IP** - Displays the currently connected LLRP client's IP address. If there is no LLRP client connection, this is 0.0.0.0.
- **Client Port** - Configures the LLRP listening port on the reader. The default is 5084.
- **Connect Status** - Indicates whether the client is connected. This button is grayed out if there is no client connected. If an LLRP client is connected to the reader, this button is enabled; click this button to disconnect the client.

LLRP configuration options when the reader is in **Client** mode:

- **Server IP** - Configures the IP address of the server to connect to.
- **Client Port** - Configures the LLRP host port to connect to. The default is 5084.
- **Allow LLRP Connection Override (From USB IF)** - This allows the reader to listen on an alternate port (49152) on the virtual network (over USB) interface. When an LLRP client is connected over the primary interface (Ethernet and primary LLRP port), a different client can override this connection on the alternate interface (Virtual Network and alternate port 49152) if this option is enabled. This also permits overriding a connection from a primary interface over an existing connection on an alternate interface. This option is off by default. Changing this option restarts the LLRP service on the reader.

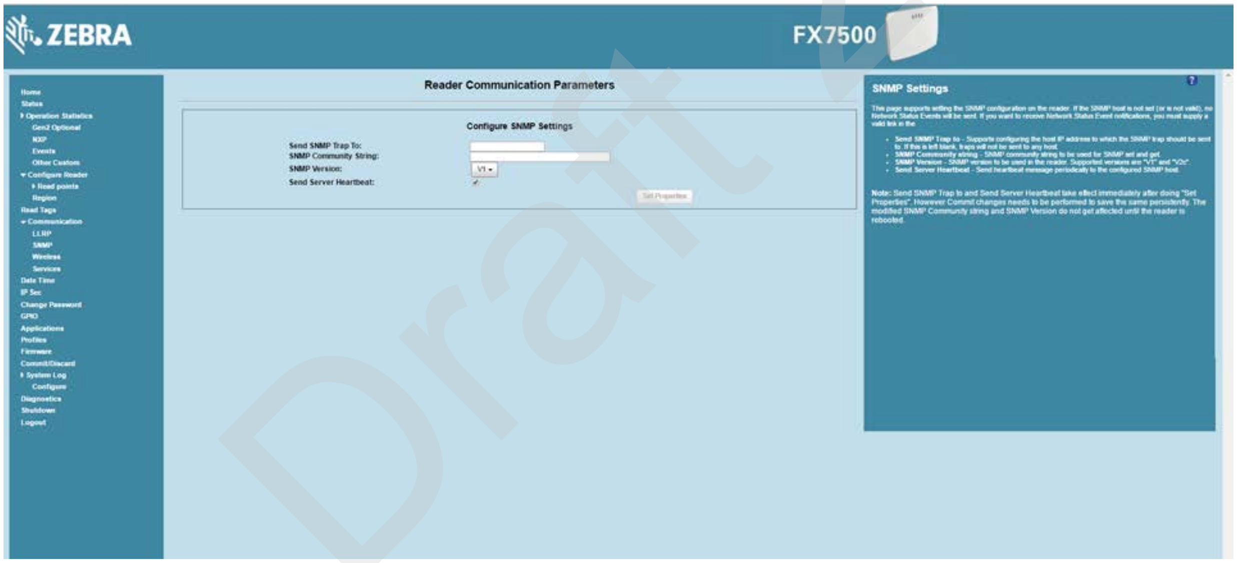
- **Connect Status** - Indicates whether the reader is connected to the LLRP host. This button toggles between **ConnectLLRP** and **DisconnectLLRP**. Clicking **ConnectLLRP** initiates an LLRP connection to the host server.

LLRP configuration options when the reader is in **Secure** mode:

- **Security Mode** - Specifies whether LLRP communicates in secure or unsecure mode. Checking **Enable Secure Mode** switches the LLRP port to 5085 by default. You can override the port value. LLRP in secure mode supports ciphers that are compliant with TLS1.2.
- **Validate Peer** - Specifies whether the validation of peer against the same certification authority issued certificate is required. If you select the validate peer option, the secure LLRP service on the reader allows connection for valid secure peer entities only if the certificate of the peer is issued from the same certification authority that issued the certificate for the reader. By default the reader uses self-signed certificates, and peer certificate based validation is disabled.

SNMP Settings

Select **SNMP** to view the **Configure SNMP Settings** window.



Reader Communication Parameters

Configure SNMP Settings

Send SNMP Trap To:
SNMP Community String:
SNMP Version: V1
Send Server Heartbeat: ☑

SNMP Settings

This page supports setting the SNMP configuration on the reader. If the SNMP host is not set (or is not valid), no Network Status Events will be sent. If you want to receive Network Status Event notifications, you must supply a valid link in the

- Send SNMP Trap to - Supports configuring the host IP address to which the SNMP trap should be sent to. If this is left blank, traps will not be sent to any host.
- SNMP Community string - SNMP community string to be used for SNMP set and get.
- SNMP Version - SNMP version to be used in the reader. Supported versions are "V1" and "V2c".
- Send Server Heartbeat - Send heartbeat message periodically to the configured SNMP host.

Note: Send SNMP Trap to and Send Server Heartbeat take effect immediately after doing "Set Properties". However Commit changes needs to be performed to save the same persistently. The modified SNMP Community string and SNMP Version do not get affected until the reader is rebooted.

Figure 4-24 *Configure SNMP Settings Window*

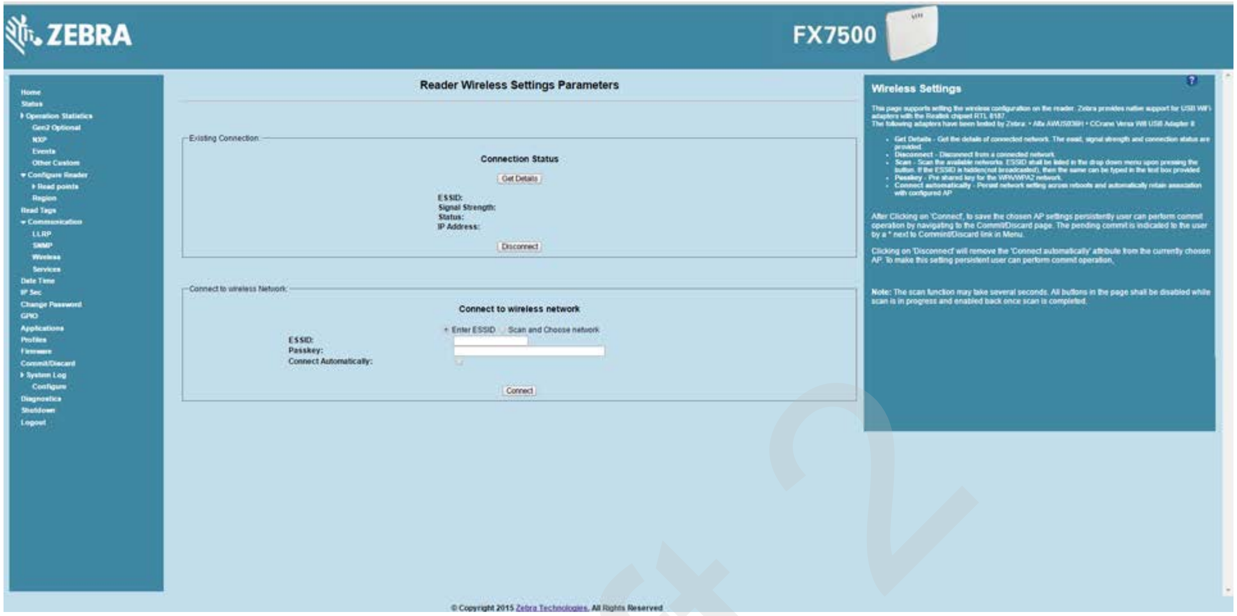
Use this window to configure the SNMP host settings to allow sending network status events and receiving network status event notifications:

- **Send SNMP Trap To** - Configures the host IP address to which the SNMP trap is sent. Leave this blank to send no traps to any host.
- **SNMP Community String** - SNMP community string to use for SNMP set and get.
- **SNMP Version** - SNMP version to use in the reader. Supported versions are **V1** and **V2c**.
- **Send Server Heartbeat** - Sends a heartbeat message periodically to the configured SNMP host.

✓ ***NOTE*** **Send SNMP Trap To** and **Send Server Heartbeat** take effect immediately after clicking **Set Properties**. However, perform a **Commit** to persist the changes. The modified **SNMP Community String** and **SNMP Version** are not affected until the reader reboots.

Wireless Settings

Select **Wireless** to view the **Reader Wireless Settings Parameters** window.



Reader Wireless Settings Parameters

Existing Connection

Connection Status

ESSID:
Signal Strength:
Status:
IP Address:

Connect to wireless Network

Connect to wireless network

ESSID:
Passkey:
Connect Automatically: □

Wireless Settings

This page supports setting the wireless configuration on the reader. Zebra provides native support for USB WiFi adapters with the Realtek chipset RTL 8187.
The following adapters have been tested by Zebra: • Alfa AWUS036H • CCrane Versa Wifi USB Adapter II

- Get Details - Get the details of connected network. The essid, signal strength and connection status are provided.
- Disconnect - Disconnect from a connected network.
- Scan - Scan the available networks. ESSID shall be listed in the drop down menu upon pressing the button. If the ESSID is hidden(not broadcasted), then the same can be typed in the text box provided.
- Passkey - Pre shared key for the WPA/WPA2 network.
- Connect automatically - Persist network setting across reboots and automatically retain association with configured AP.

After Clicking on 'Connect', to save the chosen AP settings persistently user can perform commit operation by navigating to the Commit/Discard page. The pending commit is indicated to the user by a * next to Commit/Discard link in Menu.

Clicking on 'Disconnect' will remove the 'Connect automatically' attribute from the currently chosen AP. To make this setting persistent user can perform commit operation.

Note: The scan function may take several seconds. All buttons in the page shall be disabled while scan is in progress and enabled back once scan is completed.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-25 *Wireless Settings Window*

Use this window to set the wireless configuration on the reader. Zebra provides native support for USB WiFi adapters with the Realtek chipset RTL 8187, and tested the following adapters:

- Alfa AWUS036H
- CCrane Versa Wifi USB Adapter II

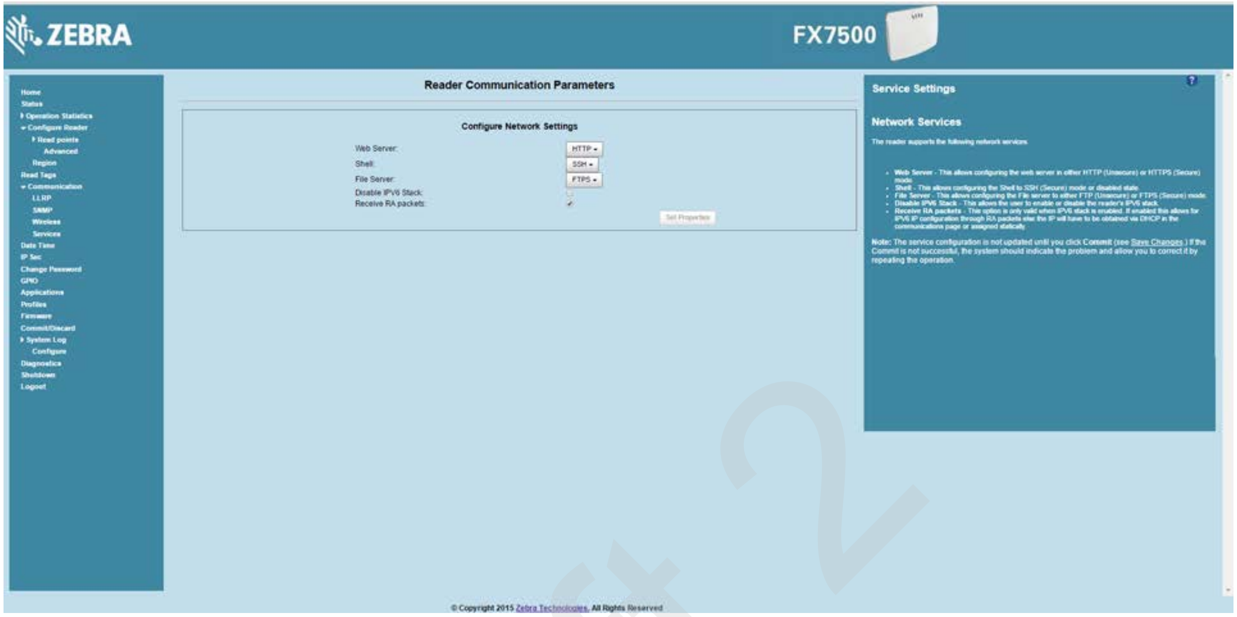
The Wireless Settings window offers the following options:

- **Get Details** - Click to get details of the connected network, including the ESSID, signal strength, and connection status.
- **Disconnect** - Click to disconnect from a connected network.
- **Scan and Choose Network** - Scan the available networks. Clicking this lists the ESSID in the drop-down menu. If the ESSID is hidden (not broadcasted), enter the ESSID in the text box provided.
- **Passkey** - Pre-shared key for the WPA/WPA2 network.
- **Connect Automatically** - Persist network setting across reboots and automatically retain association with the configured AP.

✓ ***NOTE*** The scan function can take several seconds. All buttons on the page are disabled while the scan is in progress, and re-enabled when the scan completes.

Network Services Settings

Select **Services** to view the **Configure Network Service Settings** window.



Reader Communication Parameters

Configure Network Settings

Web Server: HTTP
Shell: SSH
File Server: FTPS
Disable IPV6 Stack: □
Receive RA packets: ☑

Service Settings

Network Services

The reader supports the following network services.

- **Web Server** - This allows configuring the web server in either HTTP (Unsecure) or HTTPS (Secure) mode.
- **Shell** - This allows configuring the Shell to SSH (Secure) mode or disabled state.
- **File Server** - This allows configuring the File server to either FTP (Unsecure) or FTPS (Secure) mode.
- **Disable IPV6 Stack** - This allows the user to enable or disable the reader's IPV6 stack.
- **Receive RA packets** - This option is only valid when IPV6 stack is enabled. If enabled this allows for IPV6 IP configuration through RA packets else the IP will have to be obtained via DHCP in the communications page or assigned statically.

Note: The service configuration is not updated until you click **Commit** (see Save Changes.) If the Commit is not successful, the system should indicate the problem and allow you to correct it by repeating the operation.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-26 *Configure Network Service Settings Window*

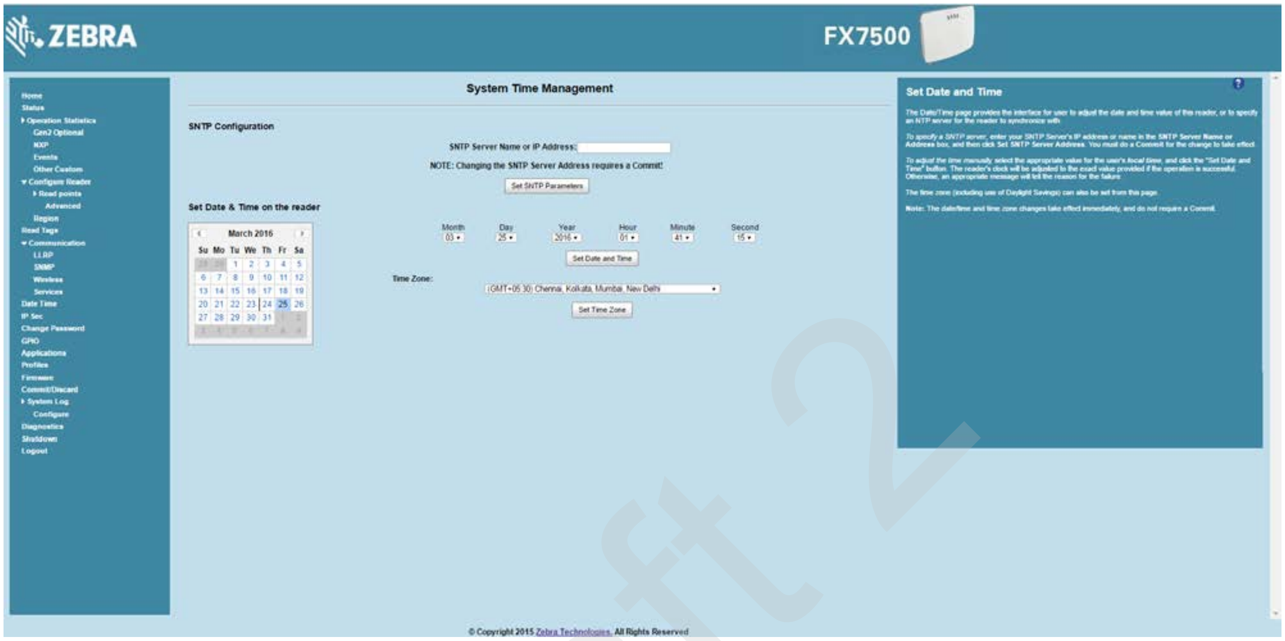
The reader supports the following network services.

- **Web Server** - Configures the web server in either HTTP (unsecure) or HTTPS (secure) mode.
- **Shell** - Sets the shell to SSH (secure) mode or a disabled state.
- **File Server** - Sets the file server to either FTP (unsecure) or FTPS (secure) mode.
- **Disable IPV6 Stack** - Select this to disable the reader's IPV6 stack.
- **Receive RA packets** - This option is only valid when the IPV6 stack is enabled. Enable this to allow IPV6 IP configuration through RA packets; otherwise obtain the IP via DHCP in the Communication window or assign statically.

✓ ***NOTE*** You must click **Commit** to update the service configuration (see Save Changes.) If the Commit is not successful, the system indicates the problem and allows correcting it by repeating the operation.

System Time Management

Select **Date Time** to view the **System Time Management** window. Use this window to set the date and time value of the reader, or to specify an NTP server for the reader to synchronize with.



SNTP Server Name or IP Address:

NOTE: Changing the SNTP Server Address requires a Commit!

Month: 03 Day: 25 Year: 2016 Hour: 01 Minute: 41 Second: 15

Time Zone: (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

The Date/Time page provides the interface for user to adjust the date and time value of this reader, or to specify an NTP server for the reader to synchronize with.

To specify a SNTP server, enter your SNTP Server's IP address or name in the SNTP Server Name or Address box, and then click Set SNTP Server Address. You must do a Commit for the change to take effect.

To adjust the time manually select the appropriate value for the user's local time, and click the "Set Date and Time" button. The reader's clock will be adjusted to the exact value provided if the operation is successful. Otherwise, an appropriate message will tell the reason for the failure.

The time zone (including use of Daylight Savings) can also be set from this page.

Note: The date/time and time zone changes take effect immediately, and do not require a Commit.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-27 *System Time Management Window*

To specify an SNTP server, enter the SNTP server's IP address or name in the **SNTP Server Name or IP Address** box, and then click **Set SNTP Parameters**. You must select Commit for the change to take effect.

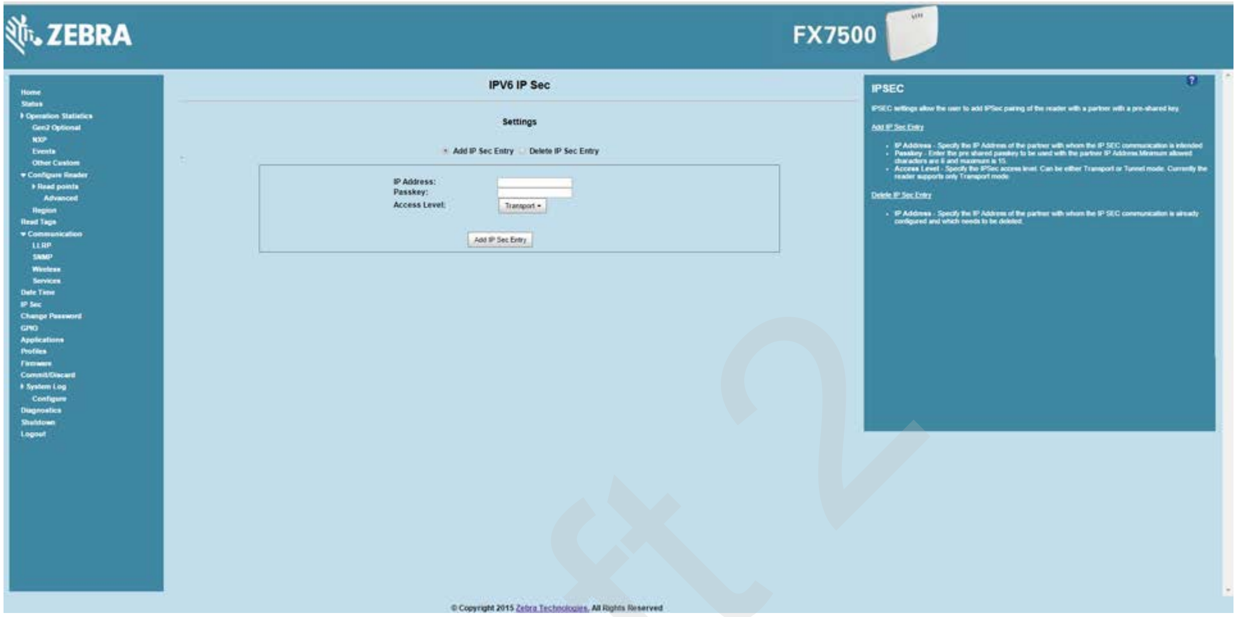
To adjust the time manually, select the appropriate value for the user's local time, and click the **Set Date and Time** button. This adjusts the reader's clock to the value provided if the operation is successful. Otherwise, an appropriate message indicates the reason for the failure.

You can also set the **Time Zone** (including use of Daylight Savings) using the drop-down menu.

✓ ***NOTE*** The date/time and time zone changes take effect immediately, and do not require a Commit.

IPV6 IP Sec

Select **IP Sec** to view the **IPV6 IP Sec** window. IP Sec settings allow adding IPSec pairing of the reader with a partner with a pre-shared key.



IPV6 IP Sec

Settings

● Add IP Sec Entry ○ Delete IP Sec Entry

IP Address:

Passkey:

Access Level: Transport

IPSEC

IPSEC settings allow the user to add IPSec pairing of the reader with a partner with a pre-shared key.

Add IP Sec Entry

- IP Address - Specify the IP Address of the partner with whom the IP SEC communication is intended
- Passkey - Enter the pre shared passkey to be used with the partner IP Address.Minimum allowed characters are 6 and maximum is 15.
- Access Level - Specify the IPSec access level. Can be either Transport or Tunnel mode. Currently the reader supports only Transport mode.

Delete IP Sec Entry

- IP Address - Specify the IP Address of the partner with whom the IP SEC communication is already configured and which needs to be deleted.

© Copyright 2015 Zebra Technologies, All Rights Reserved

Figure 4-28 *IPV6 IP Sec Window*

To add an IP Sec entry:

1. Click the **Add IP Sec Entry** radio button.
2. In the **IP Address** field, specify the IP address of the partner with whom the IP SEC communication is intended.
3. In the **Passkey** field, enter the pre-shared passkey (from 6 to 15 characters) to use with the partner IP address.
4. In the **Access Level** drop-down list, select the IPSec access level. Options are **Transport** and **Tunnel** mode. Currently the reader only supports **Transport** mode.
5. Click the **Add IP Sec Entry** button.

To delete an IP Sec entry:

1. Click **Delete IP Sec Entry** radio button.
2. In the **IP Address** field, specify the IP address of the partner with whom the IP SEC communication is configured and is to be deleted.
3. Click the **Delete IP Sec Entry** button.

Change Password

To ensure the controlled and secured access to reader **Administrator Console** functions, designate which users and computers are authorized to have system access by setting up authorized user accounts. Only users logging in with a registered user name and password can successfully access **Administrator Console** functions.

FX7500 User Accounts

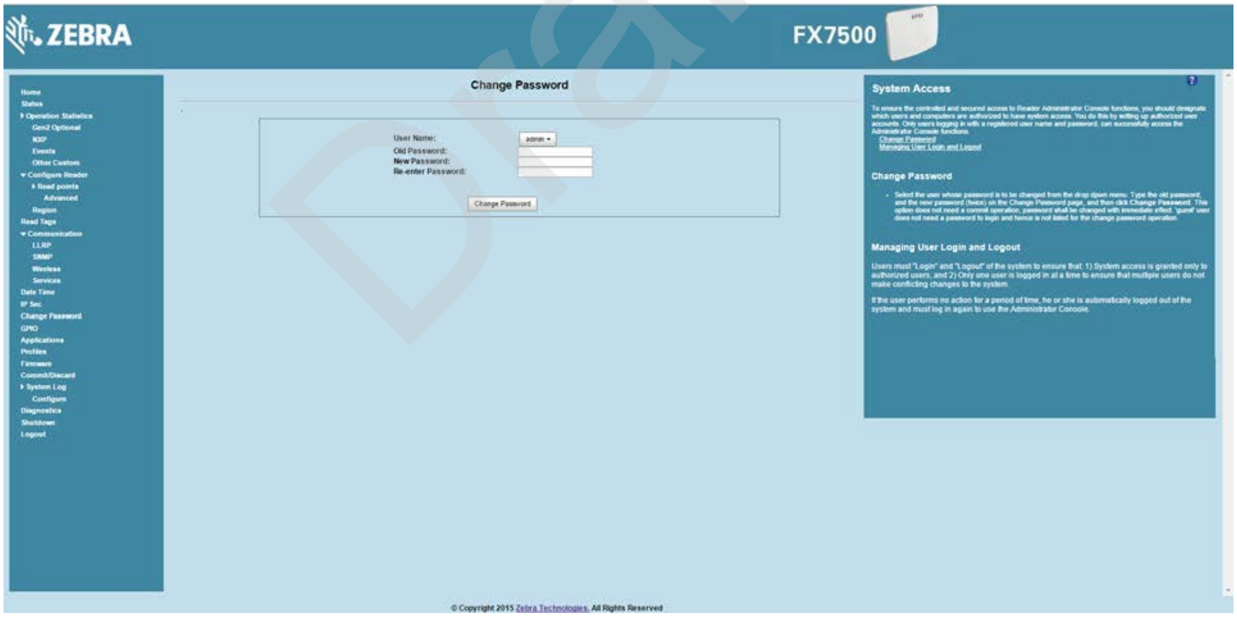
The FX7500 supports the different user accounts:

- **admin** - This user has web access but no shell access, with full privileges to make changes on the reader using the Administrator Console interface and to access to the reader using the FTP interface.
- **guest** - This user has web access but no shell access, with read-only privileges in the Administrator Console and can not make configuration changes. The **guest** user does not need a password to log in to the Administrator Console.

> ***NOTE*** The **Change Password** function is not supported for the user **guest**.

- **rfidadm** - This is the reader administrator, with shell access but no Administrator Console access. **rfidadm** has full access to the **/apps** directory and read-only access to most of the other directories, including the **/platform**, **/usr**, **/lib**, **/etc**, and **/bin** directories. The **rfidadm** user can use this account to install and uninstall RFID programs and upload user applications.

Select **Change Password** to view the **Change Password** window.



User Name: admin
Old Password:
New Password:
Re-enter Password:

System Access

To ensure the controlled and secured access to Reader Administrator Console functions, you should designate which users and computers are authorized to have system access. You do this by setting up authorized user accounts. Only users logging in with a registered user name and password, can successfully access the Administrator Console functions.

Change Password
Managing User Login and Logout

Change Password

- Select the user whose password is to be changed from the drop down menu. Type the old password, and the new password (twice) on the Change Password page, and then click Change Password. This option does not need a commit operation, password shall be changed with immediate effect. 'guest' user does not need a password to login and hence is not listed for the change password operation.

Managing User Login and Logout

Users must "Login" and "Logout" of the system to ensure that: 1) System access is granted only to authorized users, and 2) Only one user is logged in at a time to ensure that multiple users do not make conflicting changes to the system.

If the user performs no action for a period of time, he or she is automatically logged out of the system and must log in again to use the Administrator Console.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-29 *Change Password Window*

To set a user password:

1. In the **User Name** drop-down list, select the user for whom to change the password.
2. In the **Old Password** field, enter the existing password for that user.
3. In the **New Password** field, enter the new password, and again in the **Re-Enter Password** field.
4. Click **Change Password**. The password changes immediately and does not require a Commit operation.

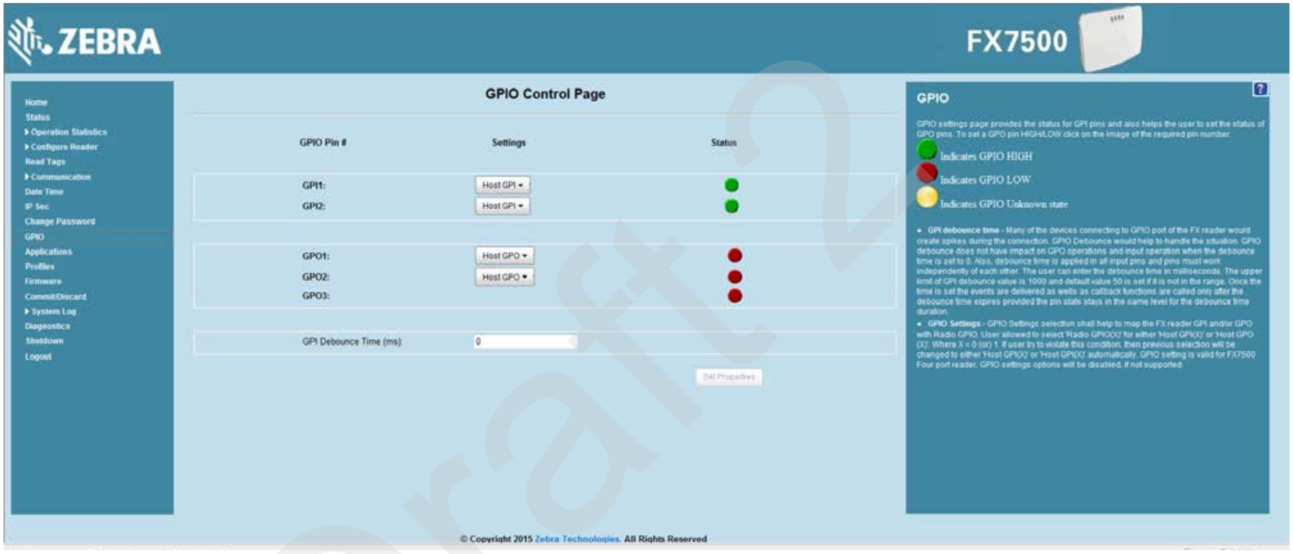
Managing User Login and Logout

Users must log in and log out of the system to ensure that system access is granted only to authorized users, and that only one user is logged in at a time to ensure that multiple users do not make conflicting changes to the system.

If the user performs no action for a period of time, the system automatically logs him or her out. The user must log in again to use the Administrator Console.

GPIO

Select **GPIO** to view the **GPIO Control Page**. This window allows viewing and setting the status for GPI pins.



GPIO Control Page

GPIO Pin #	Settings	Status
GPI1:	Host GPI	🟢
GPI2:	Host GPI	🟢
GPO1:	Host GPO	🔴
GPO2:	Host GPO	🔴
GPO3:		🔴

GPI Debounce Time (ms): 0

GPIO

GPIO settings page provides the status for GPI pins and also helps the user to set the status of GPO pins. To set a GPO pin HIGH/LOW click on the image of the required pin number.

🟢 Indicates GPIO HIGH

🔴 Indicates GPIO LOW

🟡 Indicates GPIO Unknown state

- **GPI debounce time** - Many of the devices connecting to GPIO port of the FX reader would create spikes during the connection. GPIO Debounce would help to handle the situation. GPIO debounce does not have impact on GPO operations and input operation when the debounce time is set to 0. Also, debounce time is applied in all input pins and pins must work independently of each other. The user can enter the debounce time in milliseconds. The upper limit of GPI debounce value is 1000 and default value 50 is set if it is not in the range. Once the time is set the events are delivered as wells as callback functions are called only after the debounce time expires provided the pin state stays in the same level for the debounce time duration.
- **GPIO Settings** - GPIO Settings selection shall help to map the FX reader GPI and/or GPO with Radio GPIO. User allowed to select 'Radio GPIO(X)' for either 'Host GPI(X)' or 'Host GPO (X)'. Where X = 0 (or) 1. If user try to violate this condition, then previous selection will be changed to either 'Host GPO(X)' or 'Host GPI(X)' automatically. GPIO setting is valid for FX7500 Four port reader. GPIO settings options will be disabled, if not supported.

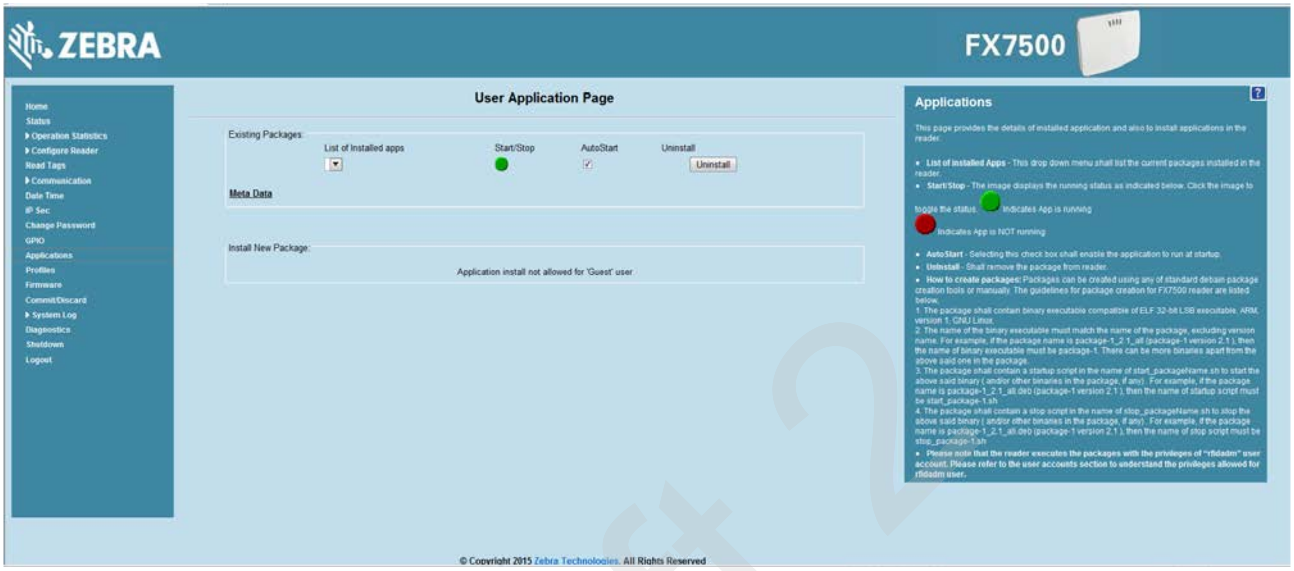
© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-30 *GPIO Control Page*

- **Settings** - Map the reader GPI and/or GPO with the radio GPIO. Select either **Radio** or **Host** for **GPI*x*** or **GPO*x*** where *x* = 0 or 1. An attempt to violate this condition changes the selection to either **Host GPI*x*** or **Host GPO*x*** automatically. These settings are valid for FX7500 four port readers and are disabled if not supported.
- **Status** - To set a GPO pin high or low, click on the image next to the required pin number:
  - Green 🟢 indicates GPIO HIGH
  - Red 🔴 indicates GPIO LOW
  - Yellow 🟡 indicates GPIO unknown
- **GPI Debounce Time** - Enter a value of up to 1000 milliseconds to minimize spikes that can occur when a device connects to the GPIO port of the FX reader. The default is 50. Debounce time applies to all input pins, and pins must work independently of each other. Events and callback functions occur only after the debounce time expires, provided the pin state remains at the same level for the debounce time duration. GPIO debounce does not impact GPO and input operations when set to 0.
- **Set Properties** - Click this when all selections are made.

Applications

Select **Applications** to view the **User Application Page**. This window allows installing applications on the reader and provides details of the installed application.



User Application Page

Application install not allowed for 'Guest' user

Applications

This page provides the details of installed application and also to install applications in the reader.

- **List of installed Apps** - This drop down menu shall list the current packages installed in the reader.
- **Start/Stop** - The image displays the running status as indicated below. Click the image to toggle the status. 🟢 Indicates App is running
🔴 Indicates App is NOT running
- **AutoStart** - Selecting this check box shall enable the application to run at startup.
- **Uninstall** - Shall remove the package from reader.
- **How to create packages:** Packages can be created using any of standard debain package creation tools or manually. The guidelines for package creation for FX7500 reader are listed below.
1. The package shall contain binary executable compatible of ELF 32-bit LSB executable, ARM, version 1, GNU Linux.
2. The name of the binary executable must match the name of the package, excluding version name. For example, if the package name is package-1_2.1_all (package-1 version 2.1), then the name of binary executable must be package-1. There can be more binaries apart from the above said one in the package.
3. The package shall contain a startup script in the name of start_packageName.sh to start the above said binary (and/or other binaries in the package, if any) . For example, if the package name is package-1_2.1_all.deb (package-1 version 2.1), then the name of startup script must be start_package-1.sh
4. The package shall contain a stop script in the name of stop_packageName.sh to stop the above said binary (and/or other binaries in the package, if any) . For example, if the package name is package-1_2.1_all.deb (package-1 version 2.1), then the name of stop script must be stop_package-1.sh
- **Please note that the reader executes the packages with the privileges of "rfidadm" user account. Please refer to the user accounts section to understand the privileges allowed for rfidadm user.**

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-31 *User Application Page*

The **Existing Packages** section includes the following options:

- **List of Installed apps** - The drop-down menu lists the current packages installed in the reader.
- **Start/Stop** - The image displays the running status as follows. Click the image to toggle the status.
  - Green 🟢 indicates application is running
  - Red 🔴 indicates application is not running
- **AutoStart** - Select this check box to run the application at startup.
- **Uninstall** - Removes the package from the reader.

To create packages for the FX7500 reader, use any of the standard Debian package creation tools, or create them manually. The *FX7500 Embedded SDK Programmers Guide* provides details on creating application packages to install on the reader.

- The package must contain a binary executable compatible with ELF 32-bit LSB executable, ARM, version 1, GNU Linux.
- The name of the binary executable must match the name of the package, excluding the version name. For example, if the package name is **package-1_2.1_all** (package 1 version 2.1), the name of the binary executable must be **package-1**. There can be more than one binary in the package.
- The package must contain a startup script in the name of **start_packageName.sh** to start the binary or binaries in the package. For example, if the package name is **package-1_2.1_all.deb** (package 1 version 2.1), the name of the startup script must be **start_package-1.sh.**
- The package must contain a stop script in the name of **stop_packageName.sh** to stop the binary or binaries in the package. For example, if the package name is **package-1_2.1_all.deb** (package 1 version 2.1), the name of stop script must be **stop_package-1.sh.**

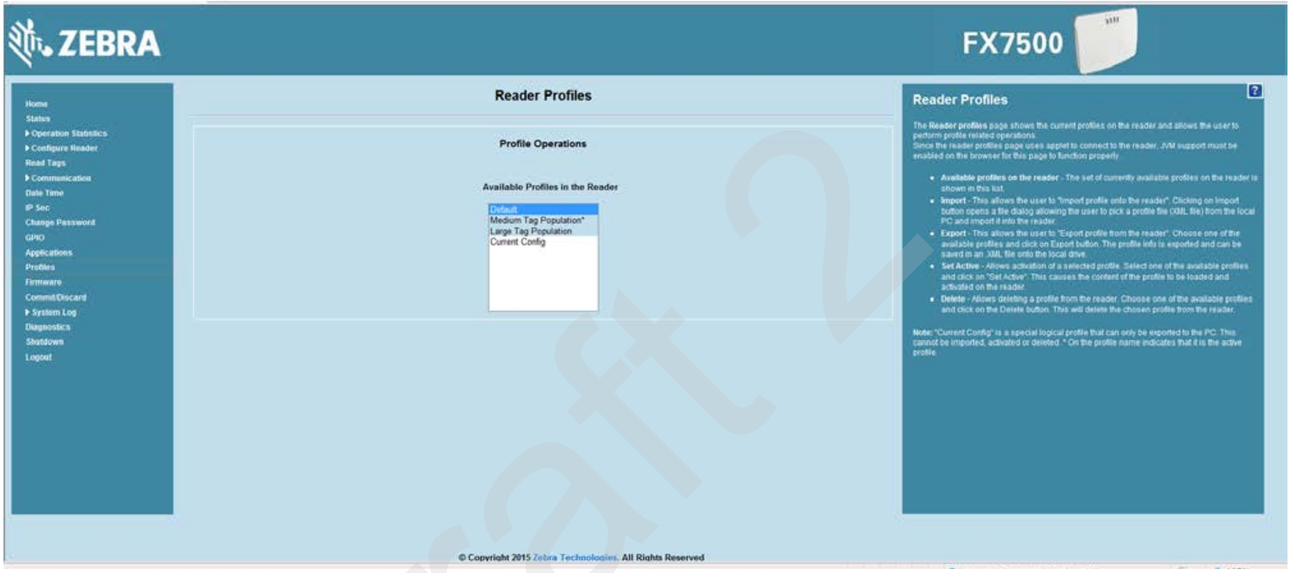
✓ ***NOTE*** The reader executes the packages with the privileges of **rfidadm** user account. See the user accounts section for information on **rfidadm** user privileges.

Reader Profiles

Select **Profiles** in the selection menu to view the **Reader Profiles** window, which shows the current profiles on the reader and allows performing profile-related operations.

✓ ***NOTE*** Because the **Reader Profiles** window uses an applet to connect to the reader, enable JVM support on the browser in order for this window to function properly.

The window displays a set of provided configuration files, or profiles, that a user can re-use and/or modify depending on the reader application or use case. The profiles serve as configuration examples.



Reader Profiles

The **Reader profiles** page shows the current profiles on the reader and allows the user to perform profile related operations.
Since the reader profiles page uses applet to connect to the reader, JVM support must be enabled on the browser for this page to function properly.

- **Available profiles on the reader** - The set of currently available profiles on the reader is shown in this list.
- **Import** - This allows the user to "Import profile onto the reader". Clicking on Import button opens a file dialog allowing the user to pick a profile file (XML file) from the local PC and import it into the reader.
- **Export** - This allows the user to "Export profile from the reader". Choose one of the available profiles and click on Export button. The profile info is exported and can be saved in an XML file onto the local drive.
- **Set Active** - Allows activation of a selected profile. Select one of the available profiles and click on "Set Active". This causes the content of the profile to be loaded and activated on the reader.
- **Delete** - Allows deleting a profile from the reader. Choose one of the available profiles and click on the Delete button. This will delete the chosen profile from the reader.

Note: "Current Config" is a special logical profile that can only be exported to the PC. This cannot be imported, activated or deleted. * On the profile name indicates that it is the active profile.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-32 *Reader Profiles Window*

The **Reader Profiles** window functions are:

- **Available Profiles in the Reader** - Displays the available reader profiles.
- **Import** - Click to open a file dialog and pick a profile (XML file) from the local PC and import it into the reader.
- **Export** - Select an available profile and click **Export** to export profile information and save an XML file onto the local drive.
- **Set Active** - Activates a selected profile. Select an available profile and click **Set Active** to load the profile content in the reader.

⚠ ***CAUTION*** Swapping profiles between readers using static IP addresses is not recommended. Activating a profile with a static IP address changes the IP of the reader, and if not done properly can make the reader inaccessible.

- **Delete** - Select an available profile and click **Delete** to delete the profile.

✓ ***NOTE*** **Current Config** is a special logical profile that can only be exported to the PC. This cannot be imported, activated, or deleted. Only the profile name indicates that it is the active profile.

Profiles can specify a number of reader parameters, including RF air link profiles. Air link profiles cannot be configured using LLRP or web page interface. See *Appendix C, RF Air Link Configuration* for more information about air link profile configuration.

FIPS Support on FX7500

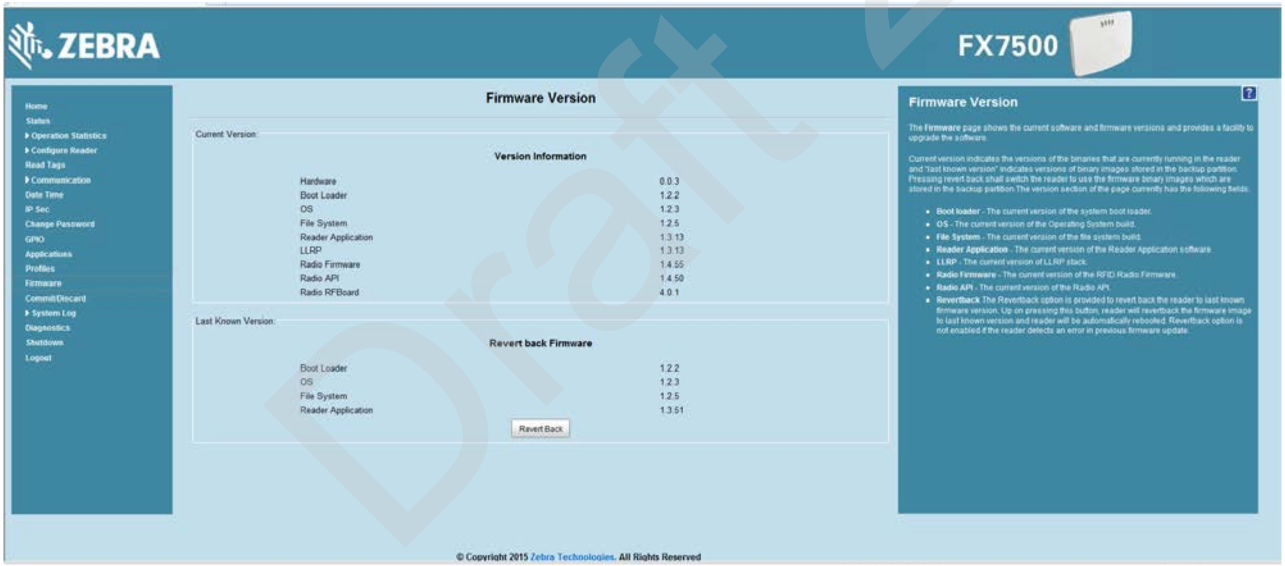
The FX7500 supports FIPS 140-2 Level 1 for the following interfaces:

- HTTPS
- FTPS
- SSH
- LLRP Server
- IPSec

To enable or disable FIPS support in the reader profile, export the profile XML (**CurrentConfig**) from the reader and set **FIPS_MODE_ENABLED** to **1** to enable FIPS, or **0** to disable FIPS. Then import the XML to the reader and activate. Changing the FIPS mode restarts the reader. By default, FIPS is disabled.

Firmware Version/Update

The **Firmware Version** window displays the current software and firmware versions and allows upgrading to new firmware. From the selection menu, click **Firmware**.



Firmware Version

Current Version:

Version Information

Hardware	0.0.3
Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.13
LLRP	1.3.13
Radio Firmware	1.4.55
Radio API	1.4.50
Radio RFBoard	4.0.1

Last Known Version:

Revert back Firmware

Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.51

Firmware Version

The **Firmware** page shows the current software and firmware versions and provides a facility to upgrade the software.

Current version indicates the versions of the binaries that are currently running in the reader and "last known version" indicates versions of binary images stored in the backup partition. Pressing revert back shall switch the reader to use the firmware binary images which are stored in the backup partition The version section of the page currently has the following fields:

- **Boot loader** - The current version of the system boot loader.
- **OS** - The current version of the Operating System build.
- **File System** - The current version of the file system build.
- **Reader Application** - The current version of the Reader Application software.
- **LLRP** - The current version of LLRP stack.
- **Radio Firmware** - The current version of the RFID Radio Firmware.
- **Radio API** - The current version of the Radio API.
- **Revertback** The Revertback option is provided to revert back the reader to last known firmware version. Up on pressing this button, reader will revertback the firmware image to last known version and reader will be automatically rebooted. Revertback option is not enabled if the reader detects an error in previous firmware update.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-33 *Firmware Version*

Current Version indicates the binary versions currently running in the reader. **Last Known Version** indicates binary image versions stored in the backup partition. This window provides version information on the following firmware:

- Boot Loader
- OS
- File System
- Reader Application
- LLRP
- Radio Firmware
- Radio API

Select **Revert Back** to revert the firmware to last known version. The reader automatically reboots. This option is not enabled if the reader detects an error in the previous firmware update.

Firmware Update

The **Firmware Update** window allows upgrading to new firmware. From the selection menu, click **Update**.

> ✓ ***NOTE*** You must be logged in with Administrator privileges in order to access this window. See *Change Password on page 4-40*.

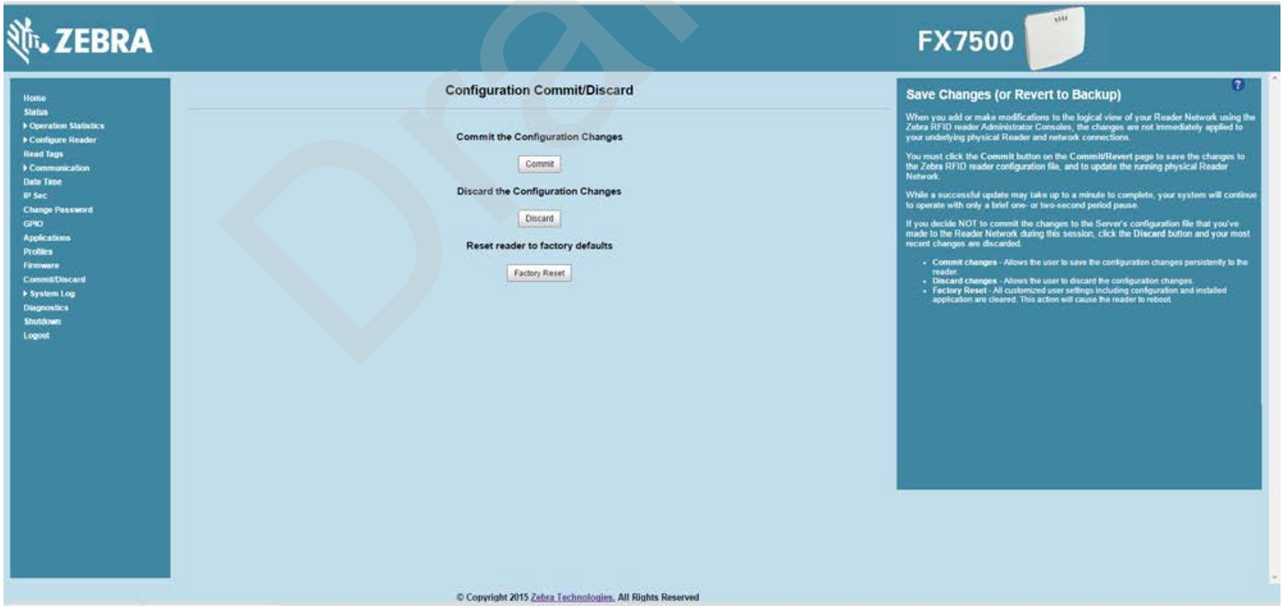
The reader supports three different methods of updating the firmware:

- Update using a USB drive.
- File-based update that allows uploading the firmware files from the PC (or a network location) to the reader and running the update.
- FTP / FTPS / SCP server-based update.

For instructions on updating the firmware, see *Chapter 7, Firmware Upgrade*.

Commit/Discard

Changes made to the logical view of the reader network using the **Administrator Console** do not immediately apply to the reader and network connections. To apply reader configuration modifications, select **Commit/Discard**, then click **Commit** to save the changes to the reader configuration file, and to update the running physical reader network. While a successful update can take up to a minute to complete, the system continues to operate with a brief one or two second pause.



Save Changes (or Revert to Backup)

When you add or make modifications to the logical view of your Reader Network using the Zebra RFID reader Administrator Consoles, the changes are not immediately applied to your underlying physical Reader and network connections.

You must click the Commit button on the Commit/Revert page to save the changes to the Zebra RFID reader configuration file, and to update the running physical Reader Network.

While a successful update may take up to a minute to complete, your system will continue to operate with only a brief one- or two-second period pause.

If you decide NOT to commit the changes to the Server's configuration file that you've made to the Reader Network during this session, click the **Discard** button and your most recent changes are discarded.

- **Commit changes** - Allows the user to save the configuration changes persistently to the reader.
- **Discard changes** - Allows the user to discard the configuration changes.
- **Factory Reset** - All customized user settings including configuration and installed application are cleared. This action will cause the reader to reboot.

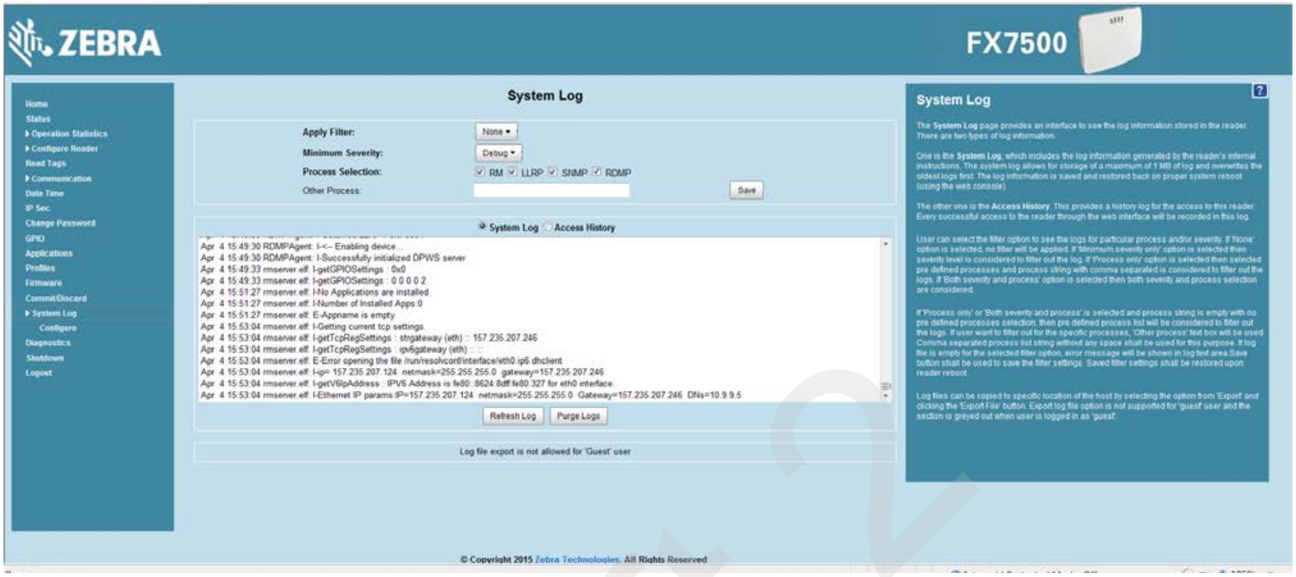
Figure 4-34 *Commit/Discard Window*

To discard changes to the server's configuration file made to the reader network during this session, click **Discard**.

Click **Factory Reset** to reset the reader to factory defaults. This clears all customized user settings, including configuration, and installed applications. The reader reboots automatically.

System Log

The **System Log** window lists reader log information.



System Log

Apply Filter: None
Minimum Severity: Debug
Process Selection: ☑ RM ☑ LLRP ☑ SNMP ☑ RDMP
Other Process: [Save]

● System Log ○ Access History

```
Apr  4 15:49:30 RDMPAgent: I-<-- Enabling device...
Apr  4 15:49:30 RDMPAgent: I-Successfully initialized DPWS server
Apr  4 15:49:33 rmserver.elf: I-getGPIOSettings : 0x0
Apr  4 15:49:33 rmserver.elf: I-getGPIOSettings : 0 0 0 0 2
Apr  4 15:51:27 rmserver.elf: I-No Applications are installed
Apr  4 15:51:27 rmserver.elf: I-Number of Installed Apps:0
Apr  4 15:51:27 rmserver.elf: E-Appname is empty
Apr  4 15:53:04 rmserver.elf: I-Getting current tcp settings.
Apr  4 15:53:04 rmserver.elf: I-getTcpRegSettings : strgateway (eth) :: 157.235.207.246
Apr  4 15:53:04 rmserver.elf: I-getTcpRegSettings : ipv6gateway (eth) :: ::
Apr  4 15:53:04 rmserver.elf: E-Error opening the file /run/resolvconf/interface/eth0.ip6.dhclient
Apr  4 15:53:04 rmserver.elf: I-ip= 157.235.207.124  netmask=255.255.255.0  gateway=157.235.207.246
Apr  4 15:53:04 rmserver.elf: I-getV6IpAddress : IPV6 Address is fe80::8624:8dff:fe80:327 for eth0 interface.
Apr  4 15:53:04 rmserver.elf: I-Ethernet IP params IP=157.235.207.124  netmask=255.255.255.0  Gateway=157.235.207.246  DNs=10.9.9.5
```

[Refresh Log] [Purge Logs]

Log file export is not allowed for 'Guest' user

System Log

The **System Log** page provides an interface to see the log information stored in the reader. There are two types of log information.

One is the **System Log**, which includes the log information generated by the reader's internal instructions. The system log allows for storage of a maximum of 1 MB of log and overwrites the oldest logs first. The log information is saved and restored back on proper system reboot (using the web console).

The other one is the **Access History**. This provides a history log for the access to this reader. Every successful access to the reader through the web interface will be recorded in this log.

User can select the filter option to see the logs for particular process and/or severity. If 'None' option is selected, no filter will be applied. If 'Minimum severity only' option is selected then severity level is considered to filter out the log. If 'Process only' option is selected then selected pre defined processes and process string with comma separated is considered to filter out the logs. If 'Both severity and process' option is selected then both severity and process selection are considered.

If 'Process only' or 'Both severity and process' is selected and process string is empty with no pre defined processes selection, then pre defined process list will be considered to filter out the logs. If user want to filter out for the specific processes, 'Other process' text box will be used. Comma separated process list string without any space shall be used for this purpose. If log file is empty for the selected filter option, error message will be shown in log text area. Save button shall be used to save the filter settings. Saved filter settings shall be restored upon reader reboot.

Log files can be copied to specific location of the host by selecting the option from 'Export' and clicking the 'Export File' button. Export log file option is not supported for 'guest' user and the section is greyed out when user is logged in as 'guest'.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-35 *System Log Window*

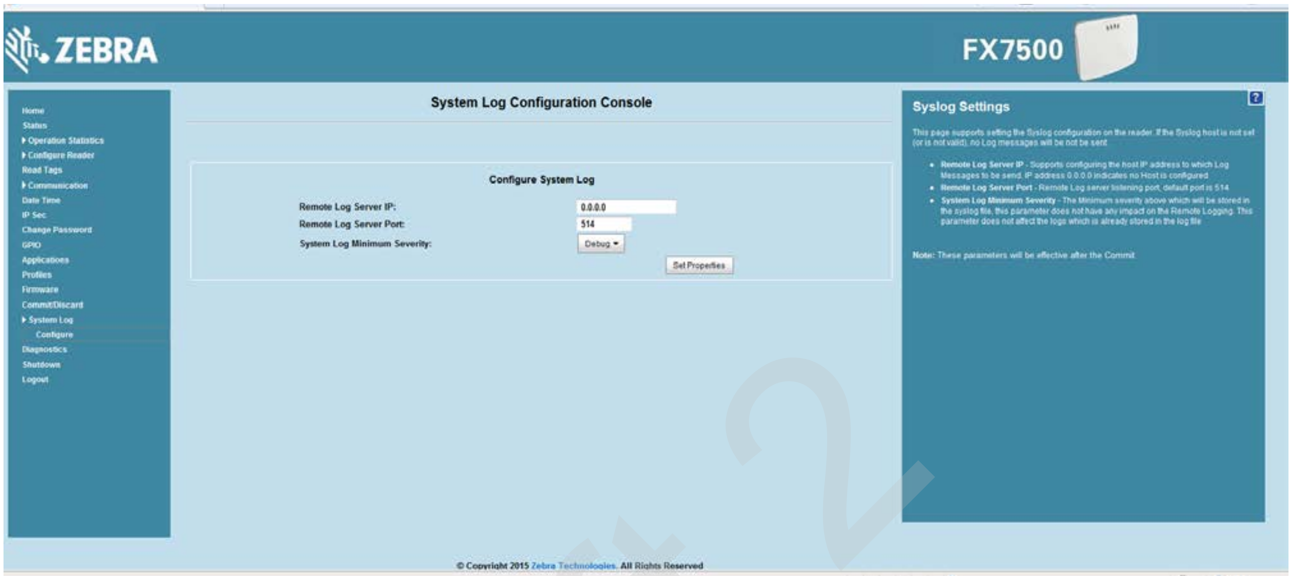
This window offers the following options:

- **Apply Filter** - Select a filter option from the drop-down menu to view logs for particular process and/or severity:
  - **None** - Do not apply a filter.
  - **Minimum Severity only** - The severity level filters the log.
  - **Process Selection only** - Selected pre-defined processes and comma-separated process strings filters the logs.
  - **Minimum Severity & Process Selection** - both severity and process selection are considered in the filter.

  If you select **Process Selection only** or **Minimum Severity & Process Selection** and the process string is empty with no pre-defined process selection, then the pre-defined process list filters the logs.
- **Minimum Severity** - Select the severity level on which to filter.
- **Process Selection** - Select the types of processes to filter upon.
- **Other process** - To filter for specific processes, enter the process in this text box using a comma-separated process list string with no spaces. If the log file is empty for the selected filter option, an error message appears in the log text area. Click **Save** to save the filter settings, which persist upon reader reboot.
- **Log area** - Select a radio button for one of the two types of log information offered:
  - **System Log** - Includes the log information generated by the reader internal instructions. This stores up to 1 MB of log information, and overwrites the oldest logs first. The log information is saved and restored on proper system reboot (via the Administrator Console).
  - **Access History** - Provides a history log for reader access, including every successful access to the reader through the Administrator Console.
- Select the **Refresh Log** to refresh the information in the log, or **Purge Logs** to clear the information.
- To copy the log file to a specific location on the host select an option from the **Export** drop-down. Enter the location in the **File Path** field, then select the **Export File** button.

Configure System Log

This window configures system log settings. If the system log host is not set (or is not valid), log messages are not sent.



System Log Configuration Console

Configure System Log

Remote Log Server IP: 0.0.0.0

Remote Log Server Port: 514

System Log Minimum Severity: Debug

Syslog Settings

This page supports setting the Syslog configuration on the reader. If the Syslog host is not set (or is not valid), no Log messages will be not be sent

- **Remote Log Server IP** - Supports configuring the host IP address to which Log Messages to be send. IP address 0.0.0.0 indicates no Host is configured
- **Remote Log Server Port** - Remote Log server listening port, default port is 514
- **System Log Minimum Severity** - The Minimum severity above which will be stored in the syslog file, this parameter does not have any impact on the Remote Logging. This parameter does not affect the logs which is already stored in the log file

Note: These parameters will be effective after the Commit

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-36 *Configure System Log Window*

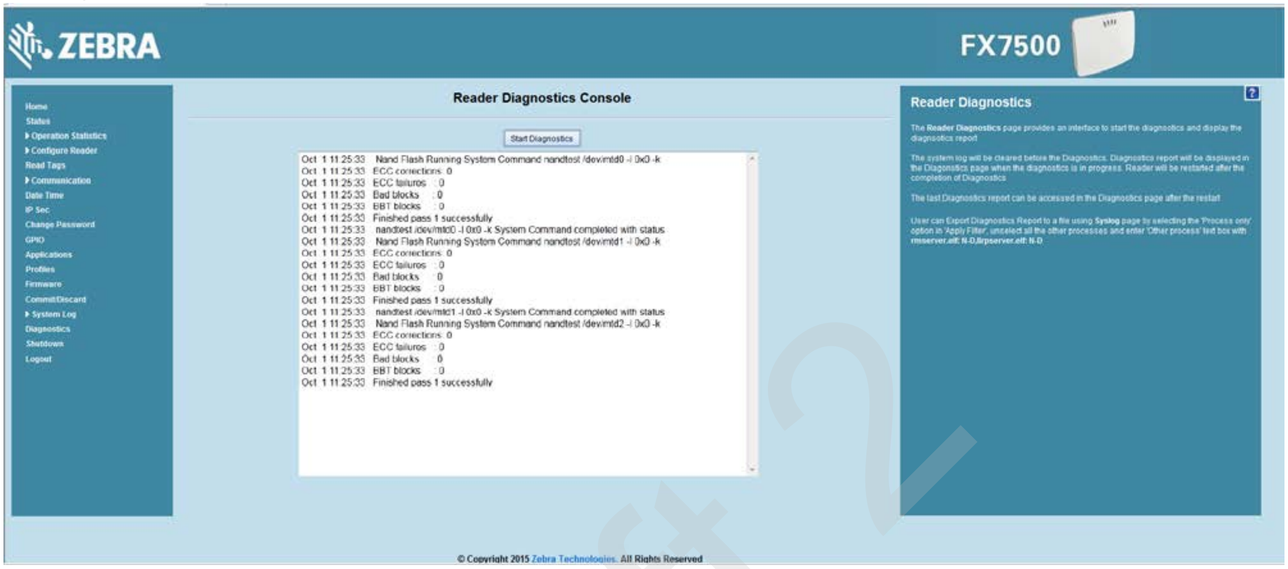
This window offers the following options:

- **Remote Log Server IP** - Configures the host IP address to which log messages are sent. IP address 0.0.0.0 indicates that no host is configured.
- **Remote Log Server Port** - Remote log server listening port. The default port is 514.
- **System Log Minimum Severity** - The minimum severity above which data is stored in the log file. This option does not impact remote logging or the logs already stored in the log file.

You must select **Commit** to activate these settings.

Reader Diagnostics

Select **Diagnostics** to view the **Reader Diagnostics** window, which allows running diagnostics and viewing the diagnostics report.



```
Oct  1 11:25:33   Nand Flash Running System Command nandtest /dev/mtd0 -l 0x0 -k
Oct  1 11:25:33  ECC corrections: 0
Oct  1 11:25:33  ECC failures    : 0
Oct  1 11:25:33  Bad blocks      : 0
Oct  1 11:25:33  BBT blocks      : 0
Oct  1 11:25:33  Finished pass 1 successfully
Oct  1 11:25:33   nandtest /dev/mtd0 -l 0x0 -k System Command completed with status
Oct  1 11:25:33   Nand Flash Running System Command nandtest /dev/mtd1 -l 0x0 -k
Oct  1 11:25:33  ECC corrections: 0
Oct  1 11:25:33  ECC failures    : 0
Oct  1 11:25:33  Bad blocks      : 0
Oct  1 11:25:33  BBT blocks      : 0
Oct  1 11:25:33  Finished pass 1 successfully
Oct  1 11:25:33   nandtest /dev/mtd1 -l 0x0 -k System Command completed with status
Oct  1 11:25:33   Nand Flash Running System Command nandtest /dev/mtd2 -l 0x0 -k
Oct  1 11:25:33  ECC corrections: 0
Oct  1 11:25:33  ECC failures    : 0
Oct  1 11:25:33  Bad blocks      : 0
Oct  1 11:25:33  BBT blocks      : 0
Oct  1 11:25:33  Finished pass 1 successfully
```

Reader Diagnostics

The **Reader Diagnostics** page provides an interface to start the diagnostics and display the diagnsotics report

The system log will be cleared before the Diagnostics. Diagnostics report will be displayed in the Diagonstics page when the diagnostics is in progress. Reader will be restarted after the completion of Diagnostics

The last Diagnostics report can be accessed in the Diagnostics page after the restart

User can Export Diagnostics Report to a file using **Syslog** page by selecting the 'Process only' option in 'Apply Filter', unselect all the other processes and enter 'Other process' text box with **rmserver.elf: N-D,llrpserver.elf: N-D**

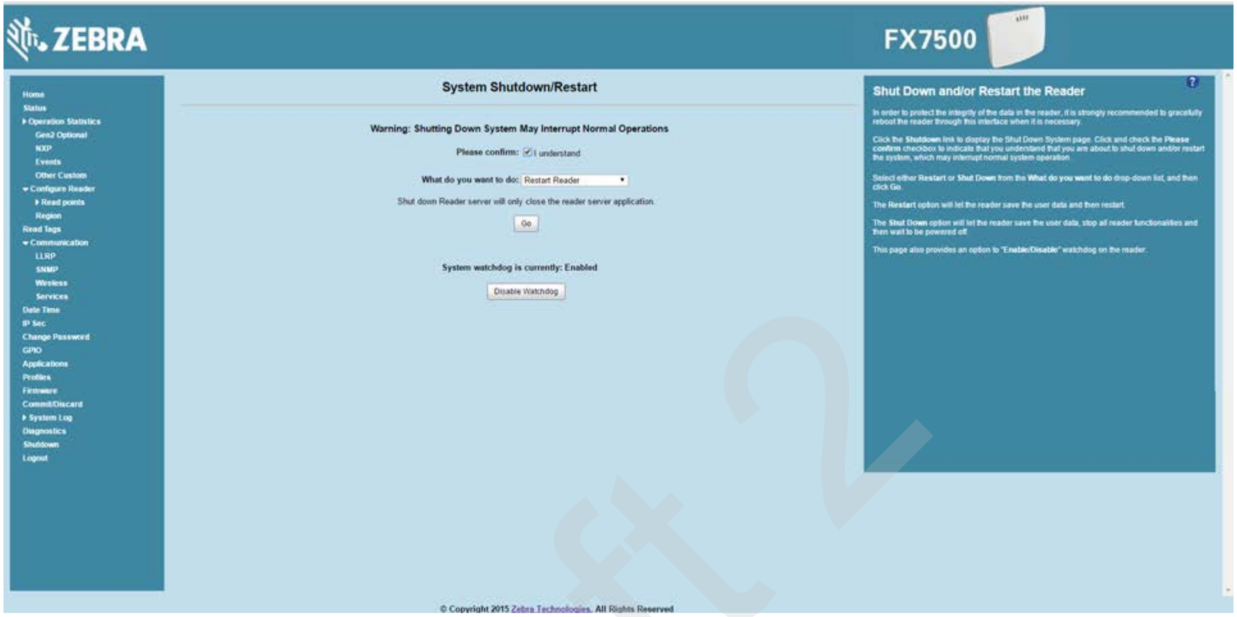
Figure 4-37 *Reader Diagnostics Window*

Selecting **Start Diagnostics** clears the system log and displays the diagnostics report. The reader reboots when the diagnostics completes. Return to the **Diagnostics** window to view the diagnostics report.

To export the diagnostics report to a file, on the *System Log* window, select **Process Selection only** in **Apply Filter**, de-select all other processes, and in the **Other Process** text box enter:
rmserver.elf: N-D,llrpserver.elf: N-D

Shutdown

To protect the integrity of the reader data, gracefully reboot the reader via the Administrator Console when necessary.



System Shutdown/Restart

Warning: Shutting Down System May Interrupt Normal Operations

Please confirm: ☑ I understand

What do you want to do: Restart Reader

Shut down Reader server will only close the reader server application.

System watchdog is currently: Enabled

Shut Down and/or Restart the Reader

In order to protect the integrity of the data in the reader, it is strongly recommended to gracefully reboot the reader through this interface when it is necessary.

Click the **Shutdown** link to display the Shut Down System page. Click and check the **Please confirm** checkbox to indicate that you understand that you are about to shut down and/or restart the system, which may interrupt normal system operation.

Select either **Restart** or **Shut Down** from the **What do you want to do** drop-down list, and then click Go.

The **Restart** option will let the reader save the user data and then restart.

The **Shut Down** option will let the reader save the user data, stop all reader functionalities and then wait to be powered off.

This page also provides an option to "Enable/Disable" watchdog on the reader.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 4-38 *System Shutdown/Restart Window*

To shut down or restart the reader:

1. Click the **Shutdown** link to display the **System Shutdown/Restart** window.
2. Check the **Please Confirm** check box to accept the system shut down and/or restart the system (this may interrupt normal system operation).
3. Select one of the following options from the **What do you want to do** drop-down list:
   - **Restart Reader** - saves the user data and then restarts.
   - **Shut down Reader server** - the reader saves the user data, stops all reader functions, and waits to be powered off.
4. Click **Go**.

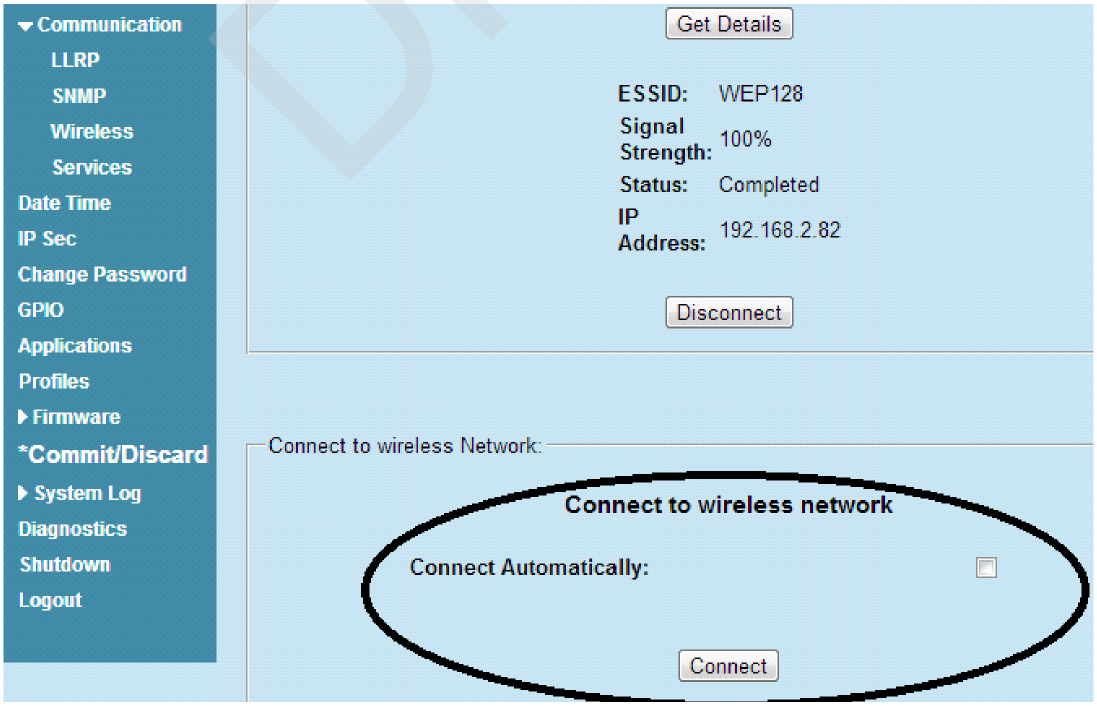
This window also provides an option to enable or disable the reader watchdog.

CHAPTER 5 WI-FI CONFIGURATION

Wireless Network Advanced Configuration

FX7500 uses the **wpa_supplicant** application to connect with wireless networks. Advanced users can place their own configuration file in the **/apps** folder to connect to wireless networks. This configuration file is **wpa_supplicant.conf**. The parameters of this file are well documented in the public domain. Refer to http://linux.die.net/man/5/wpa_supplicant.conf for the most commonly used parameters and http://www.daemon-systems.org/man/wpa_supplicant.conf.5.html for all available parameters. Also see *Appendix E, Copying Files To and From the Reader* for instructions on copying files to **/apps** directory.

If **/apps/wpa_supplicant.conf** is present in the reader, the reader uses this file to connect to a wireless network. This supersedes the configuration in the **Administrator Console**, which changes to reflect the custom configuration file.



ESSID: WEP128

Signal Strength: 100%

Status: Completed

IP Address: 192.168.2.82

Connect to wireless Network:

Connect to wireless network

Connect Automatically: □

Figure 5-1 *Administrator Console Update*

Note that there are no text boxes in the user interface for ESSID and password. The console obtains these directly from the custom configuration file.

Sample Configuration Files

Wireless network with WPA2 encryption type (AP name is "DEV"):

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1

network={
    ssid="DEV"
    proto=RSN WPA
    key_mgmt=WPA-PSK
    pairwise=CCMP TKIP
    group=CCMP TKIP
    psk="my secret password"
}
```

Open wireless network (AP Name is DEV_Open):

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1
network={
    ssid="DEV_Open"
    key_mgmt=NONE
}
```

Wireless network with WEP encryption type (AP Name is WEP128):

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
ap_scan=1

network={
    ssid="WEP128"
    key_mgmt=NONE
    wep_key0= "my secret password "
    wep_tx_keyidx=0
    priority=5
}
```

Configuration file with multiple network blocks:

```
# Simple case: WPA-PSK, PSK as an ASCII passphrase, allow all valid ciphers
network={
    ssid="RFID_TNV"
    psk="123456789"
    priority=1
}
network={
    ssid="RFID_TNV_WPA/WPA2"
    psk="123456789"
    priority=2
}
```

Refer to http://linux.die.net/man/5/wpa_supplicant.conf for further examples.

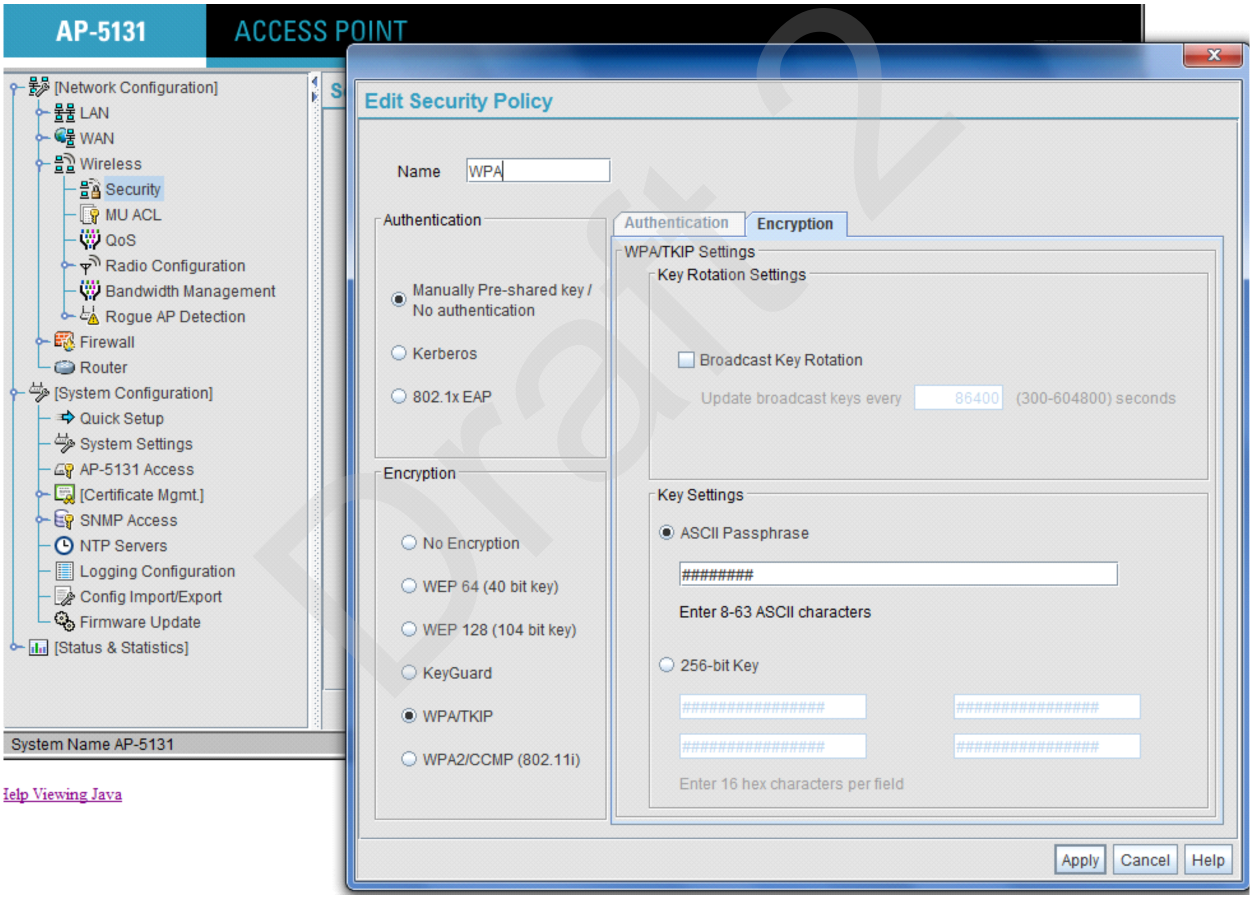
Preferred Configurations for Access Points

The FX7500 reader supports WPA/WPA2 (http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) and also WEP128 (http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) by default over the **Administrator Console**.

Other supported protocols are explained in previous sections. This section provides details on the preferred configurations for access points.

AP: Zebra AP 5131

Network Type: WPA/TKIP



Edit Security Policy

Name: WPA

Authentication

● Manually Pre-shared key / No authentication

○ Kerberos

○ 802.1x EAP

Encryption

○ No Encryption

○ WEP 64 (40 bit key)

○ WEP 128 (104 bit key)

○ KeyGuard

● WPA/TKIP

○ WPA2/CCMP (802.11i)

Authentication | Encryption

WPA/TKIP Settings

Key Rotation Settings

□ Broadcast Key Rotation

Update broadcast keys every 86400 (300-604800) seconds

Key Settings

● ASCII Passphrase

########

Enter 8-63 ASCII characters

○ 256-bit Key

################ ################

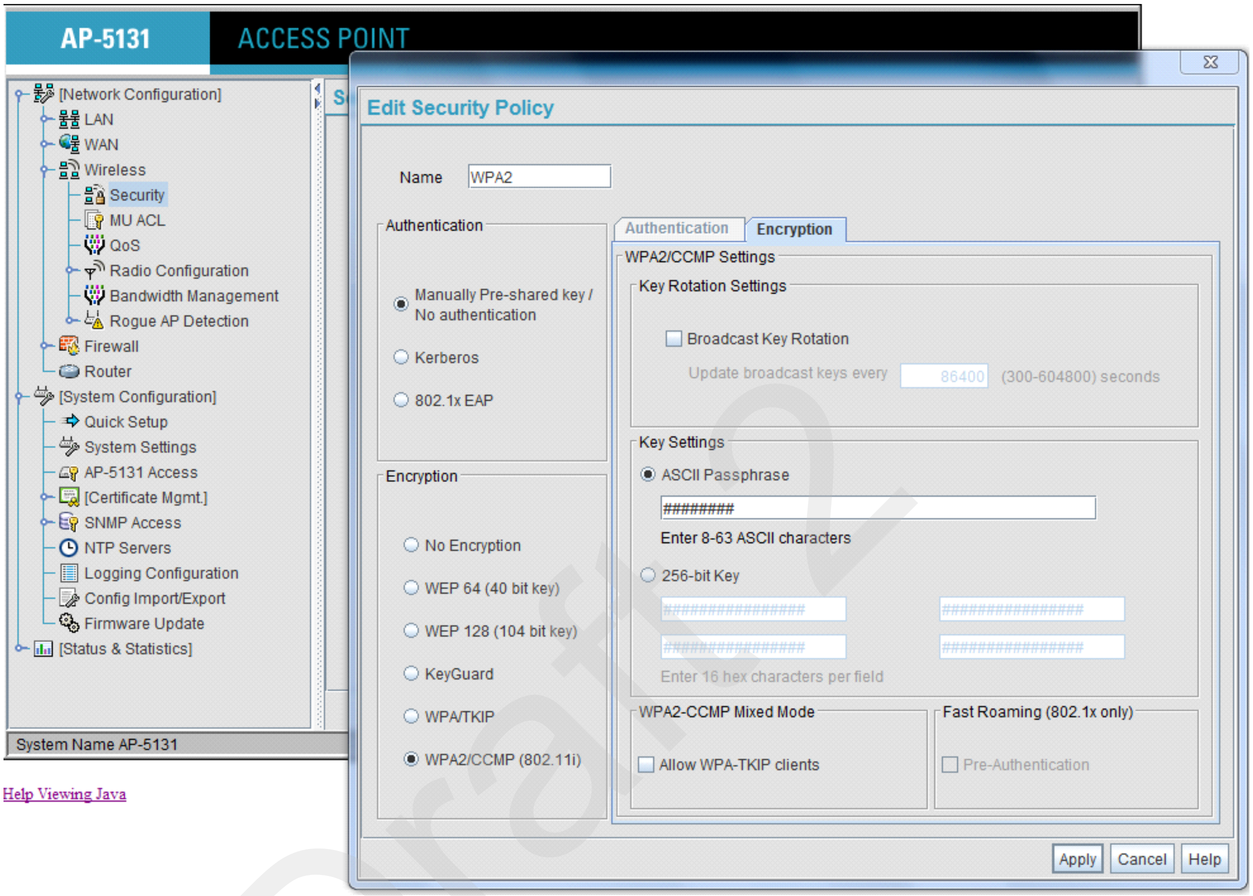
################ ################

Enter 16 hex characters per field

Figure 5-2 *AP 5131, WPA/TKIP*

Create a security policy **WPA** and select **WPA/TKIP** from the **Encryption** menu. Enter an ASCII password between 8 and 63 characters or 64 hex characters. Select **Apply** and associate the ESSID with a security policy.

Network Type: WPA2/CCMP



Name: WPA2

Authentication

● Manually Pre-shared key / No authentication
○ Kerberos
○ 802.1x EAP

Encryption

○ No Encryption
○ WEP 64 (40 bit key)
○ WEP 128 (104 bit key)
○ KeyGuard
○ WPA/TKIP
● WPA2/CCMP (802.11i)

WPA2/CCMP Settings

Key Rotation Settings

□ Broadcast Key Rotation
Update broadcast keys every 86400 (300-604800) seconds

Key Settings

● ASCII Passphrase
########
Enter 8-63 ASCII characters
○ 256-bit Key
################ ################
################ ################
Enter 16 hex characters per field

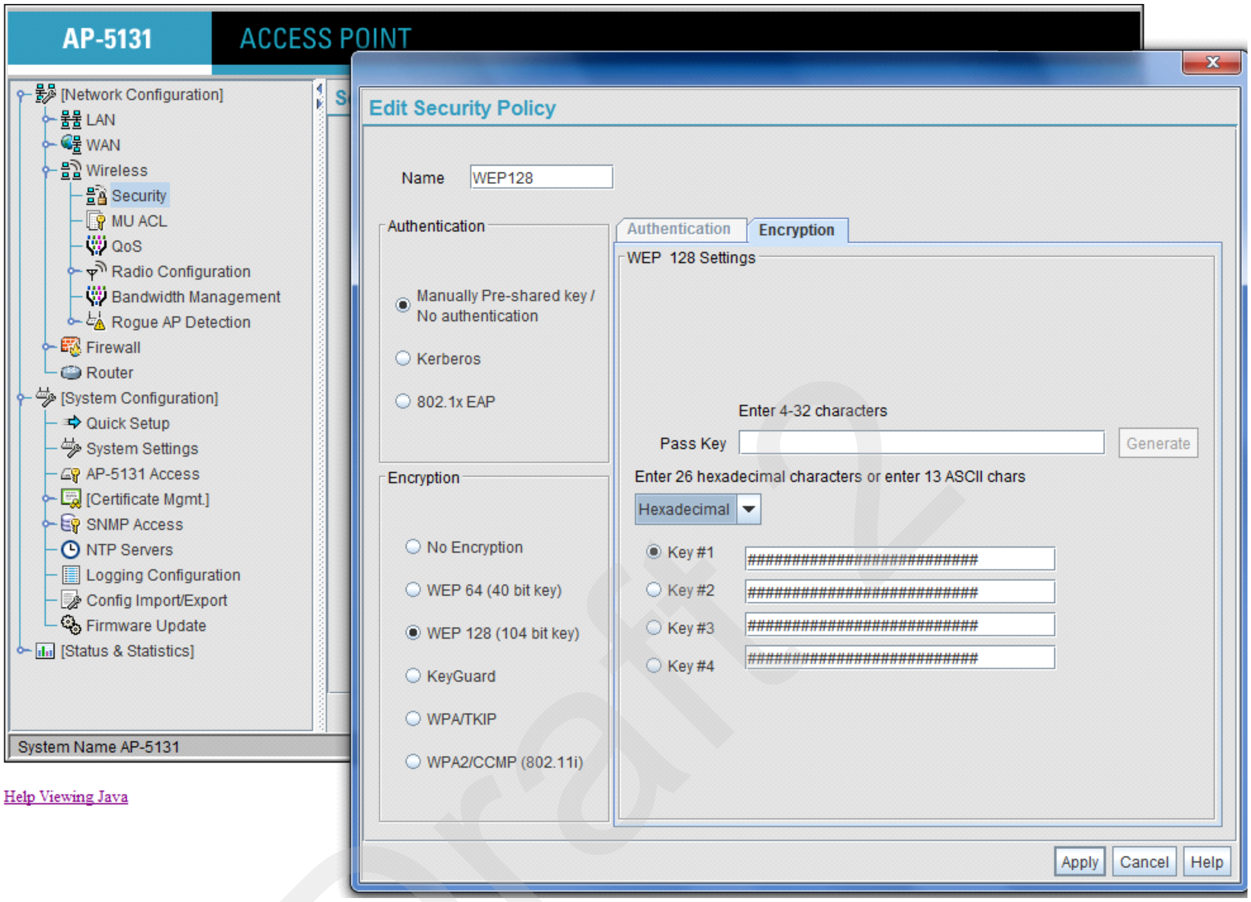
WPA2-CCMP Mixed Mode
□ Allow WPA-TKIP clients

Fast Roaming (802.1x only)
□ Pre-Authentication

Figure 5-3 *AP 5131, WPA2/CCMP*

Create a security policy **WPA2** and select **WPA/TKIP** from the **Encryption** menu. Enter an ASCII password between 8 and 63 characters or 64 hex characters. Select **Apply** and associate the ESSID with a security policy.

Network Type: WEP128



Edit Security Policy

Name: WEP128

Authentication

● Manually Pre-shared key / No authentication

○ Kerberos

○ 802.1x EAP

Encryption

○ No Encryption

○ WEP 64 (40 bit key)

● WEP 128 (104 bit key)

○ KeyGuard

○ WPA/TKIP

○ WPA2/CCMP (802.11i)

WEP 128 Settings

Enter 4-32 characters

Pass Key:

Enter 26 hexadecimal characters or enter 13 ASCII chars

Hexadecimal

● Key #1 ##########################

○ Key #2 ##########################

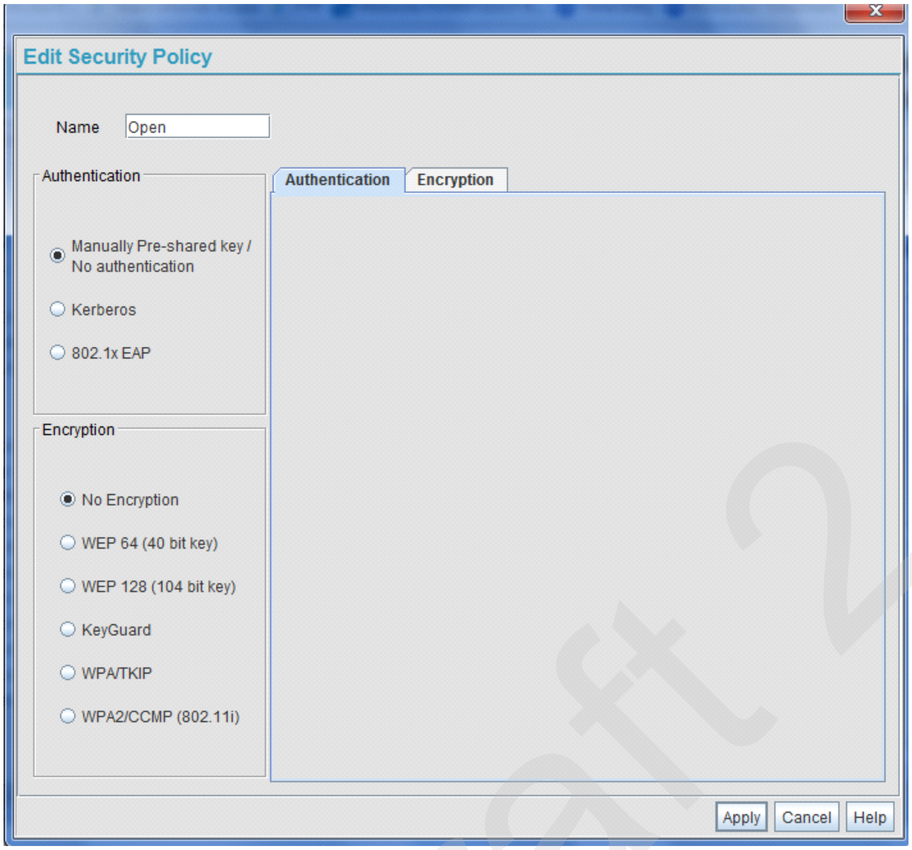
○ Key #3 ##########################

○ Key #4 ##########################

Figure 5-4 *AP 5131, WEP128*

Create a security policy **WEP128** and select **WEP** from the **Encryption** menu. Enter an ASCII password between 13 characters or HEX password of 26 characters. Select **Apply** and associate the ESSID with a security policy.

Open Network



Edit Security Policy

Name: Open

Authentication

● Manually Pre-shared key / No authentication

○ Kerberos

○ 802.1x EAP

Encryption

● No Encryption

○ WEP 64 (40 bit key)

○ WEP 128 (104 bit key)

○ KeyGuard

○ WPA/TKIP

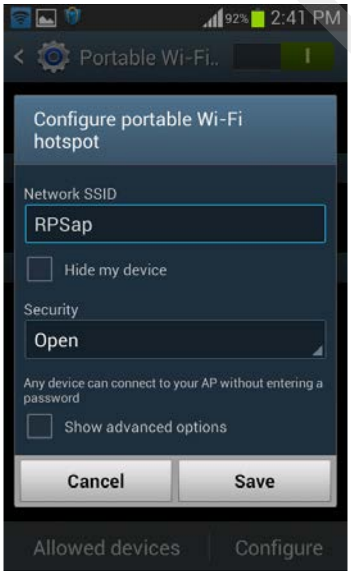
○ WPA2/CCMP (802.11i)

Figure 5-5 *Open Network*

AP: Android Device

Enable the wireless tethering from the settings menu.

Open Network



Configure portable Wi-Fi hotspot

Network SSID: RPSap

□ Hide my device

Security: Open

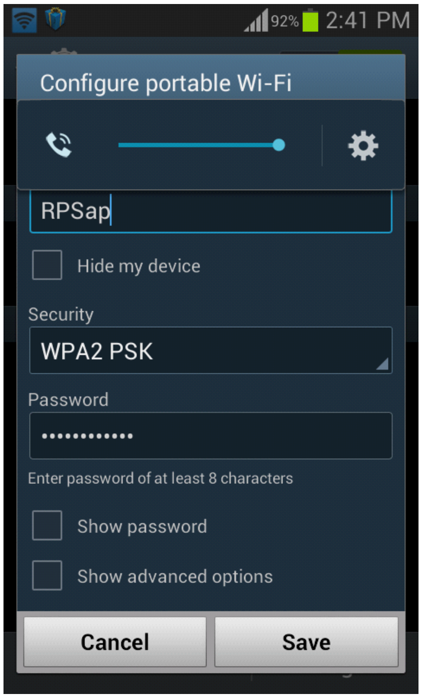
Any device can connect to your AP without entering a password

□ Show advanced options

Figure 5-6 *Android Device, Open Network*

Select **Open** from the **Security** drop-down menu and select **Save**.

Network Type: WPA2 PSK



Configure portable Wi-Fi

RPSap

□ Hide my device

Security: WPA2 PSK

Password: ••••••••••••

Enter password of at least 8 characters

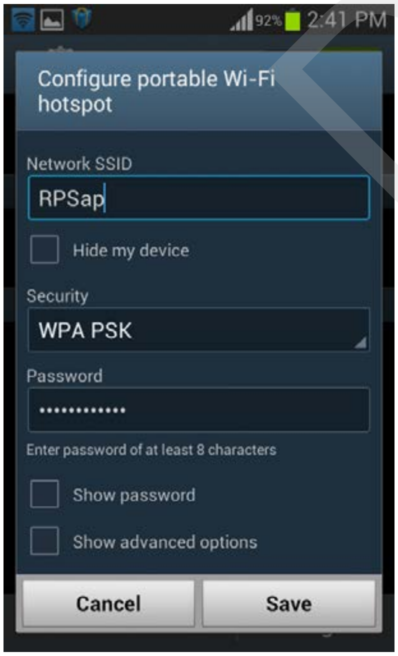
□ Show password

□ Show advanced options

Figure 5-7 *Android Device, WPA2 PSK*

Select **WPA2PSK** from the **Security** drop-down menu and enter a password. Select **Save** to start the wireless hotspot.

WPA PSK



Configure portable Wi-Fi hotspot

Network SSID: RPSap

□ Hide my device

Security: WPA PSK

Password: ••••••••••••

Enter password of at least 8 characters

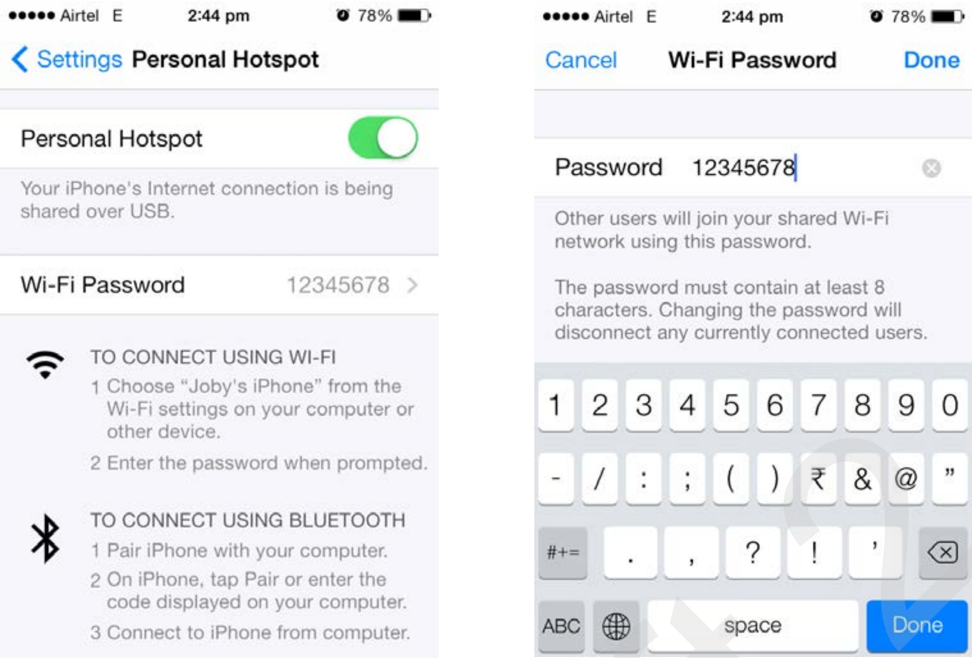
□ Show password

□ Show advanced options

Figure 5-8 *Android Device, WPA PSK*

Select **WPA PSK** from the **Security** drop-down menu and enter a password. Select **Save** to start the wireless hotspot.

iPhone



●●●●● Airtel E 2:44 pm 78%

Settings Personal Hotspot

Personal Hotspot

Your iPhone's Internet connection is being shared over USB.

Wi-Fi Password 12345678

TO CONNECT USING WI-FI

1 Choose "Joby's iPhone" from the Wi-Fi settings on your computer or other device.

2 Enter the password when prompted.

TO CONNECT USING BLUETOOTH

1 Pair iPhone with your computer.

2 On iPhone, tap Pair or enter the code displayed on your computer.

3 Connect to iPhone from computer.

●●●●● Airtel E 2:44 pm 78%

Cancel Wi-Fi Password Done

Password 12345678

Other users will join your shared Wi-Fi network using this password.

The password must contain at least 8 characters. Changing the password will disconnect any currently connected users.

Figure 5-9 *iPhone Device*

Select **Personal Hotspot** from the **Settings** menu and enter a password.

Copying Files to the Reader

See *Appendix E, Copying Files To and From the Reader* for instructions on copying files to **/apps** directory.

CHAPTER 6 APPLICATION DEVELOPMENT

Introduction

The primary communication to the Zebra FX7500 RFID reader is via the LLRP protocol interface on TCP port 5084. There are two ways to develop applications for the reader:

- Using the RFID3 API set included in the Zebra RFID SDK. The FX7500 reader supports host-based and embedded RFID3 APIs.
  - Java, C SDK support via the Eclipse IDE for host-based and embedded applications.
  - Microsoft .Net support via the Visual Studio 2005/2008 IDE for host-based applications only.
- Using the LLRP interface directly. Users can either use open source LLRP stacks, or develop their own LLRP stacks. The FX7500 supports host-based and embedded applications.

Reference Guides

The following resources can be found on http://www.zebra.com/support**:**

- *FX Series Reader Software Interface Control Guide,* p/n 72E-131718-xx
- *Programmer's Guide* provided with the Zebra RFID SDK. This introductory guide describes how to perform various functions using the RFID3 API set.
- *FX7500 Embedded SDK Installation Guide* provided with the Zebra RFID SDK.
- *FX7500 Embedded SDK Programmers Guide* provides instructions on creating new embedded applications.
- *Related Documents and Software on page xi* for more documentation regarding RFID API and application development.

CHAPTER 7 FIRMWARE UPGRADE

Introduction

This chapter provides reader firmware update information on using the web-based **Administrator Console**. The following methods are available to update the firmware on the FX7500 reader.

- Update using a USB drive.
- File-based update that allows uploading the firmware files from the PC (or a network location) to the reader and running the update.
- FTP / FTPS / SCP server-based update.

Use this procedure to update the following software components:

- uboot
- OS
- Reader Server Application (includes Radio API and Radio firmware)

Prerequisites

The following items are required to perform the update:

- Reader with power supply or POE connection
- Laptop (or other host computer)
- An Ethernet cable
- An FTP server
- Current firmware file examples:
    - OSUpdate.elf
    - response.txt
    - u-boot_*X.X.X.X*.bin (uBoot, *X.X.X.X* is a filename version)
    - uImage_ *X.X.X.X* (OS, *X.X.X.X* is a filename variable)
    - rootfs_ *X.X.X.X*.jffs2 (Root FileSystem, *X.X.X.X* is a filename variable)
    - platform_ *X.X.X.X*.tar.gz (Platform partition, *X.X.X.X* is a filename variable)

Refer to the release notes to determine which files were updated; not all of the files are updated in every release.

Failsafe Update

FX7500 provides true failsafe firmware update. Each partition (such as OS and platform) has an active and backup partition.

The firmware update process always writes the new images to the backup partition. This ensures that any power or network outages in the middle of firmware update does not prevent the reader from being operational. In the case of a firmware update failure, the power LED on the reader lights red.

Update Phases

The firmware update takes place in three phases:

- **Phase 1 -** The reader application retrieves the **response.txt** and **OSUpdate.elf** files from the ftp server.
- **Phase 2 -** The reader application shuts down and the **OSUpdate** starts. The files referenced in the **response.txt** file are retrieved from the FTP server and written to flash.
- **Phase 3 -** The reader resets after all partitions update successfully. It may also update the RFID firmware if it detects a different version in the platform partition.

A typical entry in the **Response.txt** is:

```
;platform partition
-t5 -fplatform_1.1.15.0.tar.gz -s8004561 -u8130879
```

✓ ***NOTE*** The Application Server, Radio API, and Radio firmware code all reside in the **Platform** partition.

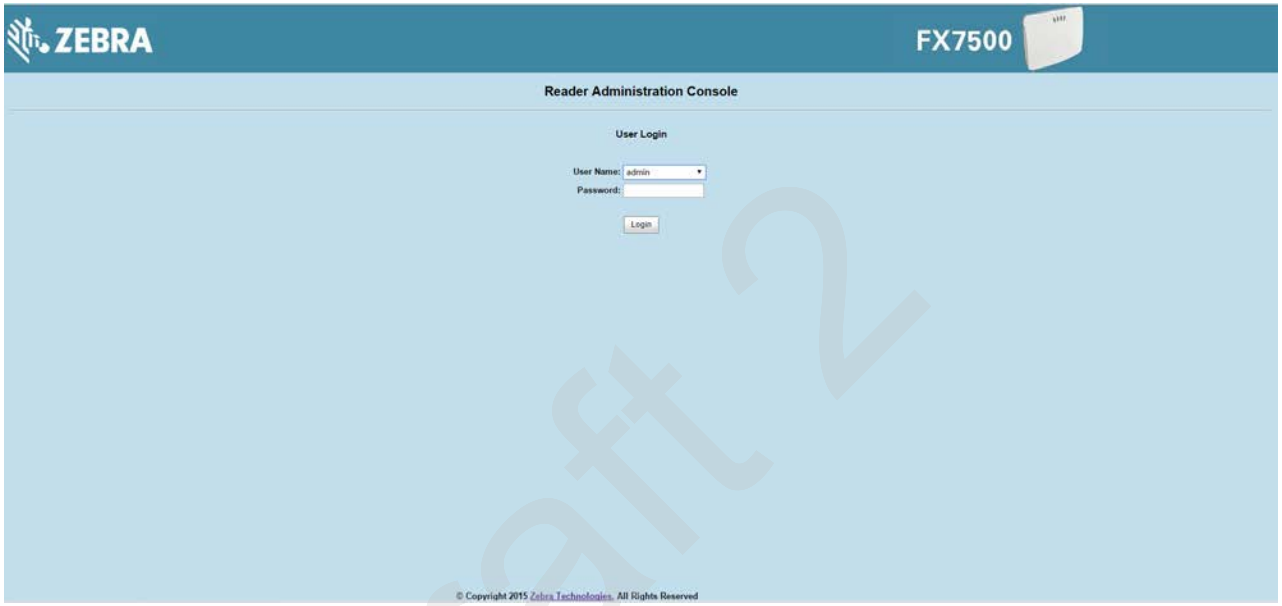
The **-t** parameter is the file type, **-f** is the name of the file, and **-s** the size. Ensure the file size is correct. "**;**" comments out the rest of the line.

Updating FX7500 Reader Software

Verifying Firmware Version

To verify that the FX7500 reader firmware is outdated:

1. Log into the reader. In the **User Login** window, enter **admin** in the **User Name:** field and enter **change** in the **Password:** field.



Reader Administration Console

User Login

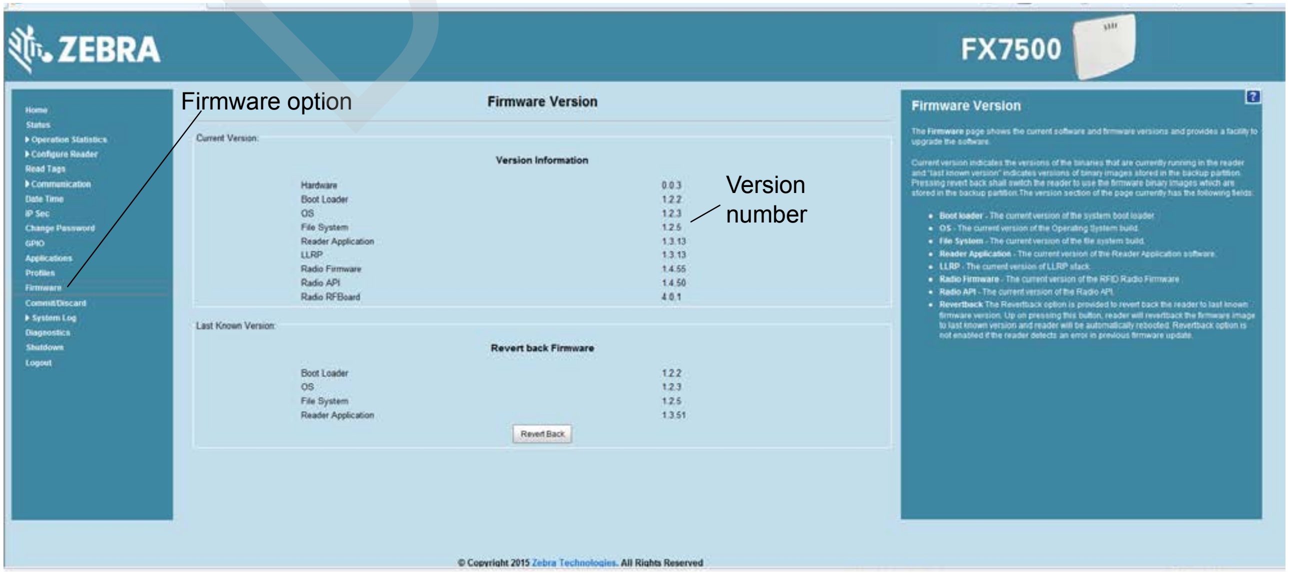
User Name: admin

Password:

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 7-1 *User Login Window*

2. Select **Firmware** on the left side panel to verify that the current version of reader software is outdated, e.g., 1.1.66.



Firmware option

Version number

Firmware Version

Current Version:

Version Information

Hardware	0.0.3
Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.13
LLRP	1.3.13
Radio Firmware	1.4.55
Radio API	1.4.50
Radio RFBoard	4.0.1

Last Known Version:

Revert back Firmware

Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.51

Firmware Version

The **Firmware** page shows the current software and firmware versions and provides a facility to upgrade the software.

Current version indicates the versions of the binaries that are currently running in the reader and "last known version" indicates versions of binary images stored in the backup partition. Pressing revert back shall switch the reader to use the firmware binary images which are stored in the backup partition.The version section of the page currently has the following fields:

- **Boot loader** - The current version of the system boot loader.
- **OS** - The current version of the Operating System build.
- **File System** - The current version of the file system build.
- **Reader Application** - The current version of the Reader Application software.
- **LLRP** - The current version of LLRP stack.
- **Radio Firmware** - The current version of the RFID Radio Firmware
- **Radio API** - The current version of the Radio API.
- **Revertback** The Revertback option is provided to revert back the reader to last known firmware version. Up on pressing this button, reader will revertback the firmware image to last known version and reader will be automatically rebooted. Revertback option is not enabled if the reader detects an error in previous firmware update.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 7-2 *Firmware Version Window*

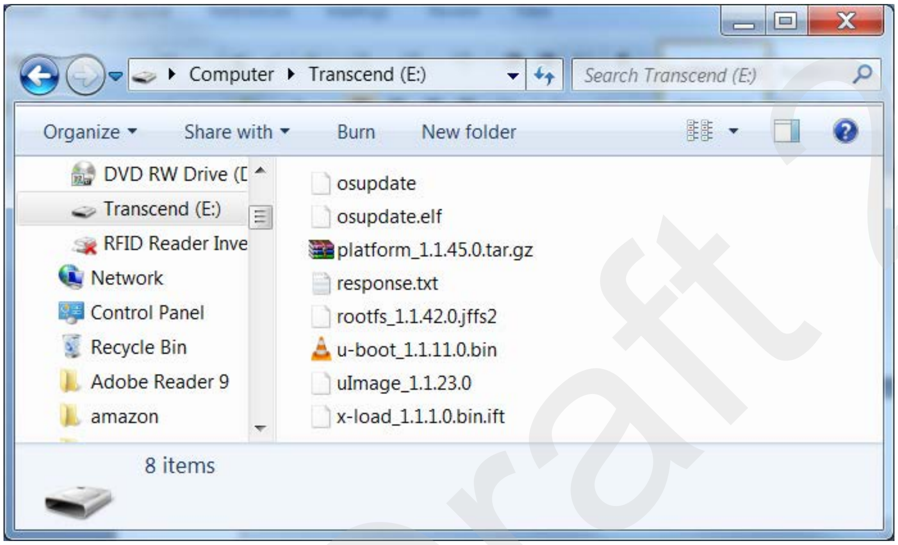
Updating Methods

Download the reader update files from http://www.zebra.com/support:, then use one of three methods to update the reader software to a later version, e.g., 1.1.45.0 or higher:

- *Update Using a USB Drive (Recommended)*
- *File-Based Update on page 7-6*
- *FTP-Based Update on page 7-8*

Update Using a USB Drive (Recommended)

1. Copy all reader update files into the root folder of the USB drive.



osupdate
osupdate.elf
platform_1.1.45.0.tar.gz
response.txt
rootfs_1.1.42.0.jffs2
u-boot_1.1.11.0.bin
uImage_1.1.23.0
x-load_1.1.1.0.bin.ift

Figure 7-3 *USB Drive Root Folder*

2. Insert the USB drive into the USB host port of the FX7500 RFID reader.

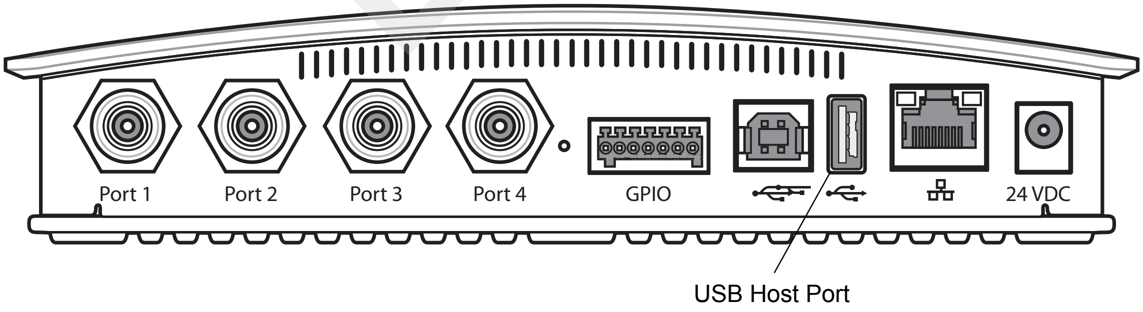


Figure 7-4 *USB Host Port Window*

The reader starts the update process in 5 - 7 seconds, and indicates progress as follows:

- The reader continuously blinks the Power LED red.
- The reader blinks all four LEDs orange once.
- The reader Power LED remains steady orange.
- The reader Power LED settles to a steady green to indicate that the update is complete.

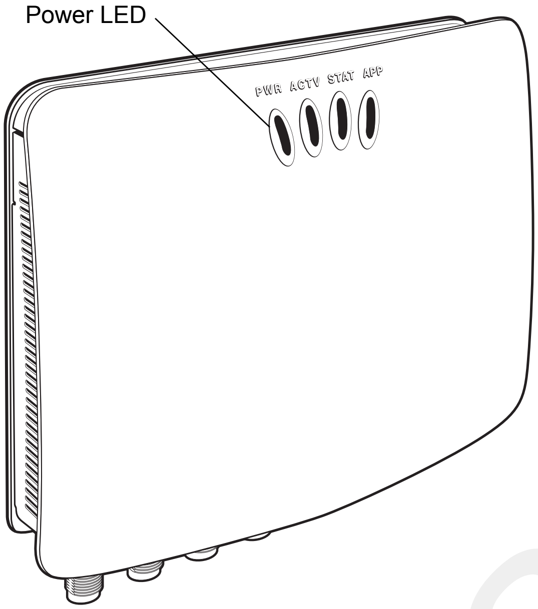
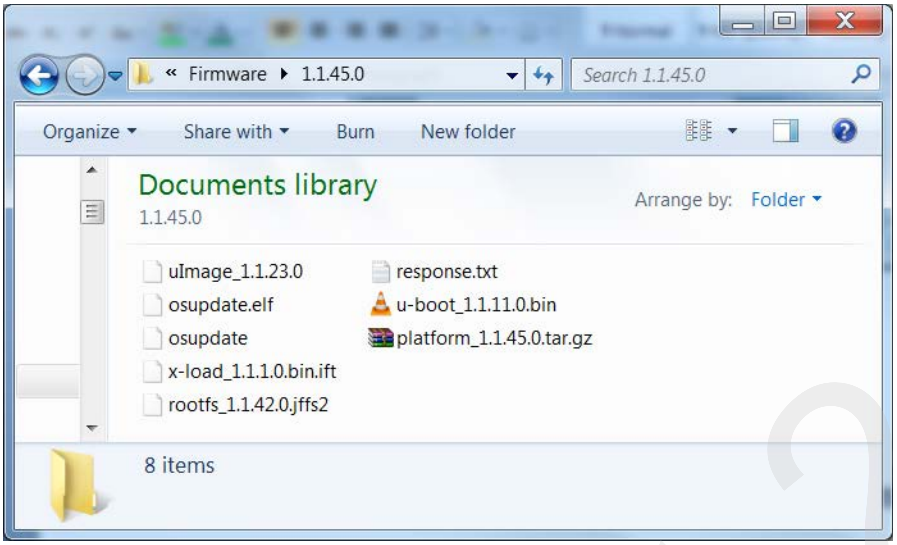


Figure 7-5 *Reader LEDs*

File-Based Update

1. Copy all reader update files into any folder on a host computer.



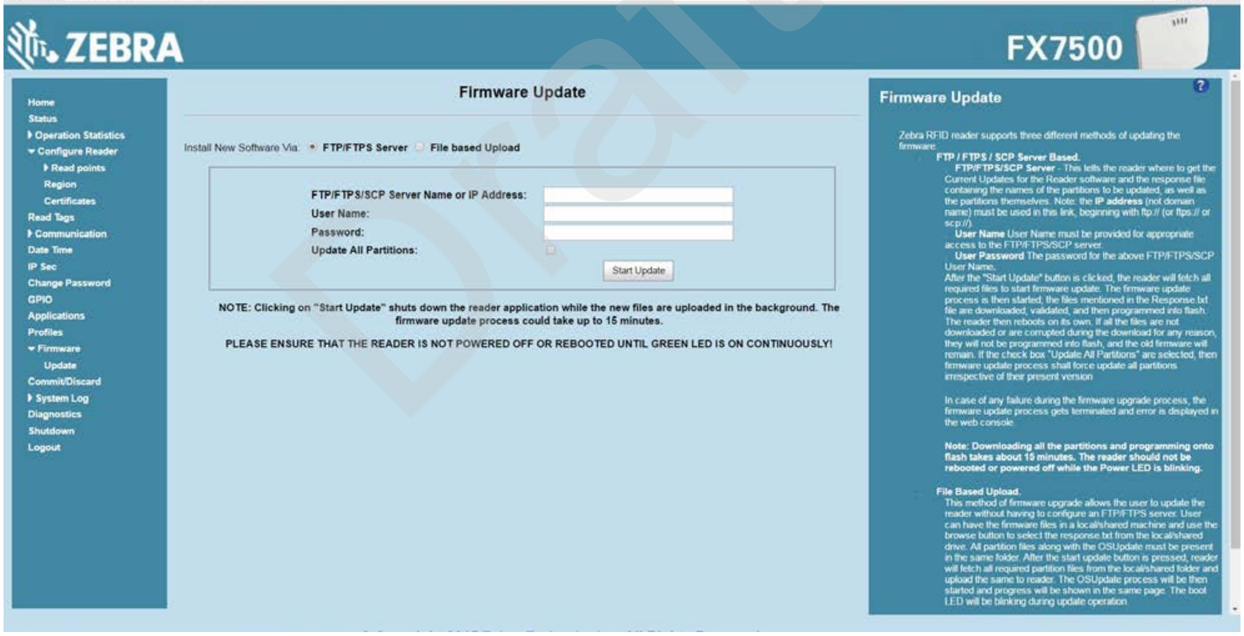
Documents library
1.1.45.0

uImage_1.1.23.0
osupdate.elf
osupdate
x-load_1.1.1.0.bin.ift
rootfs_1.1.42.0.jffs2
response.txt
u-boot_1.1.11.0.bin
platform_1.1.45.0.tar.gz

8 items

Figure 7-6 *Host Computer Folder*

2. Log into the reader and navigate to the **Firmware Update** page.



Firmware Update

Install New Software Via: ● FTP/FTPS Server ○ File based Upload

FTP/FTPS/SCP Server Name or IP Address:
User Name:
Password:
Update All Partitions: □

NOTE: Clicking on "Start Update" shuts down the reader application while the new files are uploaded in the background. The firmware update process could take up to 15 minutes.

PLEASE ENSURE THAT THE READER IS NOT POWERED OFF OR REBOOTED UNTIL GREEN LED IS ON CONTINUOUSLY!

Firmware Update

Zebra RFID reader supports three different methods of updating the firmware:

FTP / FTPS / SCP Server Based.

FTP/FTPS/SCP Server - This tells the reader where to get the Current Updates for the Reader software and the response file containing the names of the partitions to be updated, as well as the partitions themselves. Note: the **IP address** (not domain name) must be used in this link, beginning with ftp:// (or ftps:// or scp://).

User Name User Name must be provided for appropriate access to the FTP/FTPS/SCP server.

User Password The password for the above FTP/FTPS/SCP User Name.

After the "Start Update" button is clicked, the reader will fetch all required files to start firmware update. The firmware update process is then started; the files mentioned in the Response.txt file are downloaded, validated, and then programmed into flash. The reader then reboots on its own. If all the files are not downloaded or are corrupted during the download for any reason, they will not be programmed into flash, and the old firmware will remain. If the check box "Update All Partitions" are selected, then firmware update process shall force update all partitions irrespective of their present version

In case of any failure during the firmware upgrade process, the firmware update process gets terminated and error is displayed in the web console

Note: Downloading all the partitions and programming onto flash takes about 15 minutes. The reader should not be rebooted or powered off while the Power LED is blinking.

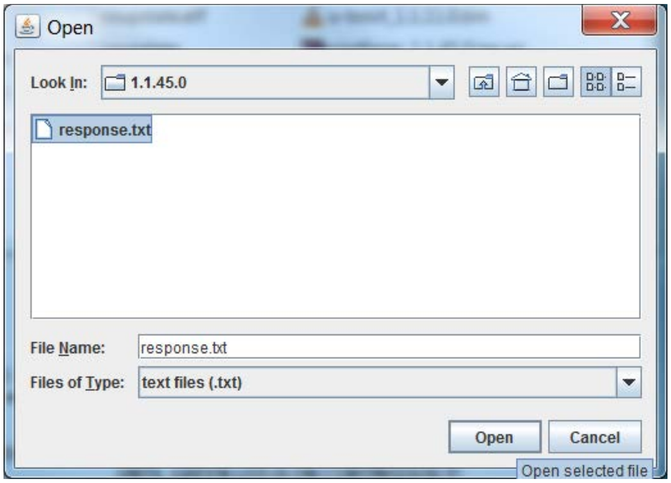
File Based Upload.

This method of firmware upgrade allows the user to update the reader without having to configure an FTP/FTPS server. User can have the firmware files in a local/shared machine and use the browse button to select the response.txt from the local/shared drive. All partition files along with the OSUpdate must be present in the same folder. After the start update button is pressed, reader will fetch all required partition files from the local/shared folder and upload the same to reader. The OSUpdate process will be then started and progress will be shown in the same page. The boot LED will be blinking during update operation

Figure 7-7 *Firmware Update Window*

3. Select **File based Upload**.

4. Click on **Browse** and navigate to the folder that contains the firmware update files.



Look In: 1.1.45.0

response.txt

File Name: response.txt

Files of Type: text files (.txt)

Figure 7-8 *Browsing Update Files*

5. Select **response.txt** and click **Open**.

6. Click **Start Update**. The reader starts the update process and displays the update status as follows:

   - The reader continuously blinks the Power LED red.
   - The reader blinks all 4 LEDs orange once.
   - The reader Power LED remains steady orange.
   - The reader Power LED settles to a steady green to indicate that the update is complete.

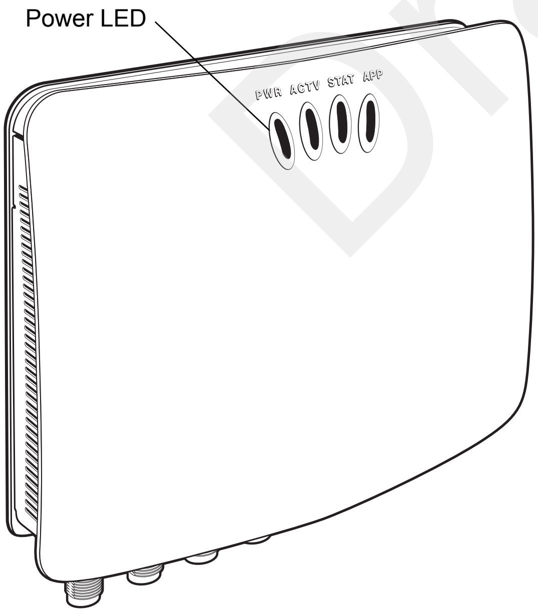


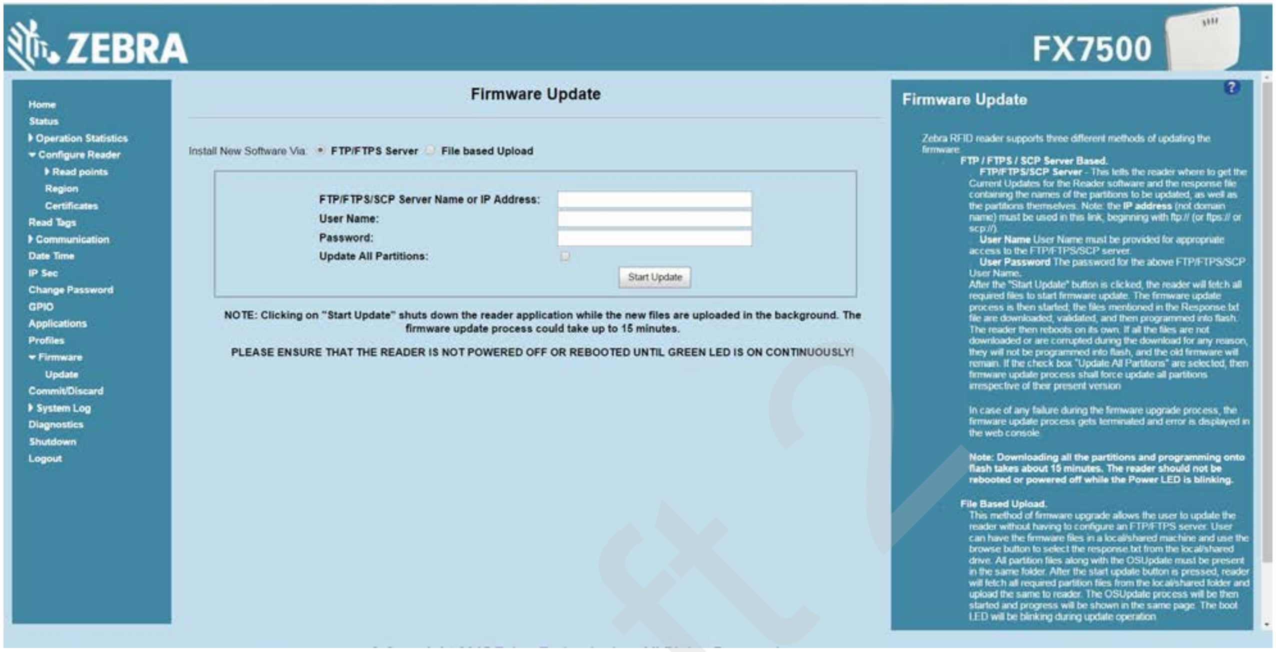
Figure 7-9 *Reader LEDs*

When the update completes, the reader reboots and returns to the FX7500 login screen.

FTP-Based Update

Copy all the update files into an appropriate FTP location.

1. Log into the reader and navigate to the **Firmware Update** page.



Firmware Update

Install New Software Via: ● FTP/FTPS Server ○ File based Upload

FTP/FTPS/SCP Server Name or IP Address:
User Name:
Password:
Update All Partitions: □

NOTE: Clicking on "Start Update" shuts down the reader application while the new files are uploaded in the background. The firmware update process could take up to 15 minutes.

PLEASE ENSURE THAT THE READER IS NOT POWERED OFF OR REBOOTED UNTIL GREEN LED IS ON CONTINUOUSLY!

Firmware Update

Zebra RFID reader supports three different methods of updating the firmware:

FTP / FTPS / SCP Server Based.

FTP/FTPS/SCP Server - This tells the reader where to get the Current Updates for the Reader software and the response file containing the names of the partitions to be updated, as well as the partitions themselves. Note: the **IP address** (not domain name) must be used in this link, beginning with ftp:// (or ftps:// or scp://).

User Name User Name must be provided for appropriate access to the FTP/FTPS/SCP server.

User Password The password for the above FTP/FTPS/SCP User Name.

After the "Start Update" button is clicked, the reader will fetch all required files to start firmware update. The firmware update process is then started; the files mentioned in the Response.txt file are downloaded, validated, and then programmed into flash. The reader then reboots on its own. If all the files are not downloaded or are corrupted during the download for any reason, they will not be programmed into flash, and the old firmware will remain. If the check box "Update All Partitions" are selected, then firmware update process shall force update all partitions irrespective of their present version

In case of any failure during the firmware upgrade process, the firmware update process gets terminated and error is desplayed in the web console

Note: Downloading all the partitions and programming onto flash takes about 15 minutes. The reader should not be rebooted or powered off while the Power LED is blinking.

File Based Upload.

This method of firmware upgrade allows the user to update the reader without having to configure an FTP/FTPS server. User can have the firmware files in a local/shared machine and use the browse button to select the response.txt from the local/shared drive. All partition files along with the OSUpdate must be present in the same folder. After the start update button is pressed, reader will fetch all required partition files from the local/shared folder and upload the same to reader. The OSUpdate process will be then started and progress will be shown in the same page. The boot LED will be blinking during update operation

Figure 7-10 *Firmware Update Window*

2. Select **FTP/FTPS Server**.
3. Enter the FTP location where the files are located.
4. Enter the **User Name** and **Password** for the FTP server login.
5. Click **Start Update**. The reader starts the update process and displays the update status as follows:
   - The reader continuously blinks the Power LED red.
   - The reader blinks all 4 LEDs orange once.
   - The reader Power LED remains steady orange.
   - The reader Power LED settles to a steady green to indicate that the update is complete.

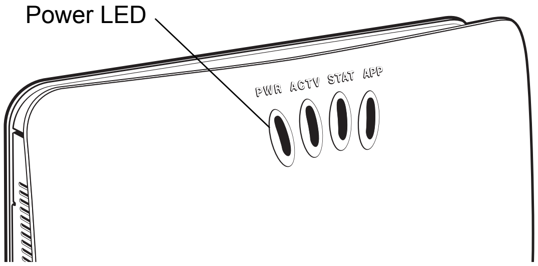


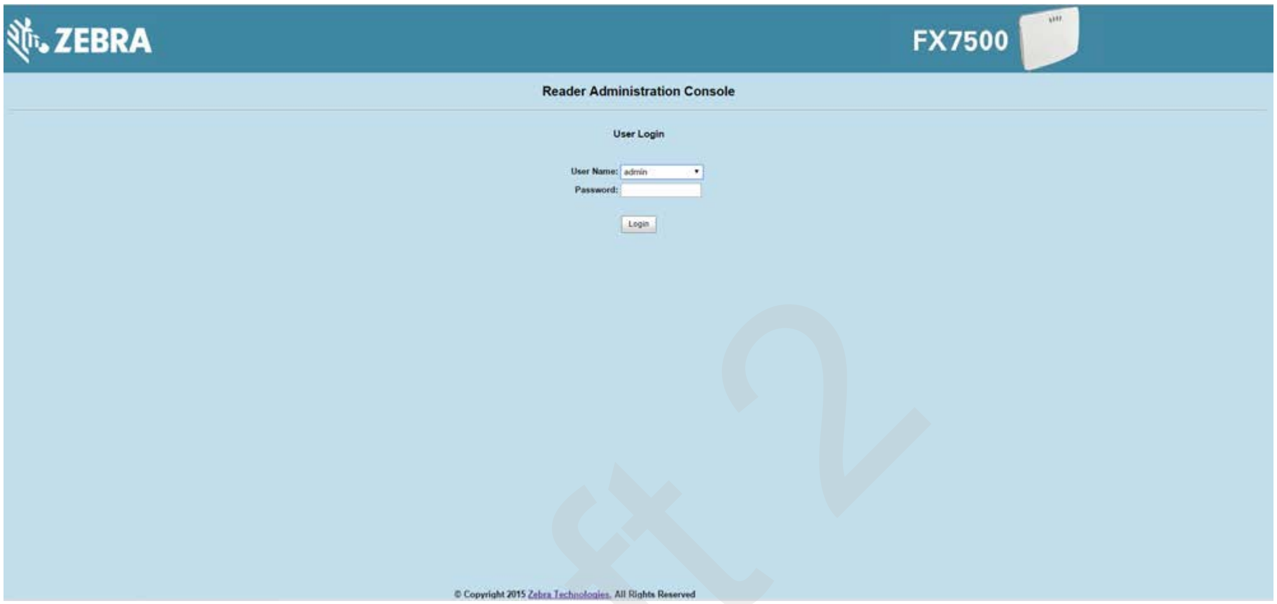
Figure 7-11 *Reader LEDs*

When the update completes, the reader reboots and returns to the FX7500 login screen.

Verifying Firmware Version

To verify reader update success:

1. Log into the reader. In the **User Login** window, enter **admin** in the **User Name:** field and enter **change** in the **Password:** field.



Reader Administration Console

User Login

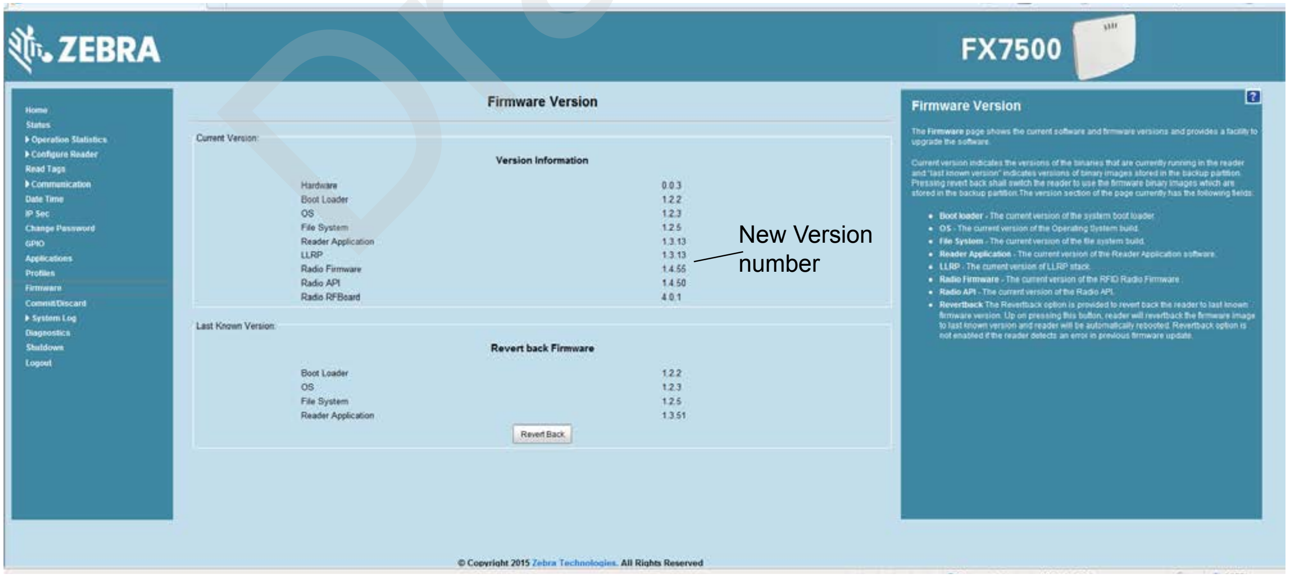
User Name: admin

Password:

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 7-12 *User Login Window*

2. Select **Firmware** on the left side panel to verify that the current version of reader software is the new version number, e.g., 1.1.68, which indicates that the update was successful.



Firmware Version

Current Version:

Version Information

Hardware	0.0.3
Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.13
LLRP	1.3.13
Radio Firmware	1.4.55
Radio API	1.4.50
Radio RFBoard	4.0.1

Last Known Version:

Revert back Firmware

Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.51

New Version number

Firmware Version

The **Firmware** page shows the current software and firmware versions and provides a facility to upgrade the software.

Current version indicates the versions of the binaries that are currently running in the reader and "last known version" indicates versions of binary images stored in the backup partition. Pressing revert back shall switch the reader to use the firmware binary images which are stored in the backup partition.The version section of the page currently has the following fields:

- **Boot loader** - The current version of the system boot loader.
- **OS** - The current version of the Operating System build.
- **File System** - The current version of the file system build.
- **Reader Application** - The current version of the Reader Application software.
- **LLRP** - The current version of LLRP stack.
- **Radio Firmware** - The current version of the RFID Radio Firmware.
- **Radio API** - The current version of the Radio API.
- **Revertback** The Revertback option is provided to revert back the reader to last known firmware version. Up on pressing this button, reader will revertback the firmware image to last known version and reader will be automatically rebooted. Revertback option is not enabled if the reader detects an error in previous firmware update.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure 7-13 *Firmware Version Window*

CHAPTER 8 TROUBLESHOOTING

Table 8-1 provides FX7500 troubleshooting information.

Table 8-1 *Troubleshooting*

Problem/Error	Possible Causes	Possible Solutions
Reader error LED lights after the reader is in operation.	The CPU cannot communicate.	Refer to the system log for error messages.
Reader error LED stays lit on power up.	An error occurred during the power up sequence.	Refer to the system log for error messages.
Cannot access the **Administrator Console**.	User name and password is unknown.	The default user name is **admin** and the default password is **change**. To change the user name and password, see *Communications Connections on page 3-5*.
Reader is not reading tags.	The tag is out of its read range.	Move the tag into read range. See *Read Tags on page 4-30*.
	Antennas are not connected.	Connect antennas.
	Tags are damaged.	Confirm that tags are good.
	Tags are not EPCgen2.	Confirm that tags are EPCgen2.
	If reading with the reader's web page, Java JRE 1.6 or later is not installed.	Install Java JRE 1.6.
Cannot connect to the reader.	The IP address is unknown.	See *Communications Connections on page 3-5* to view the IP address, or use the host name to connect to the reader.

Table 8-1 *Troubleshooting (Continued)*

Problem/Error	Possible Causes	Possible Solutions
Certain real time applications are no longer functional.	The node address, IP address, or other reader configuration parameter(s) were changed using the **Administrator Console**, and the application expects the previous configuration.	Update the settings within the application. Refer to the application manual.
	The user closed the browser without logging out of the **Administrator Console**, so other applications cannot connect to the reader.	Log out of the **Administrator Console**. The applications can use the **Force Login** option to log in even when the user closes the browser without logging out. **Force Login** option is supported for the administrative user.
Cannot log into **Administrator Console**.	The user forgot the password.	Press and hold the reset button for more than 8 seconds. This resets the reader configuration to factory defaults, including the password. This also removes the contents of the **apps** partition.
Unable to add SNTP server, reader returning error: **Error: Cannot find the specified Host Address**	SNTP server is not reachable.	Ensure the SNTP server is accessible.
	SNTP server name is not resolvable via DNS server.	Ensure the DNS server name is configured in TCP/IP configuration.
	DNS server is not reachable.	Ensure the DNS server is accessible.
Operation failed.	A user operation did not complete, typically due to invalid input.	Validate all inputs and retry the operation. If it is not successful, see *Service Information on page xii*.
Invalid User Name and/or Password - Try again.	The user name and/or password were not found in the system, or do not match the current user registry.	Accurately retype login information. If this is not successful, see *Service Information on page xii*.
Session has Timed-out - Log in again.	The current session was inactive beyond the time-out period (15 minutes), so the system automatically logged out.	Log in again. As a security precaution to protect against unauthorized system access, always log out of the system when finished.

Table 8-1 *Troubleshooting (Continued)*

Problem/Error	Possible Causes	Possible Solutions
User name is not correct.	The user name does not match the current user registry (illegal characters, too long, too short, unknown, or duplicate).	Accurately retype the user name.
	User forgot the user ID. Web console supports the following users: - **Admin** (default password is **change**) - **Guest** (no password required) - **rfidadm** - supported over SSH,FTP/FTPS, SCP, but not over **Administrator Console.**	Reset the reader to factory defaults and select **Admin** for user name and enter **change** in the password field to regain access. See *Reset to Factory Defaults LED Sequence on page 3-11*.
Not a legal IP address (1.0.0.0 - 255.255.255.255). Cannot reach the specified IP address. The SNMP Host Link is not valid.	The IP address entered is either formatted inaccurately or cannot be accessed (pinged).	Accurately retype the IP address, and make sure the host device is connected and online. If this is not successful, see *Service Information on page xii.*
Invalid network mask.	The network mask entered is not formatted correctly.	Confirm the correct network mask from the network administrator and enter it correctly.
Invalid SNMP version number.	The version number for SNMP protocol is not a supported version.	Use version number 1 for SNMP version 1, and 2 for SNMP version 2c.
Invalid description.	The description contained invalid characters (<,>,or').	Correct the description.
Invalid password.	The password does not match the current user registry (illegal characters, too long, or too short).	Accurately retype the password.
	User forgot the password.	Reset the reader to factory defaults and select **Admin** for user name and enter **change** in the password field to regain access. See *Reset to Factory Defaults LED Sequence on page 3-11*.
The name, serial number, or IP address entered already exists in the system.	The name, serial number, or IP address entered was already used.	Enter a unique value for the new name, serial number, or IP address.
Another administrator is currently logged in. Try again later.	The system does not allow more than one administrator to log in at a time.	Wait until the other administrator logs out (or times out) before logging in or override the current session with the new one.
Backup configuration file does not exist.	The system cannot revert to a backup configuration unless a backup file exists.	Commit the new configuration to create a backup file.

Table 8-1 *Troubleshooting (Continued)*

Problem/Error	Possible Causes	Possible Solutions
Failed to confirm the new password.	The system requires entering the password identically two times.	Accurately retype the password twice.
Network configuration change(s) have not been saved.	The user requested log out prior to committing/ discarding the changes made during the session.	Select one of the **Commit/Discard** options.
New password is the same as the old one.	The system requires entering a new password (different from the existing password) during the **Change Password** operation.	Enter a password that is different from the existing password.
Old password is not correct.	The system requires entering the existing password during the **Change Password** operation.	Accurately retype the existing password.
Unspecified error occurred - code: ####	A specific error message is missing for the given status code.	Note the code number, and contact Zebra support. See *Service Information on page xii*.
The requested page was not found. Internal Web Server Error.	The system experienced an internal web server error.	Contact Zebra support. See *Service Information on page xii*
Request method was NULL. No query string was provided.	The system does not permit executing a proxy program from the command line rather than the web server.	No action required. The system is reporting that this action is not permitted.
Content length is unknown.	The system cannot accept an incorrectly formatted HTTP POST request (from an unsupported browser application).	Use a GET request instead, or update the software.
Couldn't read complete post message.	The system stopped a POST operation before completion.	Retry the operation, and allow it to complete.
Unhandled reply type.	The system generated an unexpected value.	Contact Zebra support. See *Service Information on page xii*.
Failed to open port. Failed to connect. Failed to transmit. Failed to receive. Error during Receive of Command.	Error during receive of command.	Contact Zebra support. See *Service Information on page xii*.

Table 8-1 *Troubleshooting (Continued)*

Problem/Error	Possible Causes	Possible Solutions
Invalid Device Address.	The device address information (parent) is invalid, missing, or formatted inaccurately.	Contact Zebra support. See *Service Information on page xii*.
Command parsing state error. Missing argument for the command. Command internal type cast error. Missing operator. Unknown operator.	A command was formatted inaccurately.	Contact Zebra support. See *Service Information on page xii*.
The action must be confirmed.	The user must confirm the requested action before it is executed.	Select the confirmation option when issuing this request.
Invalid network adapter when navigating to the Bluetooth configuration page.	The Bluetooth dongle is not plugged in or not supported.	Plug in a supported Bluetooth dongle and refresh the browser.
Wireless scan error.	Wireless dongle is not plugged in or not supported.	Plug in a supported wireless dongle and repeat the wireless scan.
Unable to connect to the wireless network.	Access point is off or unreachable.	Turn on the access point and make sure it is accessible.
	Encryption type is not supported in the access point.	Use one of the following supported encryption types: WEP128, WPA/WPA2 and Open.
	The wireless page displays **Adapter not found**.	Connect the wireless adapter to the reader.
Wireless connection is complete, but no IP address.	No DHCP server is running in the network.	Add a DHCP server to the network.
OS update in progress.	Firmware update on the reader is ongoing. The current operation is not permitted.	Wait for the firmware update to complete and then retry the operation.
Cannot change password.	Cannot change password for guest.	Guest does not need a password to log in to the Administrator Console.

✓ ***NOTE*** If problems still occur, contact the distributor or call the local contact. See *page xii* for contact information.

APPENDIX A TECHNICAL SPECIFICATIONS

FX7500 Kits

KT-FX75004US-01 4-Port US Reader Kit

- FX7500-42310A30-US (4-port US reader)
- AN480-CL66100WR (wide-band AN-480 antenna)
- BRKT-70661-01R (antenna mounting bracket)
- CBLRD-1B4001800R (15-foot RF cable)
- 50-14000-159R (power supply)
- 23844-00-00R (US power cord)

KT-FX75002US-01 2-Port US Reader Kit

- FX7500-22310A30-US (2-port US reader)
- AN480-CL66100WR (wide-band AN-480 antenna)
- BRKT-70661-01R (antenna mounting bracket)
- CBLRD-1B4001800R (15-foot RF cable)
- 50-14000-159R (power supply)
- 23844-00-00R (US power cord)

KT-FX75004WR-01 4-Port Global Reader Kit

- FX7500-42315A30-US (4-port global reader)
- AN480-CL66100WR (wide-band AN-480 antenna)
- BRKT-70661-01R (antenna mounting bracket)
- CBLRD-1B4001800R (15-foot RF cable)
- 50-14000-159R (power supply)

KT-FX75002WR-01 2-Port Global Reader Kit

- FX7500-22315A30-US (2-port global reader)
- AN480-CL66100WR (wide-band AN-480 antenna)
- BRKT-70661-01R (antenna mounting bracket)
- CBLRD-1B4001800R (15-foot RF cable)
- 50-14000-159R (power supply)

Technical Specifications

The following tables summarize the RFID reader intended operating environment and technical hardware specifications.

Table A-1 *Technical Specifications*

Item	FX
Physical and Environmental Characteristics	
Dimensions	7.7 in. L x 5.9 in. W x 1.7 in. D (19.56 cm L x 14.99 cm W x 4.32 cm D)
Weight	1.9 lbs ± 0.1 lbs (0.86 kg +/- 0.05 kg)
Base Material	Die cast aluminum, sheet metal and plastic
Visual Status Indicators	Multi-color LEDs: Power, Activity, Status, and Applications
Mounting	Keyhole and standard VESA (75 mm x 75 mm)
FX Environmental Specifications	
Operational Temperature	-4° to +131° F / -20° to +55° C
Storage Temperature	-40° to +158° F / -40° to +70° C
Humidity	5 to 95% non-condensing
Shock and Vibration	MIL-STD-810G
Connectivity	
Communications	10/100 BaseT Ethernet (RJ45) w/ POE support USB Client (Type B), USB Host (Type A)
General Purpose I/O	2 inputs, 3 outputs, optically isolated (terminal block) External 12V ~ 48 VDC power available for GPIO
Power	POE or POE+ 12 VDC to 48 VDC, or 24 VDC Universal Power Supply
Antenna Ports	FX 7500-2: 2 mono-static ports (reverse polarity TNC) FX 7500-4: 4 mono-static ports (reverse polarity TNC)

Table A-1 *Technical Specifications (Continued)*

Item	FX
Hardware/OS and Firmware Management	
Memory	Flash 512 MB; DRAM 256 MB
Operating System	Linux
Firmware Upgrade	Web-based and remote firmware upgrade capabilities
Management Protocols	RM 1.0.1 (with XML over HTTP/HTTPS and SNMP binding)
Network Services	DHCP, HTTPS, FTPS, SFPT, SCP, SSH, HTTP, FTP, SNMP and NTP
Network Stack	IPv4, IPv6
Security	Transport Layer Security Ver. 1.2, FIPS 140-2 Level 1
Air Protocols	EPCglobal UHF Class 1 Gen2, ISO 18000-6C
Frequency (UHF Band)	Global Reader: 902 MHz to 928 MHz (Maximum, supports countries that use a part of this band) 865 MHz to 868 MHz US (only) Reader: 902 MHz to 928 MHz
Transmit Power Output	10dBm to +31.5dBm (POE+, 12V ~ 48V External DC, Universal 24 VDC Power Supply; +10dBm to +30.0dBm (POE)
Receive Sensitivity	-82dBm
IP Addressing	Static and Dynamic
Host Interface Protocol	LLRP v1.0.1
API Support	Host Applications – .NET, C and Java EMDK; Embedded Applications – C & Java SDK
Warranty	
The FX7500-4 and FX7500-2 are warranted against defects in workmanship and materials for a period of one year (12 months) from date of shipment, provided the product remains unmodified and is operated under normal and proper conditions. For the complete Zebra hardware product warranty statement, go to: http://www.zebra.com/warranty	
Recommended Services	
Support Services	Service from the Start Advance Exchange On-Site System Support Support
Advanced Services	RFID Design and Deployment Services

Cable Pinouts

10/100bT Ethernet / POE Connector

The 10/100BT Ethernet / POE connector is an RJ45 receptacle. This port complies with the IEE 802.3af specification for Powered Devices.

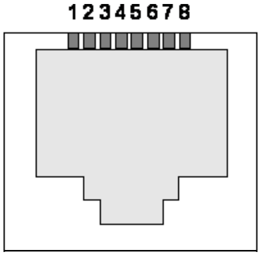


Figure A-1 *Ethernet Connections*

Table A-2 *10/100bT Ethernet / POE Connector Pinout*

Pin	Pin Name	Direction	Description	POE Mode A Function	POE Mode B Function
Pin 1	TX-P	O	TX Data Positive	Positive Vport	
Pin 2	TX-N	O	TX Data Negative	Positive Vport	
Pin 3	RX-P	I	RX Data Positive	Negative Vport	
Pin 4	NC	-	No Connect		Positive Vport
Pin 5	NC	-	No Connect		Positive Vport
Pin 6	RX_N	I	RX Data Negative	Negative Vport	
Pin 7	NC	-	No Connect		Negative Vport
Pin 8	NC	-	No Connect		Negative Vport

USB Client Connector

The USB Client port is supplied on a USB Type B connector.

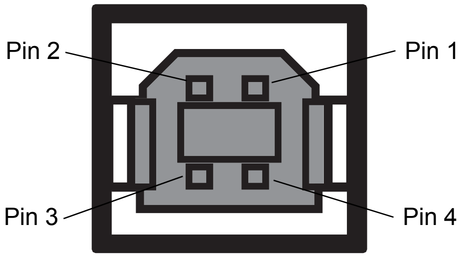


Figure A-2 *USB Client Connector*

Table A-3 *USB Client Port Connector Pinout*

Pin	Pin Name	Direction	Description
Pin 1	5.0V_USB	I	5.0V USB Power Rail
Pin 2	USB_DN	I/O	Data Negative
Pin 3	USB_DP	I/O	Data Positive
Pin 4	GND	-	Ground

USB Host Connector

The USB Host port is supplied on a USB Type A flag connector.

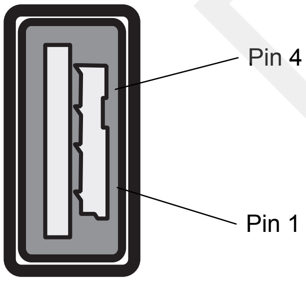


Figure A-3 *USB Host Connector (J22)*

Table A-4 *USB Host Port Connector (J22) Pinout*

Pin	Pin Name	Direction	Description
Pin 1	V_USB	I	5.0V USB Power Rail
Pin 2	USBH_DN	I/O	Data Negative Rail
Pin 3	USBH_DP	I/O	Data Positive Rail
Pin 4	GND	-	Ground

GPIO Port Connections

These plug terminal block types allow connecting and disconnecting individual wires independently. A single connector is used for both inputs and outputs. See *Table A-5* for pin descriptions.

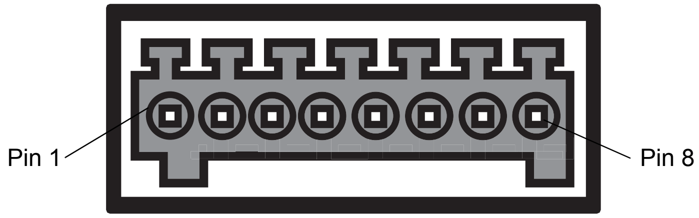


Figure A-4 *FX7500 RFID Reader GPIO Connection*

Table A-5 *GPIO Pin Outs*

Pin #	Pin Name	Direction	Description
1	+24V DC Power	O	Supplies +24V DC at up to 1 Amp
2	GP output #1	O	Signal for GP output #1
3	GP output #2	O	Signal for GP output #2
4	GP output #3	O	Signal for GP output #3
5	GND	-	Ground connection
6	GP input #1	I	Signal for GP input #1
7	GP input #2	I	Signal for GP input #2
8	GND	-	Ground connection

APPENDIX B STATIC IP CONFIGURATION

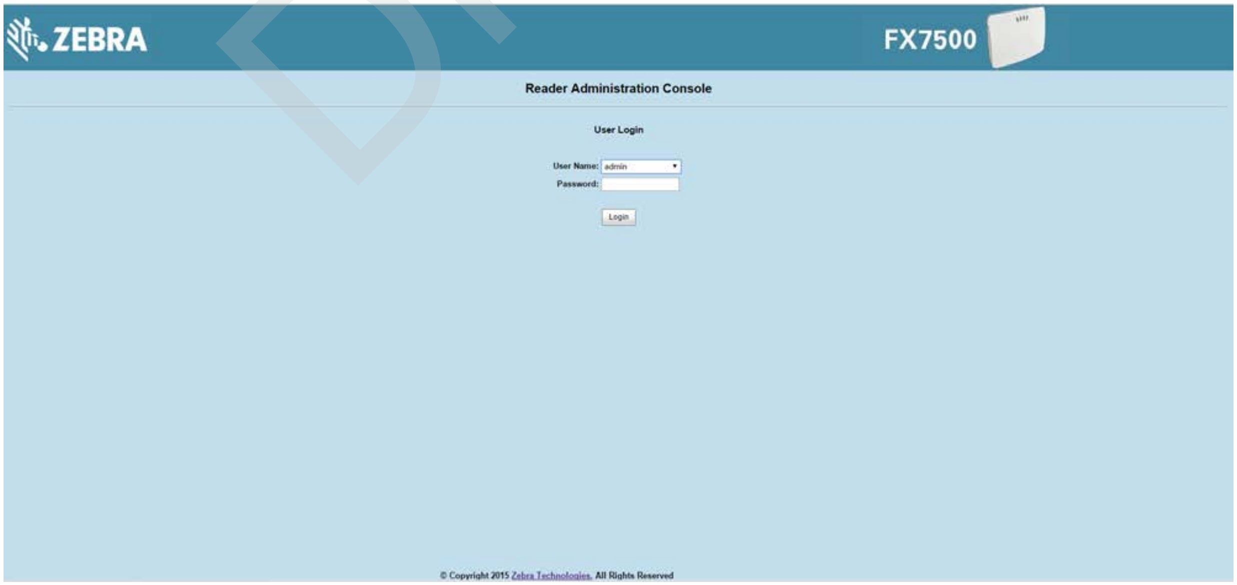
Introduction

This appendix describes three methods of setting the static IP address on an FX7500 RFID Reader.

Reader IP Address or Host Name is Known - Set the Static IP Using the Web Console

1. Browse the device using the host name, e.g., FX7500CD3B1E.

2. Log onto the device.



Reader Administration Console

User Login

User Name: admin

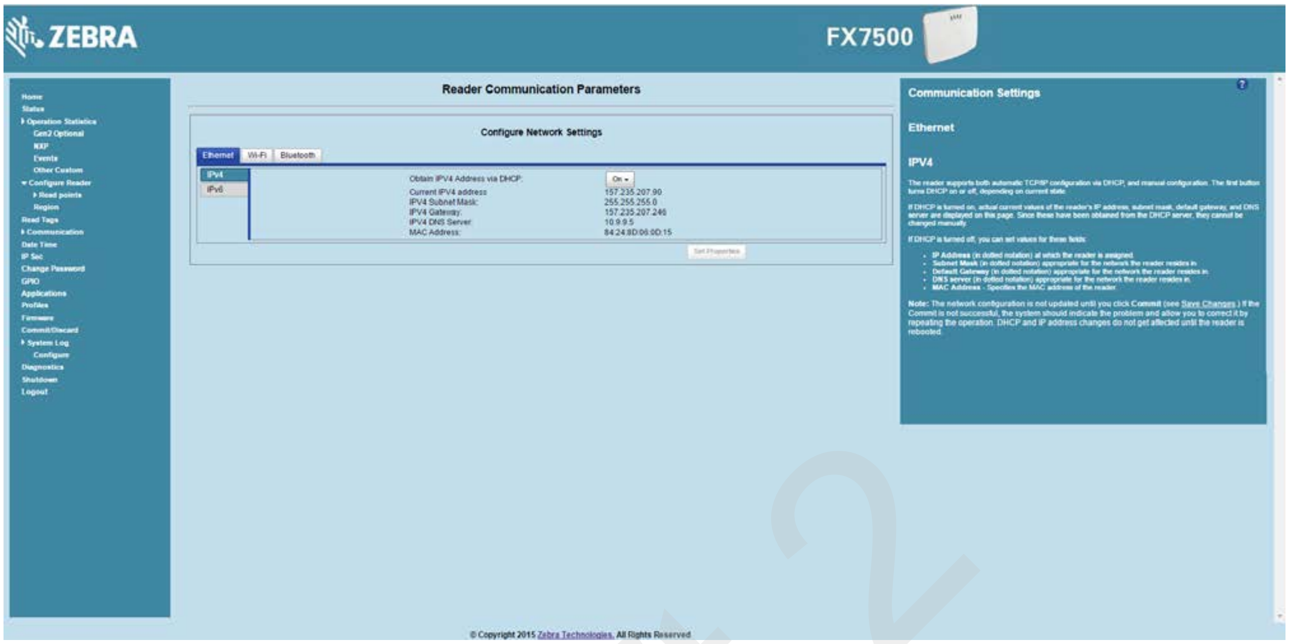
Password:

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure B-1 *Reader Administration Console Login Window*

3. Click **Communication**.

4. Set **Obtain IP Address via DHCP** to **Off** and enter all required information.



Reader Communication Parameters

Configure Network Settings

Obtain IPV4 Address via DHCP: On

Current IPV4 address 157.235.207.90

IPV4 Subnet Mask: 255.255.255.0

IPV4 Gateway: 157.235.207.246

IPV4 DNS Server: 10.9.9.5

MAC Address: 84:24:8D:06:0D:15

Communication Settings

Ethernet

IPV4

The reader supports both automatic TCP/IP configuration via DHCP, and manual configuration. The first button turns DHCP on or off, depending on current state.

If DHCP is turned on, actual current values of the reader's IP address, subnet mask, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

If DHCP is turned off, you can set values for these fields:

- **IP Address** (in dotted notation) at which the reader is assigned.
- **Subnet Mask** (in dotted notation) appropriate for the network the reader resides in.
- **Default Gateway** (in dotted notation) appropriate for the network the reader resides in.
- **DNS server** (in dotted notation) appropriate for the network the reader resides in.
- **MAC Address** - Specifies the MAC address of the reader.

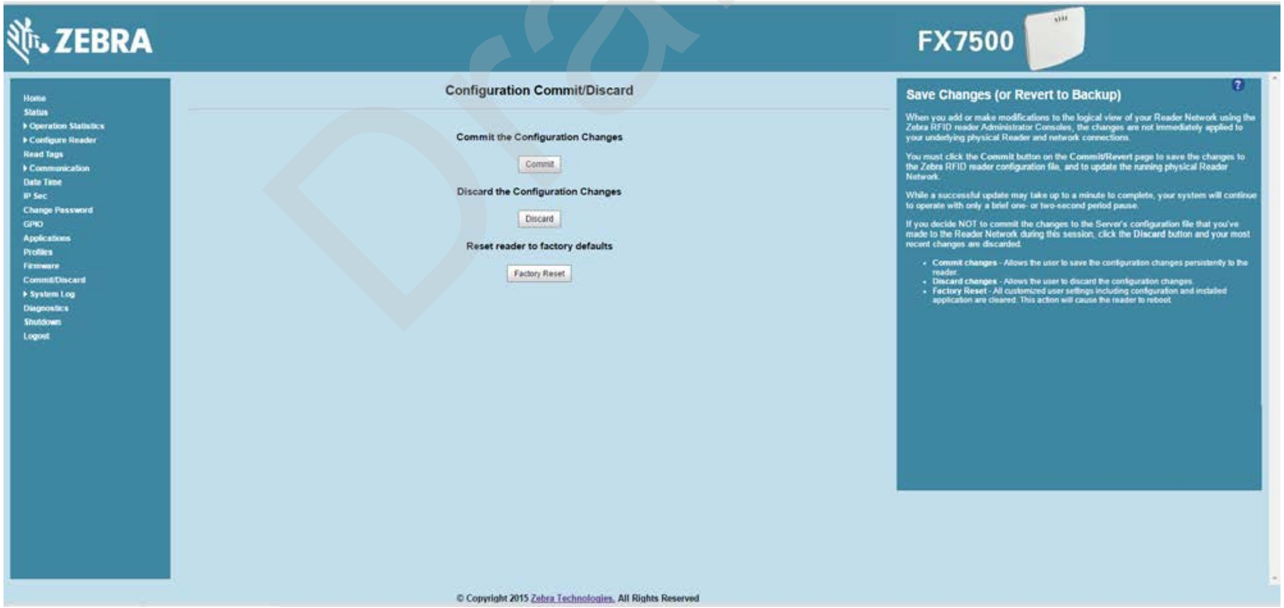
Note: The network configuration is not updated until you click **Commit** (see Save Changes.) If the Commit is not successful, the system should indicate the problem and allow you to correct it by repeating the operation. DHCP and IP address changes do not get affected until the reader is rebooted.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure B-2 *Reader Communication Parameters Window*

5. Click **Set Properties**. You can set a static IP that doesn't belong to this DHCP network.

6. Click **Commit/Discard**, then click the **Commit** button.



Configuration Commit/Discard

Commit the Configuration Changes

Discard the Configuration Changes

Reset reader to factory defaults

Save Changes (or Revert to Backup)

When you add or make modifications to the logical view of your Reader Network using the Zebra RFID reader Administrator Consoles, the changes are not immediately applied to your underlying physical Reader and network connections.

You must click the Commit button on the Commit/Revert page to save the changes to the Zebra RFID reader configuration file, and to update the running physical Reader Network.

While a successful update may take up to a minute to complete, your system will continue to operate with only a brief one- or two-second period pause.

If you decide NOT to commit the changes to the Server's configuration file that you've made to the Reader Network during this session, click the **Discard** button and your most recent changes are discarded.

- **Commit changes** - Allows the user to save the configuration changes persistently to the reader.
- **Discard changes** - Allows the user to discard the configuration changes.
- **Factory Reset** - All customized user settings including configuration and installed application are cleared. This action will cause the reader to reboot.

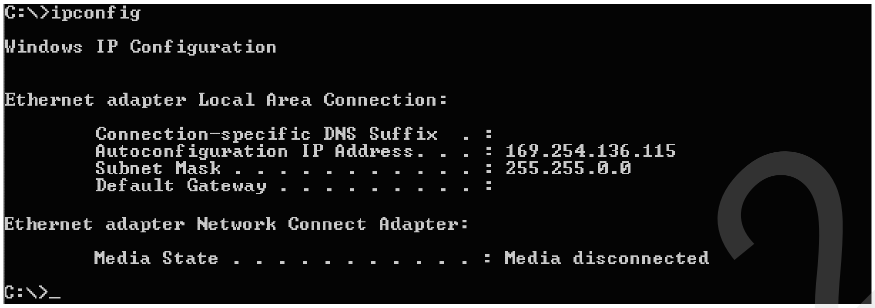
© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure B-3 *Commit/Discard Window*

7. The message **Reader IP Address config has changed. Needs reader reboot to take effect** appears. Reset the device and use the reader with the static IP network.

Reader IP is Not Known (DHCP Network Not Available) - Set the Static IP Using the Web Console

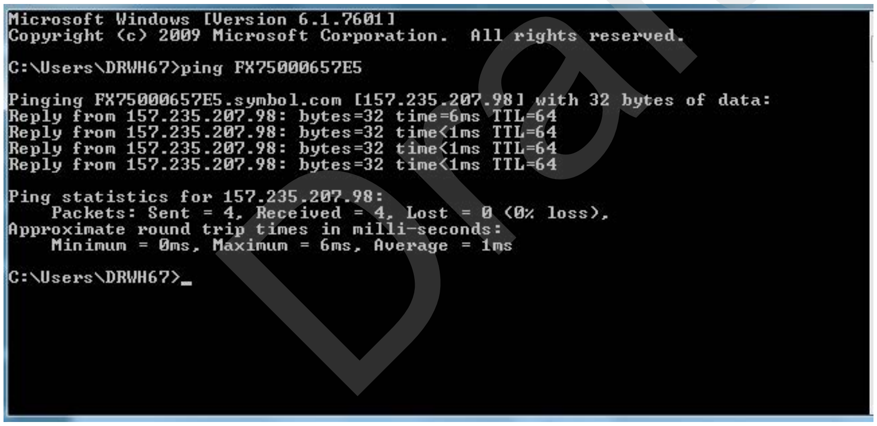
1. Connect the device and a PC running Windows XP to the same network that doesn't have a DHCP server, or connect the device directly to the PC.
2. Ensure both the device and PC Ethernet jack use at least one LED to indicate network connection detect.
3. If the PC uses an assigned static IP, update it to use DHCP. The PC obtains an IP that starts with **169**.



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Autoconfiguration IP Address. . . : 169.254.136.115
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Network Connect Adapter:

        Media State . . . . . . . . . . . : Media disconnected

C:\>_
```

Figure B-4 *Obtain IP Address*

4. When possible, ping the host name of the device.

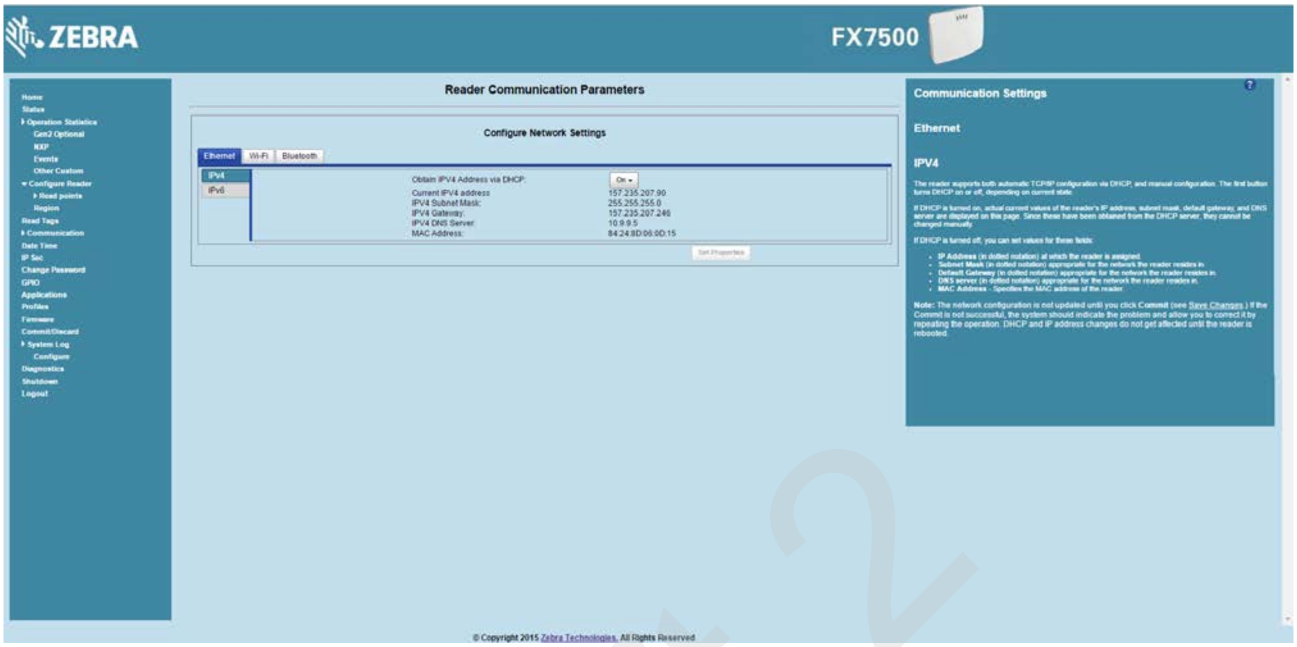


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\DRWH67>ping FX75000657E5

Pinging FX75000657E5.symbol.com [157.235.207.98] with 32 bytes of data:
Reply from 157.235.207.98: bytes=32 time=6ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64

Ping statistics for 157.235.207.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Users\DRWH67>_
```

Figure B-5 *Ping the Host Name*

5. Use a browser to connect to the device with the host name, e.g., FX7500CD3B1E, or use the IP address obtained from ping replies (e.g. 169.254.62.74).
6. Log onto the device.
7. Click **Communication**.

8. Set **Obtain IP Address via DHCP** to **Off** and enter all required information.



Reader Communication Parameters

Configure Network Settings

Obtain IPV4 Address via DHCP: On
Current IPV4 address 157.235.207.90
IPV4 Subnet Mask: 255.255.255.0
IPV4 Gateway: 157.235.207.246
IPV4 DNS Server: 10.9.9.5
MAC Address: 84:24:8D:06:0D:15

Communication Settings

Ethernet

IPV4

The reader supports both automatic TCP/IP configuration via DHCP, and manual configuration. The first button turns DHCP on or off, depending on current state.

If DHCP is turned on, actual current values of the reader's IP address, subnet mask, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

If DHCP is turned off, you can set values for these fields:

- **IP Address** (in dotted notation) at which the reader is assigned.
- **Subnet Mask** (in dotted notation) appropriate for the network the reader resides in.
- **Default Gateway** (in dotted notation) appropriate for the network the reader resides in.
- **DNS server** (in dotted notation) appropriate for the network the reader resides in.
- **MAC Address** - Specifies the MAC address of the reader.

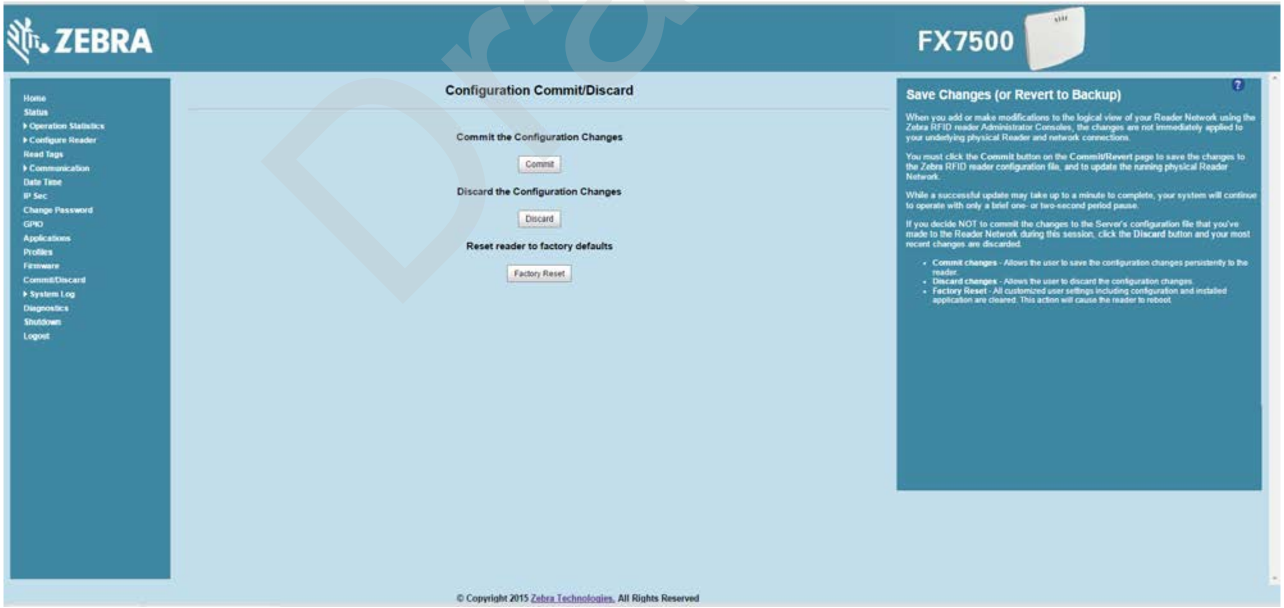
Note: The network configuration is not updated until you click **Commit** (see Save Changes.) If the Commit is not successful, the system should indicate the problem and allow you to correct it by repeating the operation. DHCP and IP address changes do not get affected until the reader is rebooted.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure B-6 *Reader Communication Parameters Window*

9. Click **Set Properties**.

10. Click **Commit/Discard**, then click the **Commit** button.



Configuration Commit/Discard

Commit the Configuration Changes

Discard the Configuration Changes

Reset reader to factory defaults

Save Changes (or Revert to Backup)

When you add or make modifications to the logical view of your Reader Network using the Zebra RFID reader Administrator Consoles, the changes are not immediately applied to your underlying physical Reader and network connections.

You must click the **Commit** button on the Commit/Revert page to save the changes to the Zebra RFID reader configuration file, and to update the running physical Reader Network.

While a successful update may take up to a minute to complete, your system will continue to operate with only a brief one- or two-second period pause.

If you decide NOT to commit the changes to the Server's configuration file that you've made to the Reader Network during this session, click the **Discard** button and your most recent changes are discarded.

- **Commit changes** - Allows the user to save the configuration changes persistently to the reader.
- **Discard changes** - Allows the user to discard the configuration changes.
- **Factory Reset** - All customized user settings including configuration and installed application are cleared. This action will cause the reader to reboot.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure B-7 *Commit/Discard Window*

11. The message **Reader IP Address config has changed. Needs reader reboot to take effect** appears. Reset the device and use the reader with the static IP network.

APPENDIX C RF AIR LINK CONFIGURATION

Introduction

This appendix lists the different air link configurations supported. The air link configuration is available through LLRP and RFID3 API interfaces.

Radio Modes

The supported modes are exposed as a list of individual **UHFC1G2RfModeTableEntry** parameters in regulatory capabilities as shown in *Table C-1* and *Table C-2*. The **Mode Index** column refers to the index used to walk the **C1G2UHFRFModeTable**. Refer to the EPCglobal *Low Level Reader Protocol (LLRP) Standard*.

Table C-1 *Radio Modes for FCC Readers*

RF Mode Index	Divide Ratio	BDR Value	M Value M2=2, FM0=1, M4=4, M8=8	FLM Value	PIE Value	Min Tari	Max Tari	Step Tari	Spectral Mask Indicator**	EPC HAG T&C Conformance
1	64/3	640000	1	PR_ASK	1500	6250	6250	0	Dense	false
2	64/3	640000	1	PR_ASK	2000	6250	6250	0	Dense	false
3	64/3	120000	2	PR_ASK	1500	25000	25000	0	Dense	false
4	64/3	120000	2	PR_ASK	1500	12500	23000	2100	Dense	false
5	64/3	120000	2	PR_ASK	2000	25000	25000	0	Dense	false
6	64/3	120000	2	PR_ASK	2000	12500	23000	2100	Dense	false
7	64/3	128000	2	PR_ASK	1500	25000	25000	0	Dense	false
8	64/3	128000	2	PR_ASK	1500	12500	23000	2100	Dense	false
9	64/3	128000	2	PR_ASK	2000	25000	25000	0	Dense	false

***RF Mode 23 is the automac air link profile which is also the default.**
****Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.**

Table C-1 *Radio Modes for FCC Readers (Continued)*

RF Mode Index	Divide Ratio	BDR Value	M Value M2=2, FM0=1, M4=4, M8=8	FLM Value	PIE Value	Min Tari	Max Tari	Step Tari	Spectral Mask Indicator**	EPC HAG T&C Conformance
10	64/3	128000	2	PR_ASK	2000	12500	23000	2100	Dense	false
11	64/3	160000	2	PR_ASK	1500	12500	18800	2100	Dense	false
12	64/3	160000	2	PR_ASK	2000	12500	18800	2100	Dense	false
13	64/3	60000	4	PR_ASK	1500	25000	25000	0	Dense	false
14	64/3	60000	4	PR_ASK	1500	12500	23000	2100	Dense	false
15	64/3	60000	4	PR_ASK	2000	25000	25000	0	Dense	false
16	64/3	60000	4	PR_ASK	2000	12500	23000	2100	Dense	false
17	64/3	64000	4	PR_ASK	1500	25000	25000	0	Dense	false
18	64/3	64000	4	PR_ASK	1500	12500	23000	2100	Dense	false
19	64/3	64000	4	PR_ASK	2000	25000	25000	0	Dense	false
20	64/3	64000	4	PR_ASK	2000	12500	23000	2100	Dense	false
21	64/3	80000	4	PR_ASK	1500	12500	18800	2100	Dense	false
22	64/3	80000	4	PR_ASK	2000	12500	18800	2100	Dense	false
*23	64/3	variable	variable	PR_ASK	variable	6250	25000	variable	variable	false
24	64/3	320000	1	PR_ASK	1500	12500	18800	2100	Dense	false
25	64/3	320000	1	PR_ASK	2000	12500	18800	2100	Dense	false
26	64/3	30000	8	PR_ASK	1500	25000	25000	0	Dense	false
27	64/3	30000	8	PR_ASK	1500	12500	23000	2100	Dense	false
28	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
29	64/3	30000	8	PR_ASK	2000	12500	23000	2100	Dense	false
30	64/3	32000	8	PR_ASK	1500	25000	25000	0	Dense	false
31	64/3	32000	8	PR_ASK	1500	12500	23000	2100	Dense	false
32	64/3	32000	8	PR_ASK	2000	25000	25000	0	Dense	false
33	64/3	32000	8	PR_ASK	2000	12500	23000	2100	Dense	false
34	64/3	40000	8	PR_ASK	1500	12500	18800	2100	Dense	false
35	64/3	40000	8	PR_ASK	2000	12500	18800	2100	Dense	false

***RF Mode 23 is the automac air link profile which is also the default.**
****Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.**

Table C-2 *Radio Modes for ETSI Readers*

RF Mode Index	Divide Ratio	BDR Value	M Value M2=2, FM0=1, M4=4, M8=8	FLM Value	PIE Value	Min Tari	Max Tari	Step Tari	Spectral Mask Indicator**	EPC HAG T&C Conformance
1	64/3	120000	2	PR_ASK	1500	25000	25000	0	Dense	false
2	64/3	120000	2	PR_ASK	1500	12500	23000	2100	Dense	false
3	64/3	120000	2	PR_ASK	2000	25000	25000	0	Dense	false
4	64/3	120000	2	PR_ASK	2000	12500	23000	2100	Dense	false
5	64/3	128000	2	PR_ASK	1500	25000	25000	0	Dense	false
6	64/3	128000	2	PR_ASK	1500	12500	23000	2100	Dense	false
7	64/3	128000	2	PR_ASK	2000	25000	25000	0	Dense	false
8	64/3	128000	2	PR_ASK	2000	12500	23000	2100	Dense	false
9	64/3	160000	2	PR_ASK	1500	12500	18800	2100	Dense	false
10	64/3	160000	2	PR_ASK	2000	12500	18800	2100	Dense	false
11	64/3	60000	4	PR_ASK	1500	25000	25000	0	Dense	false
12	64/3	60000	4	PR_ASK	1500	12500	23000	2100	Dense	false
13	64/3	60000	4	PR_ASK	2000	25000	25000	0	Dense	false
14	64/3	60000	4	PR_ASK	2000	12500	23000	2100	Dense	false
15	64/3	64000	4	PR_ASK	1500	25000	25000	0	Dense	false
16	64/3	64000	4	PR_ASK	1500	12500	23000	2100	Dense	false
17	64/3	64000	4	PR_ASK	2000	25000	25000	0	Dense	false
18	64/3	64000	4	PR_ASK	2000	12500	23000	2100	Dense	false
19	64/3	80000	4	PR_ASK	1500	12500	18800	2100	Dense	false
20	64/3	80000	4	PR_ASK	2000	12500	18800	2100	Dense	false
*21	64/3	variable	variable	PR_ASK	variable	12500	25000	variable	variable	false
22	64/3	320000	1	PR_ASK	1500	12500	18800	2100	Dense	false
23	64/3	320000	1	PR_ASK	2000	12500	18800	2100	Dense	false
24	64/3	30000	8	PR_ASK	1500	25000	25000	0	Dense	false
25	64/3	30000	8	PR_ASK	1500	12500	23000	2100	Dense	false
26	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false

***RF Mode 21 is the automac air link profile which is also the default.**
****Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.**

Table C-2 *Radio Modes for ETSI Readers (Continued)*

RF Mode Index	Divide Ratio	BDR Value	M Value M2=2, FM0=1, M4=4, M8=8	FLM Value	PIE Value	Min Tari	Max Tari	Step Tari	Spectral Mask Indicator**	EPC HAG T&C Conformance
27	64/3	30000	8	PR_ASK	2000	12500	23000	2100	Dense	false
28	64/3	32000	8	PR_ASK	1500	25000	25000	0	Dense	false
29	64/3	32000	8	PR_ASK	1500	12500	23000	2100	Dense	false
30	64/3	32000	8	PR_ASK	2000	25000	25000	0	Dense	false
31	64/3	32000	8	PR_ASK	2000	12500	23000	2100	Dense	false
32	64/3	40000	8	PR_ASK	1500	12500	18800	2100	Dense	false
33	64/3	40000	8	PR_ASK	2000	12500	18800	2100	Dense	false

***RF Mode 21 is the automac air link profile which is also the default.**
****Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.**

APPENDIX D CONNECTING WI-FI AND BLUETOOTH DONGLES

Introduction

This appendix describes how to connect to a wireless network using a USB Wi-Fi dongle on the FX7500, and how to connect to a peer device over Bluetooth using a USB Bluetooth dongle.

Connecting to a Wireless Network Using a Wi-Fi Dongle

To connect to a wireless network using a USB Wi-Fi dongle on the FX7500:

1. Plug the supported wireless dongle into the USB host port on the FX7500. Supported dongles are:
   - Wi-Fi over USB adapters with Realtek chipset RTL 8187
   - The following devices were tested:
     - Alfa AWUS036H, visit http://www.alfa.com.tw/in/front/bin/ptlist.phtml?Category=10541
     - CCrane Versa Wifi USB Adapter II, visit http://www.ccrane.com/antennas/wifi-antennas/versa-wifi-usb-adapter-II.aspx

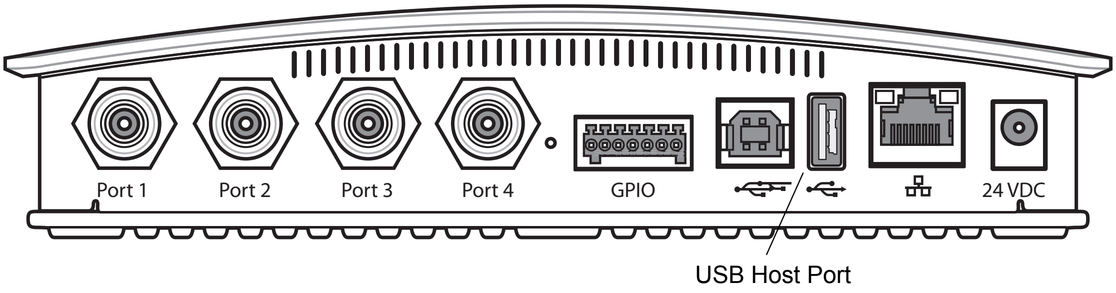
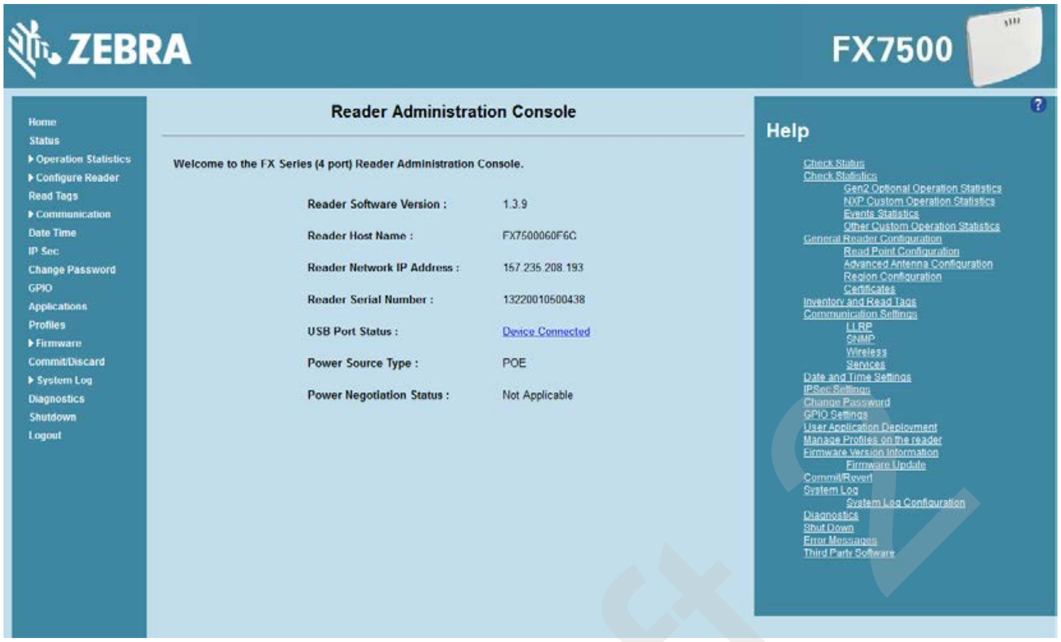


Figure D-1 *USB Host Port Location for Dongle*

2. To confirm that the Wi-Fi dongle is detected properly, log in to the reader Administrator Console. On the Home page ensure the **USB Port Status** displays **Device Connected**. Hover the mouse pointer over this link to display the WiFi dongle information shown in *Figure D-2*.



Reader Administration Console

Welcome to the FX Series (4 port) Reader Administration Console.

Reader Software Version : 1.3.9

Reader Host Name : FX7500060F6C

Reader Network IP Address : 157.235.208.193

Reader Serial Number : 13220010500438

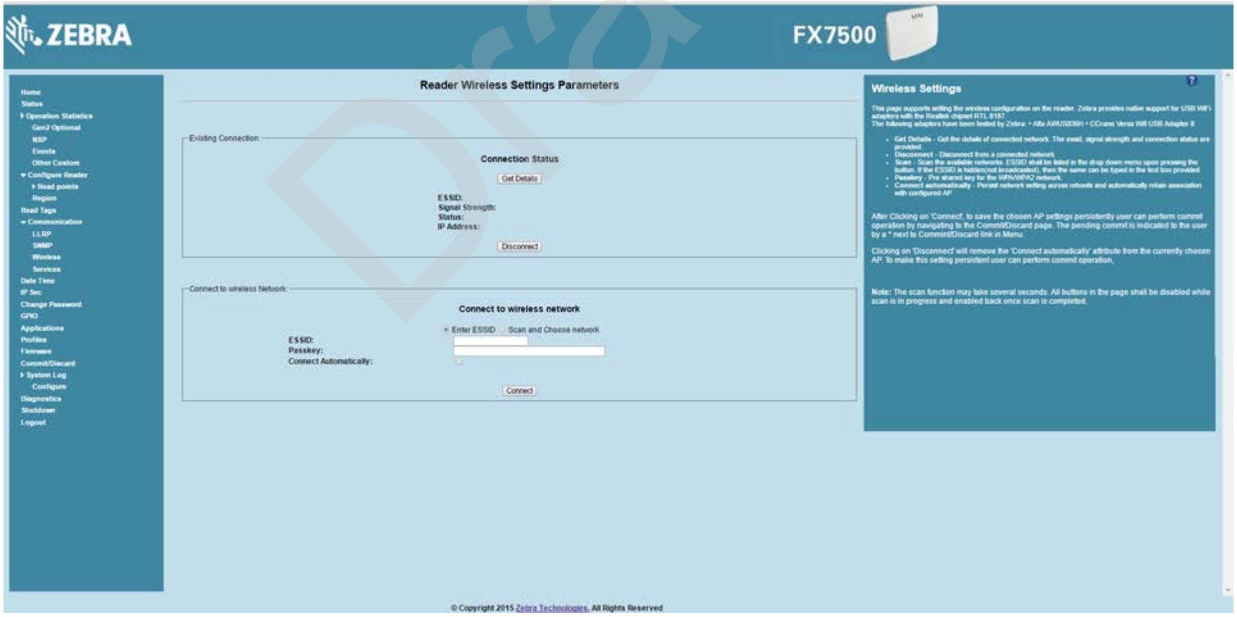
USB Port Status : Device Connected

Power Source Type : POE

Power Negotiation Status : Not Applicable

Figure D-2 *Wi-Fi Dongle Connected*

3. Select **Communication > Wireless**.



Reader Wireless Settings Parameters

Existing Connection

Connection Status

ESSID:
Signal Strength:
Status:
IP Address:

Connect to wireless Network

Connect to wireless network

● Enter ESSID ○ Scan and Choose network

ESSID:
Passkey:
Connect Automatically: □

Wireless Settings

This page supports setting the wireless configuration on the reader. Zebra provides native support for USB WiFi adapters with the Realtek chipset RTL 8187.
The following adapters have been tested by Zebra: • Alfa AWUS036H • CCrane Versa Wifi USB Adapter II

- Get Details - Get the details of connected network. The essid, signal strength and connection status are provided.
- Disconnect - Disconnect from a connected network.
- Scan - Scan the available networks. ESSID shall be listed in the drop down menu upon pressing the button. If the ESSID is hidden(not broadcasted), then the same can be typed in the text box provided.
- Passkey - Pre shared key for the WPA/WPA2 network.
- Connect automatically - Persist network setting across reboots and automatically retain association with configured AP.

After Clicking on 'Connect', to save the chosen AP settings persistently user can perform commit operation by navigating to the Commit/Discard page. The pending commit is indicated to the user by a * next to Commit/Discard link in Menu.

Clicking on 'Disconnect' will remove the 'Connect automatically' attribute from the currently chosen AP. To make this setting persistent user can perform commit operation.

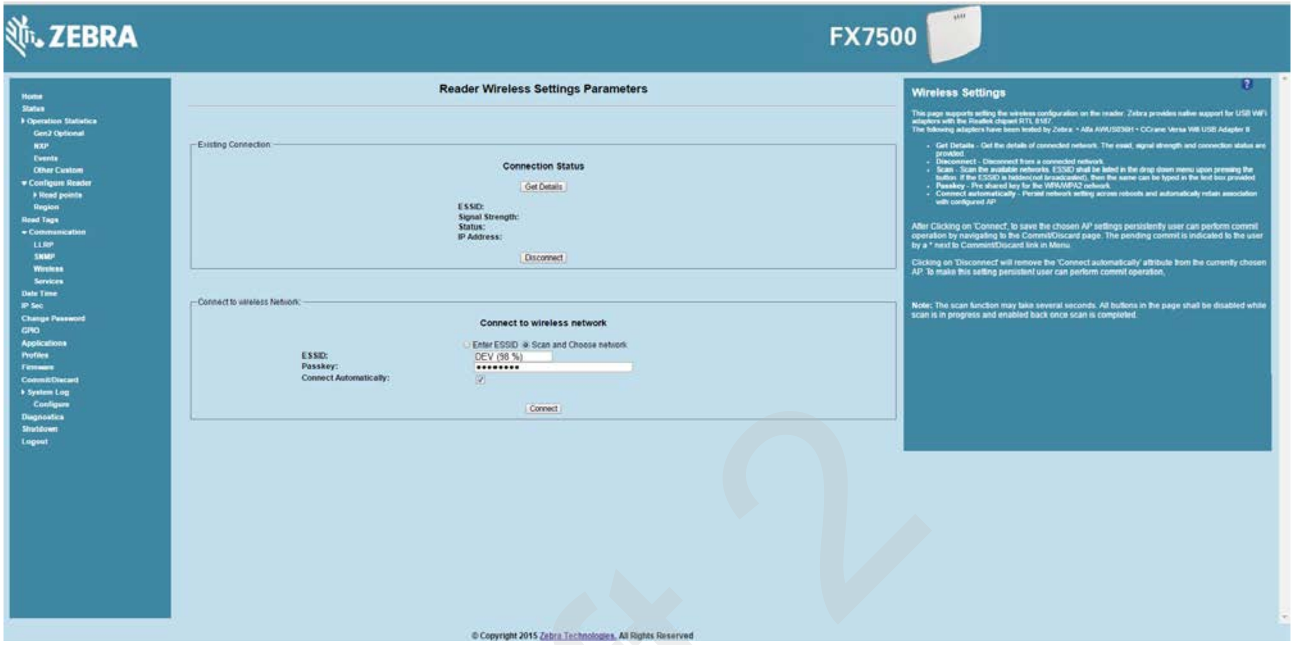
Note: The scan function may take several seconds. All buttons in the page shall be disabled while scan is in progress and enabled back once scan is completed.

Figure D-3 *Wireless Settings*

The WiFi dongle can connect to the wireless network in one of two ways:

- Manually entering the ESSID (if known).
- Scanning the current list of APs and choosing the correct one to connect to.

4. Once the APs are scanned, enter the appropriate passkey and enable **Connect Automatically** (if required to connect to the AP automatically if the connection is lost).



Reader Wireless Settings Parameters

Existing Connection

Connection Status

ESSID:
Signal Strength:
Status:
IP Address:

Connect to wireless Network:

Connect to wireless network

○ Enter ESSID ● Scan and Choose network

ESSID: DEV (98 %)
Passkey: ••••••••
Connect Automatically: ☑

Wireless Settings

This page supports setting the wireless configuration on the reader. Zebra provides native support for USB WiFi adaptors with the Realtek chipset RTL 8187.
The following adapters have been tested by Zebra: • Alfa AWUS036H • CCrane Versa Wifi USB Adapter II

- **Get Details** - Get the details of connected network. The essid, signal strength and connection status are provided.
- **Disconnect** - Disconnect from a connected network.
- **Scan** - Scan the available networks. ESSID shall be listed in the drop down menu upon pressing the button. If the ESSID is hidden(not broadcasted), then the same can be typed in the text box provided
- **Passkey** - Pre shared key for the WPA/WPA2 network.
- **Connect automatically** - Persist network setting across reboots and automatically retain association with configured AP

After Clicking on 'Connect', to save the chosen AP settings persistently user can perform commit operation by navigating to the Commit/Discard page. The pending commit is indicated to the user by a * next to Commit/Discard link in Menu

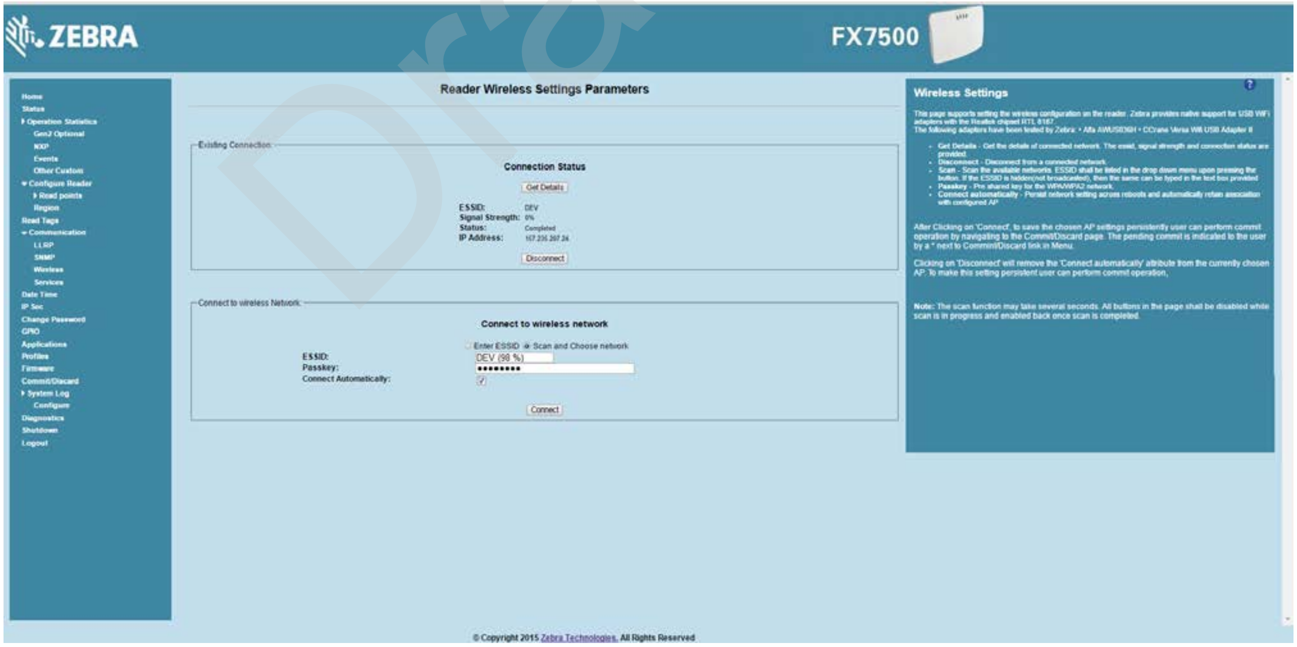
Clicking on 'Disconnect' will remove the 'Connect automatically' attribute from the currently chosen AP. To make this setting persistent user can perform commit operation.

Note: The scan function may take several seconds. All buttons in the page shall be disabled while scan is in progress and enabled back once scan is completed.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure D-4 *Entering Connect Information*

5. Select **Connect**. When the connection to the AP succeeds, an IP is assigned and appears in the **IP Address** field.



Reader Wireless Settings Parameters

Existing Connection

Connection Status

ESSID: DEV
Signal Strength: 0%
Status: Completed
IP Address: 157.235.207.24

Connect to wireless Network:

Connect to wireless network

○ Enter ESSID ● Scan and Choose network

ESSID: DEV (98 %)
Passkey: ••••••••
Connect Automatically: ☑

Wireless Settings

This page supports setting the wireless configuration on the reader. Zebra provides native support for USB WiFi adaptors with the Realtek chipset RTL 8187.
The following adapters have been tested by Zebra: • Alfa AWUS036H • CCrane Versa Wifi USB Adapter II

- **Get Details** - Get the details of connected network. The essid, signal strength and connection status are provided.
- **Disconnect** - Disconnect from a connected network.
- **Scan** - Scan the available networks. ESSID shall be listed in the drop down menu upon pressing the button. If the ESSID is hidden(not broadcasted), then the same can be typed in the text box provided
- **Passkey** - Pre shared key for the WPA/WPA2 network.
- **Connect automatically** - Persist network setting across reboots and automatically retain association with configured AP

After Clicking on 'Connect', to save the chosen AP settings persistently user can perform commit operation by navigating to the Commit/Discard page. The pending commit is indicated to the user by a * next to Commit/Discard link in Menu

Clicking on 'Disconnect' will remove the 'Connect automatically' attribute from the currently chosen AP. To make this setting persistent user can perform commit operation.

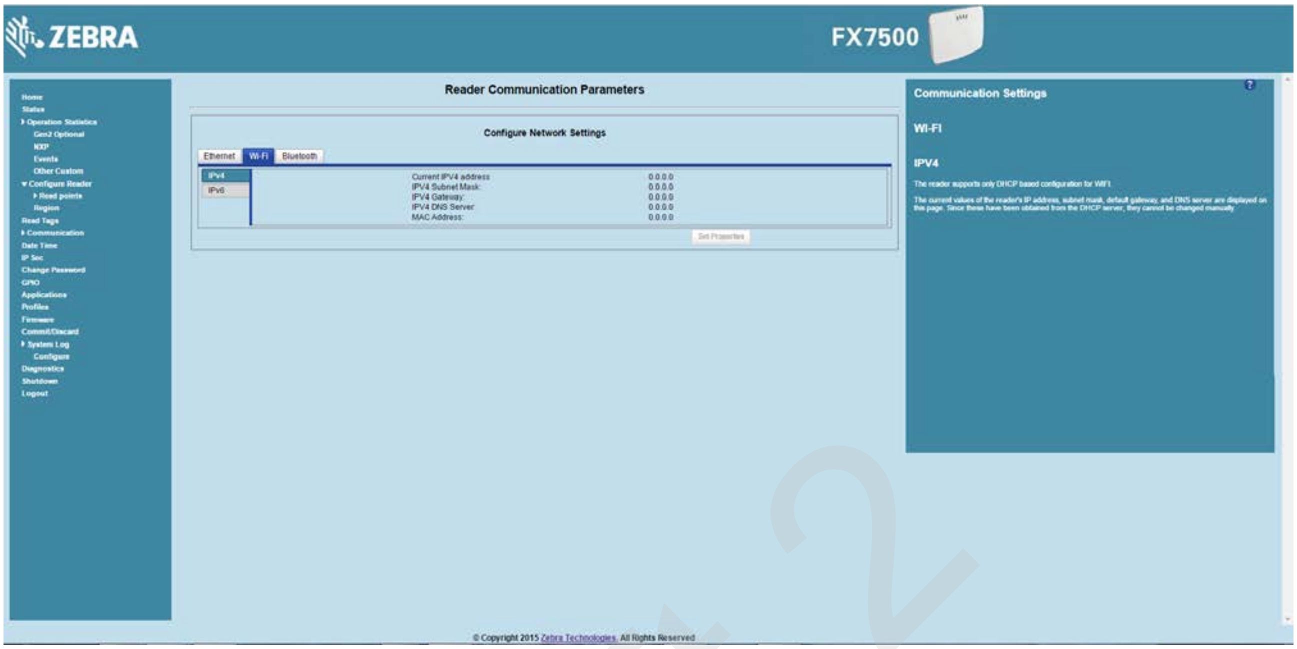
Note: The scan function may take several seconds. All buttons in the page shall be disabled while scan is in progress and enabled back once scan is completed.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure D-5 *Assigned IP Address*

The reader is now accessible using the wireless IP shown in the **IP Address** field (157.235.207.24 in this case). The WiFi interface supports dynamic addressing mechanisms for both IPV4 and IPv6. There is no provision to set a static IP address.

For wireless IP address details, select **Communication > Wi-Fi** tab.



Reader Communication Parameters

Configure Network Settings

Current IPV4 address 0.0.0.0
IPV4 Subnet Mask: 0.0.0.0
IPV4 Gateway: 0.0.0.0
IPV4 DNS Server 0.0.0.0
MAC Address: 0.0.0.0

Communication Settings

WI-FI

IPV4

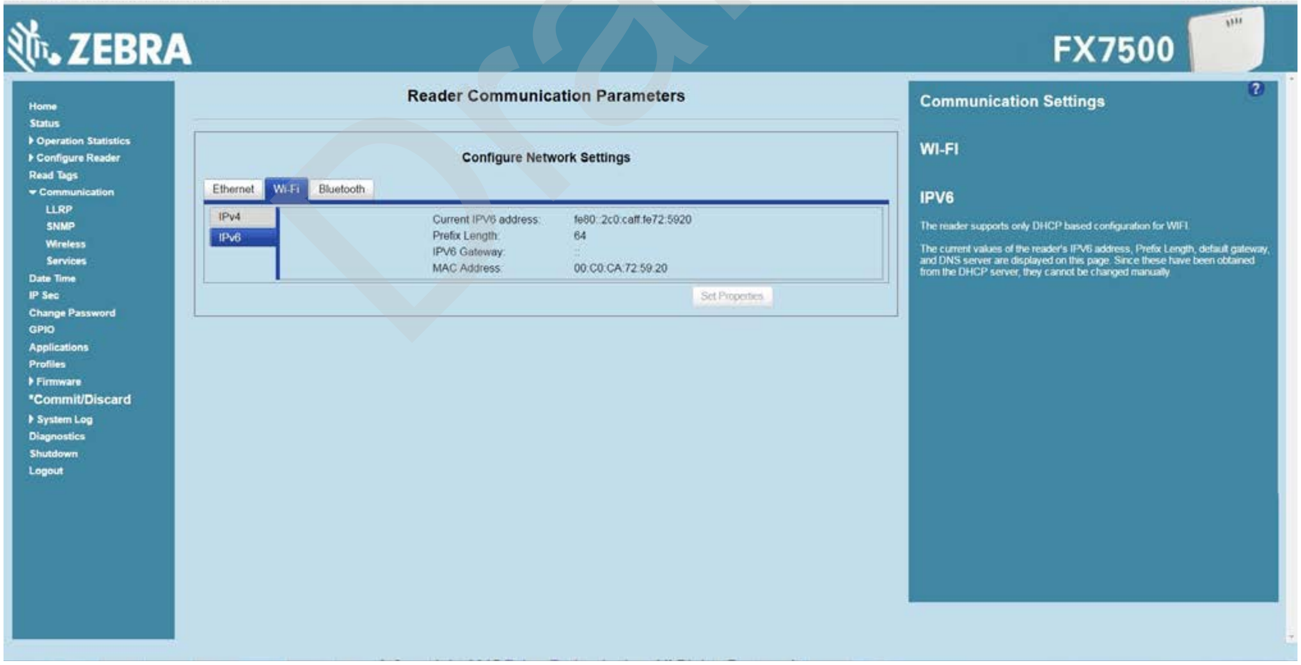
The reader supports only DHCP based configuration for WIFI.

The current values of the reader's IP address, subnet mask, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure D-6 *Wi-Fi Tab - IPV4*

The reader can also be accessed via Wi-Fi using an IPV6 address if supported by the network to which the API is connected.



Reader Communication Parameters

Configure Network Settings

Current IPV6 address: fe80::2c0:caff:fe72:5920
Prefix Length: 64
IPV6 Gateway: ::
MAC Address: 00:C0:CA:72:59:20

Communication Settings

WI-FI

IPV6

The reader supports only DHCP based configuration for WIFI.

The current values of the reader's IPV6 address, Prefix Length, default gateway, and DNS server are displayed on this page. Since these have been obtained from the DHCP server, they cannot be changed manually.

Figure D-7 *Wi-Fi Tab - IPV6*

Connecting to a Peer Device over Bluetooth Using a Bluetooth Dongle

To connect to a peer device over Bluetooth using a USB Bluetooth dongle on the FX7500:

1. Plug the supported Bluetooth dongle into the USB host port on the FX7500. The following Bluetooth dongles are supported on the FX7500:
   - Asus Mini Bluetooth Dongle USB-BT211.
   - MediaLink Bluetooth Dongle MUA-BA3.

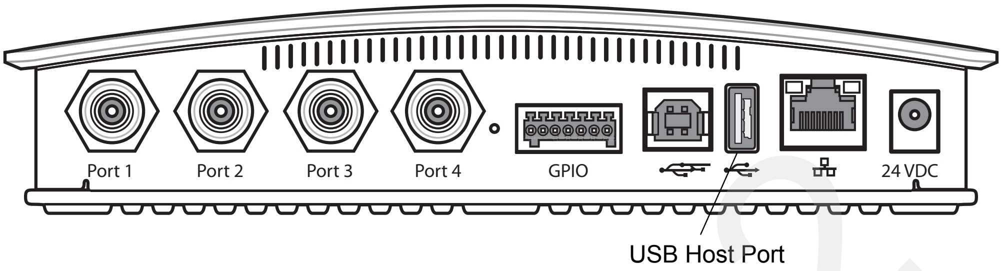
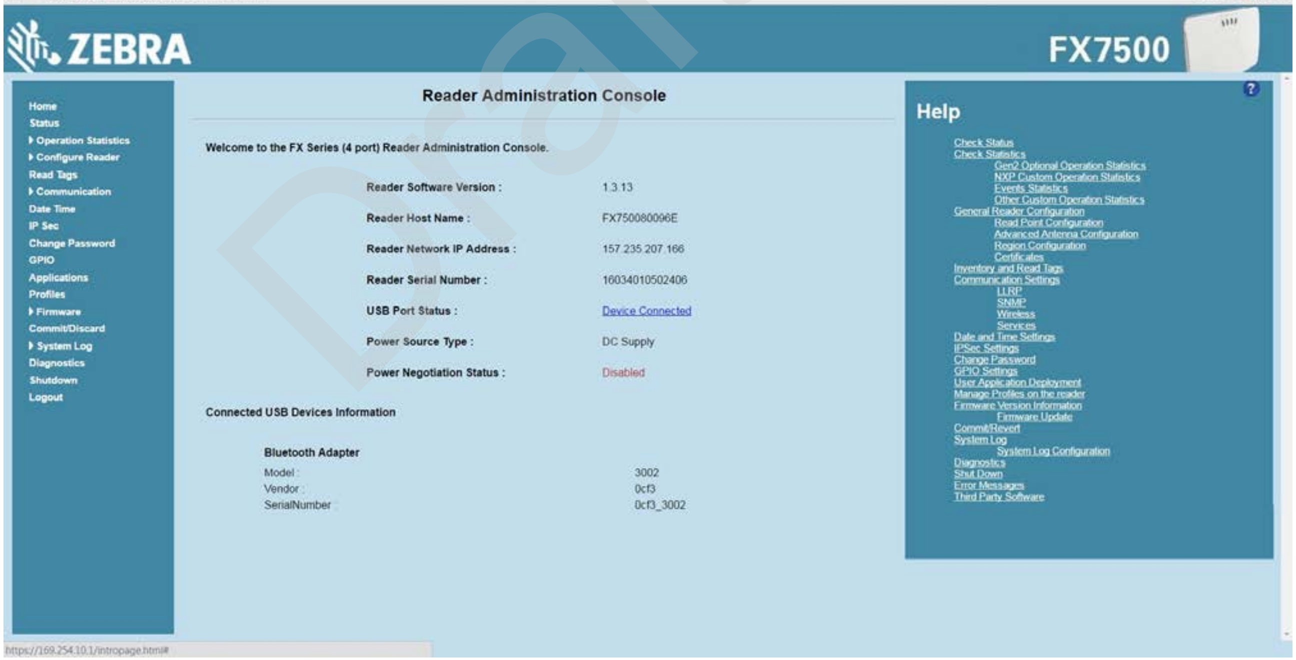


Figure D-8 *USB Host Port Location for Dongle*

2. To confirm that the Bluetooth dongle is detected properly, log in to the reader Administrator Console. On the **Home** page ensure the **USB Port Status** displays **Device Connected**. Hover the mouse pointer over this link to display the Bluetooth dongle information.



Reader Administration Console

Welcome to the FX Series (4 port) Reader Administration Console.

Reader Software Version :	1.3.13
Reader Host Name :	FX750080096E
Reader Network IP Address :	157.235.207.166
Reader Serial Number :	16034010502406
USB Port Status :	Device Connected
Power Source Type :	DC Supply
Power Negotiation Status :	Disabled

Connected USB Devices Information

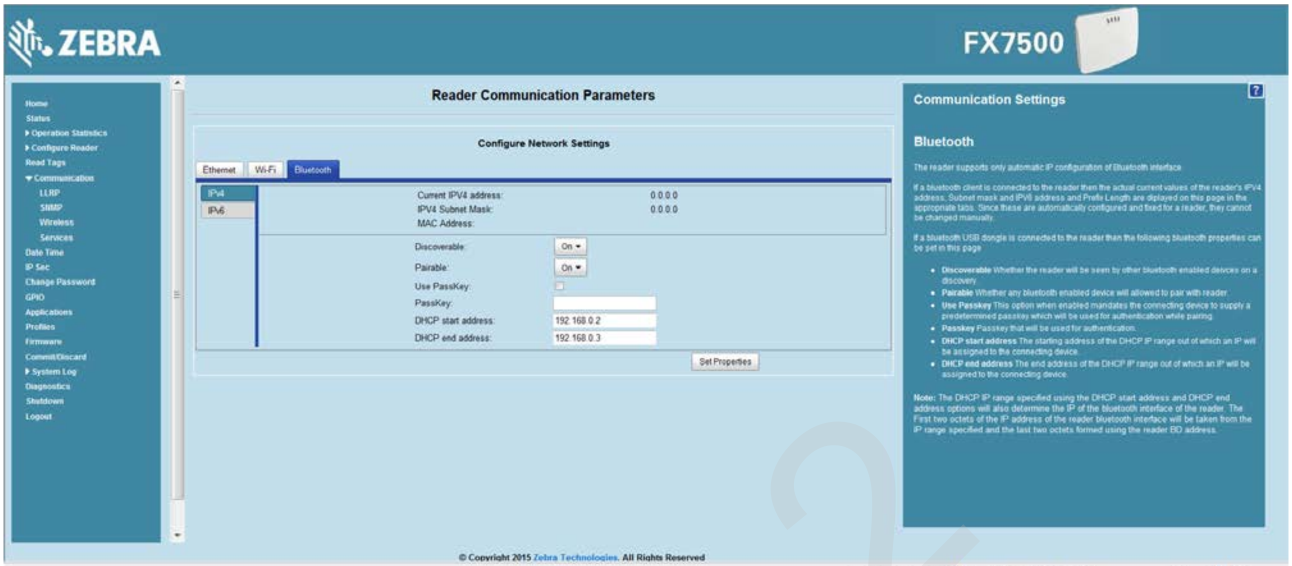
Bluetooth Adapter

Model :	3002
Vendor :	0cf3
SerialNumber :	0cf3_3002

Figure D-9 *Bluetooth Dongle Connected*

3. Select **Communication > Bluetooth**.

4. Change the **Discoverable** and **Pairable** properties to **On**.



Reader Communication Parameters

Configure Network Settings

Current IPV4 address: 0.0.0.0

IPV4 Subnet Mask: 0.0.0.0

MAC Address:

Discoverable: On

Pairable: On

Use PassKey: □

PassKey:

DHCP start address: 192.168.0.2

DHCP end address: 192.168.0.3

Communication Settings

Bluetooth

The reader supports only automatic IP configuration of Bluetooth interface

If a bluetooth client is connected to the reader then the actual current values of the reader's IPV4 address, Subnet mask and IPV6 address and Prefix Length are diplayed on this page in the appropriate tabs. Since these are automatically configured and fixed for a reader, they cannot be changed manually.

If a bluetooth USB dongle is connected to the reader than the following bluetooth properties can be set in this page

- **Discoverable** Whether the reader will be seen by other bluetooth enabled deivces on a discovery
- **Pairable** Whether any bluetooth enabled device will allowed to pair with reader
- **Use Passkey** This option when enabled mandates the connecting device to supply a predetermined passkey which will be used for authentication while pairing
- **Passkey** Passkey that will be used for authentication.
- **DHCP start address** The starting address of the DHCP IP range out of which an IP will be assigned to the connecting device.
- **DHCP end address** The end address of the DHCP IP range out of which an IP will be assigned to the connecting device.

Note: The DHCP IP range specified using the DHCP start address and DHCP end address options will also determine the IP of the bluetooth interface of the reader. The First two octets of the IP address of the reader bluetooth interface will be taken from the IP range specified and the last two octets formed using the reader BD address.

Figure D-10 *Changing Discoverable and Pairable Properties*

5. Optionally select **Use Passkey** and enter a passkey to validate the Bluetooth connection. The default passkey for the FX7500 is **0000**.

6. Discover the reader from a Bluetooth-enabled device (such as a laptop). Use the host name to identify the reader among the discovered devices (e.g., **FX7500060C17**).

7. After a successful connection, right-click the reader icon (e.g., **FX7500060C17**) in the list of Bluetooth devices and select **Connect using > Ad hoc network**. This establishes the network connection for later.

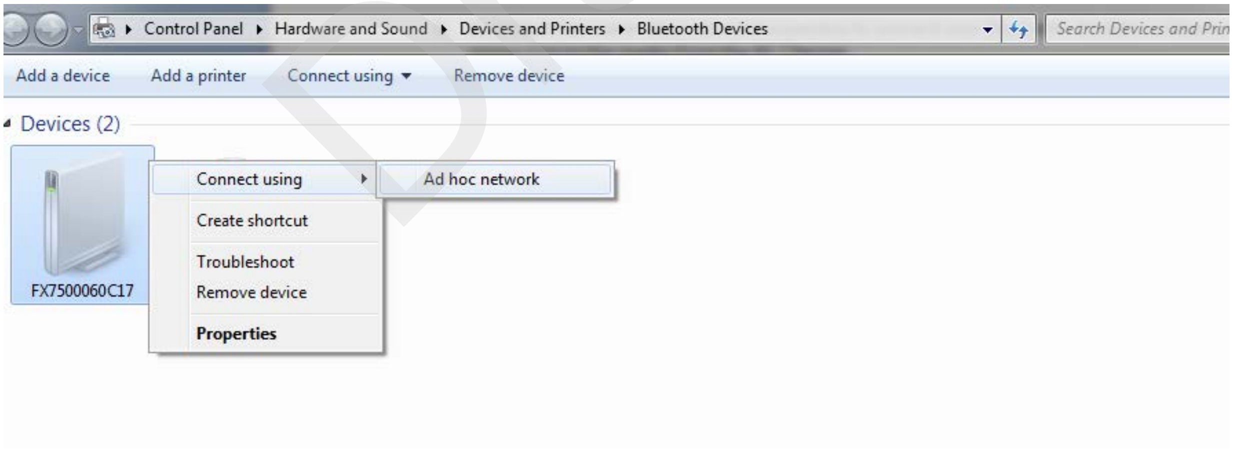
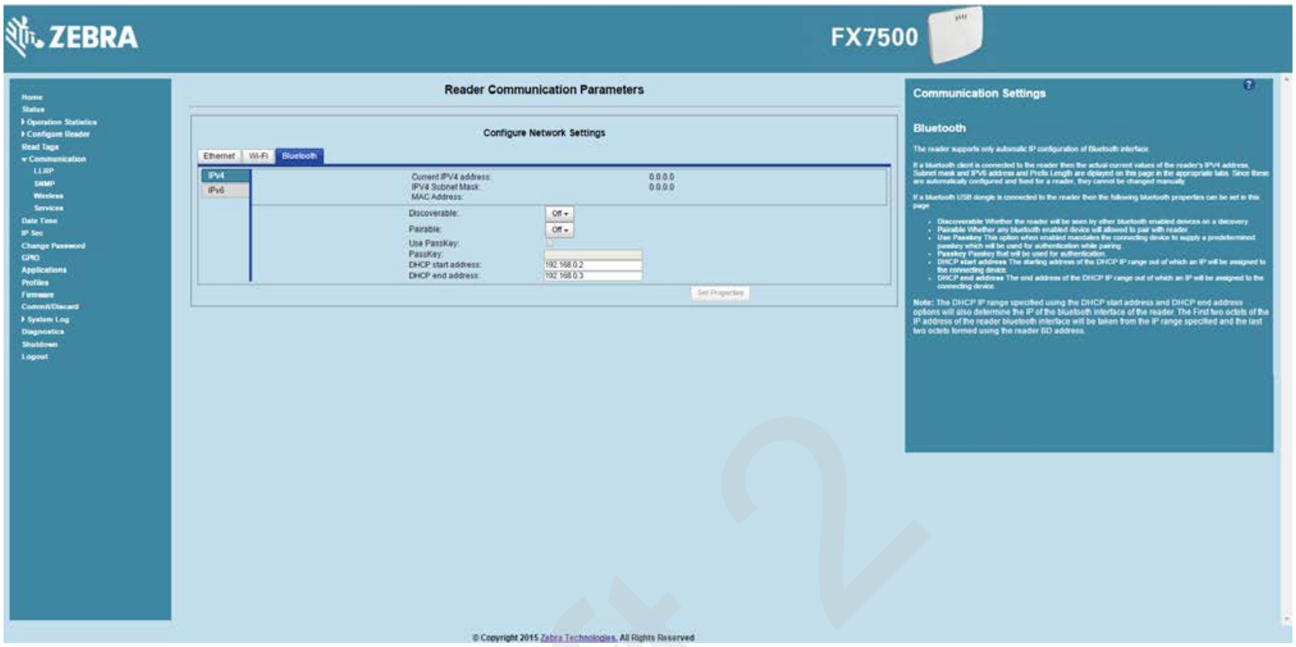


Figure D-11 *Connecting to the Reader*

8. The IP address assigned to the Bluetooth interface is 192.168.XX.XX. The last 2 octets are the last 2 octets of the Bluetooth MAC address (found in the **Properties** window on the PC once the Bluetooth

connection is established). Also find this in the **Communication > Bluetooth** page. Both IPV4 and IPV6 based IP address are supported for adhoc Bluetooth connection between the reader and the client.



Reader Communication Parameters

Configure Network Settings

Current IPV4 address: 0.0.0.0
IPV4 Subnet Mask: 0.0.0.0
MAC Address:
Discoverable: Off
Pairable: Off
Use PassKey: □
PassKey:
DHCP start address: 192.168.0.2
DHCP end address: 192.168.0.3

Communication Settings

Bluetooth

The reader supports only automatic IP configuration of Bluetooth interface.

If a bluetooth client is connected to the reader then the actual current values of the reader's IPV4 address, Subnet mask and IPV6 address and Prefix Length are diplayed on this page in the appropriate tabs. Since these are automatically configured and fixed for a reader, they cannot be changed manually

If a bluetooth USB dongle is connected to the reader then the following bluetooth properties can be set in this page

- **Discoverable** Whether the reader will be seen by other bluetooth enabled devices on a discovery
- **Pairable** Whether any bluetooth enabled device will allowed to pair with reader.
- **Use Passkey** This option when enabled mandates the connecting device to supply a predetermined passkey which will be used for authentication while pairing.
- **Passkey** Passkey that will be used for authentication.
- **DHCP start address** The starting address of the DHCP IP range out of which an IP will be assigned to the connecting device.
- **DHCP end address** The end address of the DHCP IP range out of which an IP will be assigned to the connecting device.

Note: The DHCP IP range specified using the DHCP start address and DHCP end address options will also determine the IP of the bluetooth interface of the reader. The First two octets of the IP address of the reader bluetooth interface will be taken from the IP range specified and the last two octets formed using the reader BD address.

© Copyright 2015 Zebra Technologies. All Rights Reserved

Figure D-12 *Communication Bluetooth Tab*

9. Open the web page or sample application to connect to the Bluetooth IP (192.168.67.21 in *Figure D-12*) and read tags.

APPENDIX E COPYING FILES TO AND FROM THE READER

Introduction

The FX7500 reader supports the SCP, FTP, and FTPS protocols for copying files.

SCP

The following examples illustrate SCP use:

```
scp SourceFileName rfidadm@MyReaderIP:/apps
scp rfidadm@MyReaderIP:/apps/SourceFileName  userid@MyLinuxMachineIP:/MyFolderName
```

FTP

The following examples illustrate FTP use:

```
ftp> open
To 157.235.207.146
Connected to 157.235.207.146.
220 Welcome to Thredbo FTP service.
User (157.235.207.146:(none)): rfidadm
331 Please specify the password.
Password:
230 Login successful.
ftp>
```

Use FTP commands such as **is**, **get**, and **put** to manage files. For more information on FTP commands refer to http://www.cs.colostate.edu/helpdocs/ftp.html. GUI applications such as **FileZilla** are also supported on Windows and Linux machines to connect to the FX7500.

FTPS

Use any standard GUI tool such as **FileZilla** to connect to the FX7500 reader over FTPS.

APPENDIX F DATA PROTECTION

Introduction

The FX7500 stores data in transition when it detects a network condition that prevents the reader from sending data. This applies to RFID tag data that the reader application is transmitting to the outbound TCP socket, and is no longer owned by the RFID application because it was sent to the network layer for transmission.

When the reader cannot queue RFID data in the outbound TCP socket when an LLRP connection is already established, it stores all outbound LLRP messages in the data protection queue. The queue can store up to 66,000 messages, which represents more than 5 minutes worth of data when reading 200 tags/second (the nominal data rate in DRM (dense reader mode) configuration). If the network is still unavailable when the data protection queue is full, the oldest messages are discarded to accommodate the most recent tag reports.

This feature can not be disabled and operates regardless of the physical network interface used, meaning RFID data over WiFi and Bluetooth is also protected.

INDEX

Numerics

- 10/100BaseT Ethernet 1-2, 2-4, 2-5
- 2-port reader 2-4
- 4-port reader 2-4

A

- administrator console 4-1
  - applications 4-42
  - committing changes 4-45
  - communication settings 4-31
  - configure network services 4-37
  - configure network settings 4-31, 4-32, 4-33
  - configuring system log 4-47
  - discarding changes 4-45
  - firmware version 4-44, 4-45
  - GPIO 4-41
  - IPV6 sec 4-39
  - login 4-6
  - main screen 4-9
  - managing login 4-41
  - reader diagnostics 4-48
  - reader profiles 4-43
  - scan control 1-6, 4-30
  - set password 4-40
  - setting date and time 4-38
  - shutting down 4-49
  - status 4-10
  - system log 4-46
- air link C-1
- antennas 2-2
  - configuring 4-18
  - installing 3-4
  - ports 1-2, 2-4, 2-5
- applications 4-42

B

- backup 2-7
- bluetooth D-5
  - connecting D-5

C

- cable pinouts A-4
  - ethernet A-4
  - GPIO A-6
  - USB A-5
  - USB client A-5
  - USB host A-5
- chapter descriptions x
- client applications 2-7
- commit region change 1-5
- committing changes 4-45
- communication 2-5
  - ethernet, wired 3-5
- communication settings 4-31
- configurations ix
- configure
  - administrator console 2-7
  - antenna 4-18
  - LLRP 4-34
  - read points 4-17, 4-18
  - reader 4-16
  - region 4-19
  - SNMP 4-35
  - static IP B-1
  - static IP via web console B-1, B-3
  - wireless 4-36
- configuring network
  - bluetooth 4-33
  - ethernet 4-31
  - services 4-37

wi-fi 4-32

connecting

to reader 4-3

via bluetooth D-5

via host name 4-3

via IP address 4-4

via wi-fi D-1

connection 2-7

antennas 3-4

communication 3-5

port diagram 2-4

ports 2-4

powering 3-10

wired ethernet 3-5

conventions

notational xi

copying files E-1

country list 1-5, 4-7

D

data protection F-1

date 4-38

deployments 4-2

discarding changes 4-45

E

ethernet

Bias-T port connection 3-6

pinouts A-4

POE 3-5

port 2-5

setup 3-5

wired 3-5

event management, tags 2-7

event statistics 4-14

F

files

copying E-1

filtering, tags 2-7

firmware

updating 2-7

version 4-44, 4-45

firmware update 4-44, 4-45, 7-3

prerequisites 7-1

first time login 1-3, 4-6

FTP

copying files E-1

FTPS

copying files E-2

G

GPIO 1-2, 2-4

pinouts A-6

port 2-5

GPIO control 4-41

H

host communication

ethernet, wired 3-5

host name connect 1-2

I

information, service xii

initiating reads 1-6, 4-30

installation

antennas 3-4

communication connection 3-5

mounting 3-2

powering 3-10

IP address 4-5

IP ping 4-5

K

kill tag 2-7

kits 2-4, A-1

L

LEDs 2-5

LLRP 2-7

configure 4-34

radio modes C-1, C-3

lock tag 2-7

log 4-46

configuring 4-47

logging 2-7

login 4-6

first time 4-6

managing 4-41

M

mono-static 2-3

mounting 3-2

mounting plate 3-2

multiple reader deployments 4-2

N

NXP
- statistics . . . 4-13, 4-15

O

obtain reader IP address . . . 4-5

P

Password . . . 1-3, 7-3, 7-9
password . . . 1-3, 4-6, 7-3, 7-9
- changing . . . 4-40

pinouts . . . A-4
- ethernet . . . A-4
- GPIO . . . A-6
- USB . . . A-5
- USB client . . . A-5
- USB host . . . A-5

POE . . . 1-2, 2-4, 2-5, 3-5, 3-10, A-4
ports . . . 2-4
- descriptions . . . 2-5
- ethernet . . . 3-5

power . . . 1-2, 2-4
- AC power supply . . . 3-10
- applying . . . 3-10
- options . . . 3-10
- POE . . . 3-5, 3-10
- port . . . 2-5

profiles . . . 4-43

R

read points . . . 4-17, 4-18
reader
- configuration . . . 4-16
- configurations . . . ix
- connecting . . . 4-3
- description . . . 2-2
- GEN2 statistics . . . 4-12
- kits . . . 2-4, A-1
- profiles . . . 4-43
- statistics . . . 4-11
  - event . . . 4-14
  - NXP . . . 4-13, 4-15
- status . . . 4-10
- versions . . . 2-4

reading tags . . . 2-7, 3-12
- initiating . . . 1-6, 4-30

rear panel . . . 1-2, 2-4
reboot . . . 4-2
recovery . . . 2-7
region . . . 4-7
region configuration . . . 4-19
region control . . . 4-7
region setting . . . 1-4
region settings . . . 1-4
reset . . . 1-2, 2-4, 2-5
RFID
- FX reader . . . 2-3
- overview . . . 2-1

RFID components . . . 2-2
- antennas . . . 2-2
- readers . . . 2-2
- tags . . . 2-2

RJ45 . . . 2-5

S

SCP
- copying files . . . E-1

service information . . . xii
set region . . . 1-4, 4-7
setting date . . . 4-38
setting time . . . 4-38
setup
- POE . . . 3-10
- power supply . . . 3-10
- wired ethernet . . . 3-5
- wired ethernet AC outlet . . . 3-5
- wired ethernet, power-over . . . 3-5

shutdown . . . 4-49
SNMP . . . 2-7
- configure . . . 4-35

software update . . . 7-3
specifications . . . A-2
start-up . . . 1-3
static IP configuration . . . B-1
- via web console . . . B-1, B-3

Statistics . . . 4-14
statistics . . . 4-11
- event . . . 4-14
- GEN2 . . . 4-12
- NXP . . . 4-13, 4-15

status . . . 4-10
system log . . . 4-46
- configuring . . . 4-47

system time . . . 4-38

T

tags . . . 2-2
- management . . . 2-7
- reading . . . 3-12, 4-30

technical specifications . . . A-2
time . . . 4-38
troubleshooting . . . 8-1

U

unpacking 3-1
updating firmware 2-7, 4-44, 4-45, 7-3
    prerequisites 7-1
updating software 7-3
USB 1-2, 2-4, 7-4
    client pinouts A-5
    host pinouts A-5
    pinouts A-5
user ID 4-6
user name 1-3, 7-3, 7-9
user password 4-6

V

version control 4-44, 4-45

W

wi-fi D-1
    connecting D-1
wired ethernet 3-5
wireless
    configure 4-36
write tag 2-7

Z

zero-configuration networking 4-5

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