

FX SERIES RFID FIXED READER



ZEBRA

Integration Guide

FX SERIES RFID READER INTEGRATION GUIDE

MN000026A06

Revision A

November 2017

Copyright

© 2017 ZIH Corp. and/or its affiliates. All rights reserved. ZEBRA and the stylized Zebra head are trademarks of ZIH Corp., registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to www.zebra.com/copyright.

WARRANTY: For complete warranty information, go to www.zebra.com/warranty.

END USER LICENSE AGREEMENT: For complete EULA information, go to www.zebra.com/eula.

For Australia Only

For Australia Only. This warranty is given by Zebra Technologies Asia Pacific Pte. Ltd., 71 Robinson Road, #05-02/03, Singapore 068895, Singapore. Our goods come with guarantees that cannot be excluded under the Australia Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

Zebra Technologies Corporation Australia's limited warranty above is in addition to any rights and remedies you may have under the Australian Consumer Law. If you have any queries, please call Zebra Technologies Corporation at +65 6858 0722. You may also visit our website: www.zebra.com for the most updated warranty terms.

Terms of Use

- **Proprietary Statement**

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries ("Zebra Technologies"). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

- **Product Improvements**

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

- **Liability Disclaimer**

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

- **Limitation of Liability**

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Revision History

Changes to the original manual are listed below:

Change	Date	Description
-01 Rev A	1/2014	Initial release
-02 Rev A	2/2015	Zebra Re-Branding
-03 Rev A	4/2016	Updates for SNAP; updated screen shots.
-04 Rev A	7/2016	Updates: <ul style="list-style-type: none">- 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.- Changed Max Antenna Gain Allowed for US.- Added Canada and Taiwan to Antenna Gain and Radiated Power table.
-05 Rev A	7/2016	Updates to EU column of Antenna Gain and Radiated Power table. <ul style="list-style-type: none">- Changed Max Conducted RF Power at Antenna Input.- Changed Max Antenna Gain Allowed.
-06 Rev A	11/2017	Update guide to include FX9600; Guide title updated to FX Series RFID Fixed Reader Integration Guide.

Table of Contents

Copyright	3
For Australia Only	3
Terms of Use	3
Revision History	4
About This Guide	
Introduction	9
Chapter Descriptions	10
Notational Conventions	11
Related Documents and Software	11
Service Information	12
Quick Start	
Introduction	13
Quick Start Demonstration	13
Step 1, Setup	13
Step 2, Connecting to the Reader	14
Step 3, First Time / Start-Up Login	15
Step 4, Set Region	16
Step 5, Read Tags	18
Getting Started	
Introduction	19
FX Series Features	20
FX7500 Parts	21
FX7500 Rear Panel	22
FX7500 LEDs	23
FX9600 Parts	24
FX9600 Rear Panel	25
FX9600 LEDs	26
Installation and Communication	
Introduction	27
Unpacking the Reader	27

Table of Contents

Mounting and Removing the FX Series Readers	28
Mounting the FX7500 With a Mounting Plate	28
FX7500 Direct Mounting	29
Mounting the FX9600 Reader	30
Connecting FX7500 and FX9600 RFID Reader Antennas	31
Communications and Power Connections	33
Ethernet Connection	33
USB Connection	34
GPIO Interface Connection	37
LED Sequences	38
System Start-up/Boot LED Sequence	38
PWR LED Sequence to Indicate IPv4 Status after Booting	38
Reset to Factory Defaults LED Sequence	38
LED Sequence for Software Update Status	38
Reading Tags	39
 Administrator Console	
Introduction	40
Profiles	41
Resetting the Reader	41
Auto Discovery	41
Connecting to the Reader	42
Obtaining the IP Address via Command Prompt	43
Connecting via Host Name	43
Connecting via IP Address	44
Using Zero-Configuration Networking when DHCP Server is Not Available	44
Administrator Console Login	45
First Time / Start-Up Login	45
Setting the Region	46
Reader Administrator Console	47
Administrator Console Option Selections	48
Status	49
Reader Statistics	49
Reader Gen2 Optional Operation Statistics	50
NXP Custom Command Operation Statistics	52
Event Statistics	53
Other Custom Command Operation Statistics	54
Configure Reader	55
Reader Parameters	55
Read Points	56
Read Points - Advanced	57
Configure Region	58
Certificates	59
Read Tags	72
Communication Settings	73
Configure Network Settings - Ethernet Tab	73
Configure Network Settings - Wi-Fi Tab	74
Configure Network Settings - Bluetooth Tab	75
Configure LLRP Settings	76
SNMP Settings	77

Table of Contents

Wireless Settings	78
Network Services Settings	79
System Time Management	80
IPV6 IP Sec	81
Change Password	82
FX Series User Accounts	82
Managing User Login and Logout	83
GPIO	83
Applications	84
Reader Profiles	85
FIPS Support	86
Firmware Version/Update	87
Firmware Update	88
Commit/Discard	88
System Log	89
Configure System Log	90
Reader Diagnostics	90
Shutdown	91
 Configure and Connect via Wi-Fi and Bluetooth	
Wireless Network Advanced Configuration	93
Sample Configuration Files	94
Preferred Configurations for Access Points	96
Access Point Configuration for Android Device	97
Internet Connection Configuration for iPhone	100
Connecting to a Wireless Network Using a Wi-Fi Dongle	101
Connecting to a Peer Device over Bluetooth Using a Bluetooth Dongle	105
Copying Files to the Reader	107
 Application Development	
Introduction	108
Reference Guides	108
 Firmware Upgrade	
Introduction	109
Prerequisites	109
Failsafe Update	110
Update Phases	110
Updating FX Series Reader Software	111
Verifying Firmware Version	111
Updating Methods	112
Verifying Firmware Version	117
 Troubleshooting	
Troubleshooting	118

Table of Contents

Technical Specifications	
Technical Specifications	124
Cable Pinouts	127
10/100bT Ethernet / PoE Connector	127
USB Client Connector	127
USB Host Connector	128
FX7500 GPIO Port Connections	129
FX9600 GPIO ConnectionsFX9600 GPIO Connections	130
 Static IP Configuration	
Introduction	133
Reader IP Address or Host Name is Known	133
Reader IP is Not Known (DHCP Network Not Available)	135
 RF Air Link Configuration	
Introduction	137
Radio Modes	137
 Copying Files To and From the Reader	
Introduction	141
SCP	141
FTP	141
FTPS	142
 Data Protection	
Introduction	143
 Index	

ABOUT THIS GUIDE

Introduction

This Integration Guide provides information about installing, configuring, and using the FX7500 and FX9600 RFID readers and is intended for use by professional installers and system integrators. The FX7500 and FX9600 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.

Chapter Descriptions

Topics covered in this guide are as follows:

- [Quick Start](#) provides a Quick Start tag reading demonstration.
- [Getting Started](#) provides the FX7500 and FX9600 RFID fixed readers features, parts, and LED indications.
- [Installation and Communication](#) provides information on installing and setting up the FX7500 and FX9600 readers.
- [Administrator Console](#) describes how to connect to the reader and how to use the web-based Administrator Console to configure and manage FX7500 and FX9600 readers.
- [Configure and Connect via Wi-Fi and Bluetooth](#) details wireless network advanced configuration, preferred configurations for access points, and how to connect to a peer device over Bluetooth using a USB Bluetooth dongle.
- [Application Development](#) provides information on developing applications for the FX7500 and FX9600, and includes references to the appropriate guides.
- [Firmware Upgrade](#) provides reader firmware upgrade information on using the web-based Administrator Console and an FTP or FTPS server running a host computer.
- [Troubleshooting](#) describes FX7500 and FX9600 readers troubleshooting procedures.
- [Technical Specifications](#) includes the technical specifications for the readers.
- [Static IP Configuration](#) describes three methods of setting the static IP address on an FX7500 and FX9600 RFID Reader.
- [RF Air Link Configuration](#) describes how to select air link configuration from a set of available air link profiles.
- [Copying Files To and From the Reader](#) describes the SCP, FTP, and FTPS protocols for copying files.
- [Data Protection](#) describes how the FX7500 and FX9600 protects RFID data in transition.

Notational Conventions

The following conventions are used in this document:

- “RFID reader”, “reader”, or “FX Series” refers to the Zebra FX7500 and/or FX9600 RFID readers.
- 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 MN000070Axx.
- FX9600 RFID Reader Quick Start Guide, p/n MN-003087-xx.
- 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 reader.
- RFID Demo Applications User Guide, p/n 72E-160038-xx. Provides instructions for using sample applications which demonstrate how to use Zebra RFID readers.
- FX Series Embedded SDK Installation Guide. Provides instructions for installing the embedded SDK for C and Java.
- FX Series Embedded SDK Sample Application Guide. Explains how to use the embedded sample application with an integrated development environment.
- FX Series 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: 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: 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.

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 13](#)
- [Step 2, Connecting to the Reader on page 14](#)
- [Step 3, First Time / Start-Up Login on page 15](#)
- [Step 4, Set Region on page 16](#)
- [Step 5, Read Tags on page 18](#)

Step 1, Setup

For information on complete component kits available from Zebra, see [Appendix , Technical Specifications](#).

1. Unpack the reader. See [Unpacking the Reader on page 27](#).
2. Place the reader on a desktop.
3. Connect the antenna to antenna Port 1. See [Figure 1](#) and [Figure 2](#).
4. Connect the Ethernet cable to the Ethernet port. See [Figure 1](#) and [Figure 2](#).



NOTE: 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. To connect to power:
 - When using an AC power supply, connect the AC power supply to a power outlet and connect to the power port.
 - When using PoE or PoE+, plug the ethernet cable into the PoE/PoE+ injector.
6. Wait for the green power LED to stay lit. See [System Start-up/Boot LED Sequence on page 38](#) for boot-up details.

Figure 1 FX7500 RFID Fixed Reader Rear Panel Connections

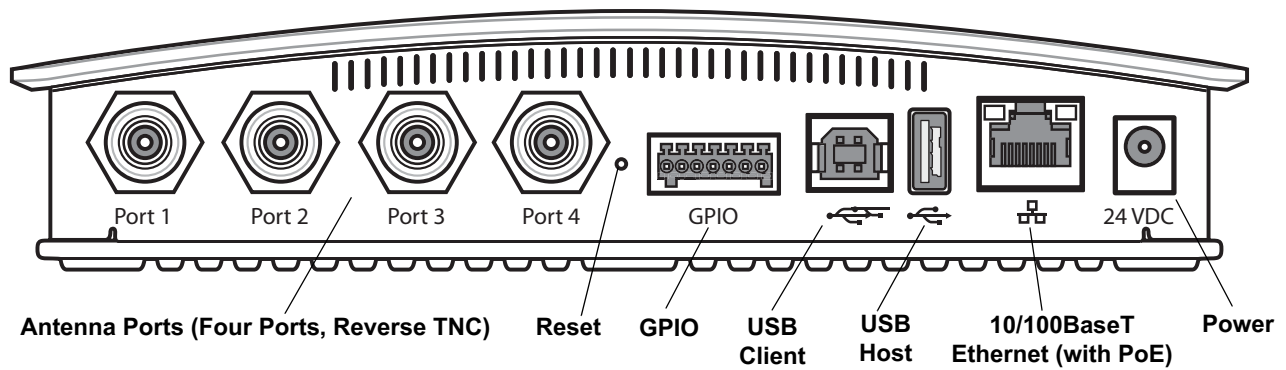
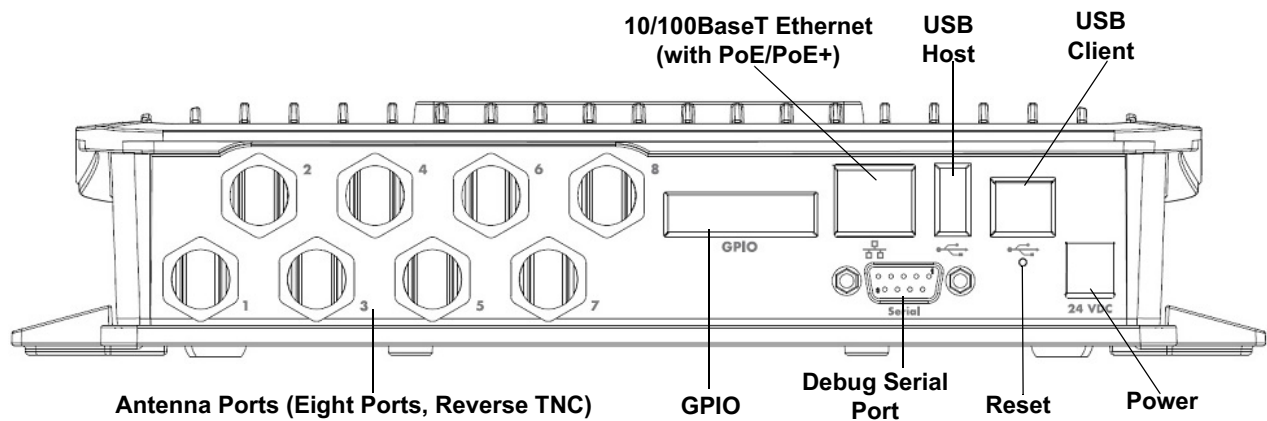


Figure 2 FX9600 RFID Fixed Reader Rear Panel Connections



Step 2, Connecting to the Reader

To connect via host name:

1. Open a browser. The minimum browser recommends are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54.
2. Enter the host name followed by the last three octets of the MAC, provided on a label on the reader, in the browser (For example, for a FX9600 MAC address of 0023683BA63A, use the prefix FX9600, followed by 3BA63A. Enter `http://FX96003BA63A` in the browser address bar) and press Enter. The User Login window appears and the reader is ready.



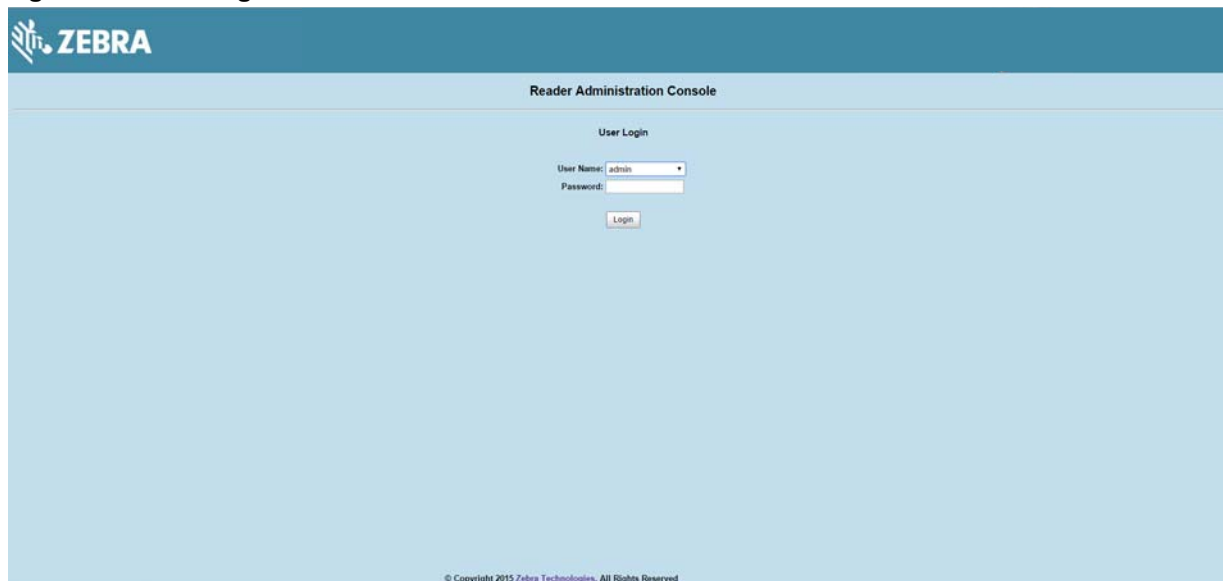
NOTE: Connect the reader to a network that supports host name registration and lookup to ensure the network can access the reader using the host name. For instance, some networks can register host names through DHCP. When first connecting to the reader, it is recommended to keep DHCP enabled in both the PC and in the reader, although it is not guaranteed that 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 bottom of the reader.

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.

Figure 3 User Login Window

The screenshot shows the Zebra Reader Administration Console interface. At the top left is the Zebra logo. The main title is "Reader Administration Console". Below this, the "User Login" section is centered. It contains a "User Name:" dropdown menu with "admin" selected, a "Password:" text input field, and a "Login" button. At the bottom of the window, there is a small copyright notice: "© Copyright 2015 Zebra Technologies, All Rights Reserved".

- ✓ **NOTE:** If you forget the user ID and/or password, see [Reset to Factory Defaults LED Sequence on page 38](#) 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 22 on page 41](#).

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.

Figure 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. Select the I understand check box.
6. Select Set Properties to complete the region selection. The Operation Successful window appears.

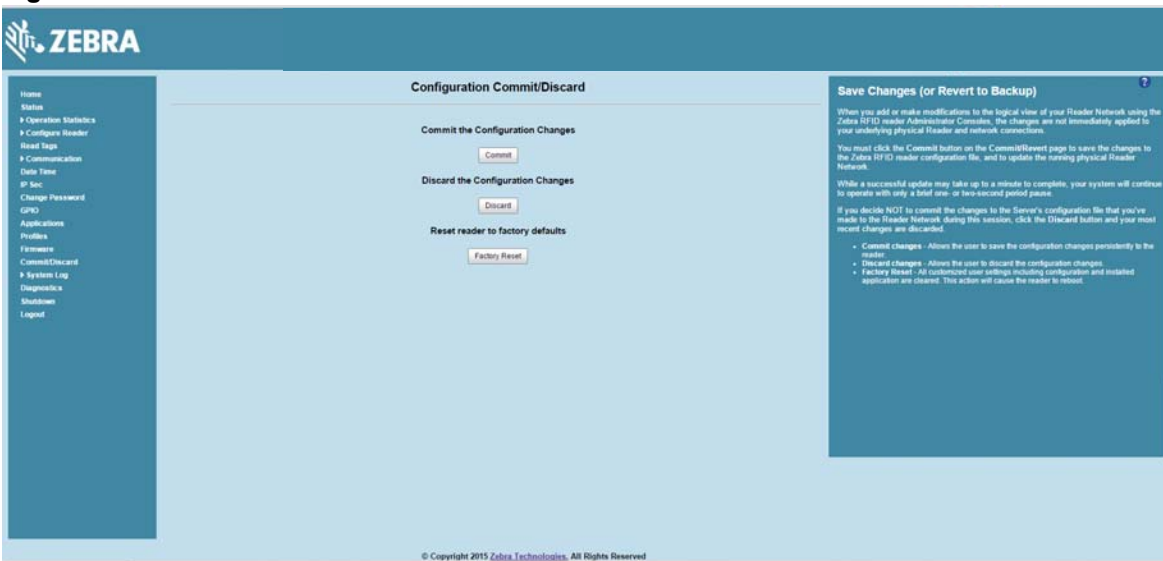
Quick Start

Figure 5 Region Configuration, Operation Successful Window



7. Select Commit/Discard.

Figure 6 Commit/Discard Window



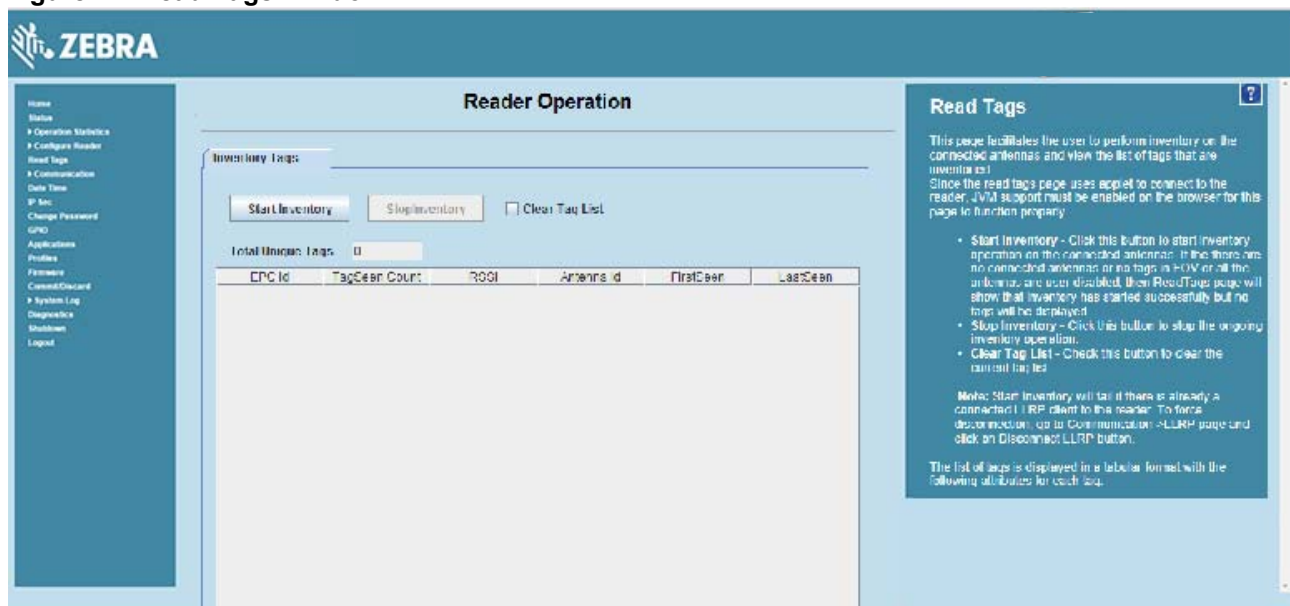
8. Click Commit to save the new region configuration and apply these changes to the reader configuration file, or click Discard to discard the region configuration changes. When the commit completes, the Commit Successful window appears.

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. To install Java Run Time, go to: <http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html>
- ✓ **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/FX9600, 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.

Figure 7 Read Tags Window



- Ensure Java JRE support is enabled on the browser for this page to function properly. To install Java Run Time, go to: <http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html>
- 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.

Getting Started

Introduction

This chapter provides the FX7500 and FX9600 RFID fixed readers features, parts, and LED indications.

FX Series Features

The Zebra FX Series RFID readers are based on Zebra's FX Series fixed reader platform and are easy to use, deploy, and manage. The RFID read performance provides real-time, seamless EPC-compliant tags processing for inventory management and asset tracking applications in large scale deployments.

The Zebra FX Series RFID readers provides a wide range of features that enable implementation of complete, high-performance, intelligent RFID solutions.

Figure 8 FX Series RFID Reader Features

Feature	Zebra FX7500	Zebra FX9600
Air Protocol	ISO 18000-63 (EPC Class 1 Gen2 V2)	ISO 18000-63 (EPC Class 1 Gen2 V2)
Housing Construction	Die-Cast Aluminum Plastic Sheet Metal	Die-Cast Aluminum
Operating System	Linux	Linux
Operating Temperature	-20° to +55° C	-20° to +55° C
Antenna Ports	2 Port, 4 Port	4 Port, 8 Port
Power Supply	+24V DC, POE, POE+	+24V DC, POE, POE+
API	RFID3	RFID3
Monostatic/Bistatic	Monostatic	Monostatic
GPIO	2 Input, 3 Output	4 Input, 4 Output
Maximum RF Output Power	+31.5 dBm	+33 dBm
RX Sensitivity	-82 dBm	-86 dBm
IP Sealing	IP40	IP53
Power-Over-Ethernet	Yes	Yes
Embedded Applications	Yes	Yes
SDKs Embedded Applications: Host Based Applications:	C, Java C, Java, .Net	C, Java C, Java, .Net
Wi-Fi/Bluetooth Dongle Support	Yes	Yes



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 Parts

Figure 9 FX7500 RFID Reader Rear Panel Connections

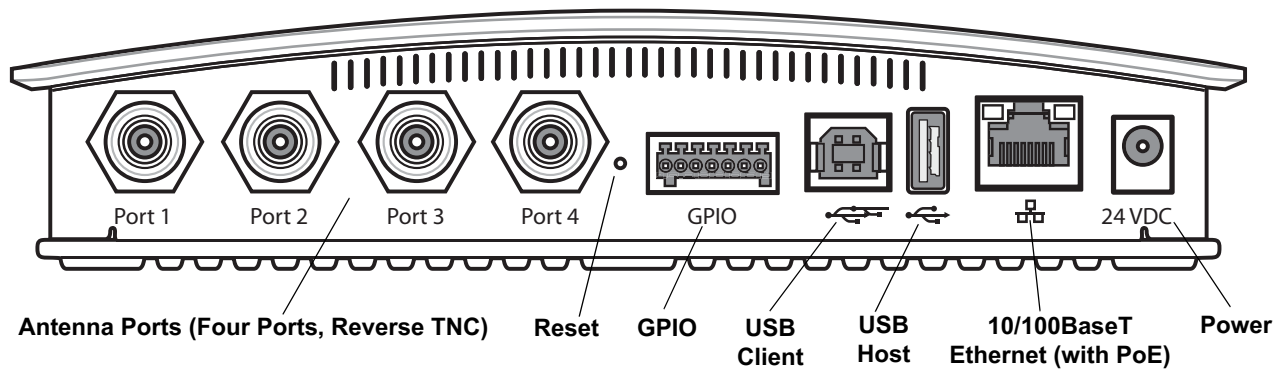
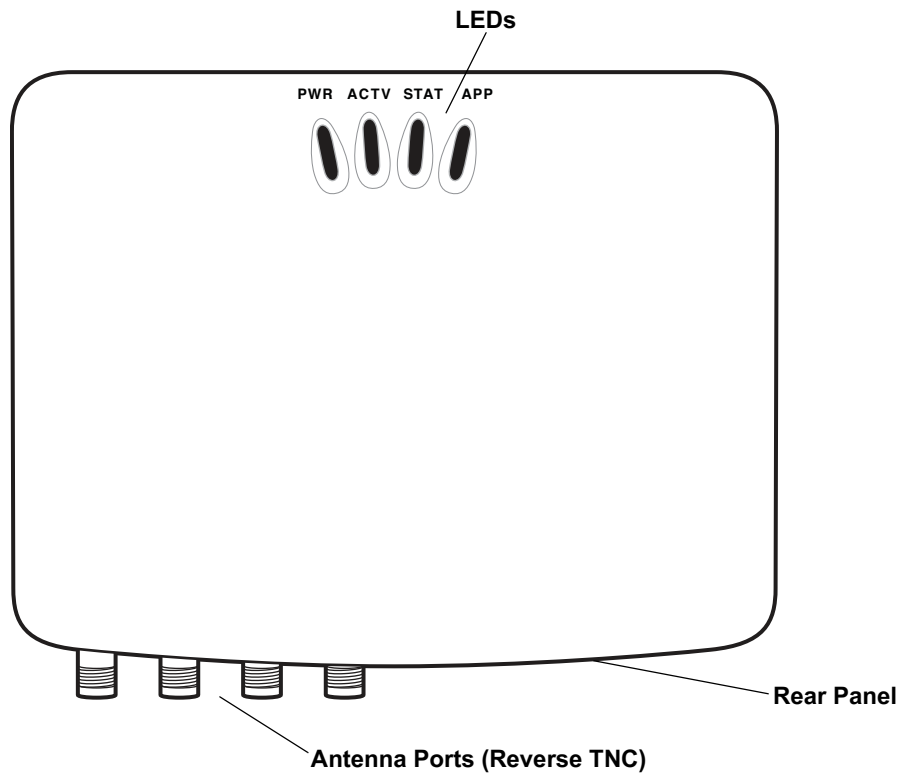


Figure 10 FX7500 RFID Reader



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 Rear Panel

Table 1 Rear Panel Descriptions

Port	Description
Antenna Ports (Reverse TNC)	<p>Two port version: Connect up to two antennas.</p> <p>Four port version: Connect up to four antennas.</p> <p>See Table 8 on page 124 for the maximum antenna gains and RF output powers for both US/Canada and EU. See Connecting FX7500 and FX9600 RFID Reader Antennas on page 31 for connection information.</p>
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 37 for more information.
USB Client	<p>The USB client port supports (by default) a network mode of operation. This enables a secondary network interface as a virtual adapter over USB.</p> <p>Advanced users can create a custom communication protocol on the USB port. See USB Connection on page 34 for connection information.</p>
USB Host	Use the USB host port to connect USB devices such as Wi-Fi / 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 33 for connection information.
Power	DC connector connects to a Zebra approved power supply AC adapter (varies depending on the country). Maximum power 24 VDC, 3.25 A.

FX7500 LEDs

The reader LEDs indicate reader status as described in [Table 2](#). For the LED boot up sequence see [System Start-up/Boot LED Sequence on page 38](#).

Figure 11 FX7500 RFID Readers LEDs

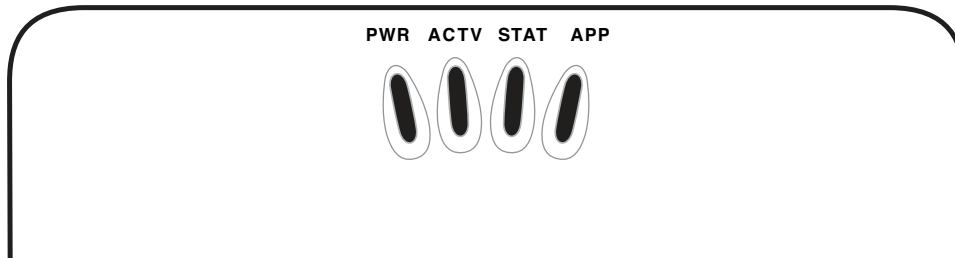


Table 2 FX7500 LED Indications

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

FX9600 Parts

Figure 12 FX9600 RFID Reader Rear Panel Connections

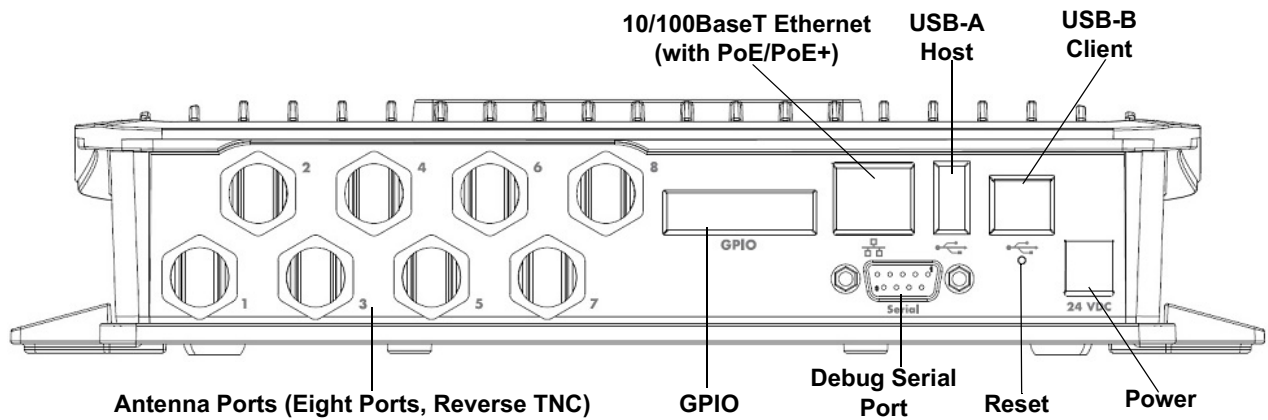
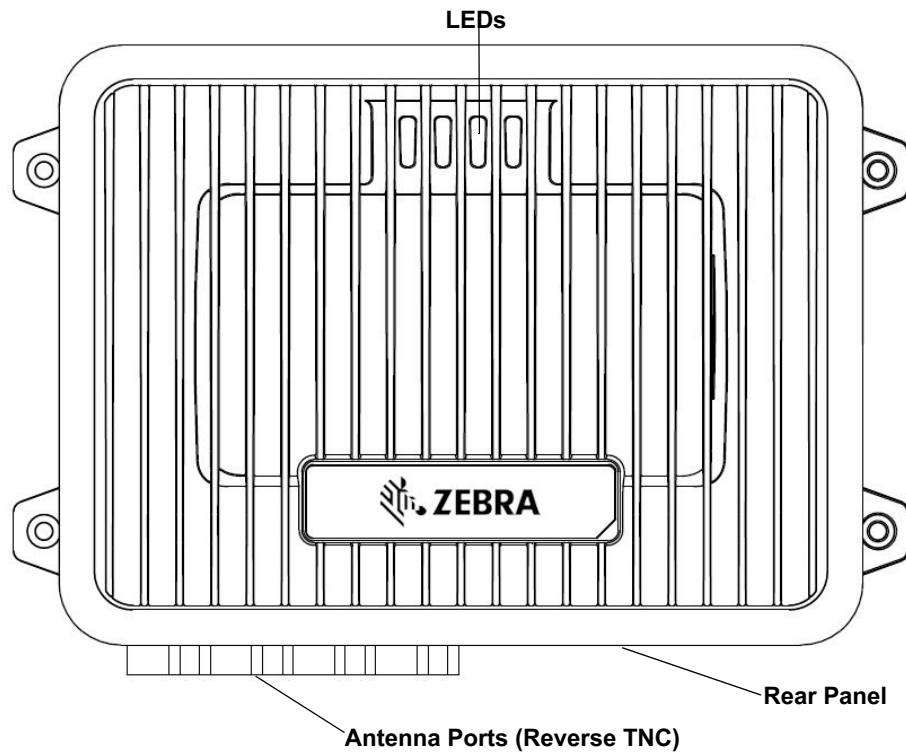


Figure 13 FX9600 RFID Reader



CAUTION: Use only parts provided with the FX9600 RFID readers, or Zebra approved/recommended parts. Substituting other cables or parts can degrade system performance, damage the reader, and/or void the warranty.

FX9600 Rear Panel

Table 3 Rear Panel Descriptions

Port	Description
Antenna Ports (Reverse TNC)	<p>Four port version: Connect up to four antennas.</p> <p>Eight port version: Connect up to eight antennas.</p> <p>See Table 8 on page 124 for the maximum antenna gains and RF output powers for both US/Canada and EU. See Connecting FX7500 and FX9600 RFID Reader Antennas on page 31 for connection information.</p>
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 37 for more information.
USB Client	<p>The USB client port supports (by default) a network mode of operation. This enables a secondary network interface as a virtual adapter over USB.</p> <p>Advanced users can create a custom communication protocol on the USB port. See USB Connection on page 34 for connection information.</p>
USB Host	Use the USB host port to connect USB devices such as Wi-Fi / Bluetooth over USB dongles and flash memory drives.
RS-232	Use the RS-232 interface for debug serial port.
10/100BaseT Ethernet	Insert a standard RJ45 Ethernet cable to connect to an Ethernet network with or without PoE/PoE+ capability, or to a local computer. See Ethernet Connection on page 33 for connection information.
Power	DC connector connects to a Zebra approved power supply AC adapter (varies depending on the country). Maximum power 24 VDC, 3.25 A.

FX9600 LEDs

The reader LEDs indicate reader status as described in [Table 2](#). For the LED boot up sequence see [System Start-up/Boot LED Sequence on page 38](#).

Figure 14 FX9600 RFID Readers LEDs

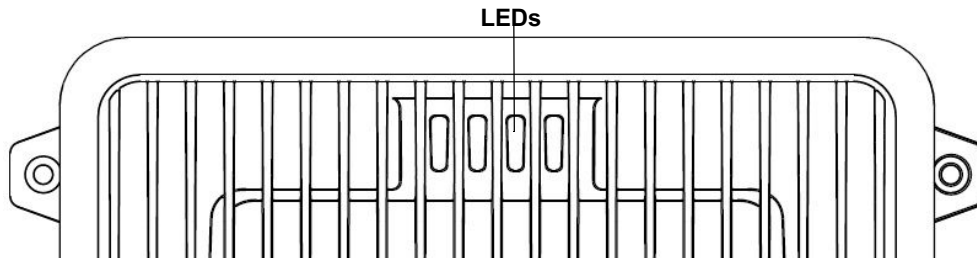


Table 4 FX9600 LED Indications

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

Installation and Communication

Introduction

This chapter includes the following FX7500 and FX9600 RFID reader installation and communication procedures:

- [Unpacking the Reader on page 27](#)
- [Mounting and Removing the FX Series Readers on page 28](#)
 - [Mounting Tips on page 28](#)
 - [Mounting the FX7500 With a Mounting Plate on page 28](#)
 - [FX7500 Direct Mounting on page 29](#)
- [Connecting FX7500 and FX9600 RFID Reader Antennas on page 31](#)
- [Communications and Power Connections on page 33](#)
 - [Ethernet Connection on page 33](#)
 - [USB Connection on page 34](#)
 - [GPIO Interface Connection on page 37](#)
- [System Start-up/Boot LED Sequence on page 38](#)



CAUTION:FX Series 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 FX Series Readers

Mounting Tips

Mount the reader in any orientation. Consider the following before selecting a location for the FX7500 and FX9600 readers:

- 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.
- Ensure that any cable losses between the reader and antenna are taken into account to ensure the desired level of system performance.
- Ensure that power can reach the reader.
- The recommended minimum horizontal mounting surface width is 7 1/2 inches for the FX7500 only. 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 the FX7500 With a Mounting Plate



WARNING: For Mounting in Environmental Air Handling Space (EAHS): Do not install the Bracket, Cables in the EAHS unless they are suitable for use in EAHS per UL 2043.



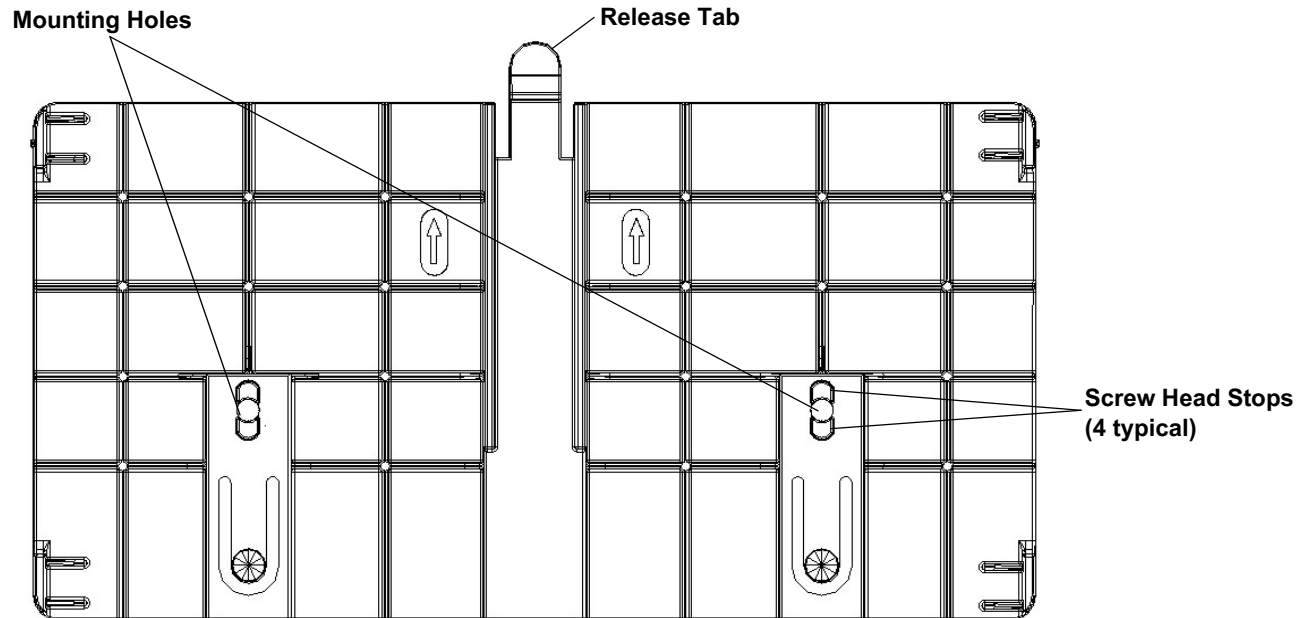
NOTE: The Mounting Plate section applies to the FX7500 RFID Fixed Reader only.

1. Position the mounting plate on a flat surface (wall or shelf). Position the release tab on the top. See [Figure 15](#).
2. Mark the hole locations using the mounting plate as a guide. See [Figure 15](#). 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 15 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 15](#)). 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.

FX7500 Direct Mounting



CAUTION: Not using the mounting plate for the FX7500 reader 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.

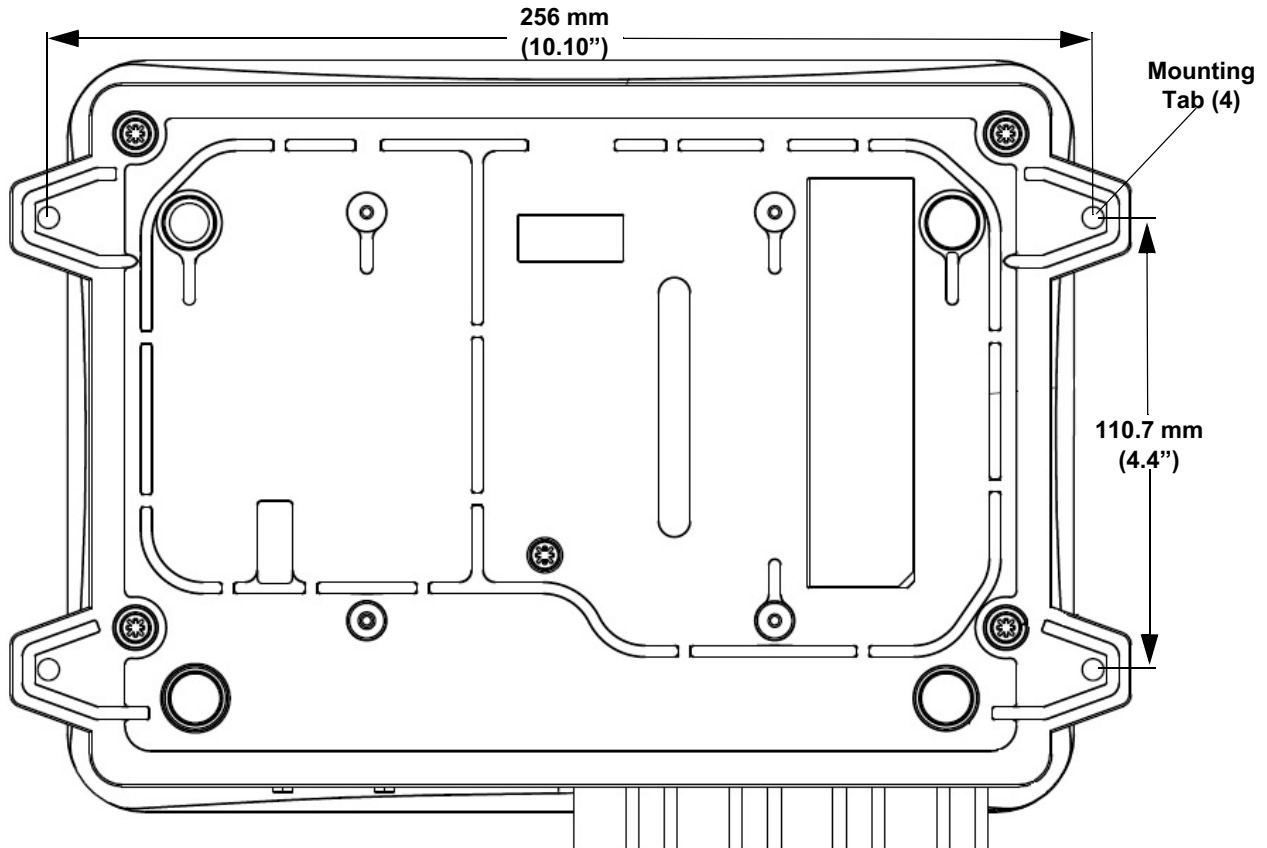
To mount the unit without using the mounting plate:

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.

Mounting the FX9600 Reader

The FX9600 is equipped with two mounting flanges and slotted keyholes that accept three #8 (M4) mounting screws. Pre-drill mounting surface according to the following dimensions. The mounting surface must be able to support up to 10 pounds (2.3 kg).

Figure 16 FX9600 Mechanical Dimensions



Concrete Wall Mounting

To mount the RFID Reader to a hollow concrete block wall, Zebra recommends metal sleeve type concrete anchors that accept #8 screws and flat washers.

Wood or Metal Wall Mounting

To mount the RFID Reader to a wood or sheet metal wall, Zebra recommends either #8 x 1 inch wood screws or #8 x 1 inch sheet metal screws and washers.

Drywall Mounting

To mount the RFID Reader to drywall, Zebra recommends either #8 toggle bolts or #8 drywall anchors.

VESA Mounting

The FX9600 may be mounted via four VESA hole on 100 mm x 100 mm pattern using 10-32 screw.

Connecting FX7500 and FX9600 RFID Reader 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. 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 dBiL. See [Table 5](#) 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 5 Maximum Antenna Power

FX7500/FX9600	US and Canada	EU	Other Countries
Max Radiated Power Allowed	4W EIRP	2W ERP	Per local regulatory requirements
Max Conducted RF Power at Antenna Input ¹	30dBm	N/A	Per local regulatory requirements
¹ Antenna Input refers to the end of the cable that plugs into the antenna (not the antenna port on the reader).			

To connect the antennas to the reader (see [Figure 17](#)):

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 17 FX7500 RFID Reader Antenna Connection

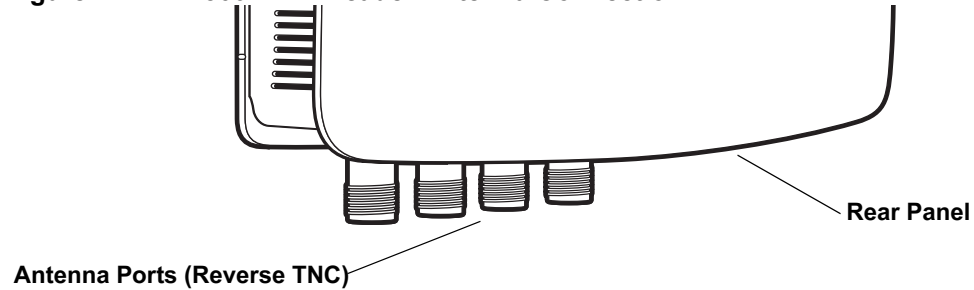
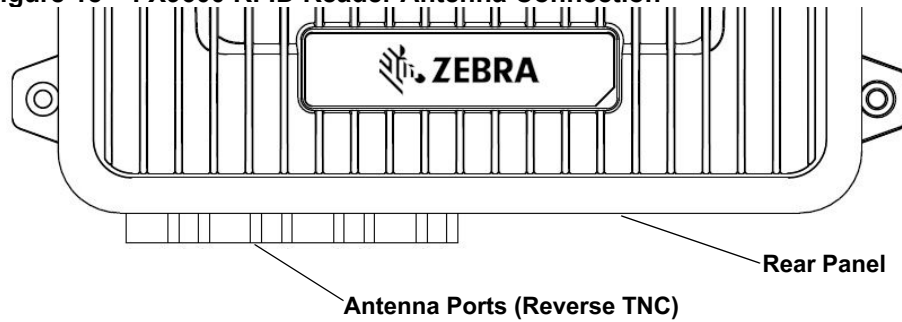


Figure 18 FX9600 RFID Reader Antenna Connection



Communications and Power Connections

Use a standard Ethernet connection, PoE to connect the FX7500 and PoE or PoE + Ethernet for the FX9600 RFID 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 or FX9600 RFID readers using either the reader Zebra AC power supply, or by Power-Over-Ethernet through the Ethernet cable.

Ethernet: Power through AC Outlet

The FX7500 and FX9600 RFID readers 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.
4. Connect the Ethernet cable to the LAN port on the FX7500 reader (see [Figure 9 on page 21](#)) or FX9600 reader (see [Figure 12 on page 24](#)).
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/FX9600 reader power port and rotate clockwise a 1/4 turn for full locking engagement.
8. Verify that the unit booted properly and is operational. See [System Start-up/Boot LED Sequence on page 38](#).
9. On a networked computer, open an internet browser and connect to the reader. See [Connecting to the Reader on page 42](#).
10. Log in to the Administrator Console. See [Administrator Console Login on page 45](#).

Ethernet: Power through Standard PoE or PoE+

The PoE installation option allows the FX7500 and FX9600 RFID readers 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 9 on page 21](#) or [Figure 12 on page 24](#).
2. Connect the other end of the cable to an Ethernet network with PoE or PoE+ capability.
3. Verify that the reader booted properly and is operational. See [System Start-up/Boot LED Sequence on page 38](#).
4. On a networked computer, open an internet browser and connect to the reader. See [Connecting to the Reader on page 42](#).
5. Log in to the Administrator Console. See [Administrator Console Login on page 45](#).



CAUTION: Do not connect to PoE networks outside the building.

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 PC or follow the instructions to install the Microsoft RNDIS driver for Windows 7 below.

To connect the FX7500 or FX9600 to the host PC, insert a USB cable into the USB client port on the reader. For the FX7500, see [Figure 9 on page 21](#) or for the FX9600, see [Figure 12 on page 24](#). 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 or FX9600. The Zebra RNDIS driver supports 32-bit version operating systems 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 35](#)).

To install the RNDIS driver on the host.

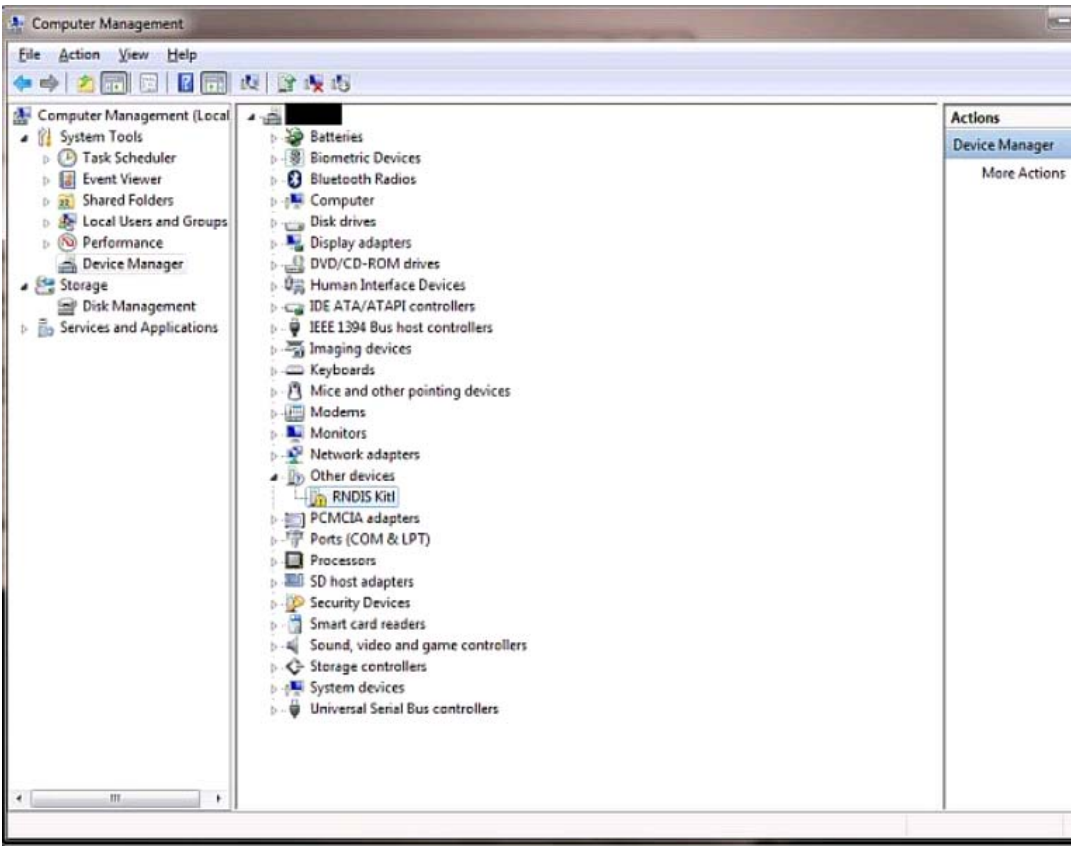
1. Download the installer file Zebra RNDIS.msi from www.zebra.com/support to the host PC.
2. Select this file on the host PC to install the host side drivers for using the USB Remote Network Device Interface on the FX7500 or FX9600.
3. Connect a USB cable between the host and the reader. The Welcome 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:

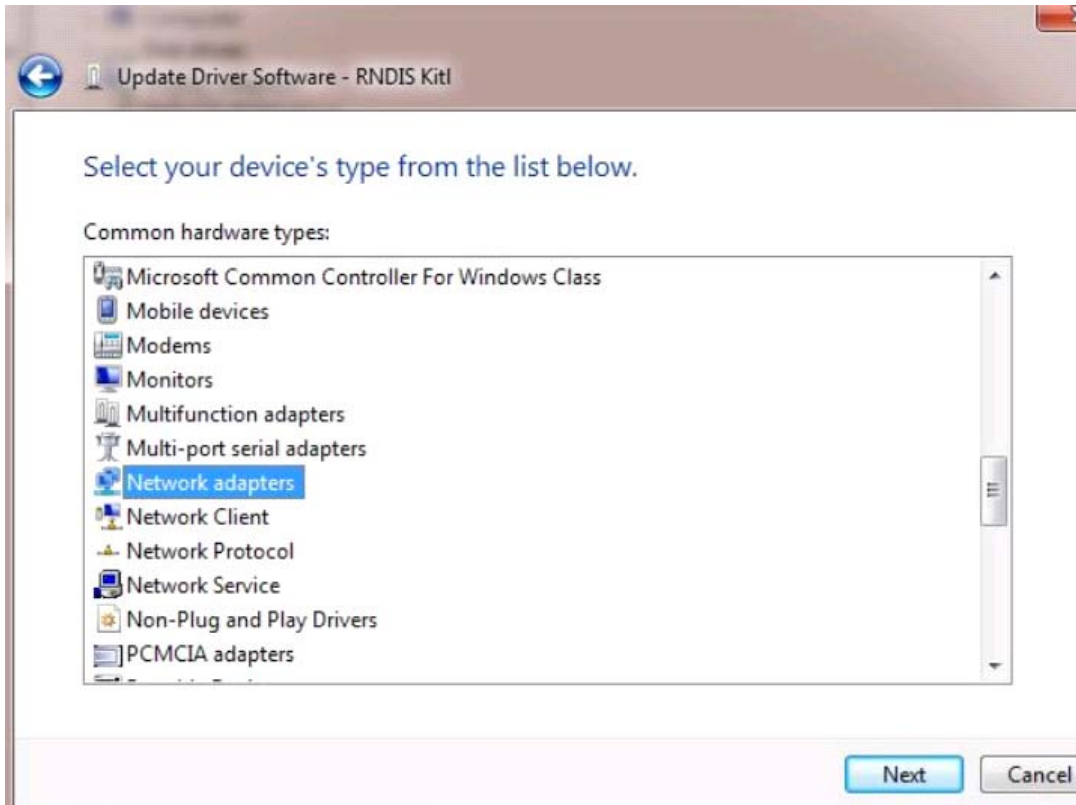
1. After connecting a USB cable between the PC and reader, the RNDIS driver automatically installs. If it does not, right-click on Computer and select Manage. From System Tools, select Device Manager. Under Other Devices, look for an entry for RNDIS with an exclamation icon indicating that the driver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

Figure 19 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.

Figure 20 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.

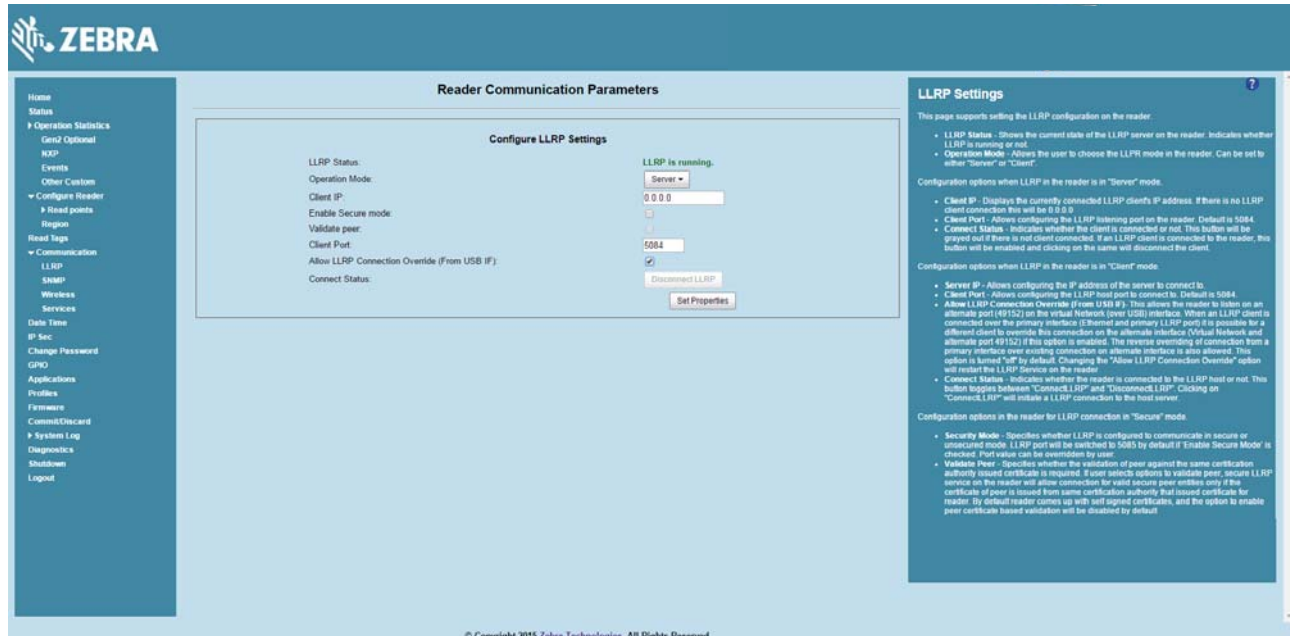
Sample Implementation

This implementation assumes that only one FX7500 or FX9600 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 or FX9600 via the Ethernet interface.
2. The host PC connects to the FX7500 or FX9600 via the USB port. An application on the host PC monitors communication between the primary RFID server and 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 and FX9600 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.

Figure 21 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 allows connecting individual wires independently. A single connector accommodates both inputs and outputs and a +24 VDC supply pin for external sensors and signaling devices. See Table 11 on page 134 for pinout information. The GPIO interface is electrically isolated from the reader's chassis ground, but its ground is common to the power return of the 24 VDC external supply when this is present.

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. They are broadly compatible with industrial sensors with NPN outputs and may also be connected directly to relays or switch contacts. Alternatively, they can be driven by 5V logic. 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 directly. Current flow in the logic high state is close to zero. Although the GPIO interface is fully operational in all power modes, the +24 VDC supply is only available when an external supply is present.



NOTE: Do not connect the +24 VDC output directly to any of the general purpose inputs. Although these can withstand voltages above 5V, they are designed to operate optimally in the range of 0 to +5 VDC.

The general-purpose outputs are open-drain (NPN type) drivers, pulled up to 5V. Each output can withstand voltages up to +30 VDC but should not be driven negative. Drive 24V relays, indicator lamps, etc., by wiring them between the +24 VDC supply pin and the general purpose output pins. 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 requirements exceeds this. Note that the state of the general purpose outputs is inverted, i.e., driving a control pin high at the processor pulls the corresponding output low.

LED Sequences

System Start-up/Boot LED Sequence

For LED locations, see [Figure 11 on page 23](#) for the FX7500 and [Figure 14 on page 26](#) for the FX9600. 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 38](#).

1. Enable tag reading using the web-based Administrator Console (see [Read Tags on page 72](#)) 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 11 on page 23](#). 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.

Administrator Console

Introduction

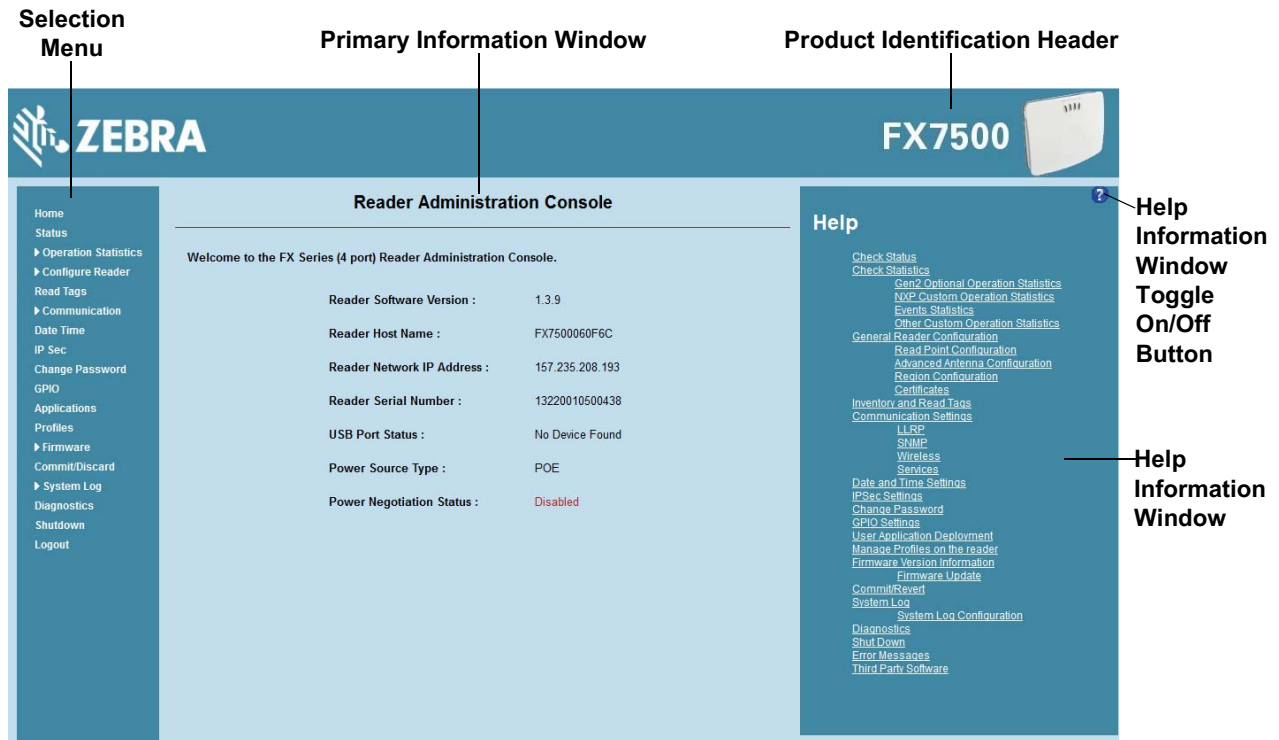
This chapter describes the FX Series web-based Reader Administrator Console functions and procedures. Access the Administrator Console using a web browser from a host computer, and use this to manage and configure the readers. The Administrator Console main window and support windows have four areas,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



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.

- **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

Figure 22 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 85](#).

Resetting the Reader

To reset the reader, press and hold the reset button for not more than 2 seconds. See [Figure 10 on page 21](#) for the reset button location. The reader reboots but retains the user ID and password. See [System Start-up/Boot LED Sequence on page 38](#).



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

Auto Discovery

The FX7500 and FX9600 readers 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 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. 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 41](#).

Connect to the reader in one of two ways:

1. [Connecting via Host Name on page 43](#)
2. [Connecting via IP Address on page 44](#). (To obtain the IP address, see [Obtaining the IP Address via Command Prompt on page 43](#))

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 44](#)
3. Statically assigning an IP. See [Static IP Configuration on page 133](#).

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 44](#).

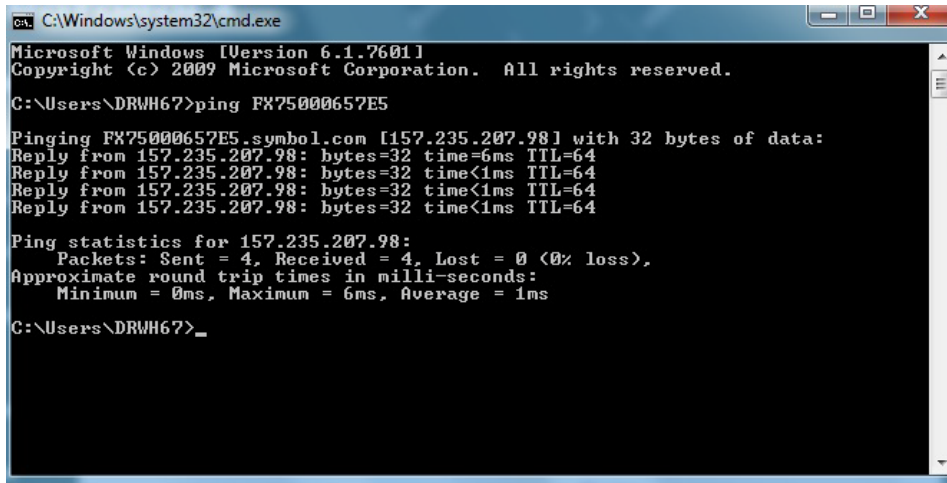


NOTE: When using zero-configuration networking, the FX7500 and FX9600 readers cannot communicate with computers on different subnets, or with computers that do not use automatic private IP addressing.

Obtaining the IP Address via Command Prompt

The Administrator Console provides the reader IP address. See [Figure 22 on page 41](#). 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 43](#).

Figure 23 IP Ping Window



```

C:\Windows\system32\cmd.exe
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>_
  
```

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 IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54.
2. Enter the host name provided on the reader label in the browser (for example: <http://fx7500cd3b0d>) and press Enter. The Console Login window appears and the reader is ready.
3. Proceed to [Administrator Console Login on page 45](#) 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 or FX9600, 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.

Connecting via IP Address

To use the IP address to connect to the reader:

1. Open a browser. The minimum browser recommends are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54.
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 45](#) to login to the reader.

Using Zero-Configuration Networking when DHCP Server is Not Available

If a DHCP server is not available, the FX7500 and FX9600 readers 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 and FX9600 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.

Administrator Console Login



NOTE: The recommended browsers are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox 54. 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 the region of reader operation. Setting the reader to a different region is illegal.

Logging In with Default User ID and Password

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

Figure 24 User Login Window

1. 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.

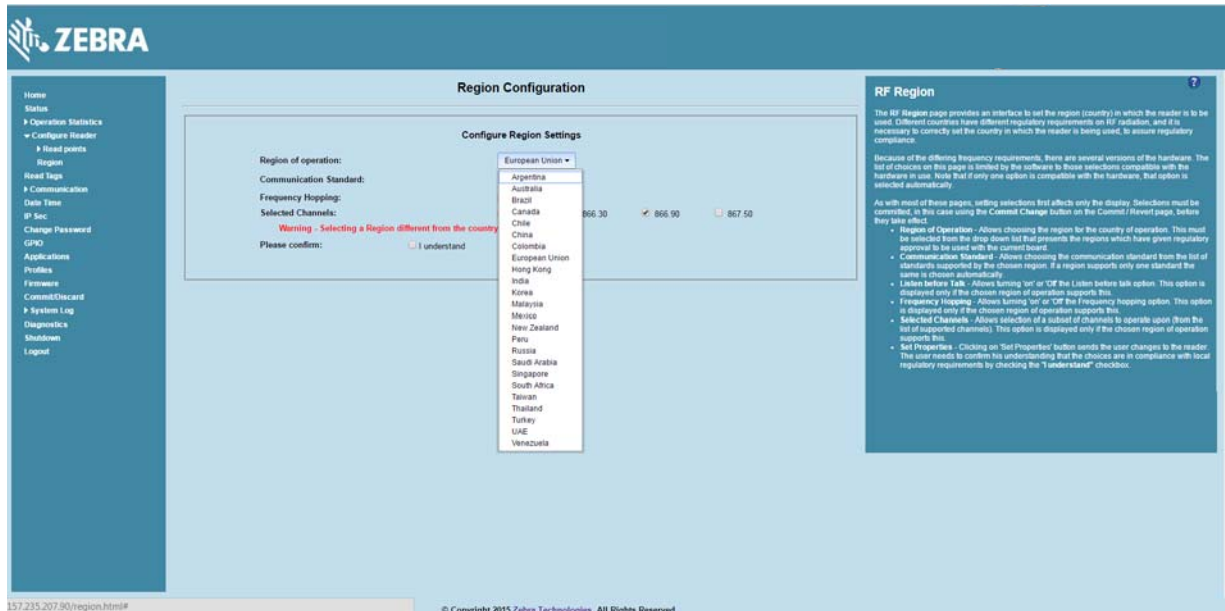
Setting the Region

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.

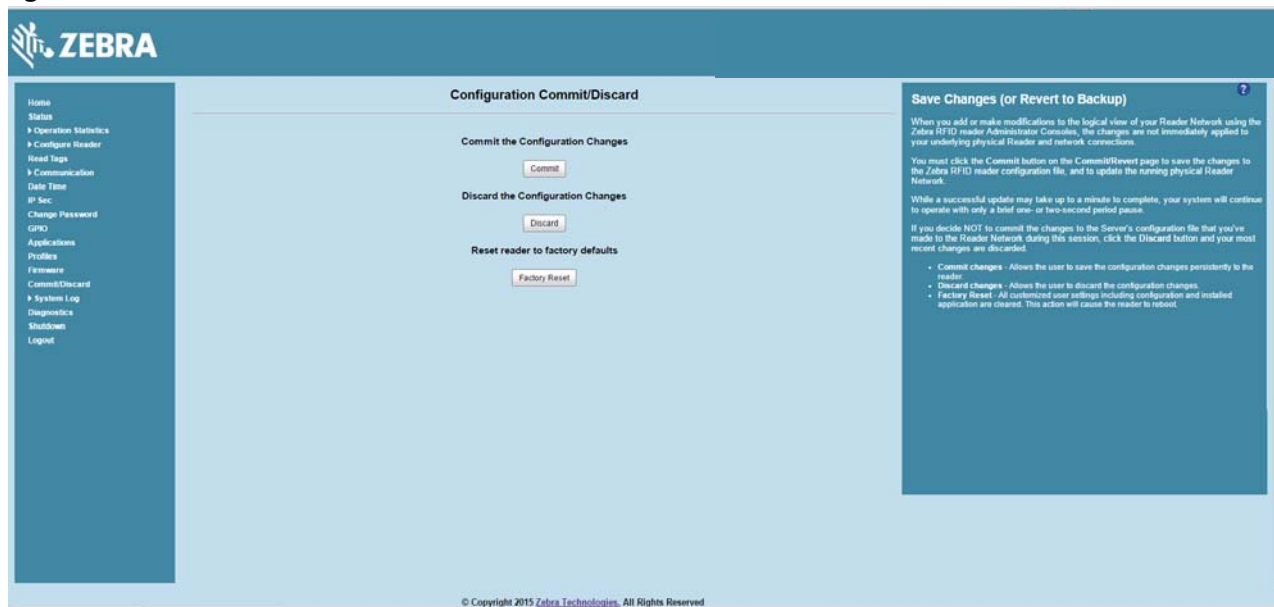
Figure 25 Selecting the Region



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.

Figure 26 Commit/Discard Window



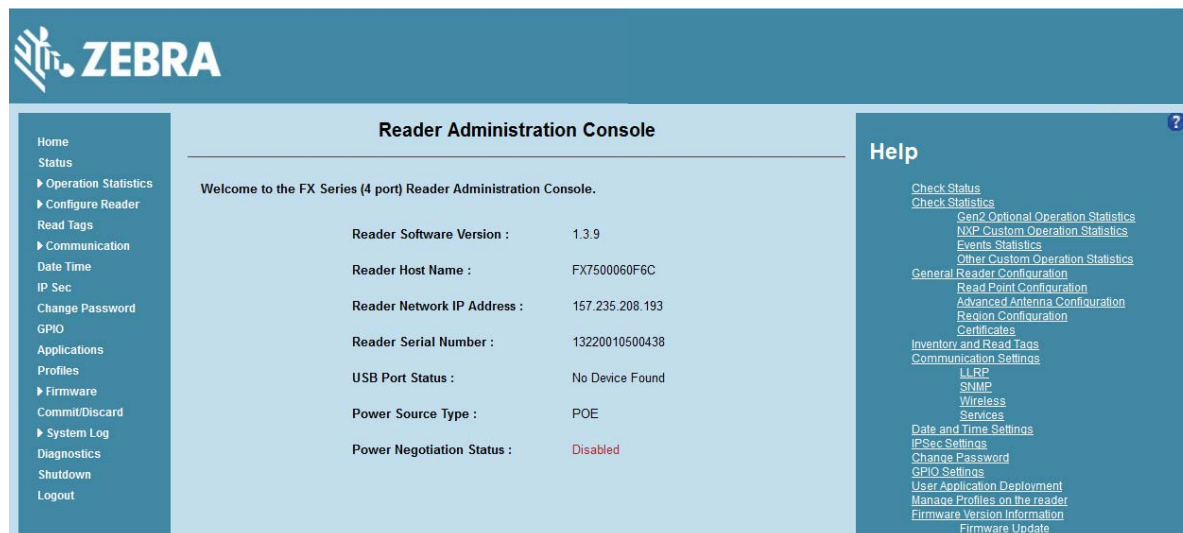
- Click Commit to apply the changes to the reader configuration file, or Discard to discard the new region configuration changes.

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.

Figure 27 Reader Administrator Console Main Window



Administrator Console Option Selections

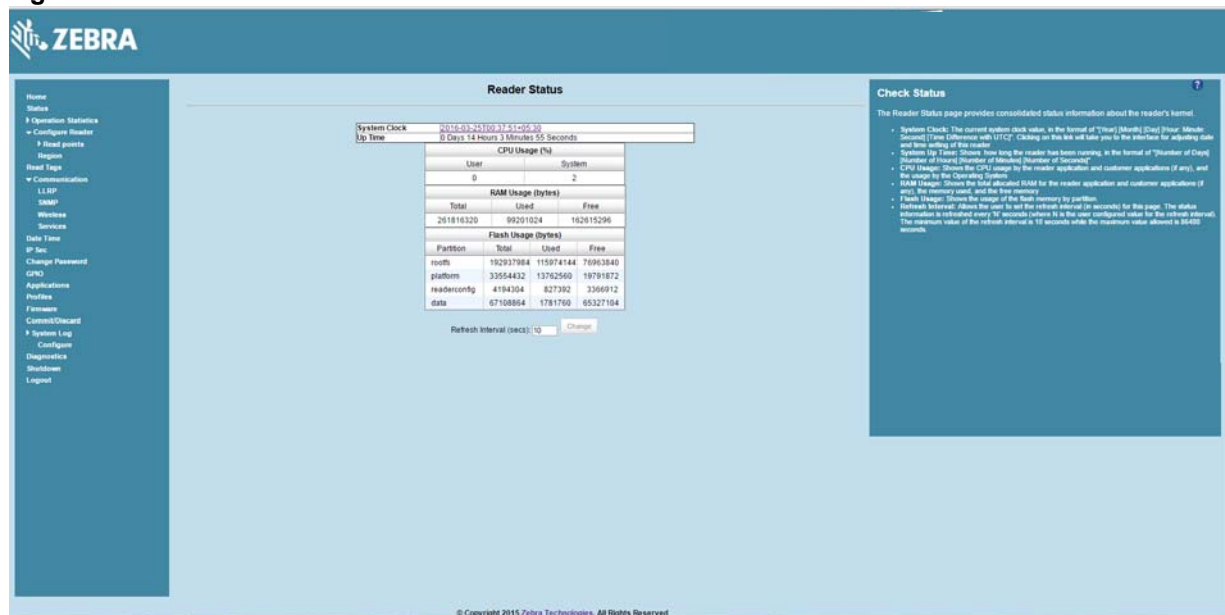
Click an item from the selection menu on the left to select:

- Status - see [Status on page 49](#)
- Operation Statistics - see [Reader Statistics on page 49](#)
 - Gen2 Optional - see [Reader Gen2 Optional Operation Statistics on page 50](#)
 - NXP - see [NXP Custom Command Operation Statistics on page 52](#)
 - Events - see [Event Statistics on page 53](#)
 - Other Custom - see [Other Custom Command Operation Statistics on page 54](#)
- Configure Reader - see [Configure Reader on page 55](#)
 - Read Points - see [Read Points on page 56](#)
 - Advanced - see [Read Points - Advanced on page 57](#)
 - Region - see [Configure Region on page 58](#)
 - Certificates - see [Certificates on page 59](#)
- Read Tags - see [Read Tags on page 72](#)
- Communication - see [Communication Settings on page 73](#)
 - LLRP - see [Configure LLRP Settings on page 76](#)
 - SNMP - see [SNMP Settings on page 77](#)
 - Wireless - see [Wireless Settings on page 78](#)
 - Services - see [Network Services Settings on page 79](#)
- Date/Time - see [System Time Management on page 80](#)
- IP Sec - see [IPV6 IP Sec on page 81](#)
- Change Password - see [Change Password on page 82](#)
- GPIO - see [GPIO on page 83](#)
- Applications - see [Applications on page 84](#)
- Profiles - see [Reader Profiles on page 85](#)
- Firmware - see [Firmware Version/Update on page 87](#)
 - Update - see [Firmware Update on page 88](#)
- Commit/Discard - see [Commit/Discard on page 88](#)
- System Log - see [System Log on page 89](#)
 - Configure - see [Configure System Log on page 90](#)
- Diagnostics - see [Reader Diagnostics on page 90](#)
- Shutdown - see [Shutdown on page 91](#)
- 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).

Figure 28 Reader Status Window



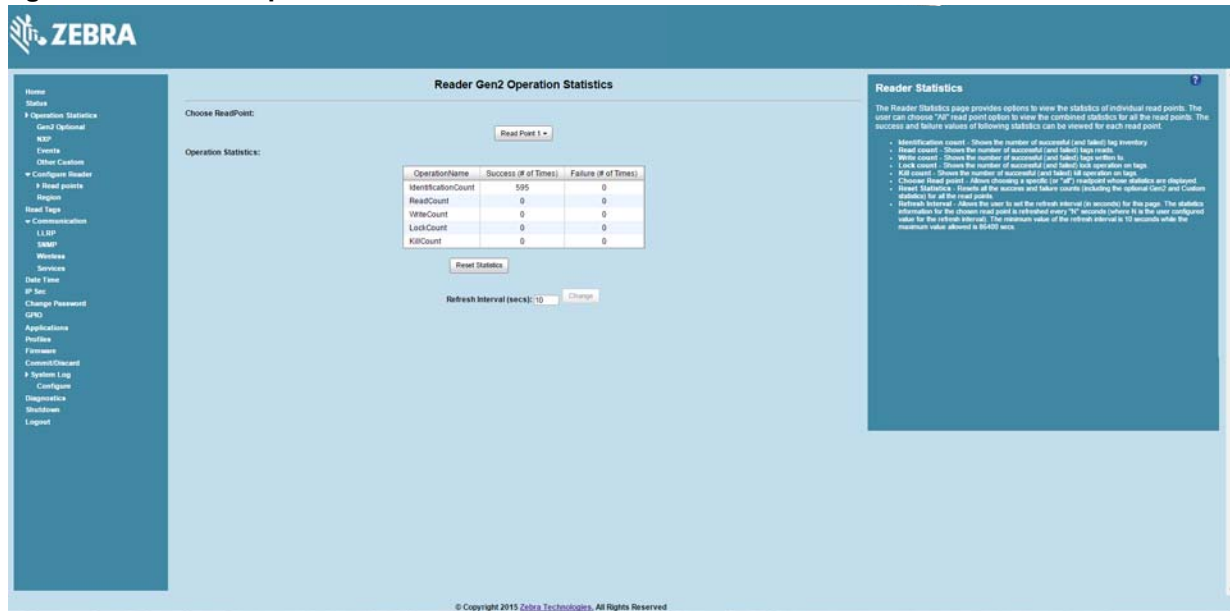
The Reader Status window provides consolidated reader status information:

- **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.

Figure 29 Reader Operation Statistics Window

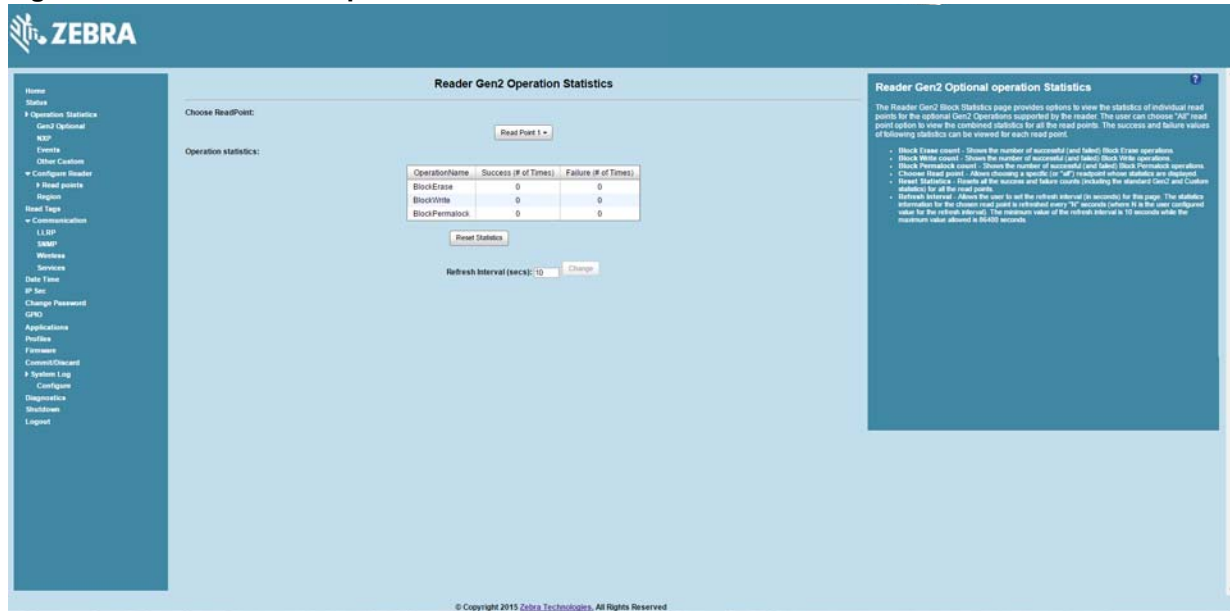


- **Choose ReadPoint** - Select a specific read point or select All from the drop-down list to display the statistics.
- **IdentificationCount** - Displays the number of successful (and failed) tag inventories.
- **ReadCount** - Displays the number of successful (and failed) tag reads.
- **WriteCount**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

Figure 30 Reader Gen2 Operation Statistics Window

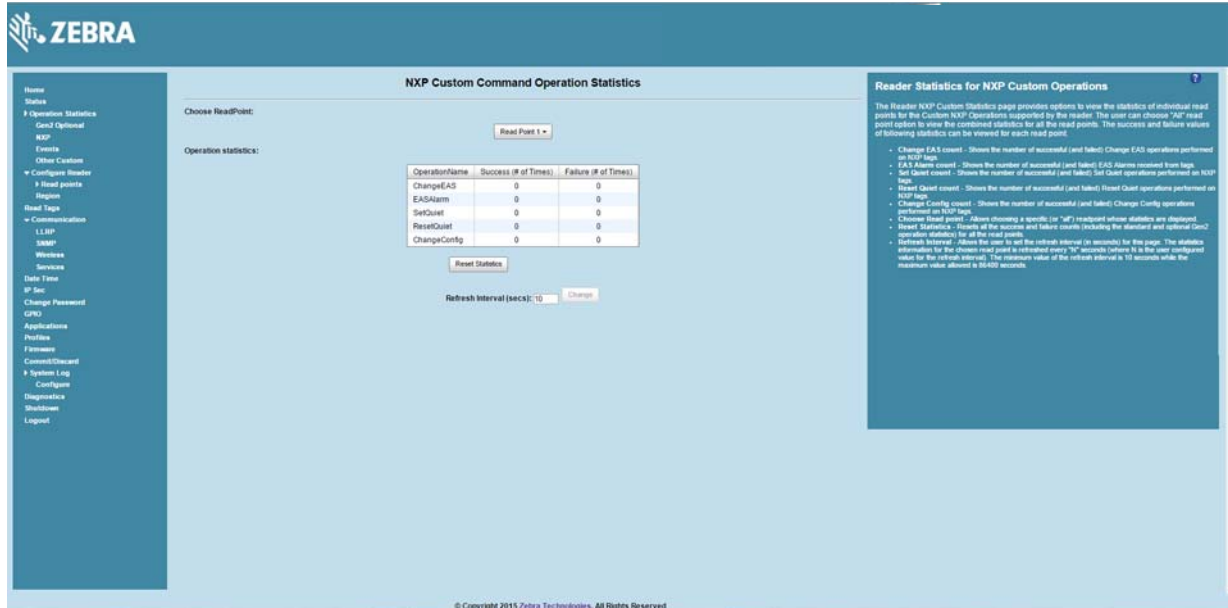


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select All to view the combined statistics for all read points.
- **BlockErase** - Displays the number of successful (and failed) block erase operations.
- **BlockWrite** - Displays the number 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.

Figure 31 NXP Custom Command Operation Statistics Window

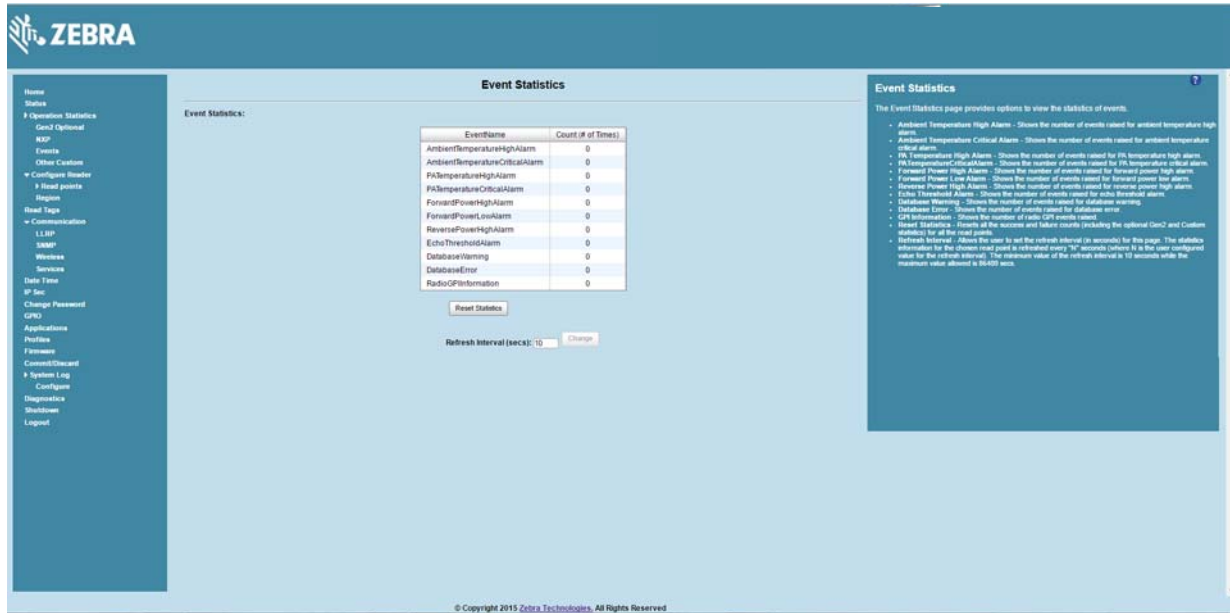


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select All to view the combined statistics for all read points.
- **ChangeEAS** - Displays the number of successful (and failed) change EAS operations performed on NXP tags.
- **EASAlarm** - Displays 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.

Figure 32 Event Statistics Window

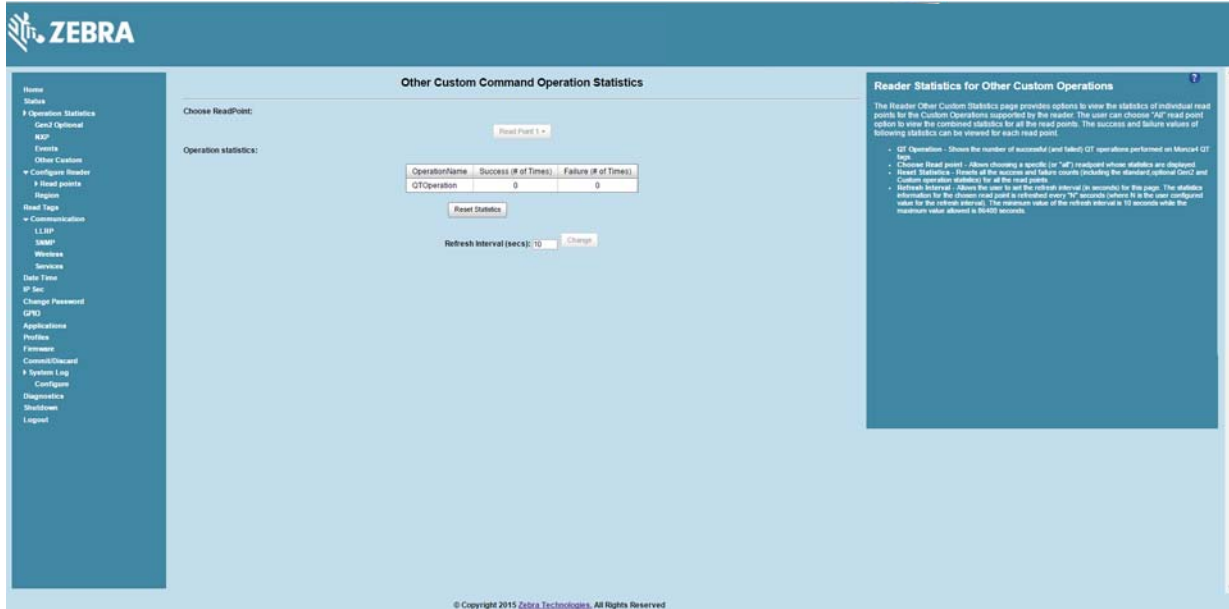


- **AmbientTemperatureHighAlarm** - Displays the number of events raised for ambient temperature high alarm.
- **AmbientTemperatureCriticalAlarm** - Displays the number of events raised for ambient temperature critical alarm.
- **PATemperatureHighAlarm** - Displays the number of events raised for PA 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.

Figure 33 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 menus to access the following functions.

Reader Parameters

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

Figure 34 Reader Parameters

Reader Parameters

Zebra - FX7500 13220010500438

Configure Reader

Name: FX7500060FBC FX75
 Description: FX7500060FBC 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 negotiation 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 attempt 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.

- **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 and FX9600 readers start 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.

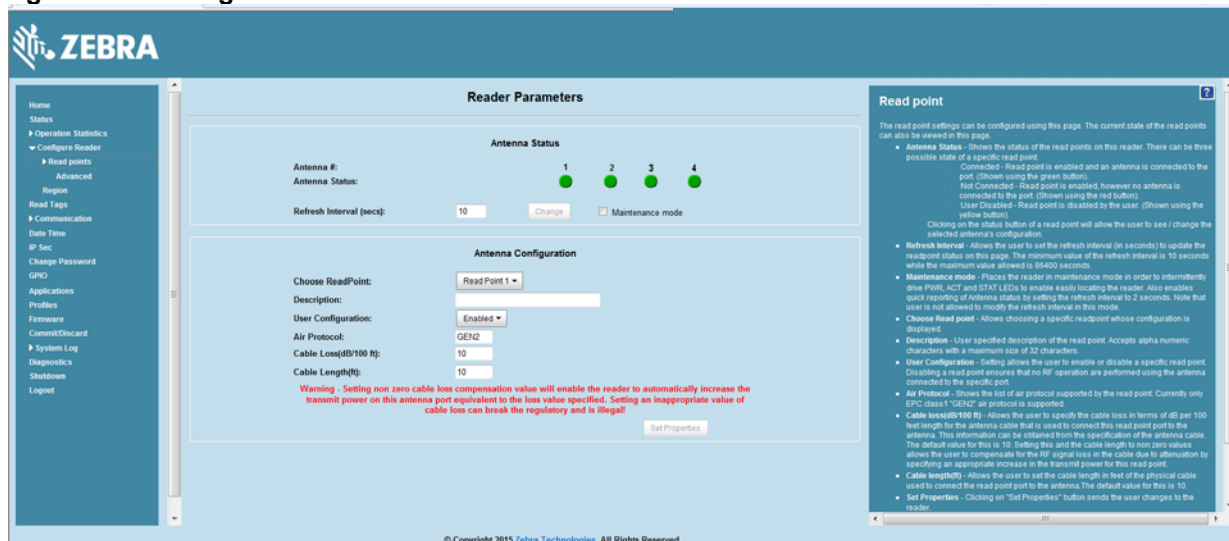
After power negotiation is enabled, and committed, it takes approximately 2 to 5 minutes to reach the PoE+ level. This is the time taken for LLDP packet exchange between the reader and the switch for power negotiation.

These settings only affect the display. Use [Commit/Discard on page 88](#) 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.

Figure 35 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 read point 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.

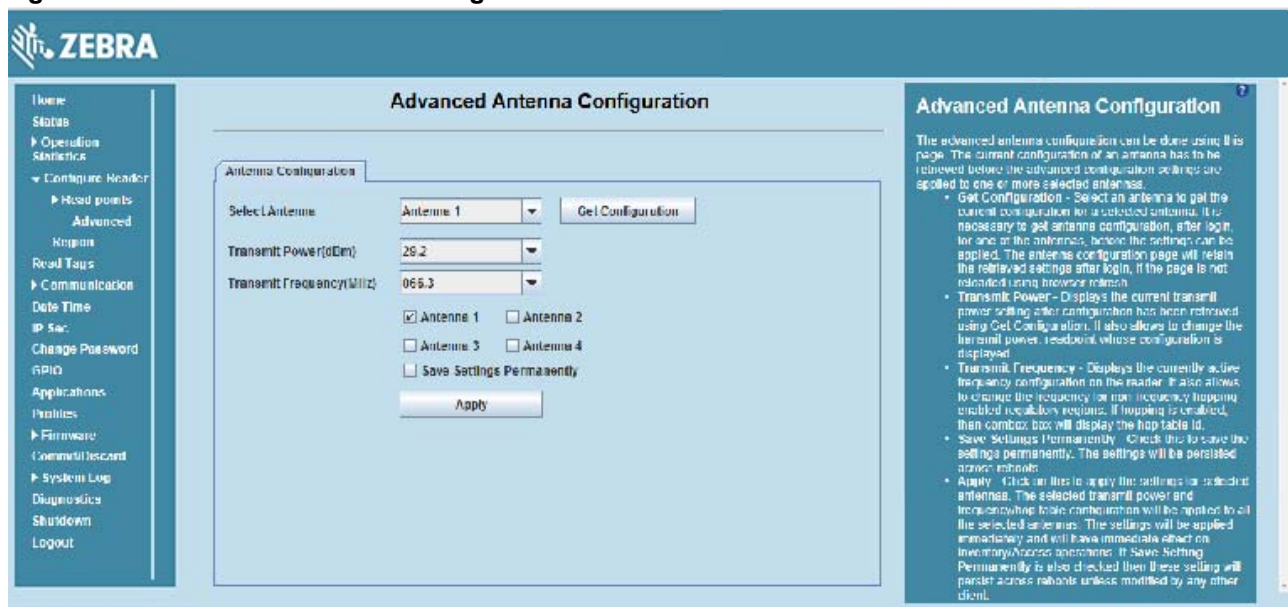
Antenna Configuration

- **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 88](#) 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.

Figure 36 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.

Figure 37 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 88](#) 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 79](#).
- **File Transfer Service (FTPS - explicit SSL/TLS over FTP)**. See [Network Services Settings on page 79](#).
- **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 76](#).

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

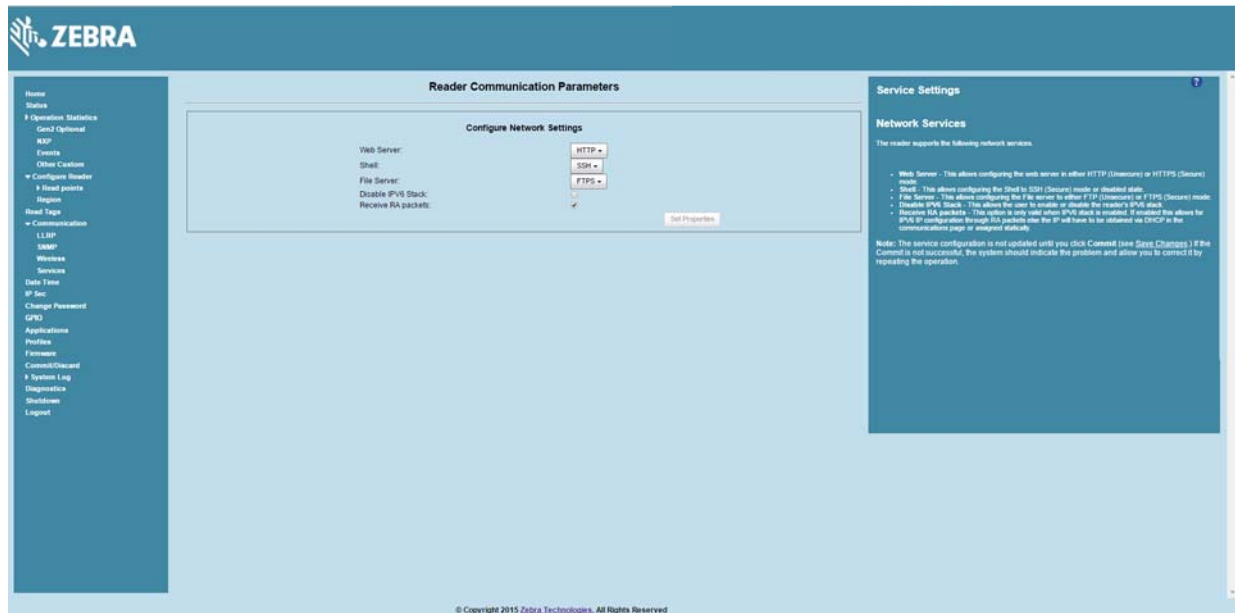
✓ **NOTE:** The **Validate Peer** option in Secure LLRP Service configuration enables authentication of reader and/or clients using digital certificates. You must import a custom certificate (instead of the default self-signed certificate) to the reader to enable this option. See [Configure LLRP Settings on page 76](#) 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

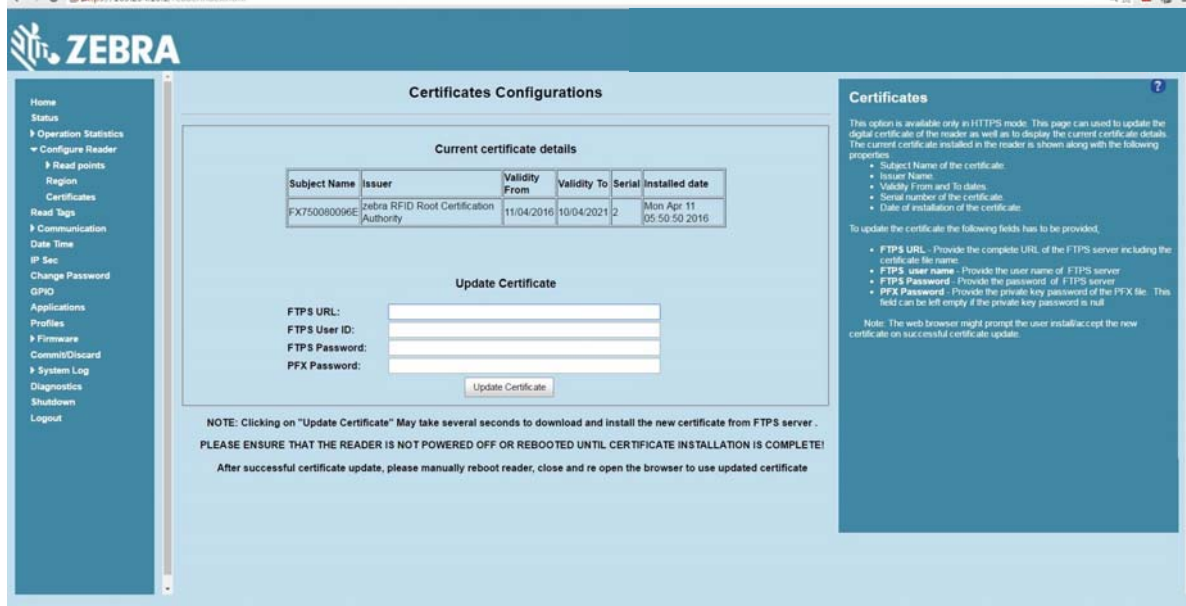
The Certificate Configuration page is available under the Configure Reader menu when the Administrator Console is in HTTPS mode only. To enable HTTPS mode, select **Communication > Services**, and on the **Reader Communication Parameters** page select **HTTPS** from the **Web Server** drop-down menu.

Figure 38 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.

Figure 39 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 76](#).
- 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 79](#). 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.

FX Series readers do 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 and FX9600 support 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 and FX9600 support 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

FX Series readers require 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 on the host machine:

- **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 signing request
echo 'CA Signing reader certificate....'

export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf

openssl ca -extensions ssl_client_server -in tempreq.pem -out reader_cert.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_cert.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 signing request
echo 'CA Signing client certificate....'

export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf

openssl ca -in tempreq.pem -out client_cert.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_cert.pem'
```

Script Usage

The following section illustrates how to use the previous scripts on the host machine.

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 `samplerreader.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.

Figure 40 Read Tags Window

Reader Operation

Inventory Tags

Start Inventory Stop Inventory Clear Tag List

Total Unique Tags 8

EPC Id	TagSeen Count	RSSI	Antenna Id	FirstSeen	LastSeen
9229a229a229a2...	259	38	13812254050402	13812254050402	13812254050402
9229a229a229a2...	250	38	13812254050402	13812254050402	13812254050402
00d30303030303...	257	42	13812254050402	13812254050402	13812254050402
76125425425425...	250	30	13812254050402	13812254050402	13812254050402
11111111111111...	258	38	13812254050402	13812254050402	13812254050402
h0d0c0d0c0d0c0...	258	37	13812254050402	13812254050402	13812254050402
11111111111111...	250	30	13812254050402	13812254050402	13812254050402
a000c0c0c0c0c0...	258	40	13812254050402	13812254050402	13812254050402

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 ajax to connect to the reader, JRE 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 there are no connected antennas or no tags in EPC 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.

Notes: Start Inventory will fail if there is already a connected LLRP client to the reader. To force disconnection, go to Communications->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.

- **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:

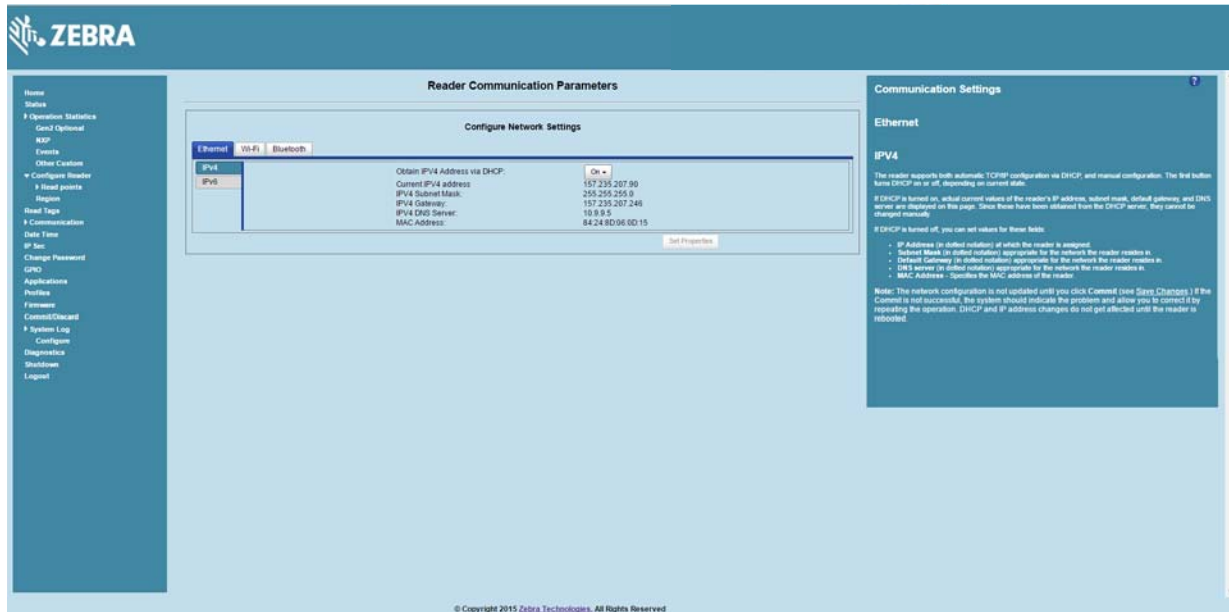
- **EPC Id** - Unique tag EPC ID.
- **TagSeen Count** - Number of times the tag was identified on the specific antenna.
- **RSSI** - Received Signal Strength Indication.
- **Antenna Id** - Antenna ID on which the tag is seen.
- **FirstSeen time stamp** - UTC time (in microseconds) when the tag was first 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, Wi-Fi, and Bluetooth. Each tab has options for IPV4 and IPV6.

Configure Network Settings - Ethernet Tab

Figure 41 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.

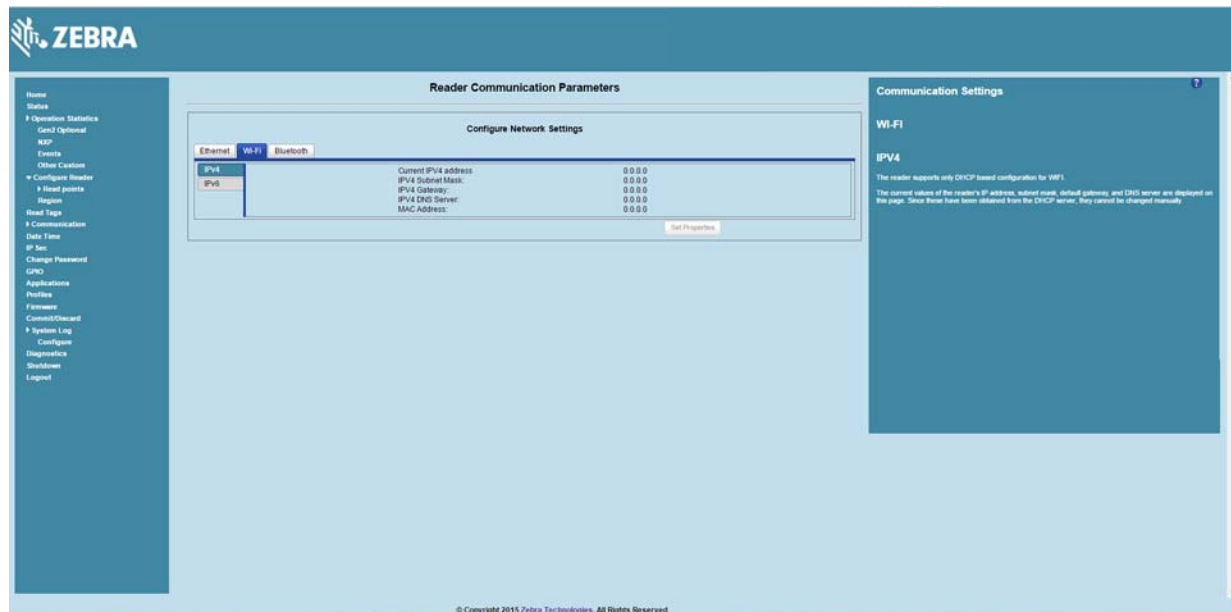
- **Current IPV6 Address** - IP address (in dotted notation) at which the reader is assigned.
- **Prefix Length** - Prefix length appropriate for the network in which the reader resides.
- **IPV6 Default Gateway** - Default gateway (in dotted notation) appropriate for the network in which the reader 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

Figure 42 Configure Network Settings - Wi-Fi Tab



IPV4

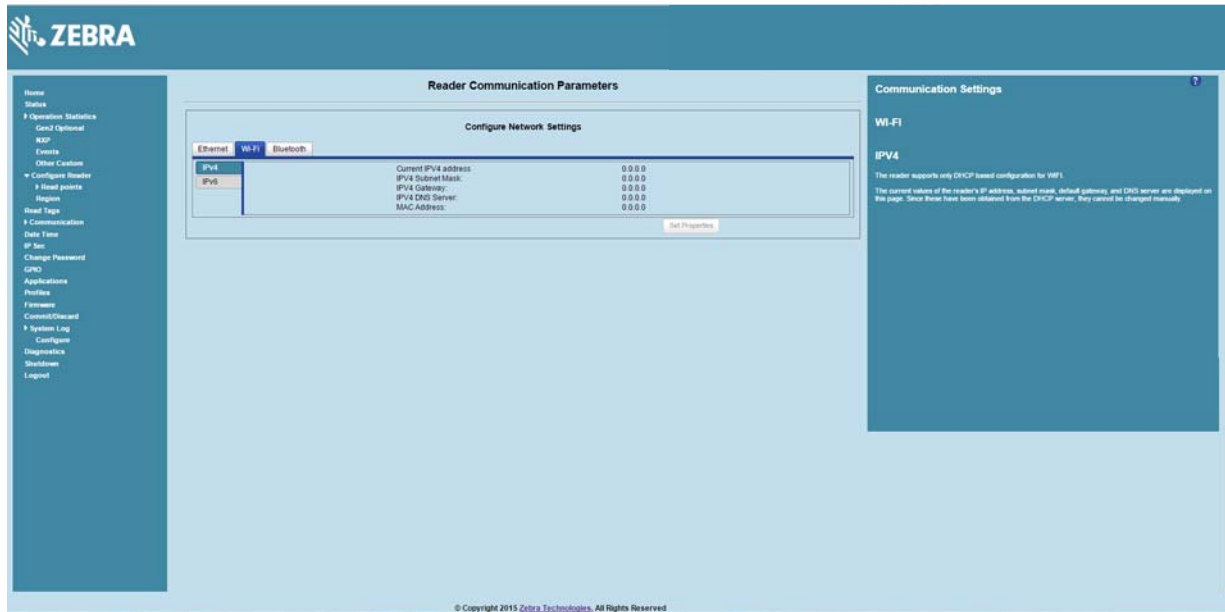
The reader supports only DHCP-based configuration for Wi-Fi. This window displays the current values of the reader's IP address, subnet mask, default gateway, and DNS server. Since these are obtained from the DHCP server, they cannot be changed manually.

IPV6

The reader supports only DHCP based configuration for Wi-Fi. 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

Figure 43 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:

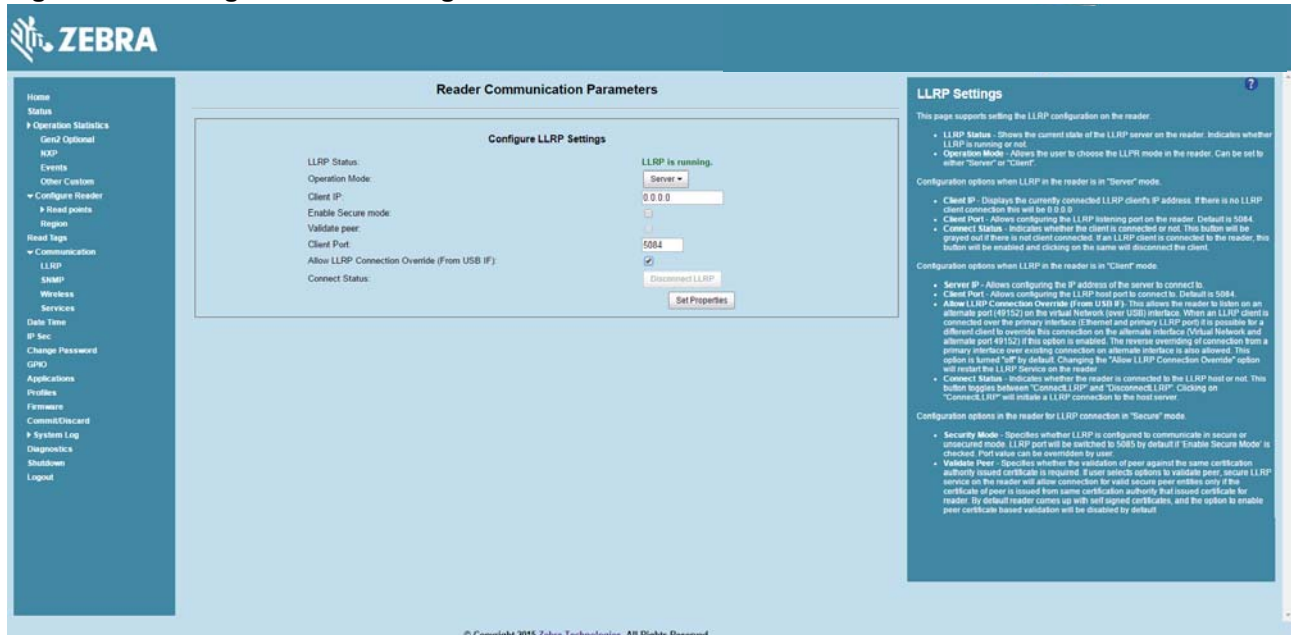
- **Discoverable** - Select whether the reader is seen by other Bluetooth-enabled devices on discovery.
- **Pairable** - Select whether any Bluetooth-enabled device can pair with reader.
- **Use Passkey** - Enable this option to mandate the connecting device to supply a pre-determined passkey to use 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

Figure 44 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.

Figure 45 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 LLRP 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 unsecured 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.

Figure 46 Configure SNMP Settings Window

The screenshot shows the ZEBRA Administrator Console interface. On the left is a sidebar with a tree view containing options like Home, Status, Operation Statistics, and Configuration. The main content area is titled 'Reader Communication Parameters'. Inside this area is a sub-section 'Configure SNMP Settings' which includes four configuration fields: 'Send SNMP Trap To' (a text input), 'SNMP Community String' (a text input), 'SNMP Version' (a dropdown menu currently showing 'V1'), and 'Send Server Heartbeat' (a checkbox that is checked). A 'Set Properties' button is located at the bottom right of this configuration section. To the right of the main configuration area is a panel titled 'SNMP Settings' which contains a warning message and a list of bullet points explaining the configuration options. A note at the bottom of this panel states that changes to 'Send SNMP Trap To' and 'Send Server Heartbeat' take effect immediately after clicking 'Set Properties', while changes to 'SNMP Community String' and 'SNMP Version' require a reboot.

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

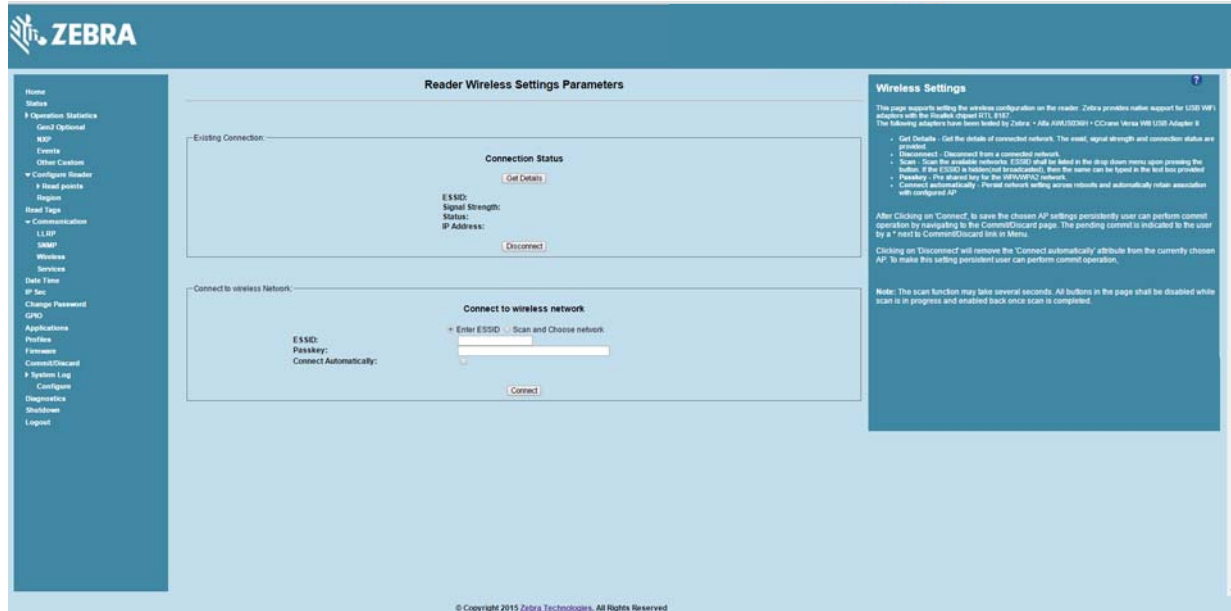
- **Send SNMP Trap To** - Configures the host IP address to which the SNMP trap is sent. Leave this blank to send no traps to any host.
- **SNMP Community String** - SNMP community string to use for SNMP set and get.
- **SNMP Version** - SNMP version to use in the reader. Supported versions are V1 and 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 Setting Parameters window.

Figure 47 Wireless Settings Window



Use the Wireless Setting window to set the wireless configuration on the reader. Zebra provides native support for USB Wi-Fi adapters with the Realtek chipset RTL 8187 and RTL 8812AU. The following dongles have been tested:

Table 6 Supported Wi-Fi Dongles

Dongle Model	Zebra FX7500	Zebra FX9600
TP-Link: AC 1200 Realtek RTL8812AU	No	Yes
ASUS: USB-AC56 Realtek RTL8812AU	No	Yes
Alfa Network Realtek RTL8812AU	No	Yes
Alfa AWUS036H	Yes	Yes
CCrane Versa Wifi USB Adapter II	Yes	Yes

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.

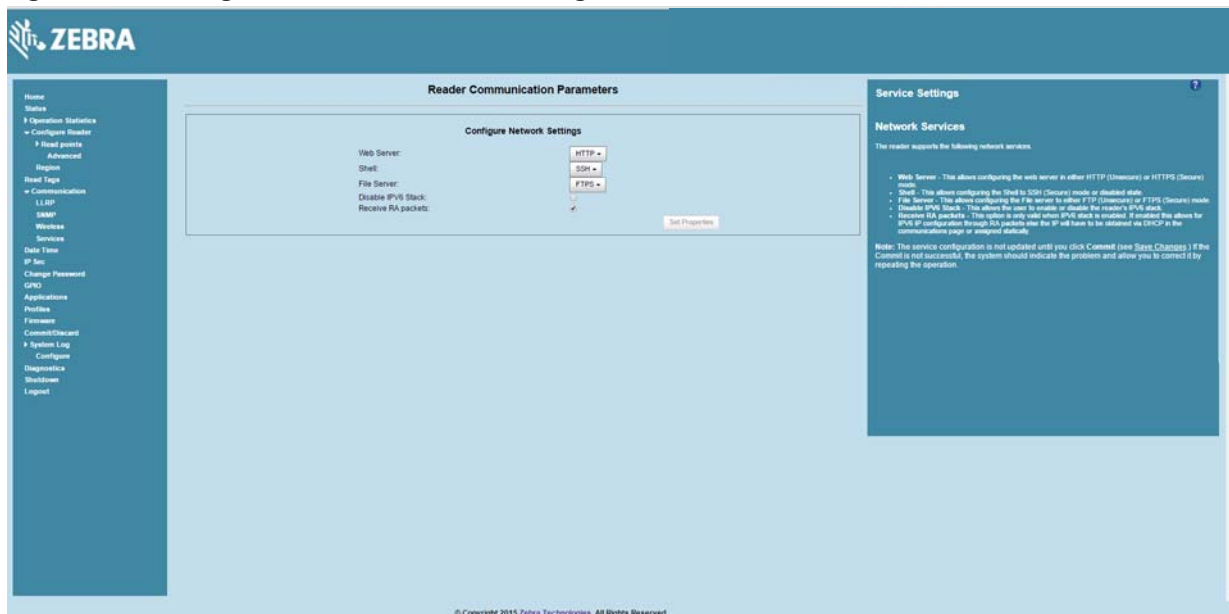


NOTE: The scan function can take several seconds. All buttons on the page are disabled while the scan is in progress, and re-enabled when the scan completes.

Network Services Settings

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

Figure 48 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.

Figure 49 System Time Management Window

System Time Management

SNTP Configuration

SNTP Server Name or IP Address:

NOTE: Changing the SNTP Server Address requires a Commit!

Set Date & Time on the reader

Month: Day: Year: Hour: Minute: Second:

Time Zone:

Set Date and Time

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 IP 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 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

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.

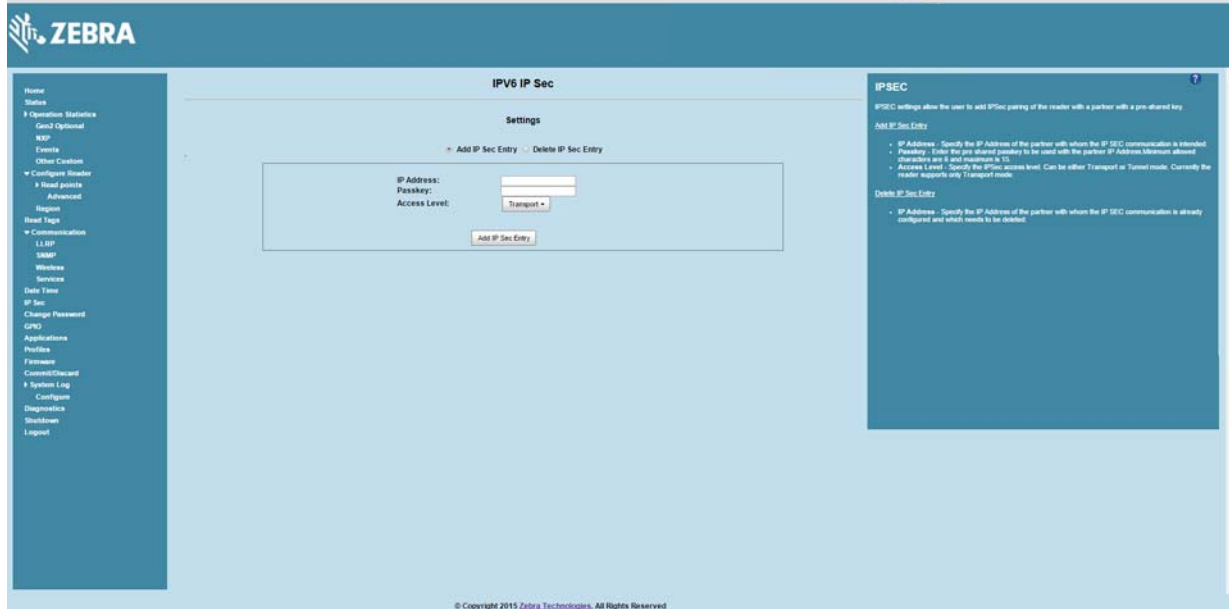


NOTE: The date/time and time zone changes take effect immediately, and do not require a Commit.

IPv6 IP Sec

Select IP Sec to view the IPv6 IP Sec window. IP Sec settings allow adding IP Sec pairing of the reader with a partner with a pre-shared key.

Figure 50 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 IP Sec 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.

FX Series User Accounts

The FX Series supports the following 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.

Figure 51 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.

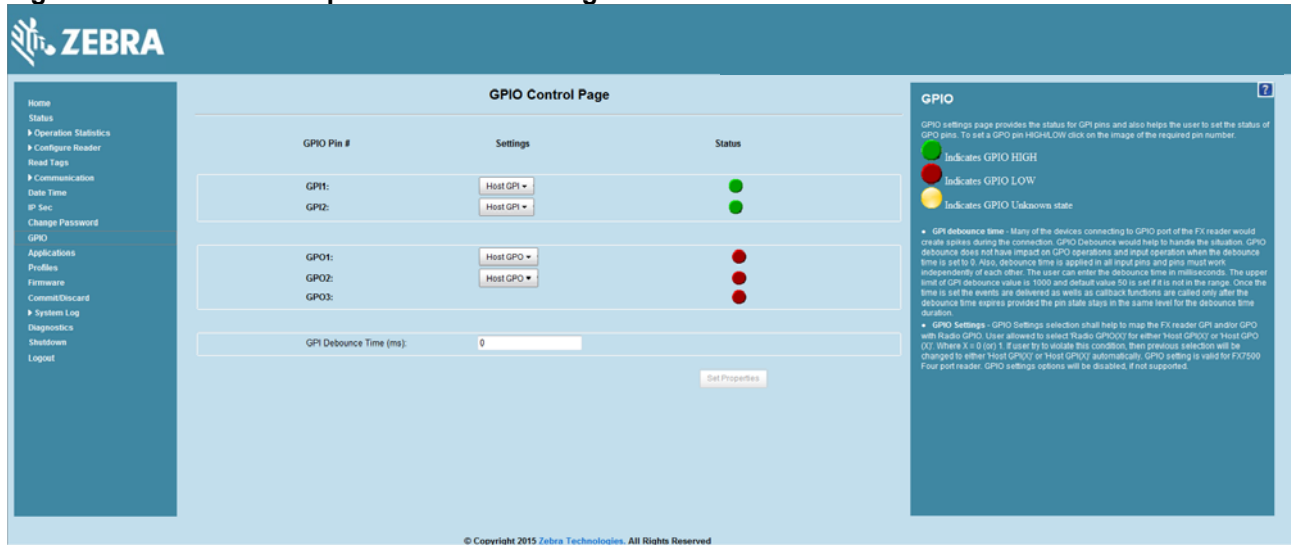
GPIO




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



NOTE: The FX7500 has two inputs and three outputs. The FX9600 has four inputs and four outputs.

Figure 52 FX7500 Example GPIO Control Page

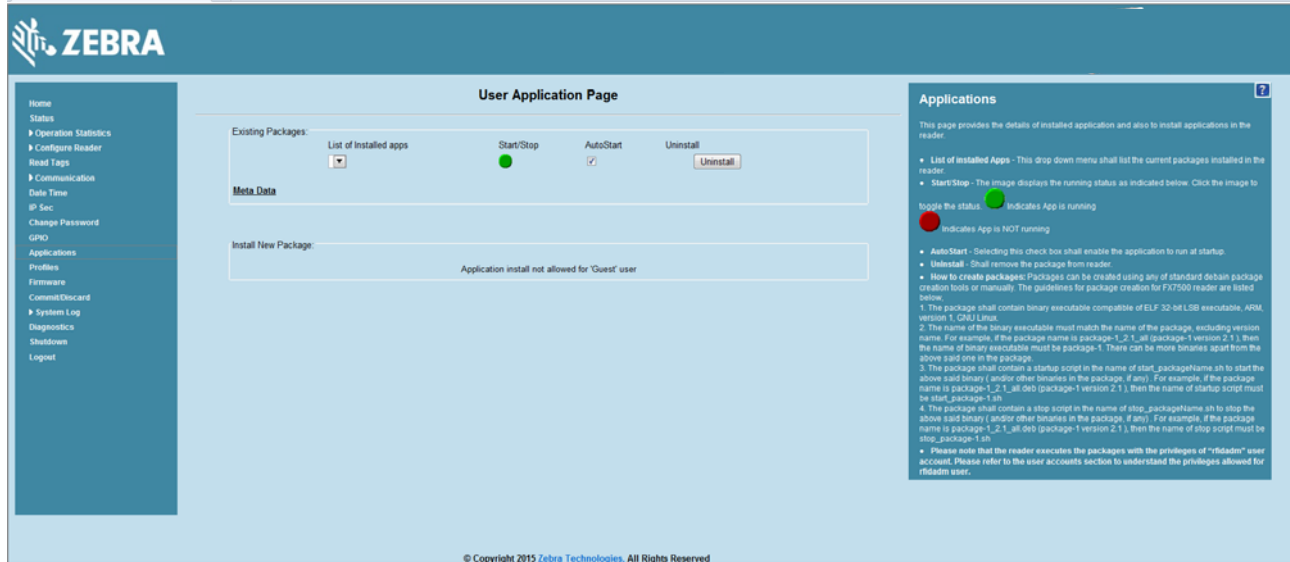


- **Settings** - Map the reader GPI and/or GPO with the radio GPIO. Select either Radio or Host for GPIx or GPOx where x = 0 or 1. An attempt to violate this condition changes the selection to either Host GPIx or Host GPOx automatically. The settings are disabled if a configuration is not supported.
- **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.

Figure 53 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 FX Series readers, use any of the standard Debian package creation tools, or create them manually. The FX Series 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.

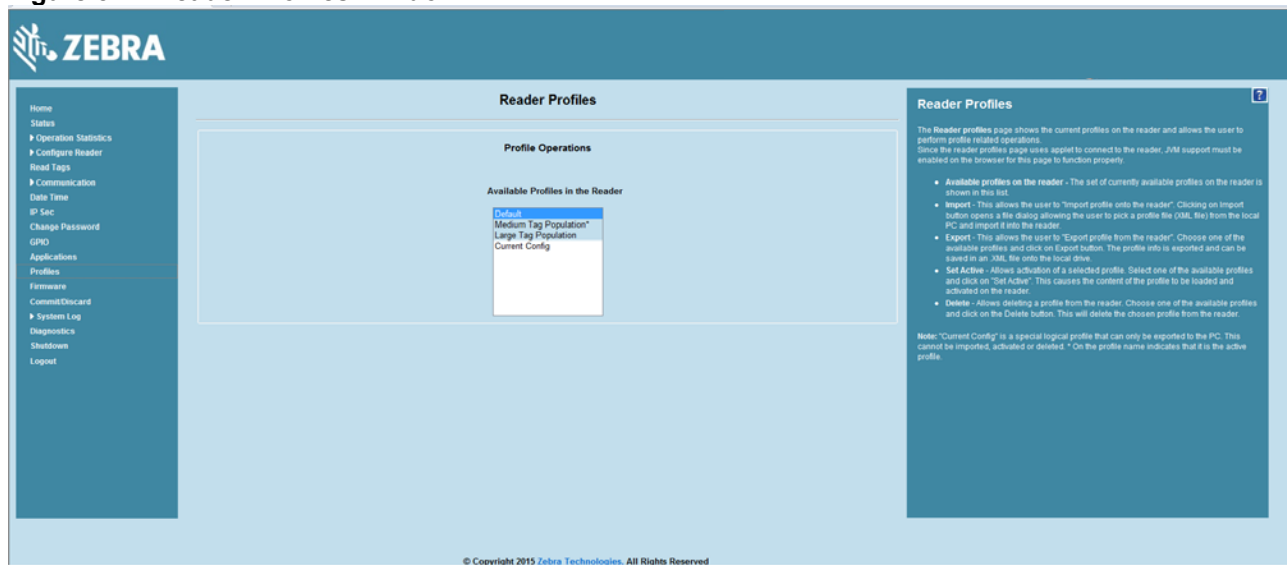
Reader Profiles

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.

Figure 54 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 , RF Air Link Configuration](#) for more information about air link profile configuration.

FIPS Support

The FX7500 and FX9600 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.

Figure 55 Firmware Version

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.

Current Version:	
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 RFBord	4.0.1

Last Known Version:	
Boot Loader	1.2.2
OS	1.2.3
File System	1.2.5
Reader Application	1.3.51

Revert back Firmware

Revert Back

© Copyright 2015 Zebra Technologies. All Rights Reserved

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 82](#).

The reader supports three different methods of updating the firmware:

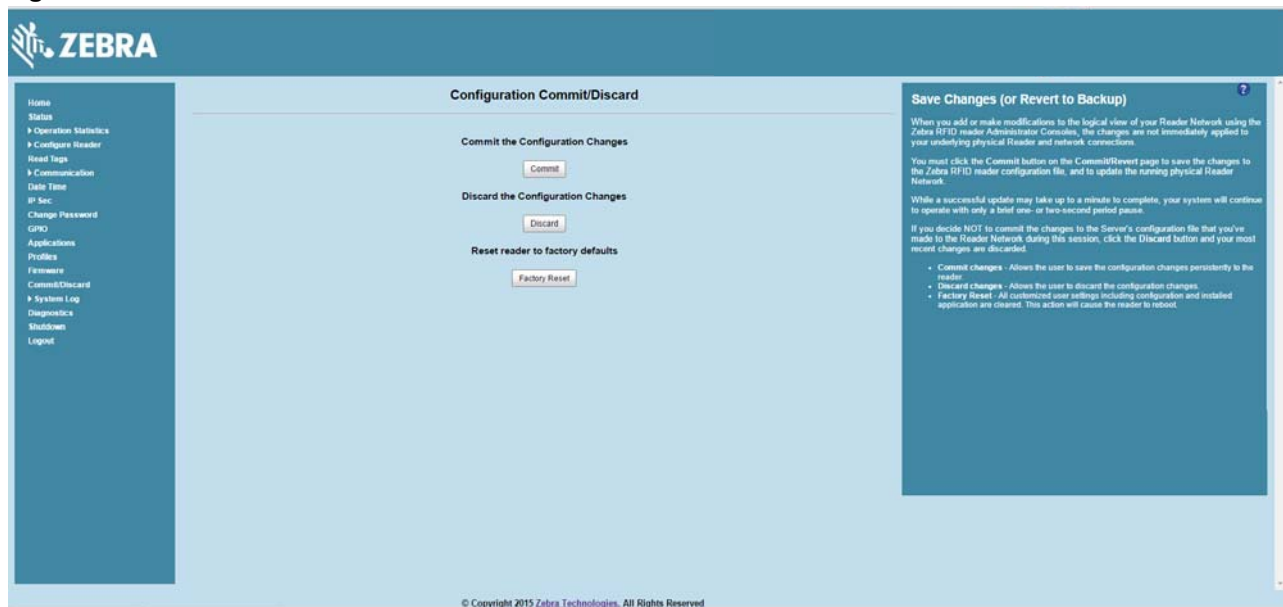
- Update using a USB drive.
- File-based update that allows uploading the firmware files from the PC (or a network location) to the reader and running the update.
- FTP / FTPS / SCP server-based update.

For instructions on updating the firmware, see [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.

Figure 56 Commit/Discard Window



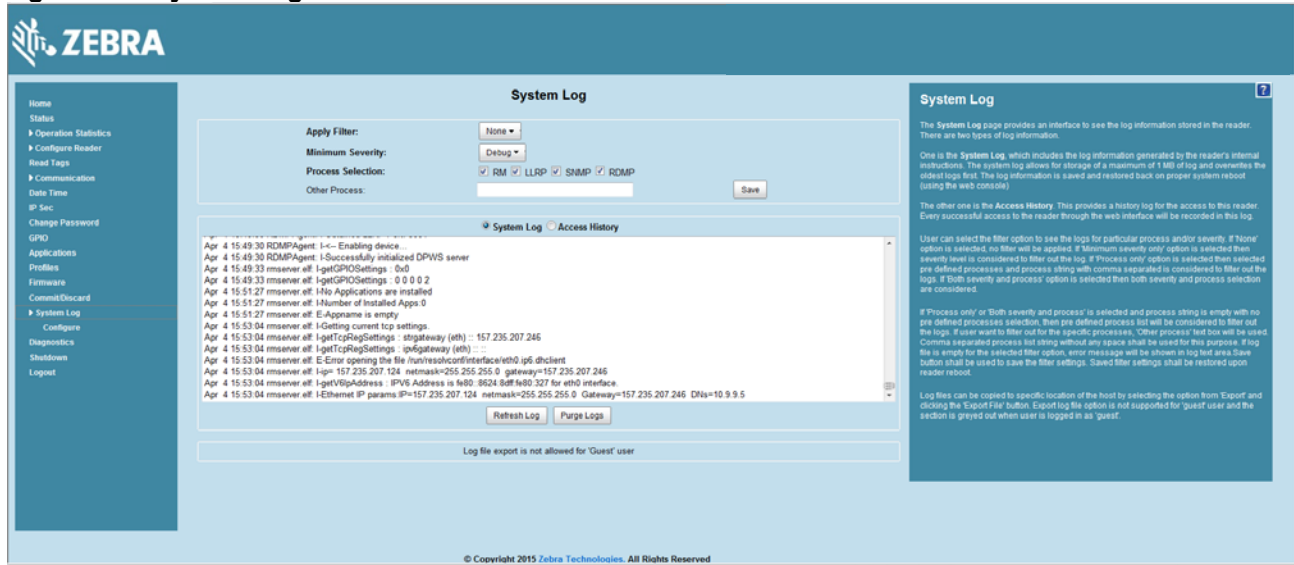
To discard changes to the server's configuration file made to the reader network during this session, click Discard.

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.

Figure 57 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.

Figure 58 Configure System Log Window

This window offers the following options:

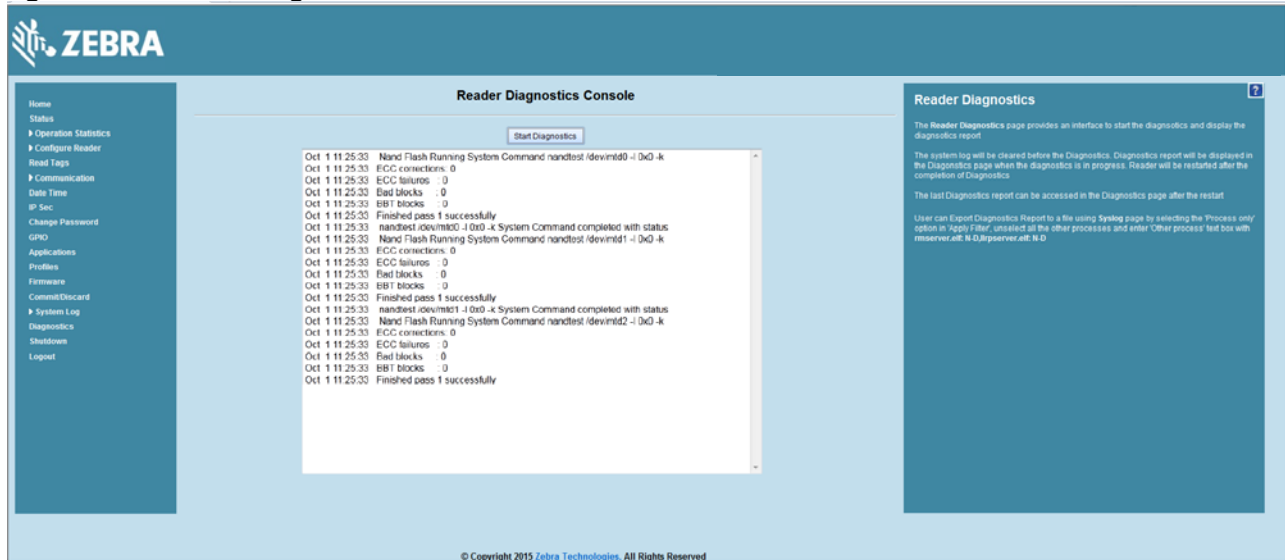
- **Remote Log Server IP** - Configures the host IP address to which log messages are sent. IP address 0.0.0.0 indicates that no host is configured.
- **Remote Log Server Port** - Remote log server listening port. The default port is 514.
- **System Log Minimum Severity** - The minimum severity above 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.

Figure 59 Reader Diagnostics Window



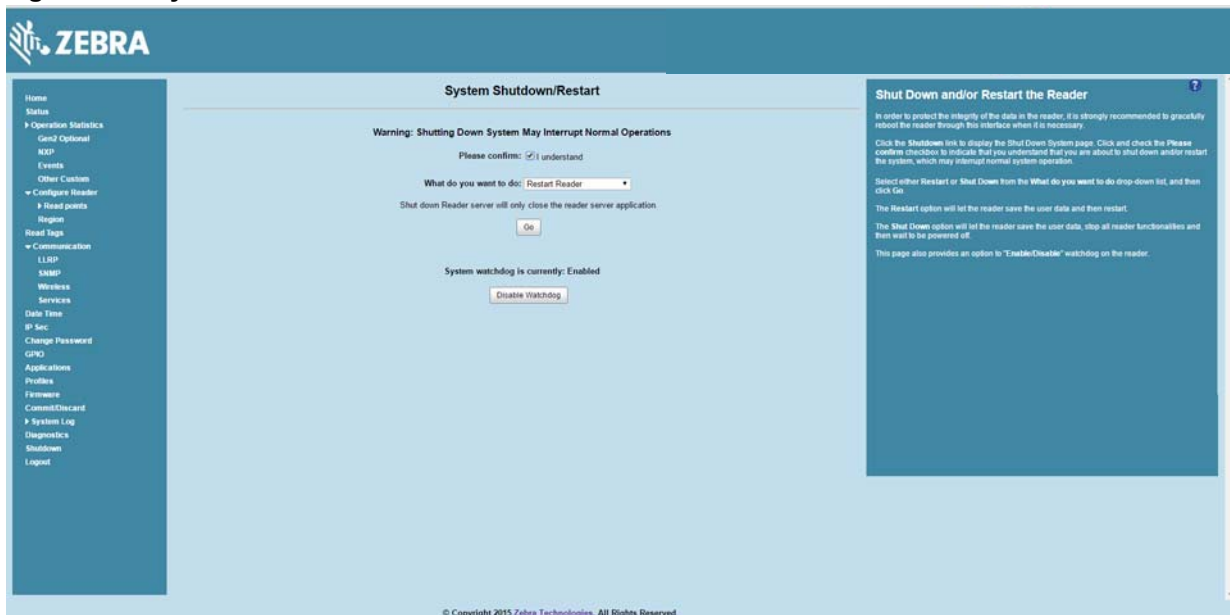
Selecting **Start Diagnostics** clears the system log and displays the diagnostics report. The reader reboots when the diagnostics completes. Return to the Diagnostics window to view the diagnostics report.

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.

Figure 60 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.

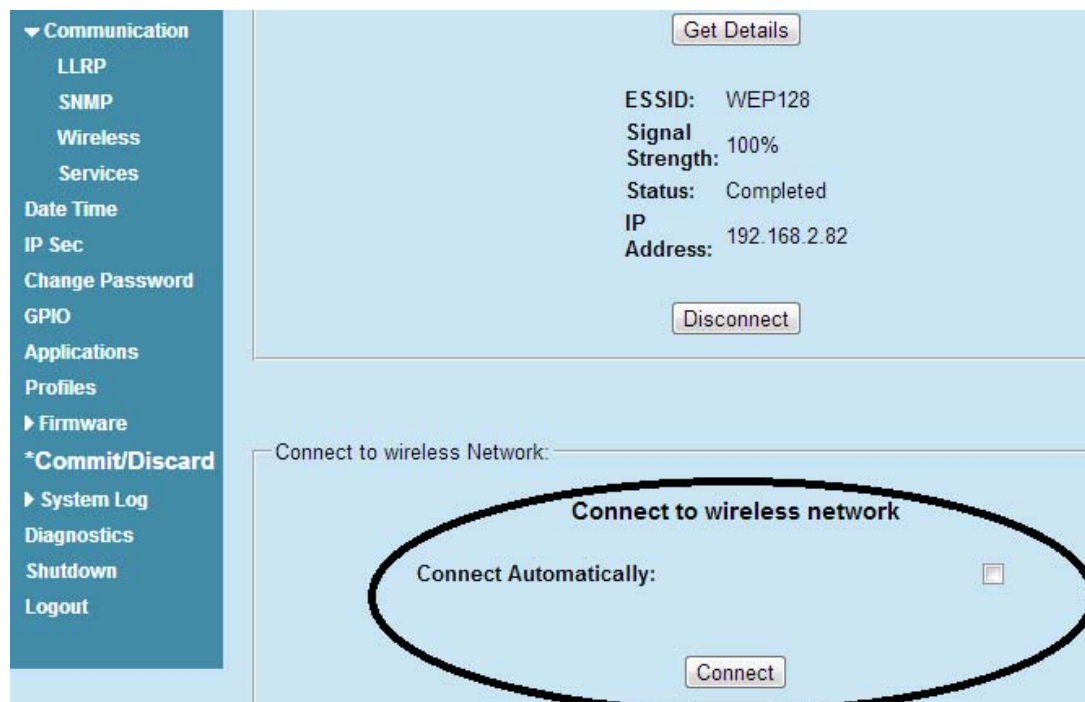
Configure and Connect via Wi-Fi and Bluetooth

Wireless Network Advanced Configuration

The FX Series 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 , 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.

Figure 61 Administrator Console Update



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.

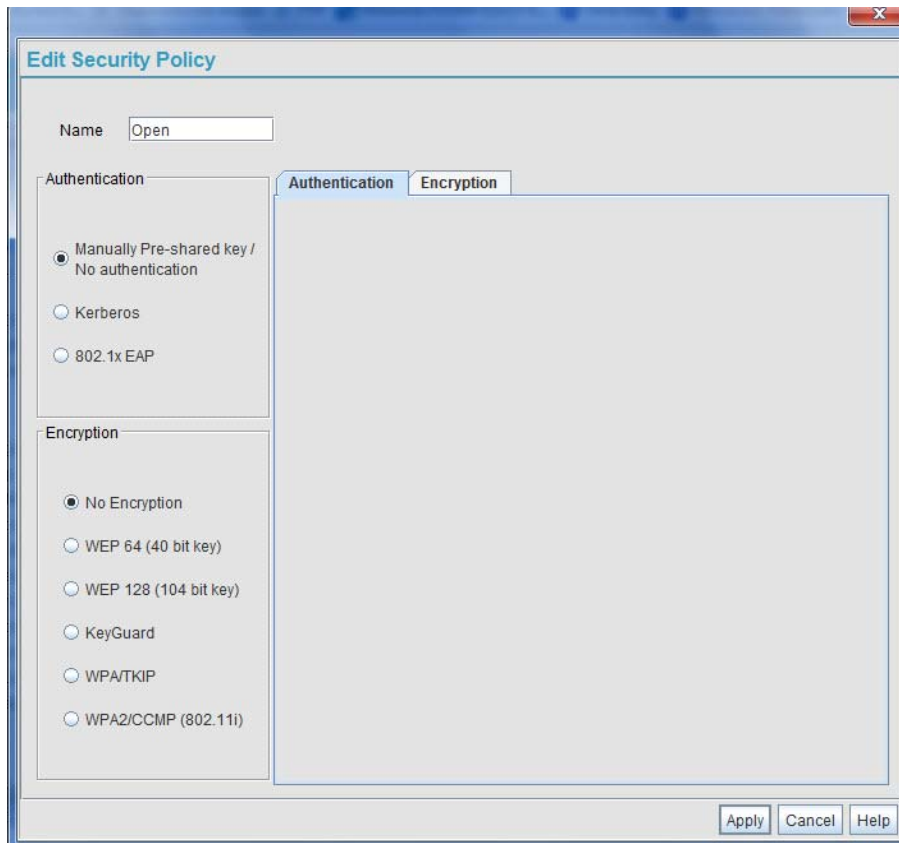
Preferred Configurations for Access Points

The FX Series readers support WPA/WPA2 (http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) and WEP128 (http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) by default over the Administrator Console.

Other supported protocols are explained in this guide. Refer to the Access Point configuration manual to configure the Access Point to one of the following modes that match the reader configuration:

- **WPA / TKIP**
- **WPA1 / CCMP**
- **WEP128**
- **Open Network**

Figure 62 Example Open Network Mode



Access Point Configuration for Android Device

Open Network

To configure the access point to an open network for an Android device:

1. Enable the wireless tethering from the settings menu.
2. Select Open from the Security drop-down menu.
3. Select Save.

Figure 63 Open Network Configuration for Android Device

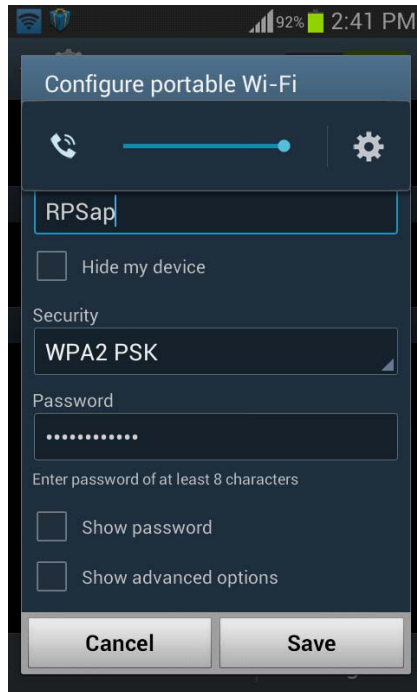


WPA2 PSK

To configure the access point to WPA2 PSK for an Android device:

1. Select WPA2 PSK from the Security drop-down menu.
2. Enter a password.
3. Select Save to start the wireless hotspot.

Figure 64 WPA2 PSK Configuration for Android Device



WPA PSK

To configure the access point to WPA PSK for an Android device:

1. Select WPA PSK from the Security drop-down menu.
2. Enter a password.
3. Select Save to start the wireless hotspot.

Figure 65 WPA PSK Configuration for Android Device

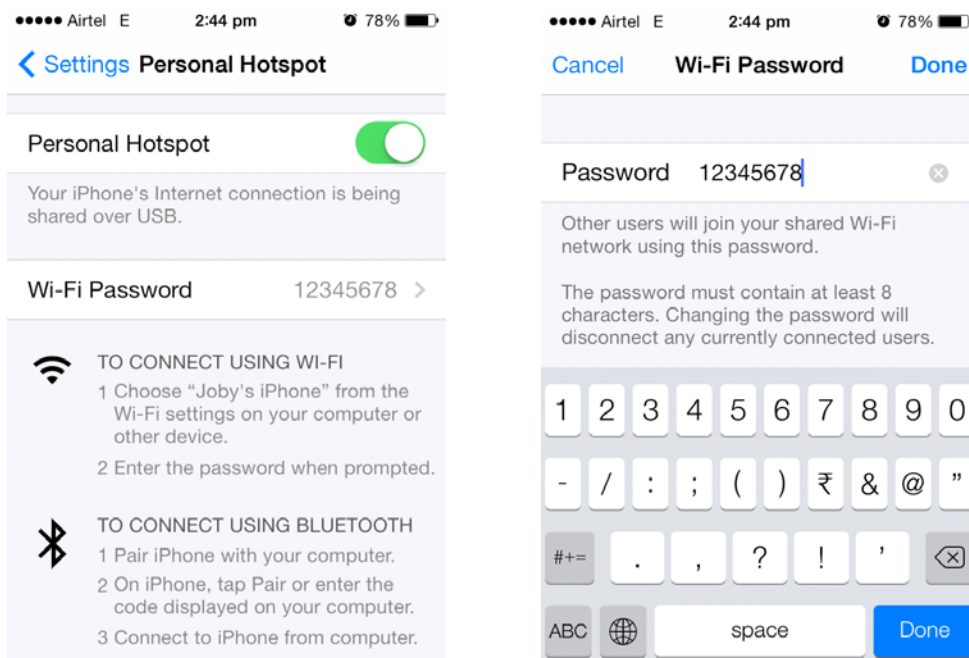


Internet Connection Configuration for iPhone

To configure the personal hotspot for an iPhone:

1. Select **Setting**.
2. Select the **Personal Hotspot** button to turn on the internet connection.
3. Enter a password.

Figure 66 iPhone Device



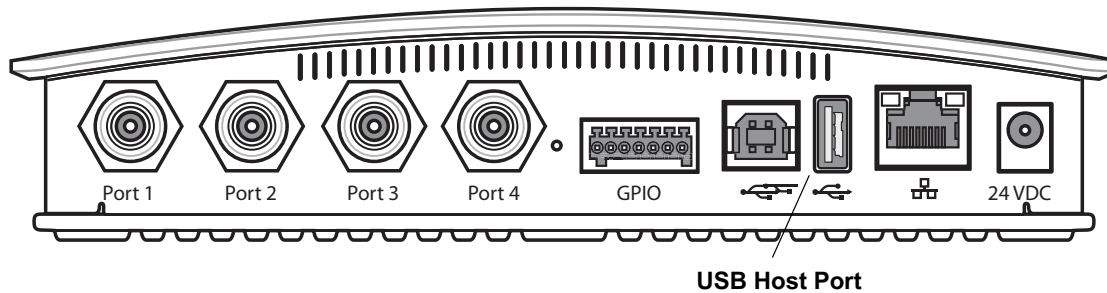
Connecting to a Wireless Network Using a Wi-Fi Dongle

✓ **NOTE:** The screens in this chapter may differ from actual screens. The applications described may not be available on (or applicable to) all devices. Procedures are not device-specific and are intended to provide a functional overview.

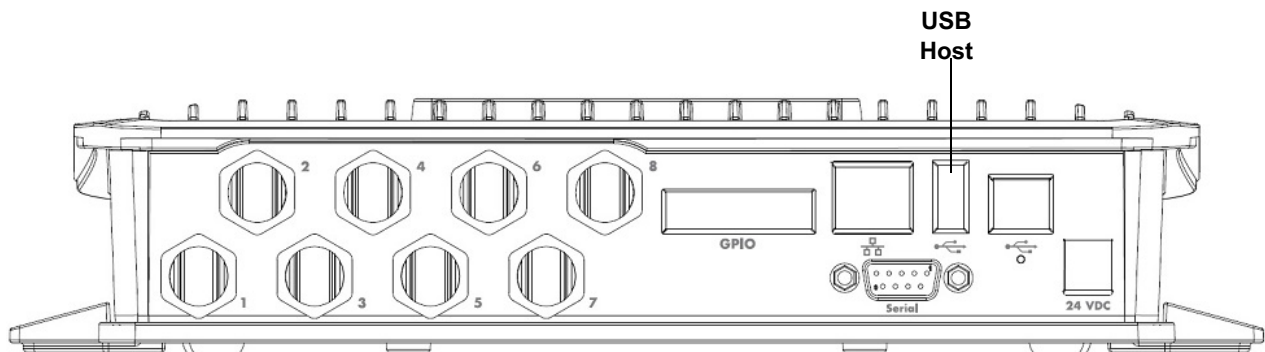
To connect to a wireless network using a USB Wi-Fi dongle on the FX7500 and FX9600:

1. Plug the supported wireless dongle into the USB host port on the FX7500 and FX9600. Zebra provides native support for USB Wi-Fi adapters with the Realtek chipset RTL 8187 and RTL 8812AU. See [Table 6 on page 78](#) for a list of supported Wi-Fi dongles.

Figure 67 FX7500 USB Host Port Location for Dongle



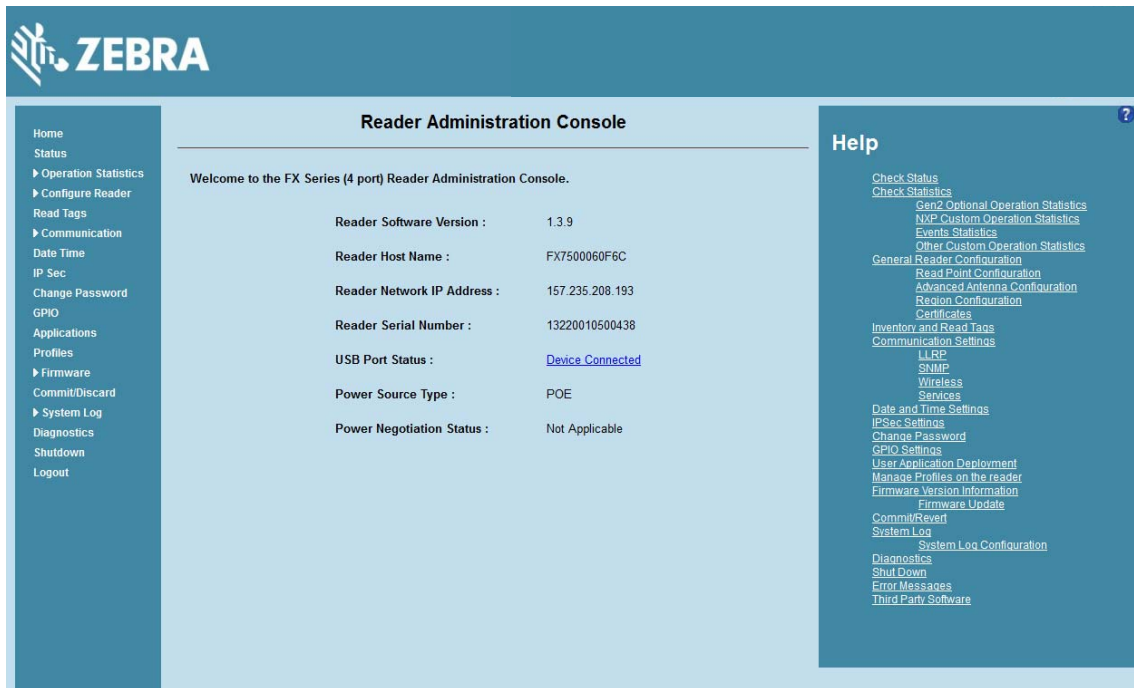
FX9600 USB Host Port Location for Dongle



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 Wi-Fi dongle information shown in [Figure 68](#).

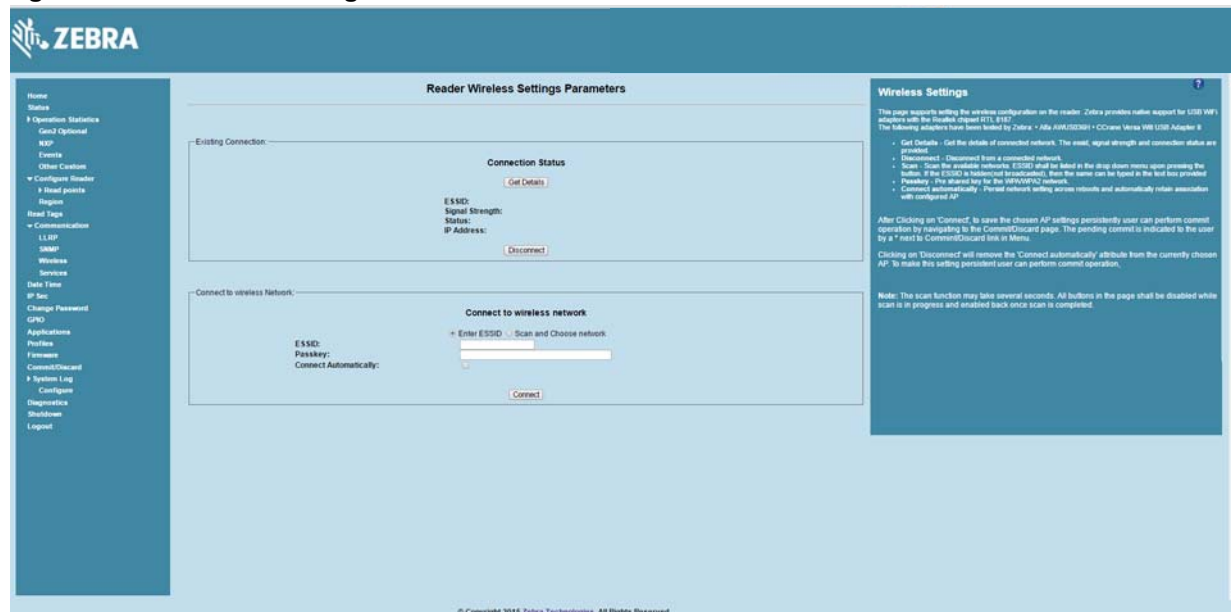
Wi-Fi Configuration

Figure 68 Wi-Fi Dongle Connected



3. Select Communication > Wireless.

Figure 69 Wireless Settings



The Wi-Fi dongle can connect to the wireless network in one of two ways:

- Manually entering the ESSID.
- 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).

Wi-Fi Configuration

Figure 70 Entering Connect Information

The screenshot shows the Zebra Reader Wireless Settings Parameters page. The left sidebar contains navigation links: Home, Status, Operation Statistics, Gen2 Optional, RSP, Events, Other Custom, Configure Reader, Read points, Region, Read Tags, Communication, LLRP, SNRP, Wireless, Services, Date Time, IP Set, Change Password, GPRS, Applications, Profiles, Firmware, Connect/Disconnect, System Log, Configure, Diagnostics, Shutdown, and Logout. The main content area is titled 'Reader Wireless Settings Parameters' and is divided into two sections: 'Existing Connection' and 'Connect to wireless network'. The 'Existing Connection' section shows 'Connection Status' with fields for ESSID (DEV), Signal Strength (0%), Status (Completed), and IP Address (157.235.207.24). The 'Connect to wireless network' section has radio buttons for 'Enter ESSID & Scan and Choose network' (selected) and 'Connect Automatically'. It includes fields for ESSID (DEV), Password (DEV (96 %)), and a 'Connect Automatically' checkbox. A 'Connect' button is at the bottom. A 'Wireless Settings' sidebar on the right provides instructions on how to use the settings page, including a note about the scan function taking several seconds.

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

Figure 71 Assigned IP Address

This screenshot is identical to Figure 70, showing the Zebra Reader Wireless Settings Parameters page. The 'Existing Connection' section now displays the assigned IP Address as 157.235.207.24. The 'Connect to wireless network' section remains the same, with the 'Connect' button visible at the bottom.

The reader is now accessible using the wireless IP shown in the IP Address field (157.235.207.24 in this case). The Wi-Fi 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.

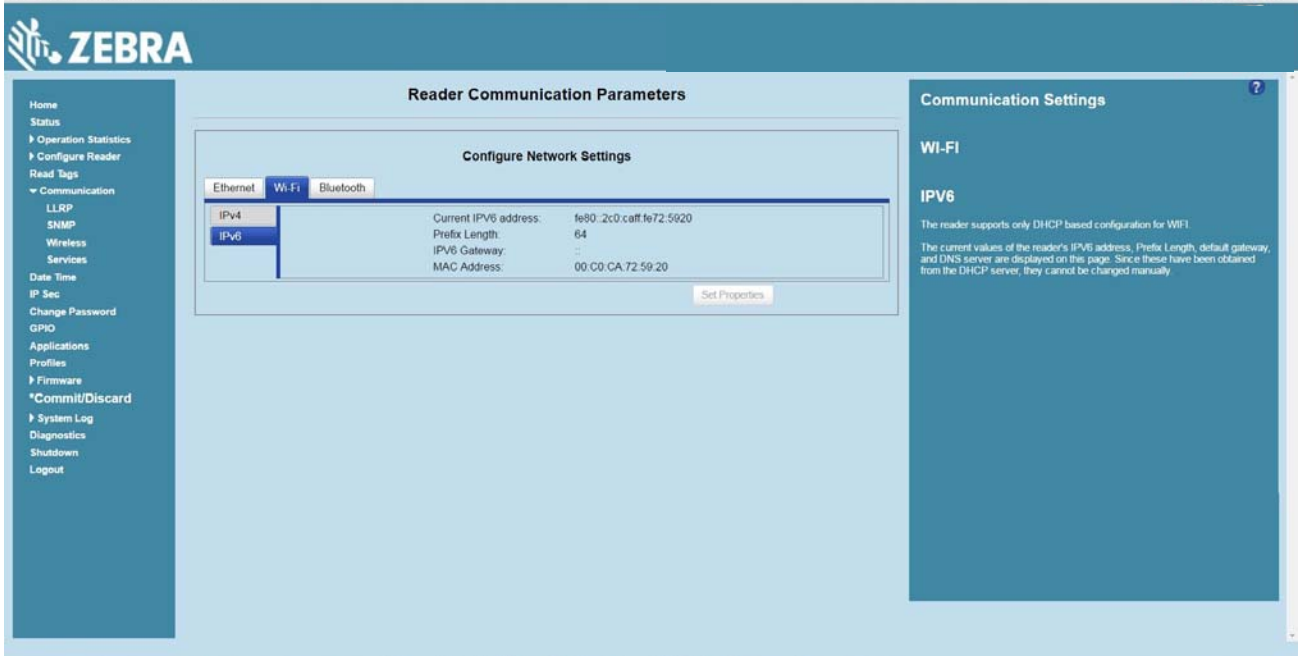
Wi-Fi Configuration

Figure 72 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.

Figure 73 Wi-Fi Tab - IPV6Connecting to a Peer Device over Bluetooth Using a Bluetooth Dongle



Connecting to a Peer Device over Bluetooth Using a Bluetooth Dongle

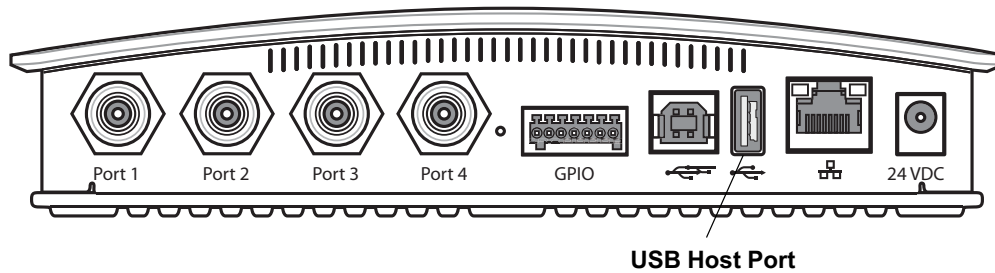
To connect to a peer device over Bluetooth using a USB Bluetooth dongle on the FX7500 and FX9600:

1. Plug the supported Bluetooth dongle into the USB host port on the FX Reader. The following Bluetooth dongles are supported:

Figure 74 Supported Bluetooth Dongles.

Dongle Model	Zebra FX7500	Zebra FX9600
Bluetooth CSR 4.0 dongle Qualcomm / Atheros CSR8510	No	Yes
Bluetooth 3.0+HS Ralink RT5370L	No	Yes
Asus Mini Bluetooth Dongle USB-BT211	Yes	Yes
MediaLink Bluetooth Dongle MUA-BA3	Yes	Yes

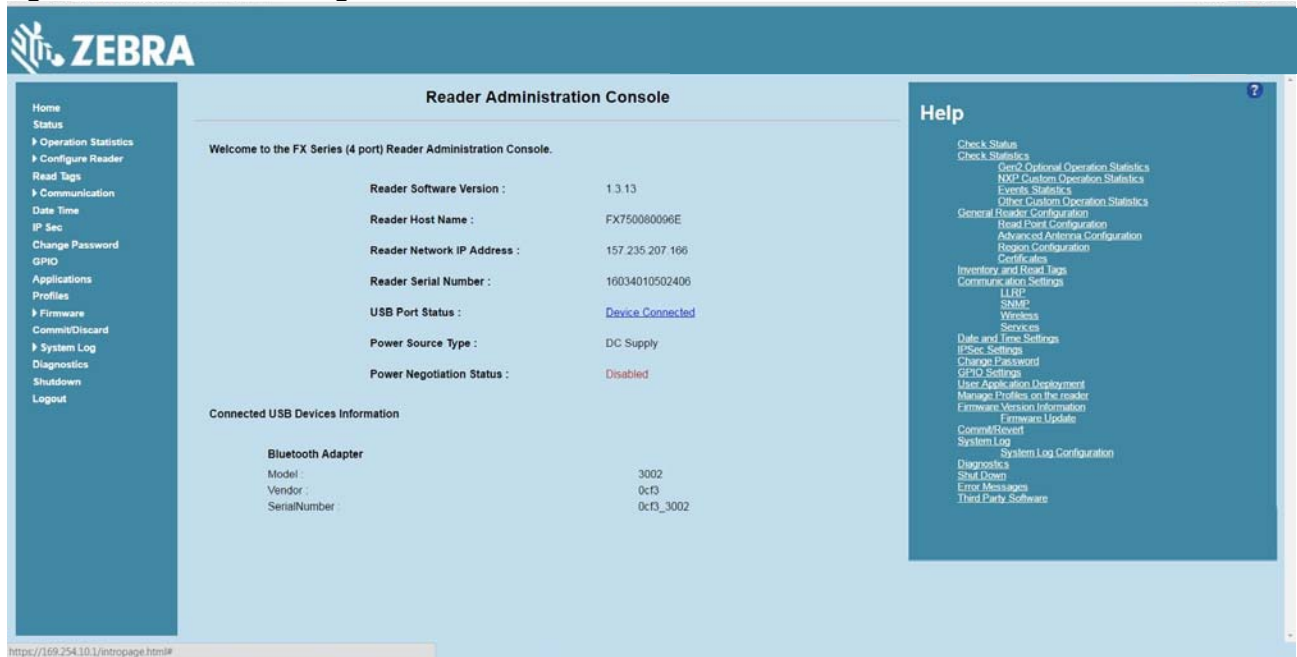
Figure 75 USB Host Port Location for Dongle



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.

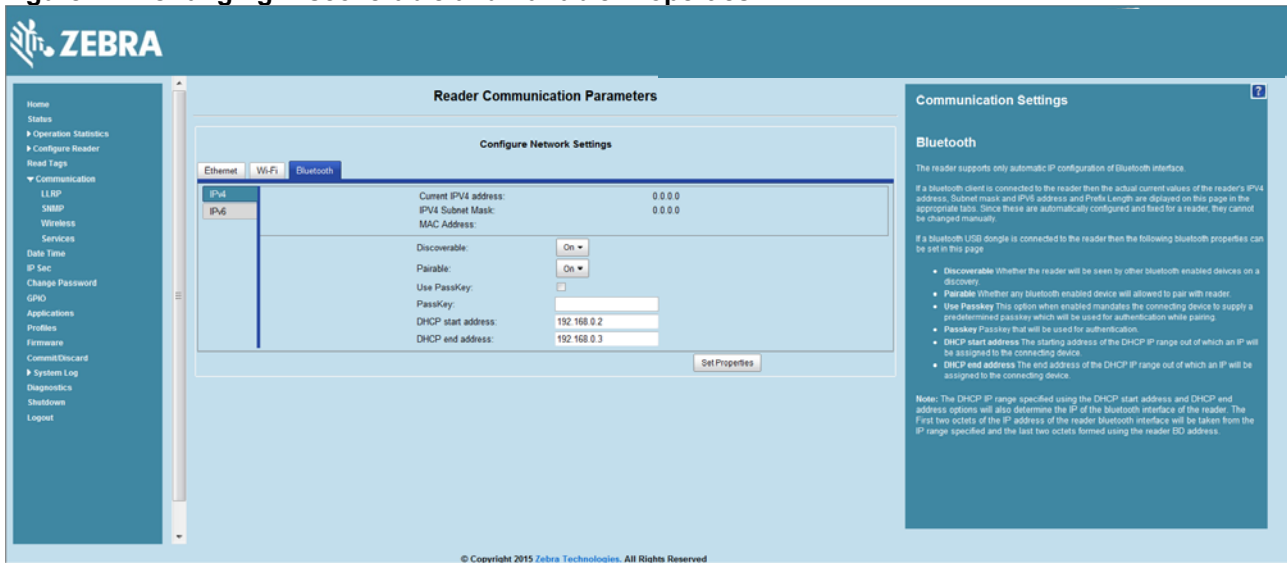
Wi-Fi Configuration

Figure 76 Bluetooth Dongle Connected Select Communication > Bluetooth.



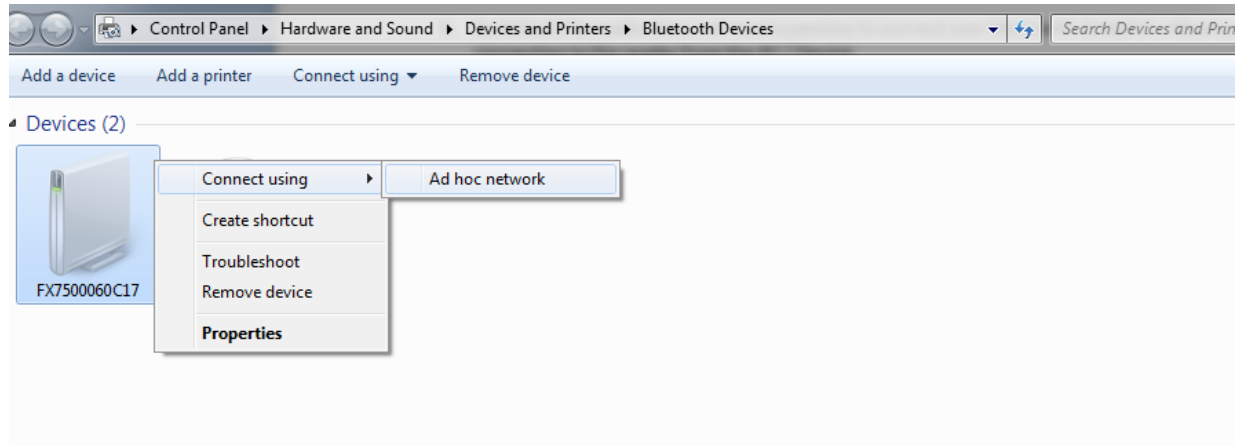
3. Change the Discoverable and Pairable properties to On.

Figure 77 Changing Discoverable and Pairable Properties



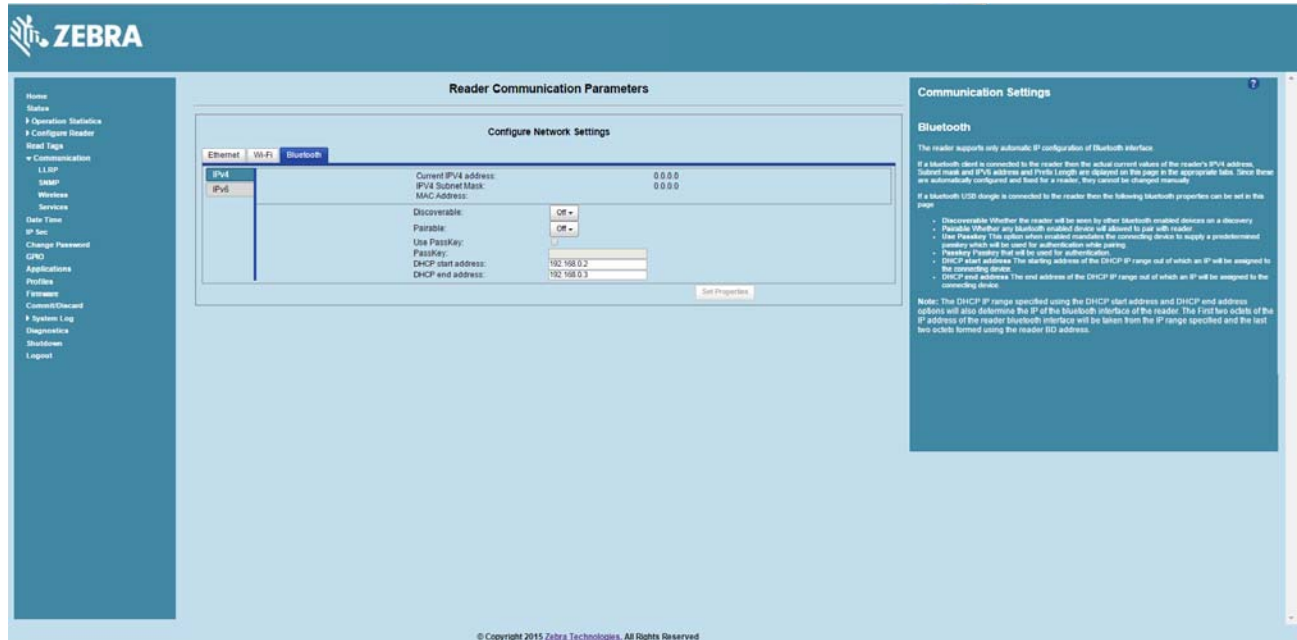
4. Optionally select Use Passkey and enter a passkey to validate the Bluetooth connection. The default passkey for the FX7500 and FX9600 is 0000.
5. Discover the reader from a Bluetooth-enabled device (such as a laptop). Use the host name to identify the reader among the discovered devices (for example: FX7500060C17).
6. After a successful connection, right-click the reader icon (for example: FX7500060C17) in the list of Bluetooth devices and select Connect using > Ad hoc network. This establishes the network connection for later.

Figure 78 Connecting to the Reader



7. 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.

Figure 79 Communication Bluetooth Tab



Open the web page or sample application to connect to the Bluetooth IP (192.168.67.21 in [Figure 79](#)) and read tags.

Copying Files to the Reader

The FX7500 and FX9600 RFID readers support the SCP, FTP, and FTPS protocols for copying files. See [Copying Files To and From the Reader](#) for instructions on copying files to /apps directory.

Application Development

Introduction

The FX Series RFID readers can host embedded applications, so data can be parsed directly on the reader. Since data is processed in real time at the network edge, the amount of data transmitted to your backend servers is substantially reduced, increasing network bandwidth and improving network performance. Latencies are reduced, improving application performance. And the integration of data into a wide variety of middleware applications is simplified, reducing deployment time and cost. The FX Series also provides flexibility for host embedded applications on the reader or on a separate PC.

Reference Guides

The following resources can be found on 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.
- FX Series Embedded SDK Installation Guide provided with the Zebra RFID SDK.
- FX Series Embedded SDK Programmers Guide provides instructions on creating new embedded applications.
- See [Related Documents and Software on page 11](#) for more documentation regarding RFID API and application development.

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 FX Series readers.

- 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/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)
 - ulmage_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 are updated; not all of the files are updated in every release.

Failsafe Update

The FX Series readers provide true failsafe firmware updates. 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.

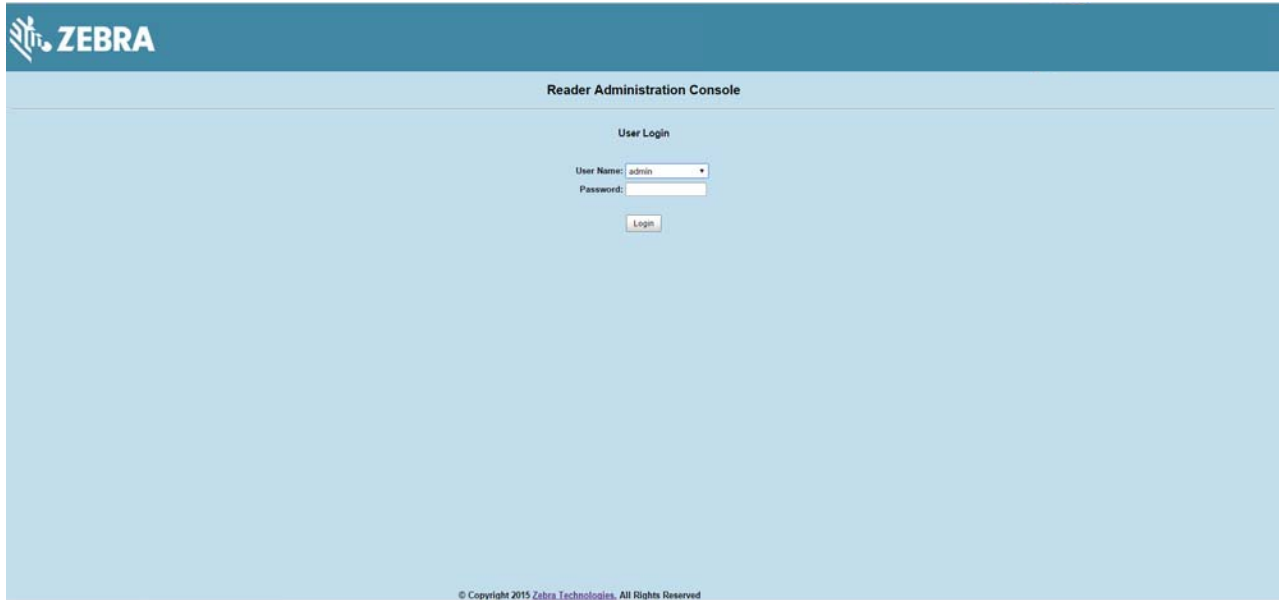
Updating FX Series Reader Software

Verifying Firmware Version

To verify that the FX7500 and FX9600 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.

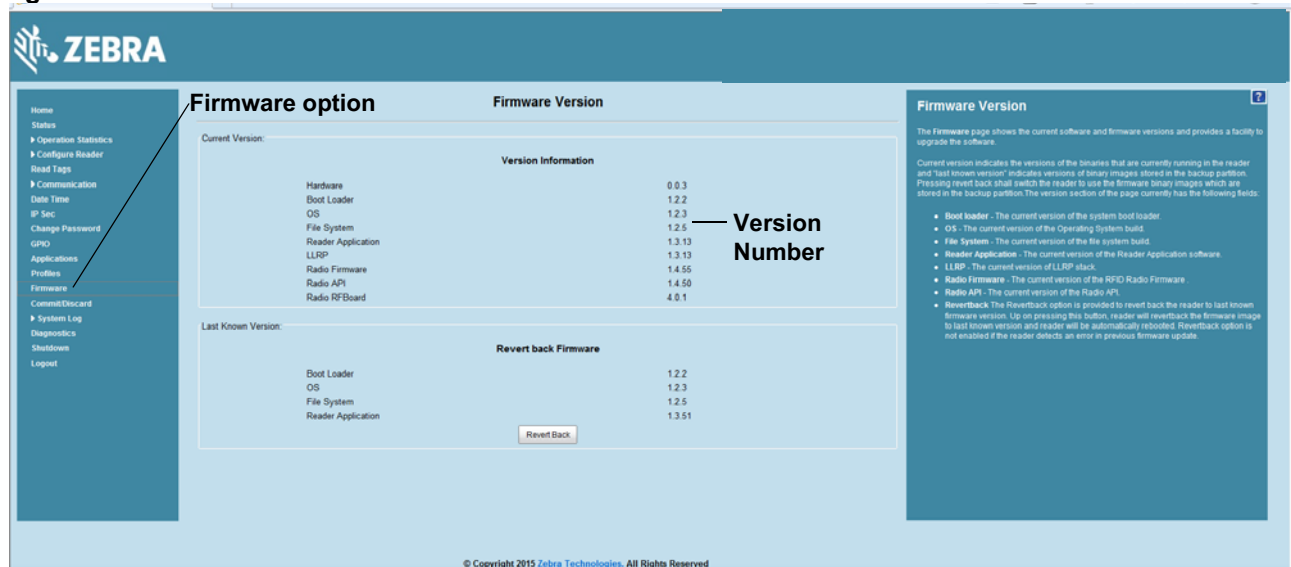
Figure 80 User Login Window



The screenshot shows the Zebra Reader Administration Console User Login window. The window has a blue header with the Zebra logo and the text "ZEBRA". Below the header, the title "Reader Administration Console" is displayed. The main content area is light blue and contains the "User Login" section. This section includes a "User Name:" dropdown menu with "admin" selected, a "Password:" text input field, and a "Login" button. At the bottom of the window, there is a small copyright notice: "© Copyright 2015 Zebra Technologies, All Rights Reserved".

2. Select Firmware on the left side panel to verify that the current version of reader software is outdated (for example, 1.1.66).

Figure 81 Firmware Version Window



Updating Methods

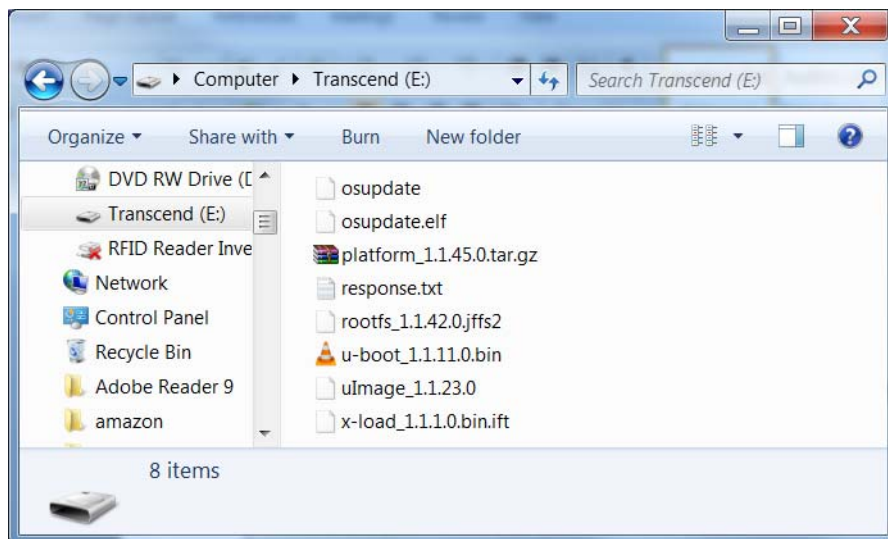
Download the reader update files from www.zebra.com/support, then use one of three methods to update the reader software to a later version, e.g., 1.1.45.0 or higher:

- **Update Using a USB Drive (Recommended)**
- **File-Based Update on page 114**
- **FTP-Based Update on page 116**

Update Using a USB Drive (Recommended)

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

Figure 82 USB Drive Root Folder



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

Figure 83 FX7500 USB Host Port Window

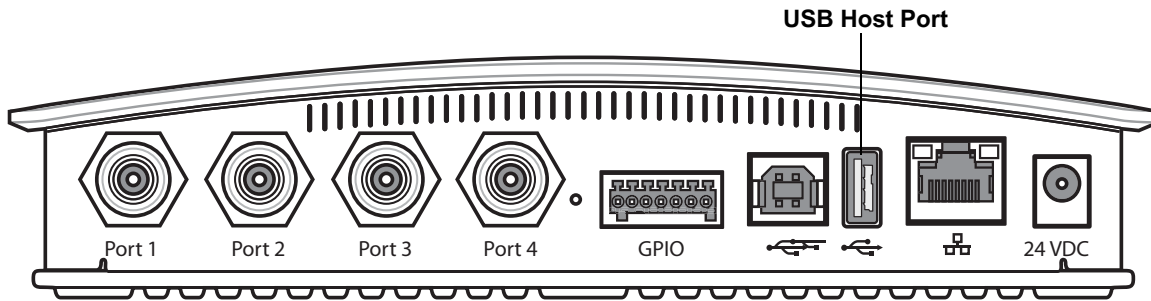
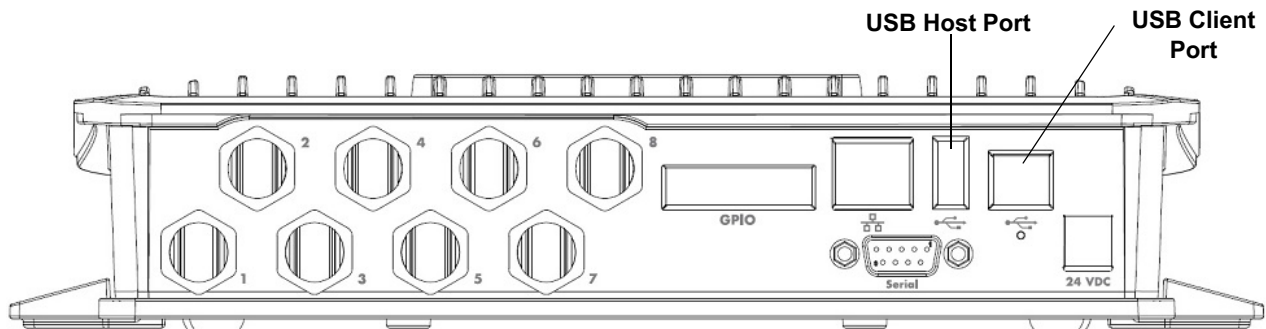


Figure 84 FX9600 USB Host Port Window



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 85 FX7500 Reader LEDs

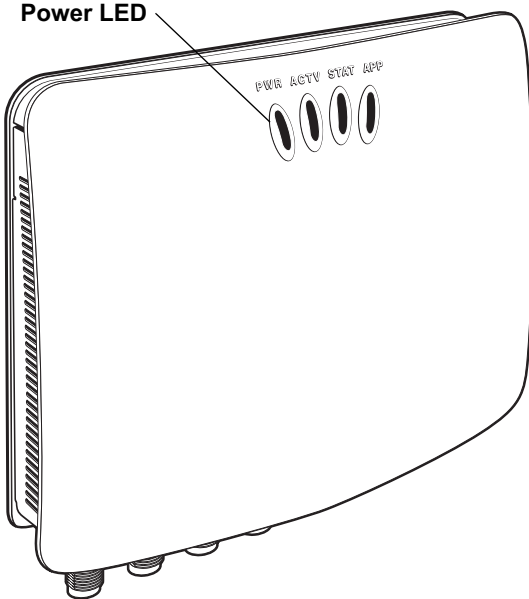
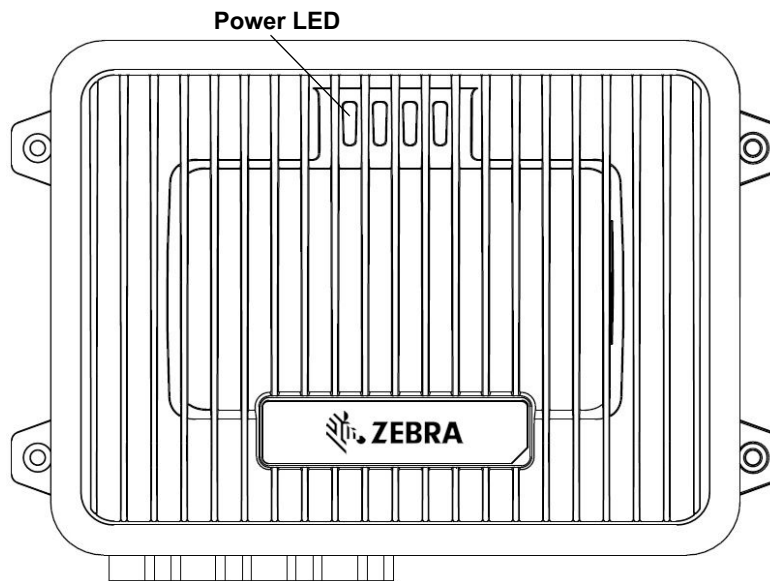


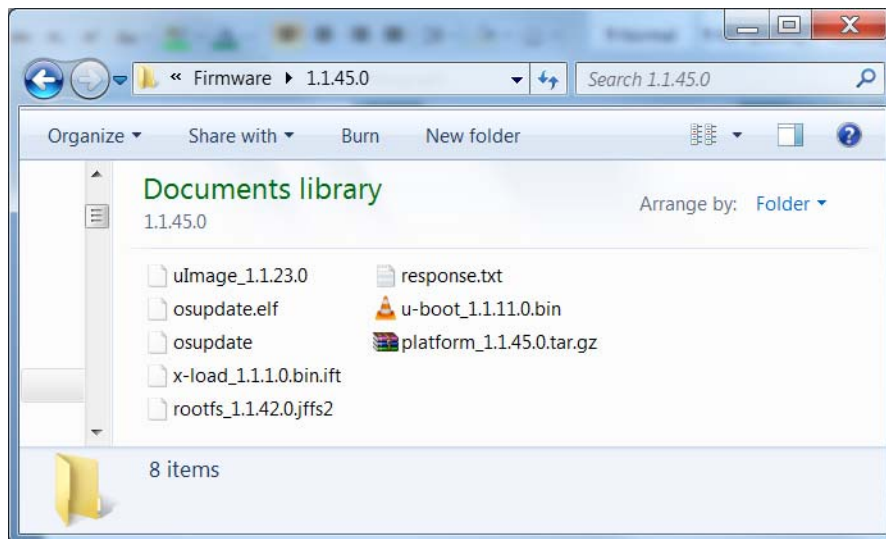
Figure 86 FX9600 Reader LEDs



File-Based Update

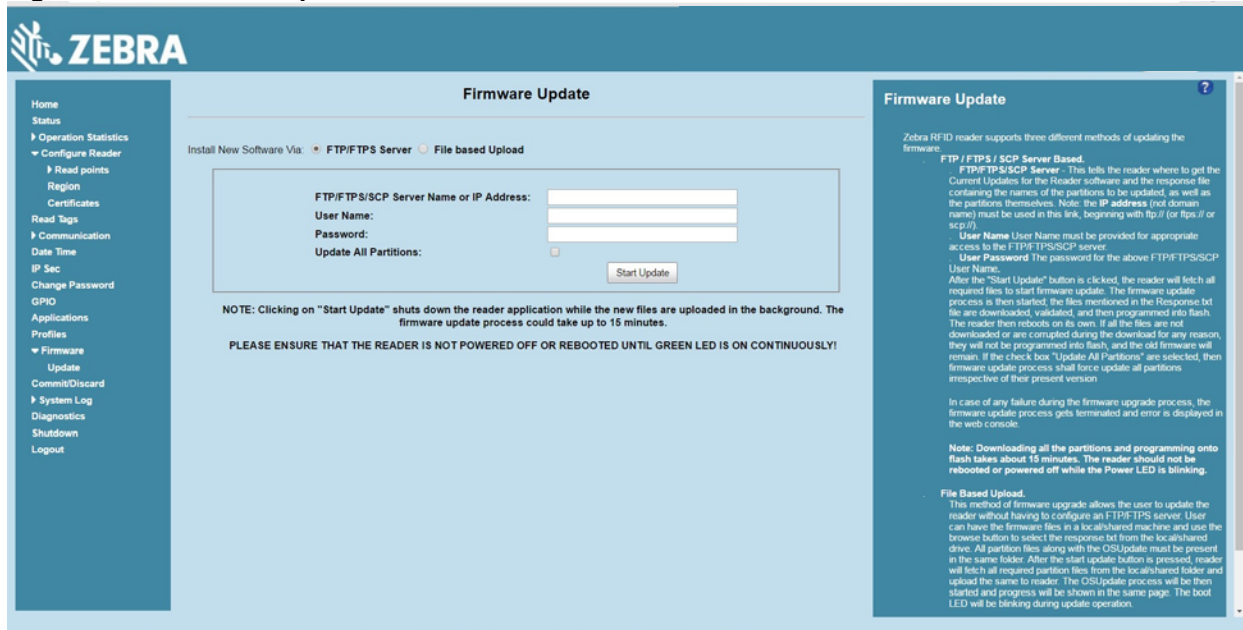
1. Copy all reader update files into any folder on a host computer.

Figure 87 Host Computer Folder



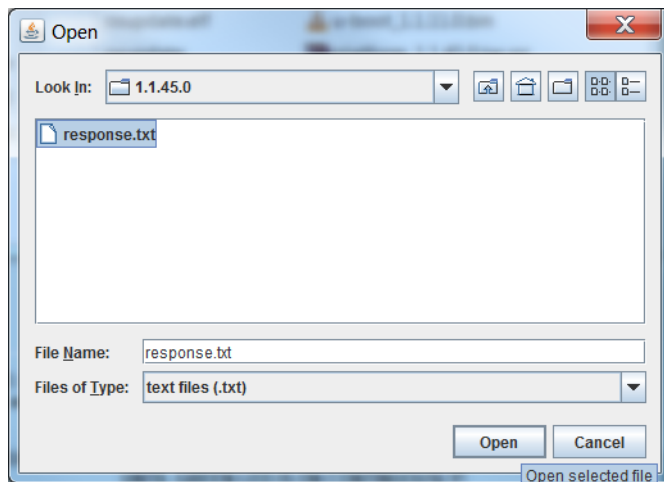
2. Log into the reader and navigate to the Firmware Update page.

Figure 88 Firmware Update Window



3. Select File based Upload.
4. Click on Browse and navigate to the folder that contains the firmware update files.

Figure 89 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.
7. When the update completes, the reader reboots and returns to the 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.

Figure 90 Firmware Update Window

ZEBRA

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: ☐

Start Update

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 checkbox "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 browser 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.

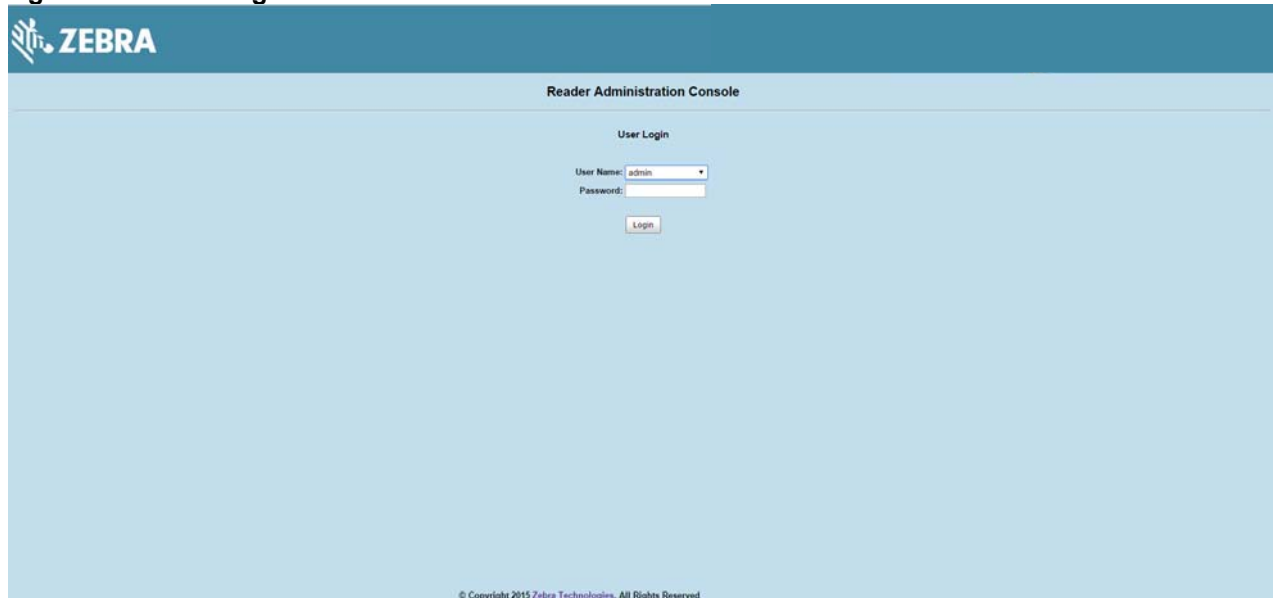
2. Select FTP/FTPS Server.
3. Enter the FTP location where the files are located.
4. Enter the User Name and Password for the FTP server login.
5. Click Start Update. The reader starts the update process and displays the update status as follows:
 - The reader continuously blinks the Power LED red.
 - 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.
6. When the update completes, the reader reboots and returns to the FX login screen.

Verifying Firmware Version

To verify reader update success:

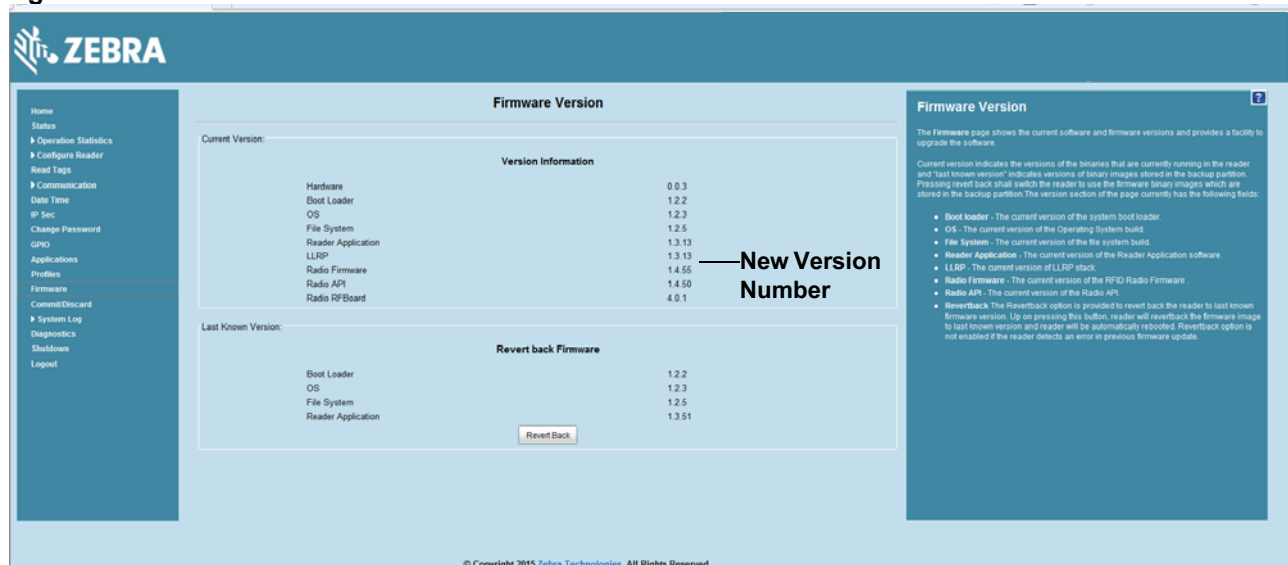
1. Log into the reader. In the User Login window, enter admin in the User Name: field and enter change in the Password: field.

Figure 91 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.

Figure 92 Firmware Version Window



Troubleshooting

Troubleshooting

Table 7 provides FX Series troubleshooting information.

Table 7 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 and Power Connections on page 33 .
Reader is not reading tags.	The tag is out of its read range.	Move the tag into read range. See Read Tags on page 72 .
	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 and Power Connections on page 33 to view the IP address, or use the host name to connect to the reader.

Table 7 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 12 .
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 12 .
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 7 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 38 .
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 12 .
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 38 .
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.

Table 7 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
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.
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 12 .
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 12
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.

Troubleshooting

Table 7 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
Unhandled reply type.	The system generated an unexpected value.	Contact Zebra support. See Service Information on page 12 .
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 12 .
Invalid Device Address.	The device address information (parent) is invalid, missing, or formatted inaccurately.	Contact Zebra support. See Service Information on page 12 .
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 12 .
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.

Table 7 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
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 12](#) for contact information.

Technical Specifications

Technical Specifications

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

Table 8 Technical Specifications

Item	Description
Physical and Environmental Characteristics	
Dimensions	
FX7500	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)
FX9600	9.72 in. L x 7.25 in. W x 2.2 in. D (24.67 cm x 18.42 cm W x 5.56 cm D mm)
Weight	
FX7500	1.9 lbs ± 0.1 lbs (0.86 kg +/- 0.05 kg)
FX9600	4.5 lbs (2.1 kg)
Base Material	
FX7500	Die cast aluminum, sheet metal and plastic
FX9600	Die cast aluminum
Visual Status Indicators	Multi-color LEDs: Power, Activity, Status, and Applications
Mounting	
FX7500	Keyhole and standard VESA (75 mm x 75 mm)
FX9600	Four mounting flanges and Four 100 mm x 100 mm VESA holes for 10-32 screw.
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

Technical Specifications

Table 8 Technical Specifications (Continued)

Item	Description
Shock and Vibration	
FX7500	MIL-STD-810G
FX9600	MIL-STD-810G
Connectivity	
Communications	10/100 BaseT Ethernet (RJ45) w/ PoE support, PoE+, USB Client (Type B), USB Host (Type A)
General Purpose I/O	
FX7500	2 inputs, 3 outputs, optically isolated (terminal block) External 12V ~ 48 VDC power available for GPIO
FX9600	4 inputs, 4 outputs, optically isolated (terminal block) External 12V ~ 24 VDC power available for GPIO
Power	
FX7500	PoE (802.3af), PoE+ (802.3at) 12 VDC to 48 VDC, or 24 VDC Universal Power Supply
FX9600	PoE (802.3af), PoE+ (802.3at) 12 VDC to 24 VDC, or 24 VDC Universal Power Supply
Antenna Ports	
FX7500	FX7500-2: 2 mono-static ports (reverse polarity TNC) FX7500-4: 4 mono-static ports (reverse polarity TNC)
FX9600	FX9600-4: 4 mono-static ports (reverse polarity TNC) FX7500-8: 8 mono-static ports (reverse polarity TNC)
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

Technical Specifications

Table 8 Technical Specifications (Continued)

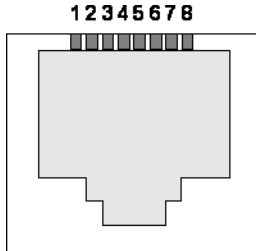
Item	Description
Transmit Power Output	
FX7500	10dBm to +31.5dBm (PoE+, 12V ~ 48V External DC, Universal 24 VDC Power Supply; +10dBm to +30.0dBm (PoE)
FX9600	0dBm to +33.0dBm (PoE+, 12V ~ 24V External DC, Universal 24 VDC Power Supply; +0dBm to +31.5dBm (PoE)
Max Receive Sensitivity	
FX7500	-82dBm
FX9600	-86dBm
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	
For the complete Zebra hardware product warranty statement, go to: www.zebra.com/warranty	
Recommended Services	
Support Services	Zebra One Care Select and Zebra One Care On Site
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 93 Ethernet Connections



USB Client Connector

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

Figure 94 USB Client Connector

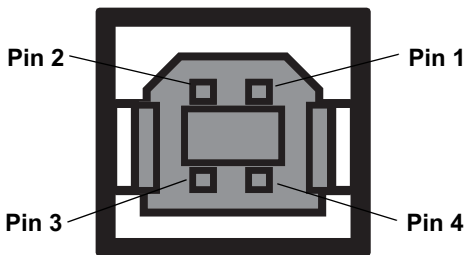


Table 9 USB Client Port Connector Pinout

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 95 USB Host Connector (J22)

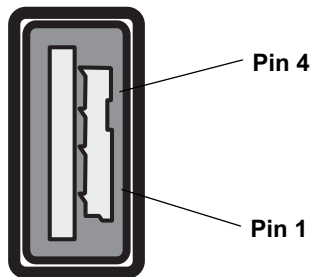


Table 10 USB Host Port Connector (J22) Pinout

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

FX7500 GPIO Port Connections

The FX7500 GPIO connector pinouts include the following:

Figure 96 FX7500 RFID Reader GPIO Connection



Table 11 FX7500 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

FX9600 GPIO ConnectionsFX9600 GPIO Connections

The FX9600 GPIO connector pinouts include the following:

Figure 97 FX9600 RFID Reader GPIO Connection

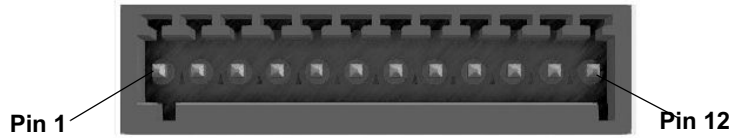


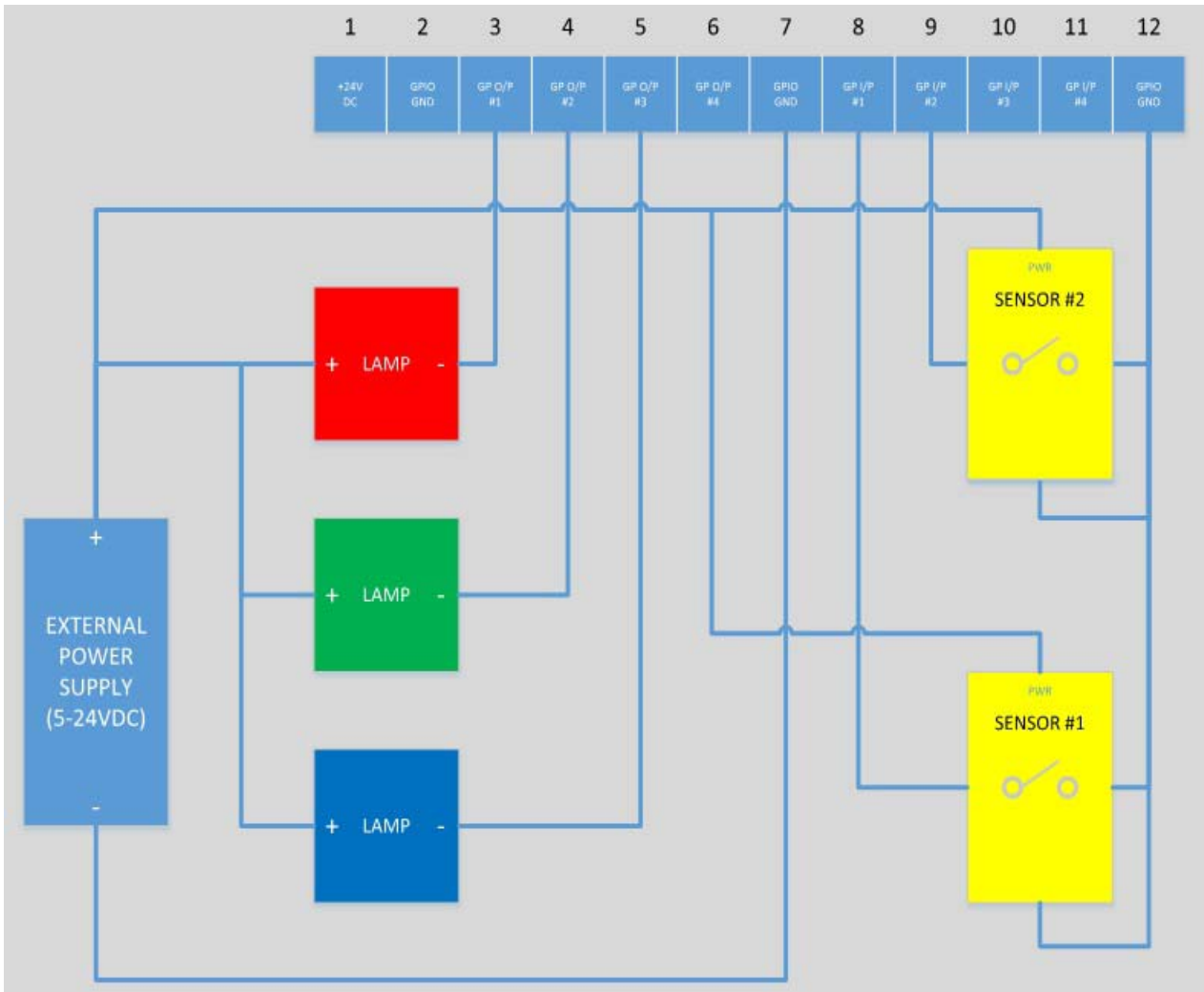
Table 12 FX9600 GPIO Pin Outs

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

Technical Specifications

The following figure provides an example of a typical GPIO setup with the power derived from an external power supply.

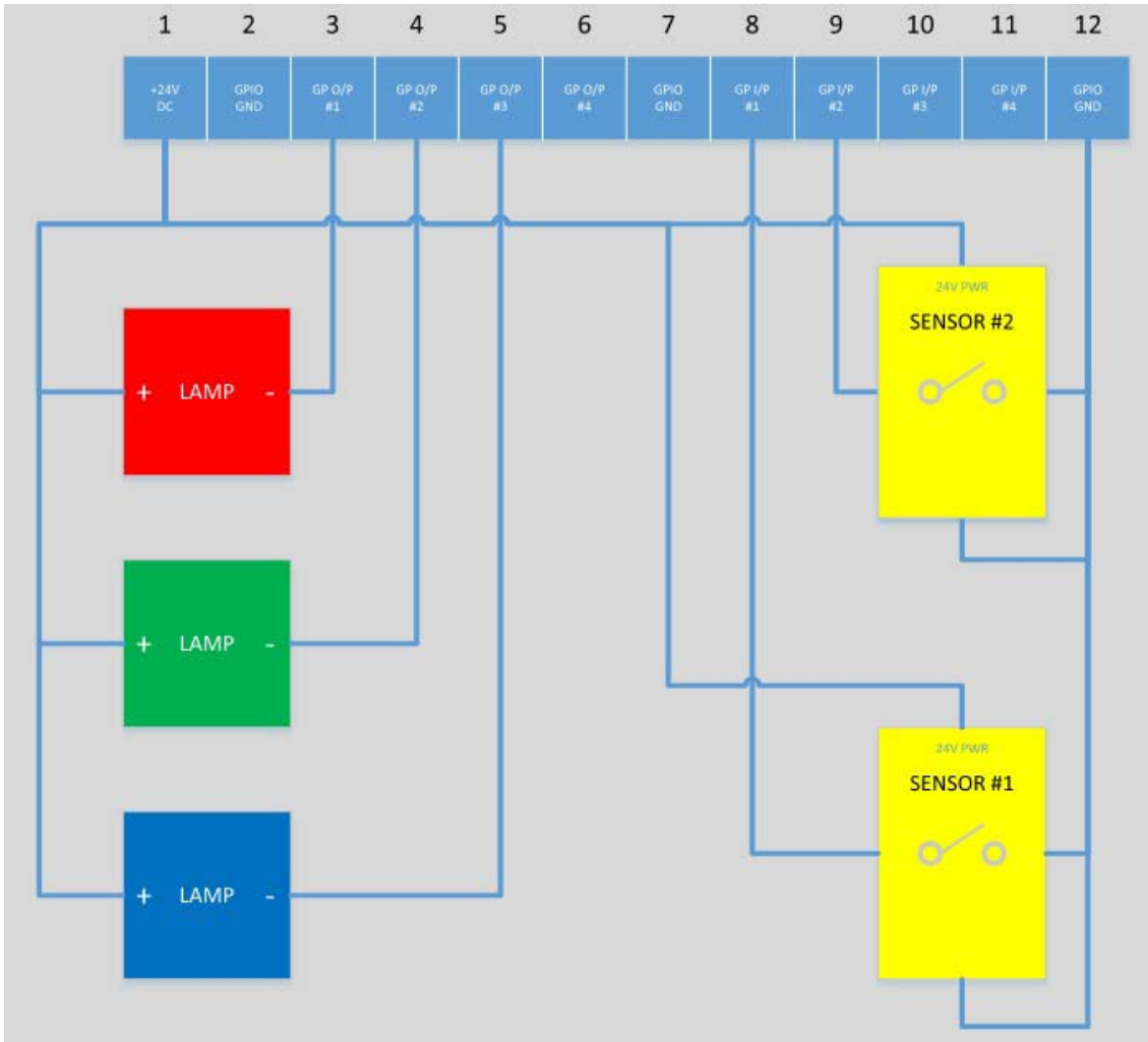
Figure 98 FX9600 GPIO Setup Example with Power Derived from External Power Supply



Technical Specifications

The following figure provides an example of a typical GPIO setup with the power derived from GPIO 24V Pin.

Figure 99 FX9600 GPIO Setup Example with Power Derived from GPIO 24V Pin



Static IP Configuration

Introduction

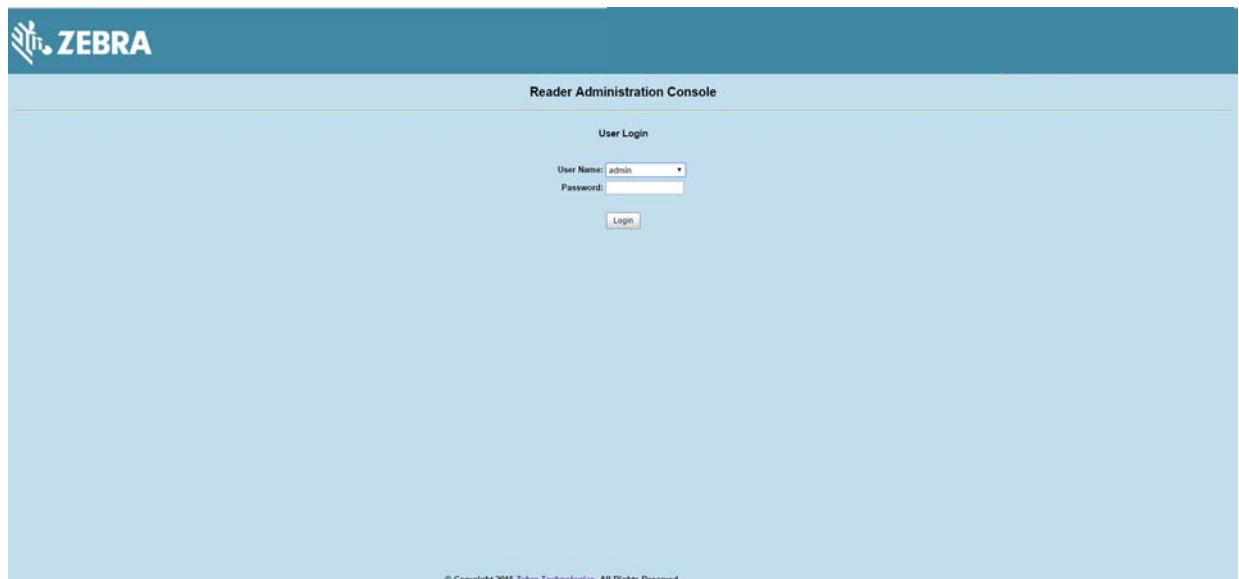
This chapter describes three methods of setting the static IP address on an FX7500 and FX9600 RFID Readers.

Reader IP Address or Host Name is Known

Set the Static IP Using the Web Console

1. Browse the device using the host name, for example: FX7500CD3B1E.
2. Log onto the device.

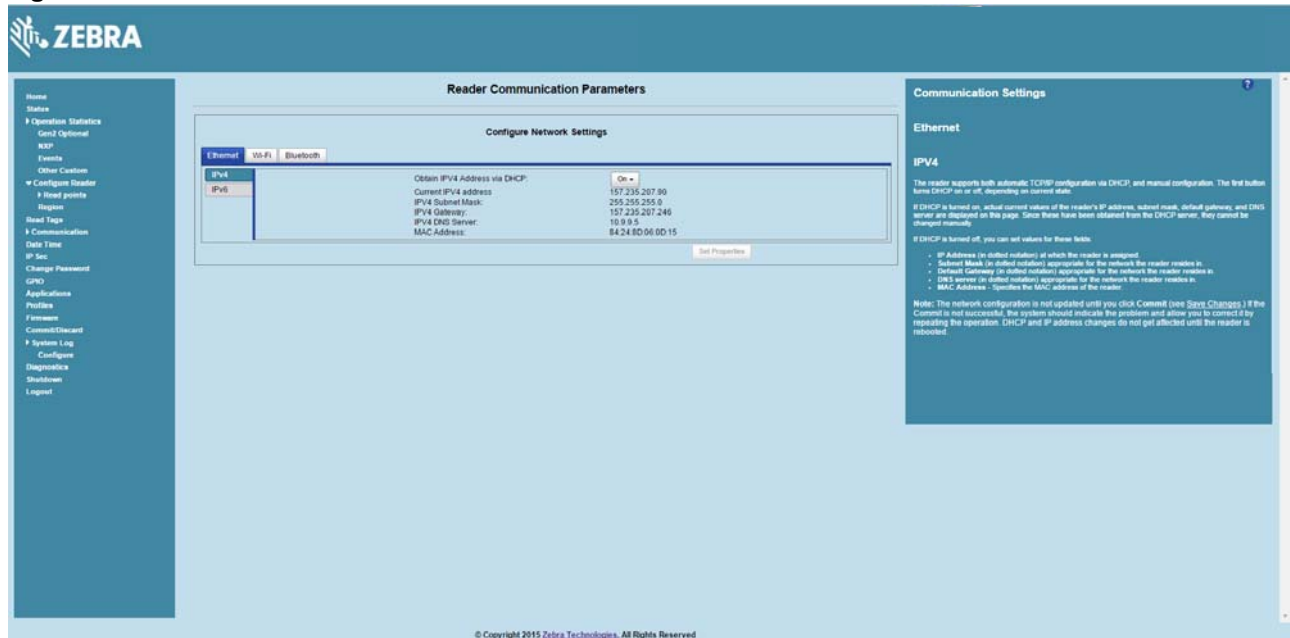
Figure 100 Reader Administration Console Login Window



3. Click Communication.
4. Set Obtain IP Address via DHCP to Off and enter all required information.

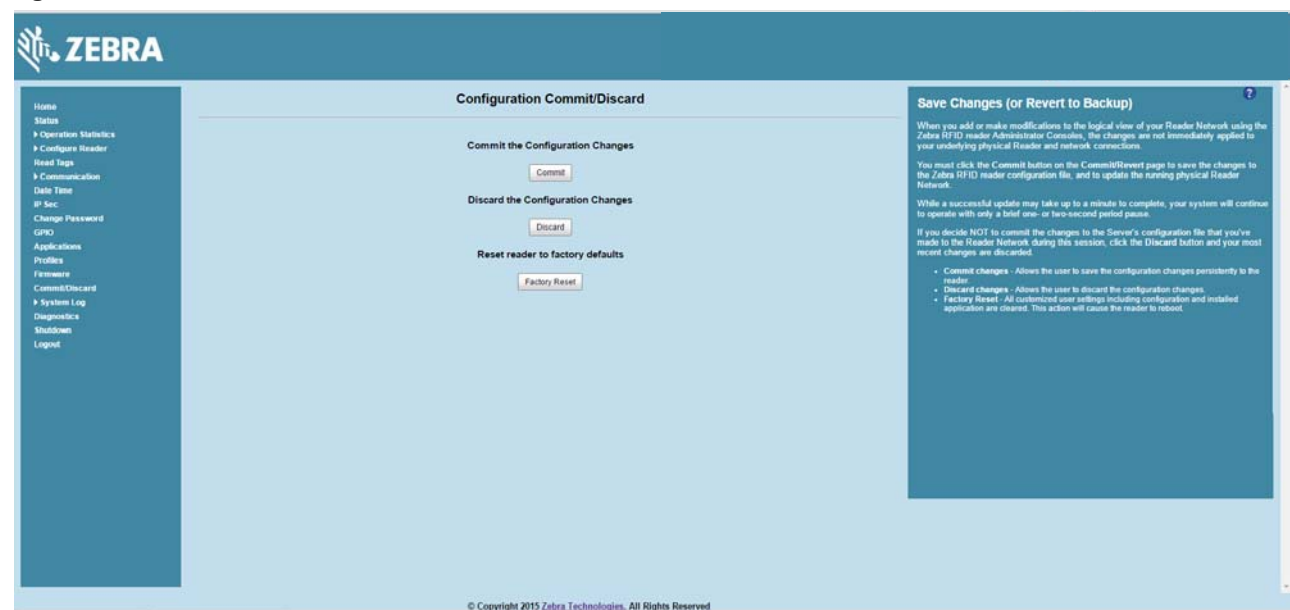
Static IP Configuration

Figure 101 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.

Figure 102 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.

Figure 103 Obtain IP Address

```
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:\>_
```

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

Figure 104 Ping the Host Name

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

C:\Users\DRWH67>ping FX7500657E5

Pinging FX7500657E5.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

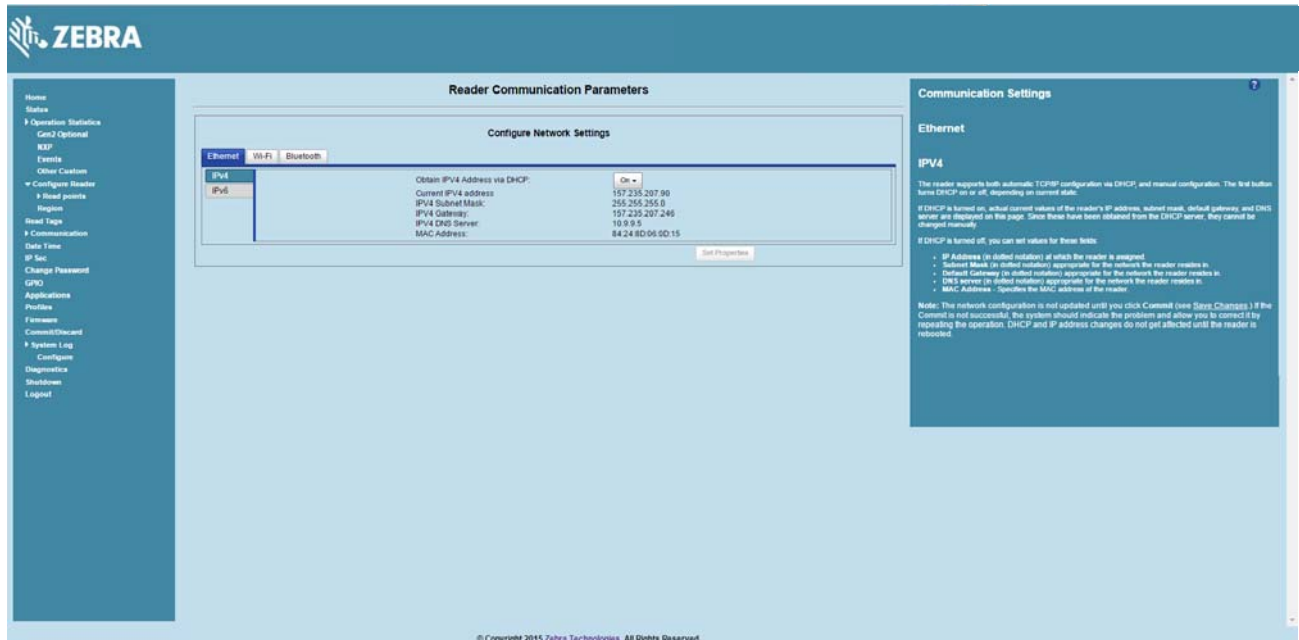
Ping statistics for 157.235.207.98:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\Users\DRWH67>_
```

5. Use a browser to connect to the device with the host name, for example: FX7500CD3B1E, or use the IP address obtained from ping replies (for example, 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.

Static IP Configuration

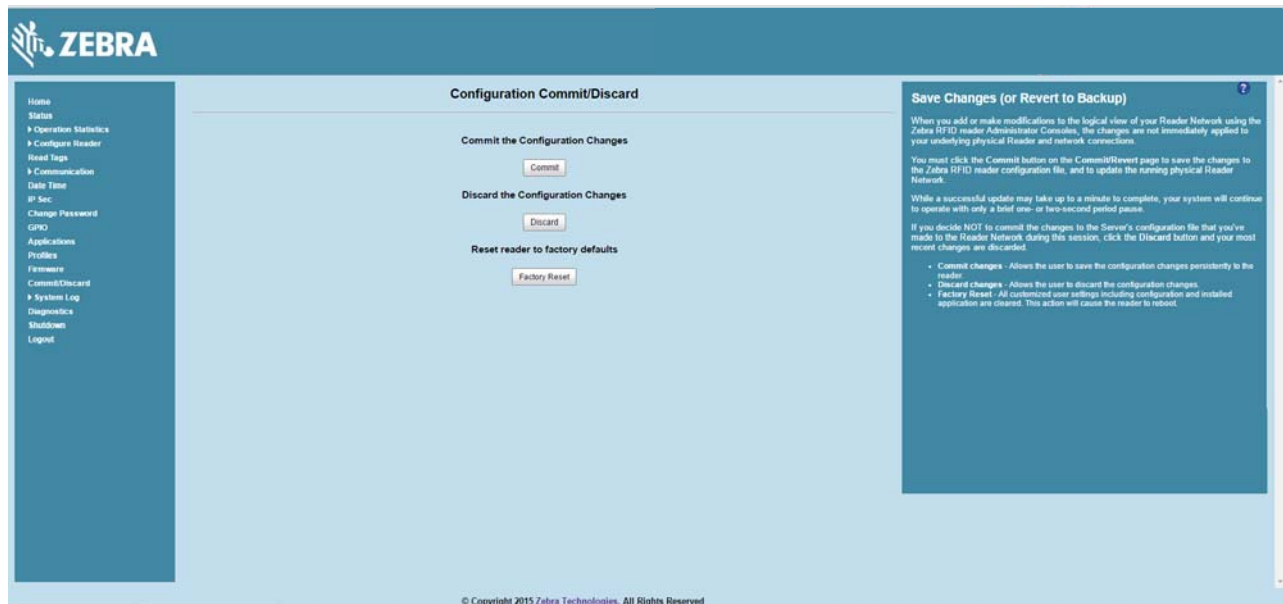
Figure 105 Reader Communication Parameters Window



9. Click Set Properties.

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

Figure 106 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.

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 13](#) and [Table 14](#). The Mode Index column refers to the index used to walk the C1G2UHFModeTable. Refer to the EPCglobal Low Level Reader Protocol (LLRP) Standard.

Table 13 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
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

*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.

RF Air Link Configuration

Table 13 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
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.

RF Air Link Configuration

Table 14 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

*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.

RF Air Link Configuration

Table 14 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
26	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
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.

Copying Files To and From the Reader

Introduction

The FX7500 and FX9600 RFID readers support 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 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 and FX9600.

FTPS

Use any standard GUI tool such as FileZilla, to connect to the FX7500 and FX9600 RFID readers over FTPS.

Data Protection

Introduction

The FX7500 and FX9600 RFID readers store 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 Wi-Fi and Bluetooth is also protected.

Index

Numerics

10/100BaseT Ethernet 14, 21, 22, 24, 25

A

administrator console 40
 applications 84
 committing changes 88
 communication settings 73
 configure network services 79
 configure network settings 73, 74, 75
 configuring system log 90
 discarding changes 88
 firmware version 87, 88
 GPIO 83
 IPV6 sec 81
 login 45
 main screen 47
 managing login 83
 reader diagnostics 90
 reader profiles 85
 scan control 18, 72
 set password 82
 setting date and time 80
 shutting down 91
 status 49
 system log 89
air link 137
antennas
 configuring 57
 installing 31
 ports 14, 21, 22, 24, 25
applications 84

B

bluetooth 104, 105
 connecting 104, 105

C

cable pinouts
 ethernet 127
 GPIO 129
 USB 127, 128
 USB client 127
 USB host 128
chapter descriptions 10
commit region change 16
committing changes 88
communication 22, 25
 ethernet, wired 33
communication settings 73
configure
 antenna 57
 LLRP 76
 read points 56, 57
 reader 55
 region 58
 SNMP 77
 static IP 133
 static IP via web console 133, 135
 wireless 78
configuring network
 bluetooth 75
 ethernet 73
 services 79
 wi-fi 74
connecting
 to reader 42
 via bluetooth 104, 105
 via host name 43
 via IP address 44
 via wi-fi 101
connection
 antennas 31
 communication 33
 port diagram 24
 ports 21, 24
 wired ethernet 33
conventions

notational 11
 copying files 107, 141
 country list 16, 46

D

data protection 143
 date 80
 deployments 41
 discarding changes 88

E

ethernet
 pinouts 127
 POE 33
 port 22, 25
 setup 33
 wired 33
 event statistics 53

F

files
 copying 107, 141
 firmware
 version 87, 88
 firmware update 87, 88, 111
 prerequisites 109
 first time login 15, 45
 FTP
 copying files 107, 141
 FTPS
 copying files 142

G

GPIO 14, 21, 24
 GPIO connections 130
 pinouts 129
 port 22, 25
 GPIO control 83

H

host communication
 ethernet, wired 33
 host name connect 14

I

information, service 12
 initiating reads 18, 72
 installation
 antennas 31

communication connection 33
 mounting 28
 IP address 43
 IP ping 43

L

LEDs 23, 26
 LLRP
 configure 76
 radio modes 137, 139
 log 89
 configuring 90
 login 45
 first time 45
 managing 83

M

mounting 28, 30
 concrete wall mounting 30
 drywall mounting 30
 wood or metal wall mounting 30
 mounting plate 28
 multiple reader deployments 41

N

NXP
 statistics 52, 54

O

obtain reader IP address 43

P

Password 15, 111, 117
 password 15, 45, 111, 117
 changing 82
 pinouts
 ethernet 127
 GPIO 129
 USB 127, 128
 USB client 127
 USB host 128
 POE 14, 21, 22, 24, 25, 33, 127
 ports 21, 24
 descriptions 22, 25
 ethernet 33
 power 14, 21, 24
 POE 33
 port 22, 25
 profiles 85

R

read points	56, 57
reader	
configuration	55
connecting	42
GEN2 statistics	50
profiles	85
statistics	49
event	53
NXP	52, 54
status	49
reading tags	39
initiating	18, 72
rear panel	14, 24
reboot	41
region	46
region configuration	58
region control	46
region setting	16
region settings	16
reset	14, 21, 22, 24, 25
RFID	
FX reader	20, 24
RJ45	22, 25

S

SCP	
copying files	107, 141
service information	12
set region	16, 46
setting date	80
setting time	80
setup	
wired ethernet	33
wired ethernet AC outlet	33
wired ethernet, power-over	33
shutdown	91
SNMP	
configure	77
software update	111
specifications	124
start-up	15
static IP configuration	133
via web console	133, 135
Statistics	53
statistics	49
event	53
GEN2	50
NXP	52, 54
status	49
system log	89
configuring	90
system time	80

T

tags	
reading	39, 72
technical specifications	124
time	80
troubleshooting	118

U

unpacking	27
updating firmware	87, 88, 111
prerequisites	109
updating software	111
USB	14, 21, 24, 101, 113
client pinouts	127
host pinouts	128
pinouts	127, 128
user ID	45
user name	15, 111, 117
user password	45

V

version control	87, 88
-----------------------	--------

W

wi-fi	101
connecting	101
wired ethernet	33
wireless	
configure	78

Z

zero-configuration networking	44
-------------------------------------	----

