

FX SERIES RFID FIXED READER



ZEBRA

Integration Guide

FX SERIES RFID READER INTEGRATION GUIDE

MN000026A10

Revision A

August 2019

Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2019 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

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.
-07 Rev A	12/2017	Correction to antenna port technical specification for FX9600.
-08 Rev A	7/2018	Updates: <ul style="list-style-type: none">- FX9600 Bluetooth dongle support information.- Air Protocol ISO/IEC 18000-63.
-09 Rev A	9/2018	Added: <ul style="list-style-type: none">- "Requirements" section to "Quick Start".- "Install" below Applications.- FX9600 Serial Port Data Configuration. Updated: <ul style="list-style-type: none">- "Quick Start" steps 1 & 2.- Warning statement below "Connecting FX7500 and FX9600 RFID Reader Antennas".- Statement below "Microsoft RNDIS Driver for Windows 7."- Several items on page 34.- Global update -> 'click' to 'select' (techpubs style change).- Replaced the following screen shots and corresponding screen selections: Figures 7, 35, 39, 51, 52, 55- Tables 7 and 8.- System Log field definitions. Deleted: <ul style="list-style-type: none">- All instances of Java JRE.- 'Read Tags' notes (security and clearing java cache).- JVM references in Reader Profiles.

Change	Date	Description
-10 Rev A	8/2019	<p>Added:</p> <ul style="list-style-type: none"> - FX Connect information. - New troubleshooting information. - New Important statement in the Connecting FX7500 and FX9600 RFID Reader Antennas section. <p>Updated:</p> <ul style="list-style-type: none"> - 123RFID to 123RFID Desktop. - Administrator Console introduction. - Commit/Discard section. - Screen shots. - Related documents, software and reference guide. - Auto Discovery section. - Cable loss and cable length default value. - Data Prefix/Data Suffix in Table 9 and 11. - Server URL in Manage License section. - Capability response valid period. - FX Connect Licensing Mechanism

Table of Contents

Copyright	3
For Australia Only	3
Terms of Use	3
Revision History	4

About This Guide

Introduction	10
Chapter Descriptions	10
Notational Conventions	11
Related Documents and Software	11
Service Information	11

Quick Start

Introduction	12
Requirements	12
Quick Start Demonstration	12
Step 1, Setup	13
Step 2, Connecting to the Reader	14
Step 3, First Time / Start-Up Login	14
Step 4, Set Region	15
Step 5, Read Tags	17

Getting Started

Introduction	18
FX Series Features	18
FX7500 Parts	19
FX7500 Rear Panel	20
FX7500 LEDs	20
FX9600 Parts	21
FX9600 Rear Panel	22
FX9600 LEDs	23

Installation and Communication

Introduction	24
--------------------	----

Table of Contents

Unpacking the Reader	24
Mounting and Removing the FX Series Readers	25
Mounting the FX7500 With a Mounting Plate	25
FX7500 Direct Mounting	26
Mounting the FX9600 Reader	27
Connecting FX7500 and FX9600 RFID Reader Antennas	28
Communications and Power Connections	29
Ethernet Connection	29
USB Connection	30
GPIO Interface Connection	33
LED Sequences	34
System Start-up/Boot LED Sequence	34
PWR LED Sequence to Indicate IPv4 Status after Booting	34
Reset to Factory Defaults LED Sequence	34
LED Sequence for Software Update Status	34
Reading Tags	35
 123RFID Desktop	
Introduction	36
Features	37
Communication with 123RFID Desktop	37
123RFID Desktop Requirements	37
 Administrator Console	
Introduction	38
Reader Administrator Console Selections	38
Profiles	39
Resetting the Reader	39
Auto Discovery	40
Connecting to the Reader	41
Obtaining the IP Address via Command Prompt	41
Connecting via Host Name	42
Connecting via IP Address	42
Using Zero-Configuration Networking when DHCP Server is Not Available	42
Administrator Console Login	43
First Time / Start-Up Login	43
Setting the Region	44
Reader Administrator Console	45
Administrator Console Option Selections	45
Status	47
Reader Statistics	48
Reader Gen2 Optional Operation Statistics	49
NXP Custom Command Operation Statistics	50
Event Statistics	51
Other Custom Command Operation Statistics	52
Configure Reader	53
Reader Parameters	53
Read Points	54
Read Points - Advanced	55

Table of Contents

Configure Region	56
Certificates	57
Read Tags	67
Communication Settings	68
Configure Network Settings - Ethernet Tab	68
Configure Network Settings - Wi-Fi Tab	69
Configure Network Settings - Bluetooth Tab	70
Configure LLRP Settings	71
SNMP Settings	72
Wireless Settings	73
Network Services Settings	74
FX9600 Serial Port Configuration	74
FX Connect	77
FX Connect Licensing Management	89
System Time Management	96
IPV6 IP Sec	97
Change Password	98
FX Series User Accounts	98
Managing User Login and Logout	99
GPIO	99
Applications	100
Reader Profiles	101
FIPS Support	102
Firmware Version/Update	102
Firmware Update	103
Commit/Discard Functionality Changes	103
Region Configuration Commit	103
New Property Change Work Flow	105
System Log	107
Configure System Log	108
Reader Diagnostics	109
Shutdown	110
 Configure and Connect via Wi-Fi and Bluetooth	
Wireless Network Advanced Configuration	111
Sample Configuration Files	112
Preferred Configurations for Access Points	113
Access Point Configuration for Android Device	114
Internet Connection Configuration for iPhone	115
Connecting to a Wireless Network Using a Wi-Fi Dongle	116
Connecting to a Peer Device over Bluetooth Using a Bluetooth Dongle	120
Copying Files to the Reader	122
 Application Development	
Introduction	123
Reference Guides	123

Firmware Upgrade

Introduction	124
Prerequisites	124
Failsafe Update	125
Update Phases	125
Updating FX Series Reader Software	126
Verifying Firmware Version	126
Updating Methods	127
Verifying Firmware Version	132

Troubleshooting

Troubleshooting	134
-----------------------	-----

Technical Specifications

Technical Specifications	140
Cable Pinouts	142
10/100bT Ethernet / PoE Connector	142
USB Client Connector	143
USB Host Connector	143
FX7500 GPIO Port Connections	144
FX9600 GPIO Connections	144

Static IP Configuration

Introduction	147
Reader IP Address or Host Name is Known	147
Reader IP is Not Known (DHCP Network Not Available)	149

RF Air Link Configuration

Introduction	151
Radio Modes	151

Copying Files To and From the Reader

Introduction	155
SCP	155
FTP	155
FTPS	155

Data Protection

Introduction	156
--------------------	-----

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.
- [123RFID Desktop](#) describes 123RFID Desktop for fixed RFID readers.
- [Administrator Console](#) describes how to connect to the reader, how to use the web-based Administrator Console to configure and manage FX7500 and FX9600 readers and detailed information about FX Connect.
- [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.
- Zebra FX Series Embedded C/CPP SDK User Guide Linux. Provides instructions for using the FX Series Embedded native C/C++ SDK for Linux.
- Zebra FX Series Embedded Java SDK User Guide Linux. Explains how to use the FX Series Embedded Java SDK for Linux.
- Zebra FX Series Embedded Java SDK User Guide Windows. Describes instruction for using the FX Series Embedded Java SDK for Windows.
- 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 system requirements and a Quick Start setup demonstration.

Requirements

- Fixed reader.
- Ethernet cable.
- Personal computer running Windows with Internet Explorer 11.
- Antenna cable.
- Antenna.
- Power supply (AC power supply or PoE/PoE+ injector).
- RFID tags (EPC Global Gen2 compliant).

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 14](#)
- [Step 4, Set Region on page 15](#)
- [Step 5, Read Tags on page 17](#)

Step 1, Setup

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

1. Unpack the reader. See [Unpacking the Reader on page 24](#).
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 34](#) for boot-up details.

Figure 1 FX7500 RFID Fixed Reader Rear Panel Connections

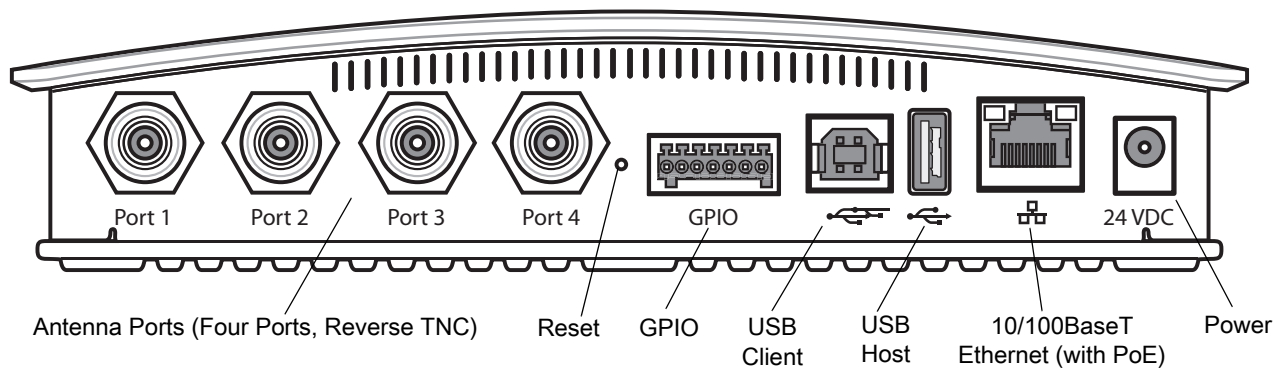
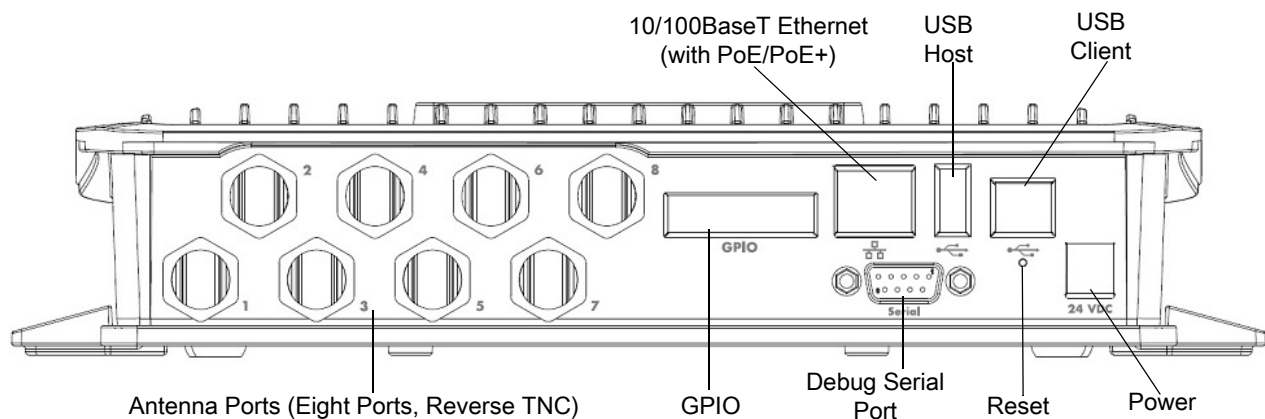


Figure 2 FX9600 RFID Fixed Reader Rear Panel Connections



Step 2, Connecting to the Reader

To connect via host name:

1. Open a web browser to connect to the reader.
2. Enter the host name printed on the reader label in the browser address bar. If the label is missing or damaged, it is possible to create the host name by using the reader model name as a prefix followed by the last six hex numbers from the MAC address. For example, for an FX9600 with the MAC address 0023683BA63A, the host name is FX96003BA63A. The string to enter in the browser address bar is `http://FX96003BA63A`.



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



NOTE: If you forget the user ID and/or password, see [Reset to Factory Defaults LED Sequence on page 34](#) 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. Select **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 21 on page 39](#).

Step 4, Set Region

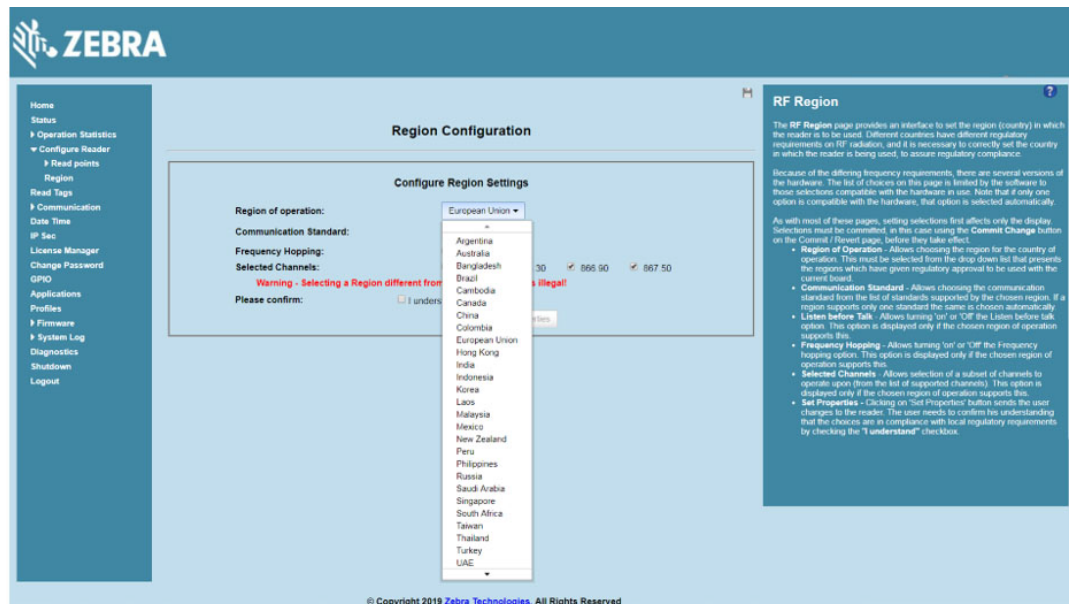
Set the region of operation. **Setting the unit to a different region is illegal.**



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.

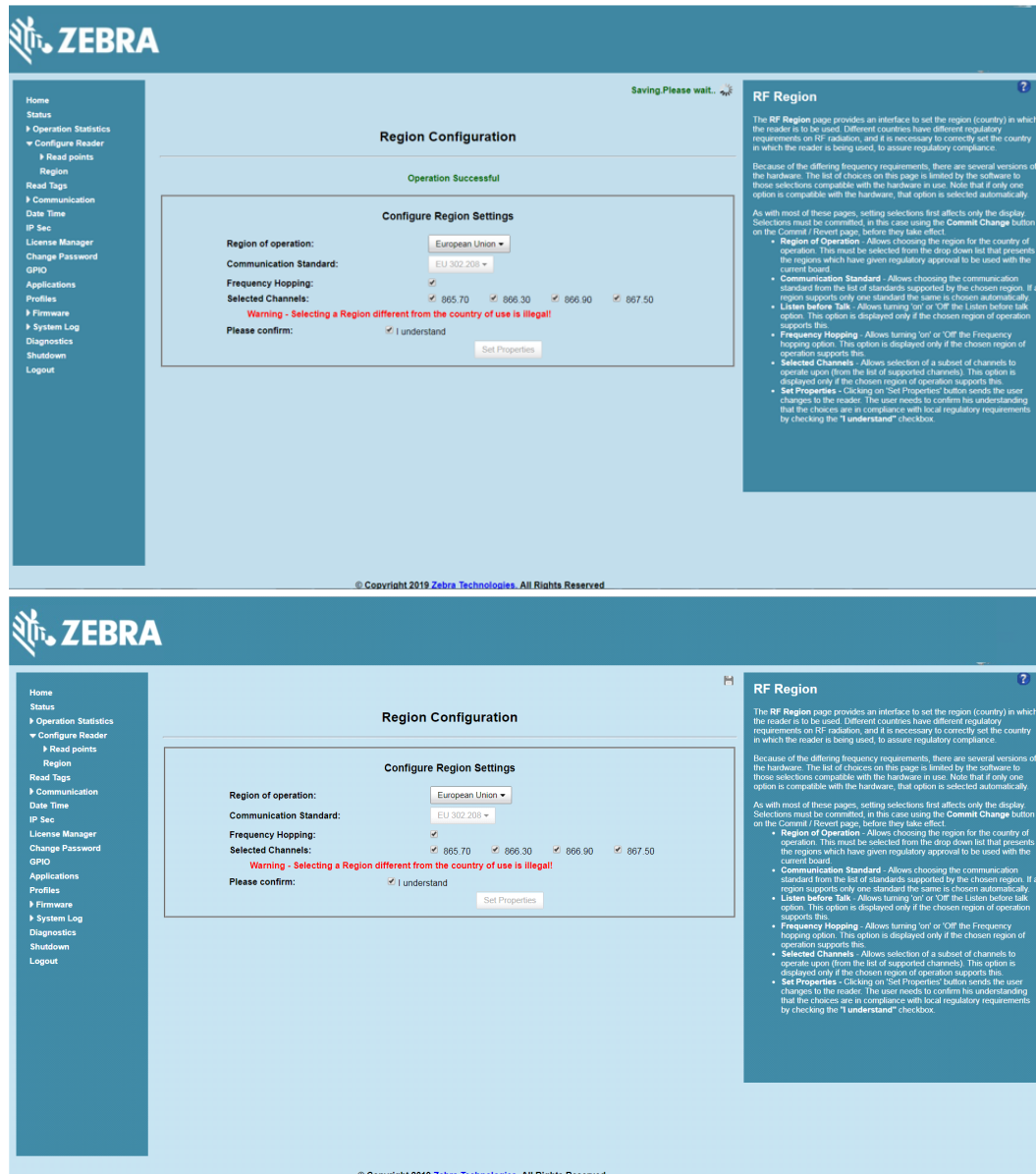
1. In the **Configure Region Settings** window, select the region from the drop-down menu.

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 displays a **Saving. Please wait...** message with a progress symbol until the commit completes.
7. When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully. See [Commit/Discard Functionality Changes on page 103](#) for more information.

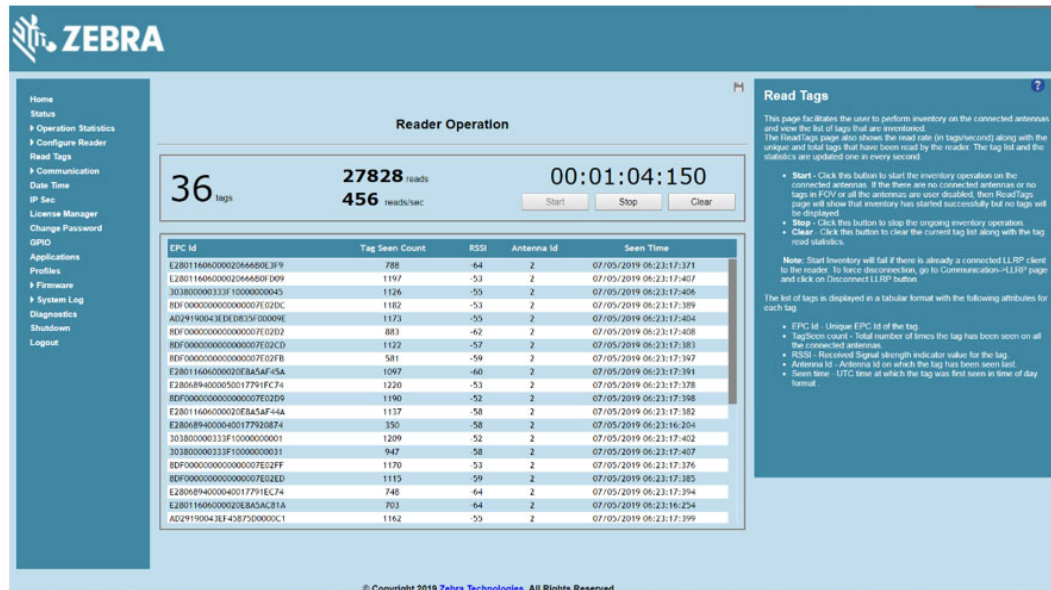
Figure 5 Region Configuration, Operation Successful Window



Step 5, Read Tags

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

Figure 6 Read Tags Window



- Select **Start** to initiate an on-demand scan on the connected antennas that are enabled.
- Select **Stop** to stop the inventory operation.
- Select **Clear** 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.
- **Tag Seen 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.
- **Seen Time:** UTC time (in microseconds) showing when the tag was first 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 provide a wide range of features that enable implementation of complete, high-performance, intelligent RFID solutions.

Table 1 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

Table 1 FX Series RFID Reader Features (Continued)

Feature	Zebra FX7500	Zebra FX9600
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 7 FX7500 RFID Reader Rear Panel Connections

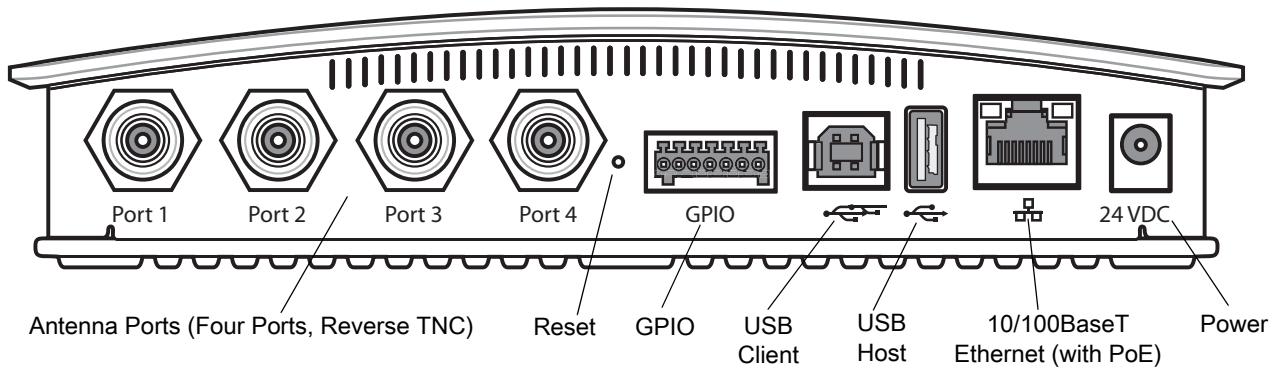
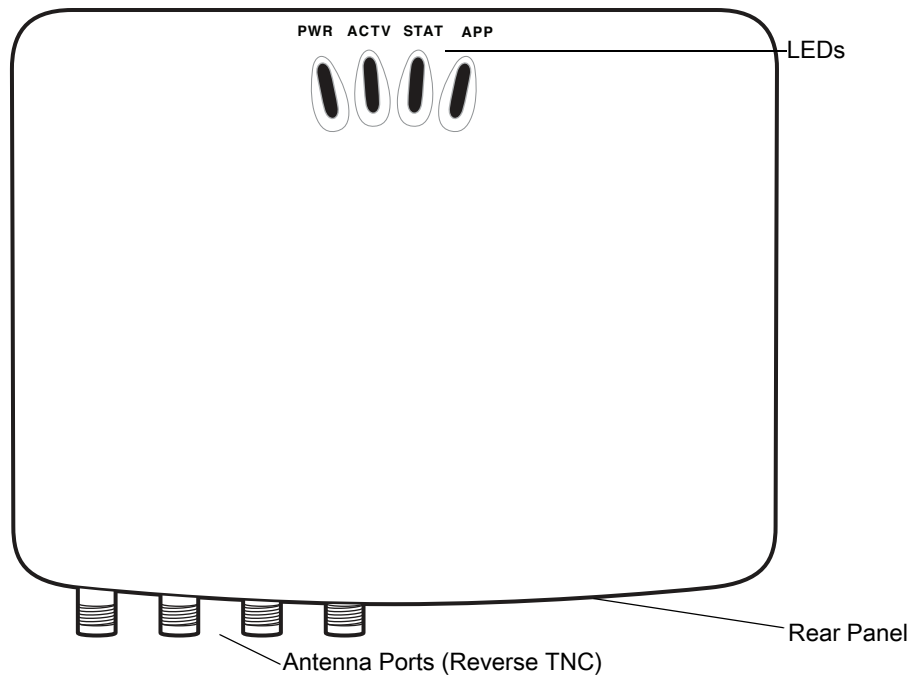


Figure 8 FX7500 RFID Reader



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 2 Rear Panel Descriptions

Port	Description
Antenna Ports (Reverse TNC)	Two port version: Connect up to two antennas. Four port version: Connect up to four antennas. See Table 14 on page 140 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 28 for connection information.
Reset	To reset the reader insert a paper clip into the reset hole, press and hold the reset button for not more than 2 seconds. This resets the reader, but retains the user ID and password.
GPIO	See GPIO Interface Connection on page 33 for more information.
USB Client	The USB client port supports (by default) a network mode of operation. This enables a secondary network interface as a virtual adapter over USB. Advanced users can create a custom communication protocol on the USB port. See USB Connection on page 30 for connection information.
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 29 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 3](#). For the LED boot up sequence see [System Start-up/Boot LED Sequence on page 34](#).

Figure 9 FX7500 RFID Readers LEDs

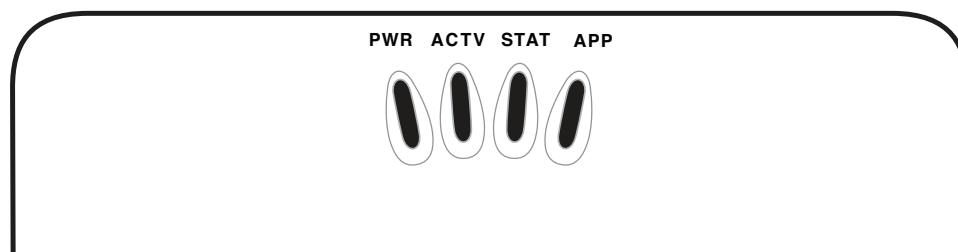


Table 3 FX7500 LED Indications

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 10 FX9600 RFID Reader Rear Panel Connections

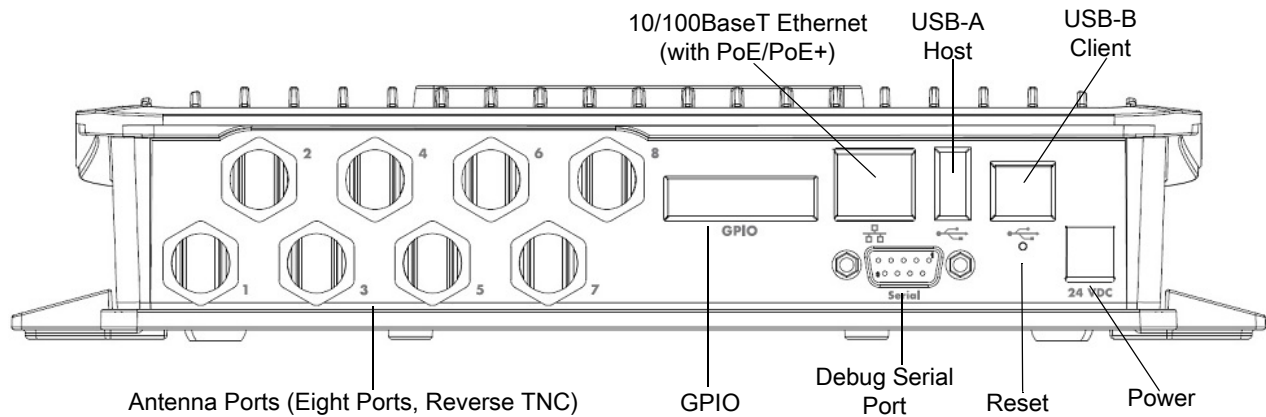
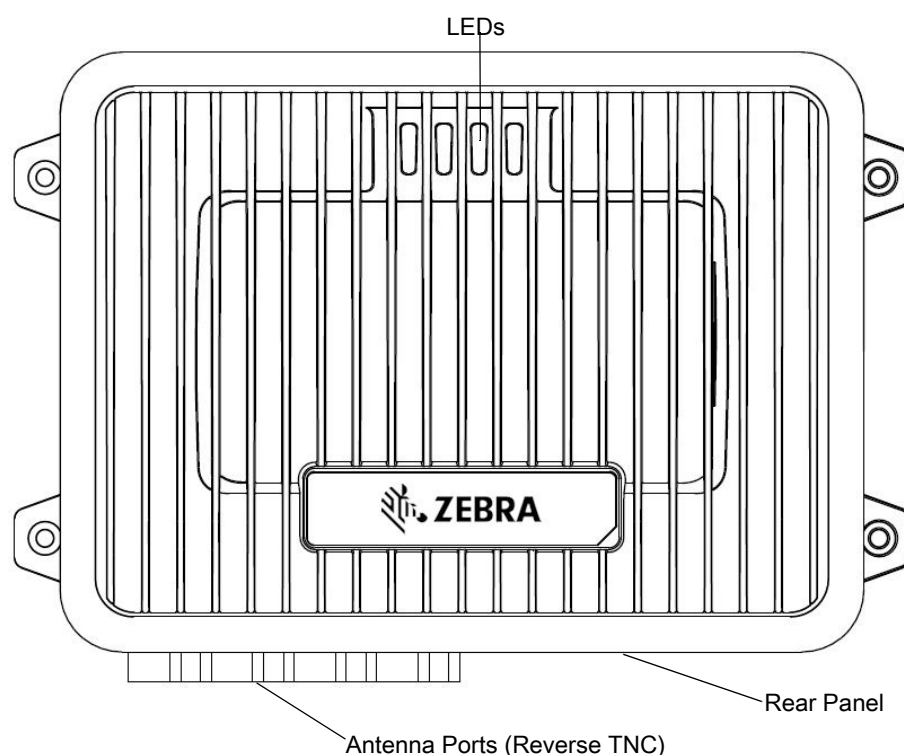


Figure 11 FX9600 RFID Reader

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 4 Rear Panel Descriptions

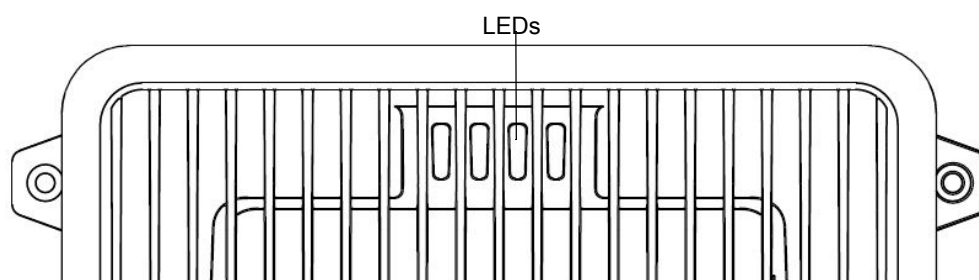
Port	Description
Antenna Ports (Reverse TNC)	<p>Four port version: Connect up to four antennas.</p> <p>Eight port version: Connect up to eight antennas.</p> <p>See Table 14 on page 140 for the maximum antenna gains and RF output powers for both US/Canada and EU.</p> <p>See Connecting FX7500 and FX9600 RFID Reader Antennas on page 28 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 33 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 30 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.

Table 4 Rear Panel Descriptions (Continued)

Port	Description
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 29 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 3](#). For the LED boot up sequence see [System Start-up/Boot LED Sequence on page 34](#).

Figure 12 FX9600 RFID Readers LEDs**Table 5** 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 24](#)
- [Mounting and Removing the FX Series Readers on page 25](#)
 - [Mounting Tips on page 25](#)
 - [Mounting the FX7500 With a Mounting Plate on page 25](#)
 - [FX7500 Direct Mounting on page 26](#)
- [Connecting FX7500 and FX9600 RFID Reader Antennas on page 28](#)
- [Communications and Power Connections on page 29](#)
 - [Ethernet Connection on page 29](#)
 - [USB Connection on page 30](#)
 - [GPIO Interface Connection on page 33](#)
- [System Start-up/Boot LED Sequence on page 34](#)



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.



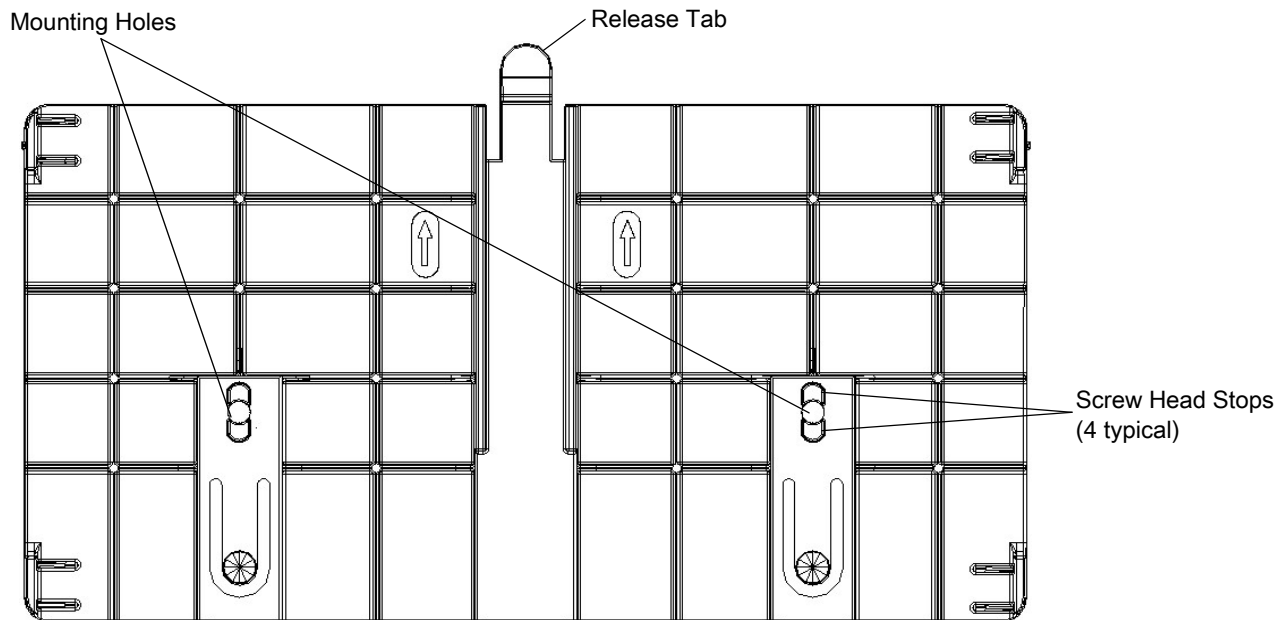
NOTE: The Mounting Plate section applies to the FX7500 RFID Fixed Reader only.

1. Position the mounting plate on a flat surface (wall or shelf). Position the release tab on the top. See [Figure 13](#).
2. Mark the hole locations using the mounting plate as a guide. See [Figure 13](#). 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 13 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 13). 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.

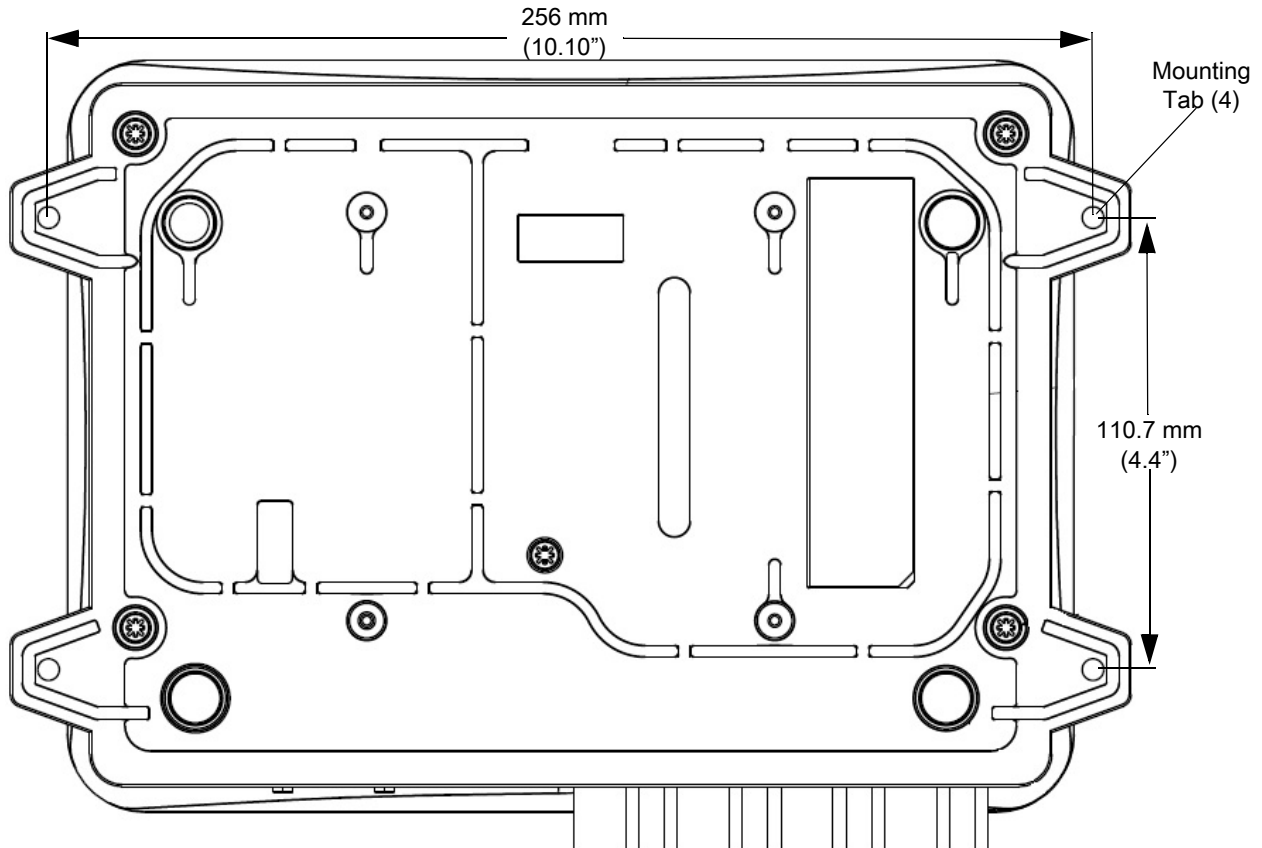
To mount the unit without using the mounting plate:

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 14 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



IMPORTANT: The Zebra antennas that are approved and provide optimal performance for various uses cases are AN510, AN440, AN480, AN610, AN620, AN710, and AN720. To meet optimum RF specifications, an antenna with maximum VSWR = 1.4 must be used.



WARNING: Follow antenna installation and power connection instructions in its entirety before operating the FX readers to avoid personal injury or equipment damage that may result from improper use. To safeguard personnel, be sure to position all antenna(s) according to the specified requirements for your regulatory region.



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 6](#) 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 6 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 15](#)):

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 15 FX7500 RFID Reader Antenna Connection

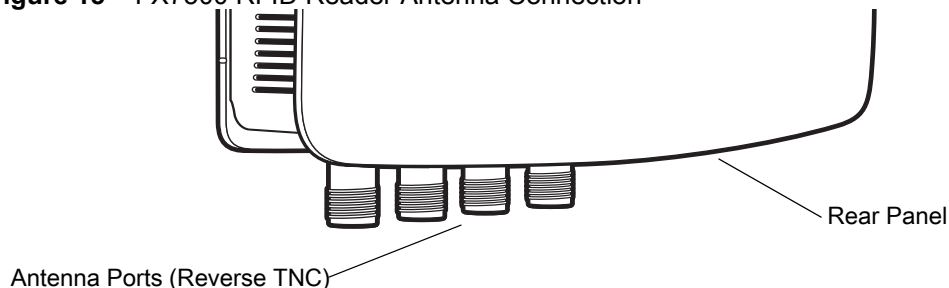
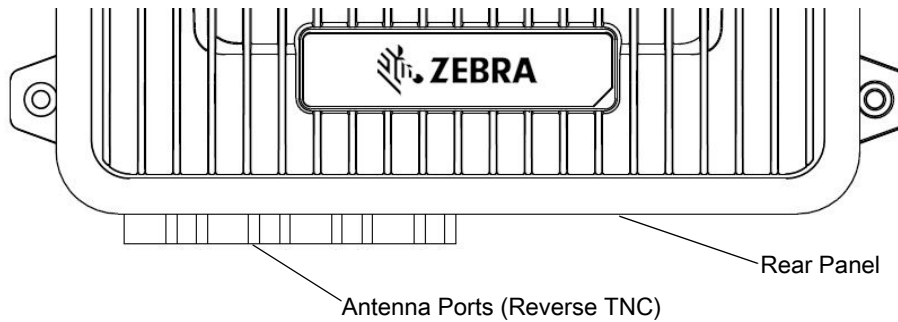


Figure 16 FX9600 RFID Reader Antenna Connection



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 7 on page 19](#)) or FX9600 reader (see [Figure 10 on page 21](#)).
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 34](#).
9. On a networked computer, open an Internet browser and connect to the reader. See [Connecting to the Reader on page 41](#).
10. Log in to the **Administrator Console**. See [Administrator Console Login on page 43](#).

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 7 on page 19](#) or [Figure 10 on page 21](#).
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 34](#).
4. On a networked computer, open an Internet browser and connect to the reader.
See [Connecting to the Reader on page 41](#).
5. Log in to the **Administrator Console**. See [Administrator Console Login on page 43](#).



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 network adapter over USB. The Ethernet network interfaces co-exists with the USB virtual network adapter. However, only one application connection (RFID connection or web console connection) is allowed at any time. See [Sample Implementation on page 32](#) for an example of how the standard network adapter can be used in conjunction with the USB virtual network adapter. To use the USB virtual network adapter, 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 7 on page 19](#) or for the FX9600, see [Figure 10 on page 21](#). Connect the other end of the cable to a USB port on the host PC.

Zebra USB RNDIS Driver

To use the USB virtual network adapter, 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 31](#)).

To install the RNDIS driver on the host.

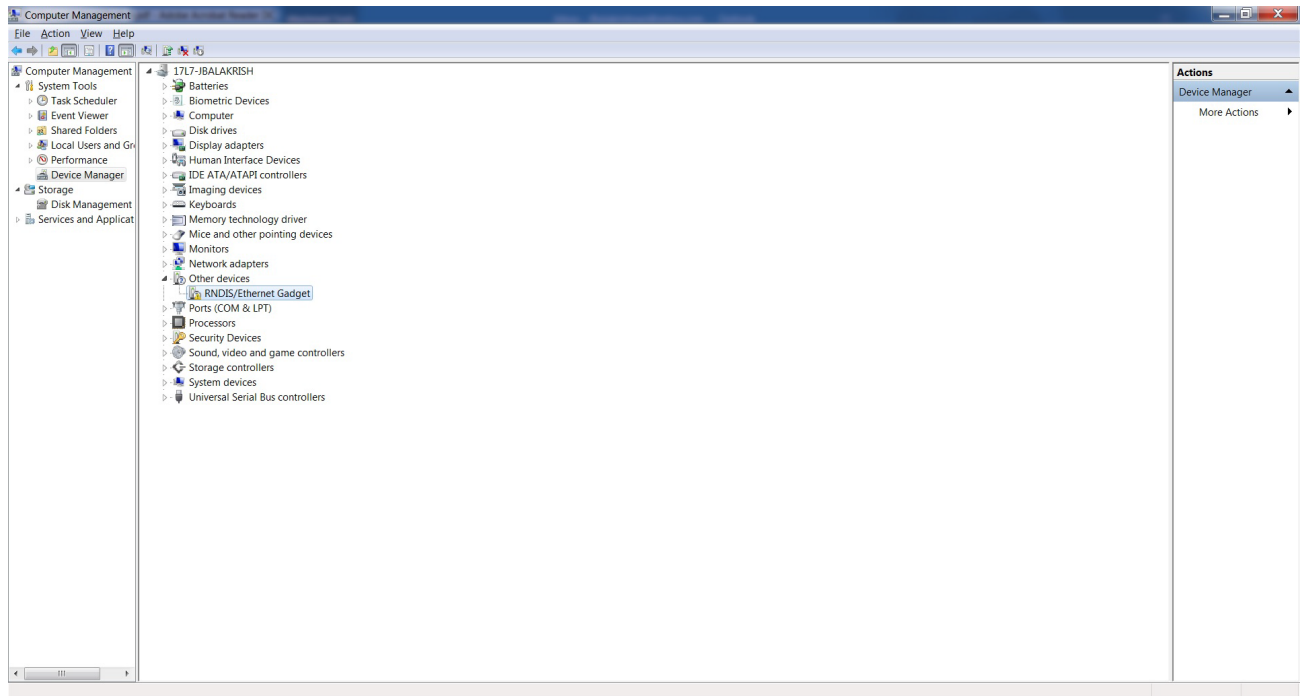
1. Download the installer file **Zebra RNDIS.msi** from www.zebra.com/support to the host PC.
2. Select this file on the host PC to install the host side drivers for using the USB Remote Network Device Interface on the FX7500 or FX9600.
3. Connect a USB cable between the host and the reader. The **Welcome to the Found New Hardware Wizard** screen appears.
4. Select the **No, not this time** radio button and select **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

The following steps are the recommended procedure for Windows 7:

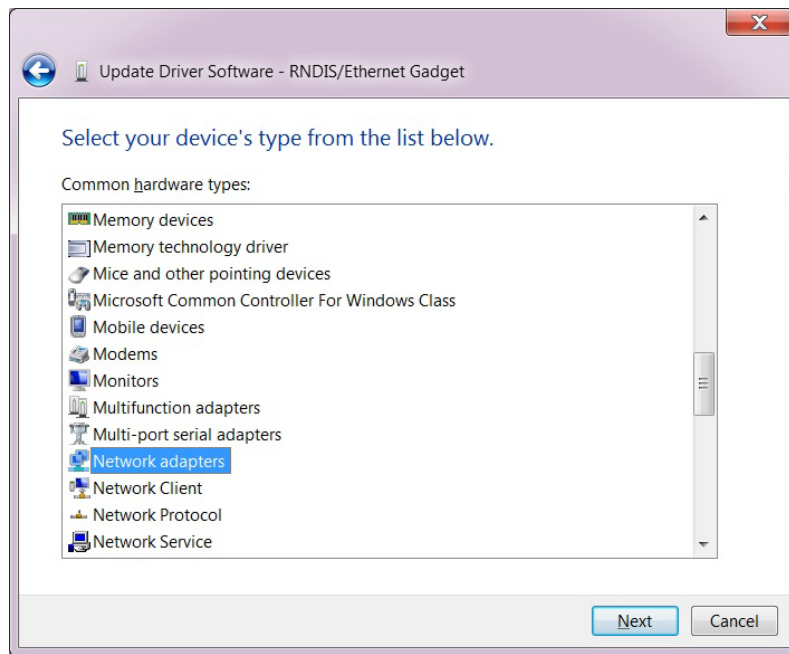
1. After connecting a USB cable between the PC and reader, the RNDIS driver automatically installs. If it does not, right-click on **Computer** and select **Manage**. From **System Tools**, select **Device Manager**. Under **Other Devices**, look for an entry for RNDIS with an exclamation icon indicating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

Figure 17 Computer Management Window



2. Right-click the icon and select **Update Driver Software**. Search for the device driver software by selecting **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 18 Selecting Device Type



5. Select **Microsoft Corporation** from the manufacturer list.
6. Under **Network Adapter**, select **Remote NDIS Compatible Device**, and select **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.

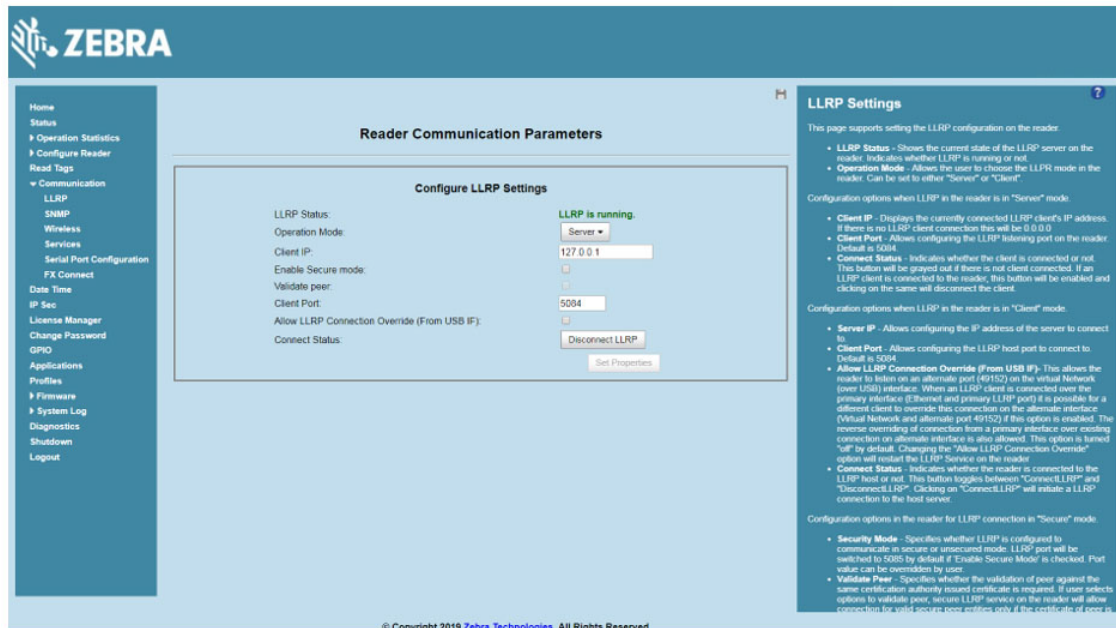
Sample Implementation

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 19 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 17 on page 144](#) 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 9 on page 20](#) for the FX7500 and [Figure 12 on page 23](#) 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 34](#).

1. Enable tag reading using the web-based **Administrator Console** (see [Read Tags on page 67](#)) 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 9 on page 20](#). 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.

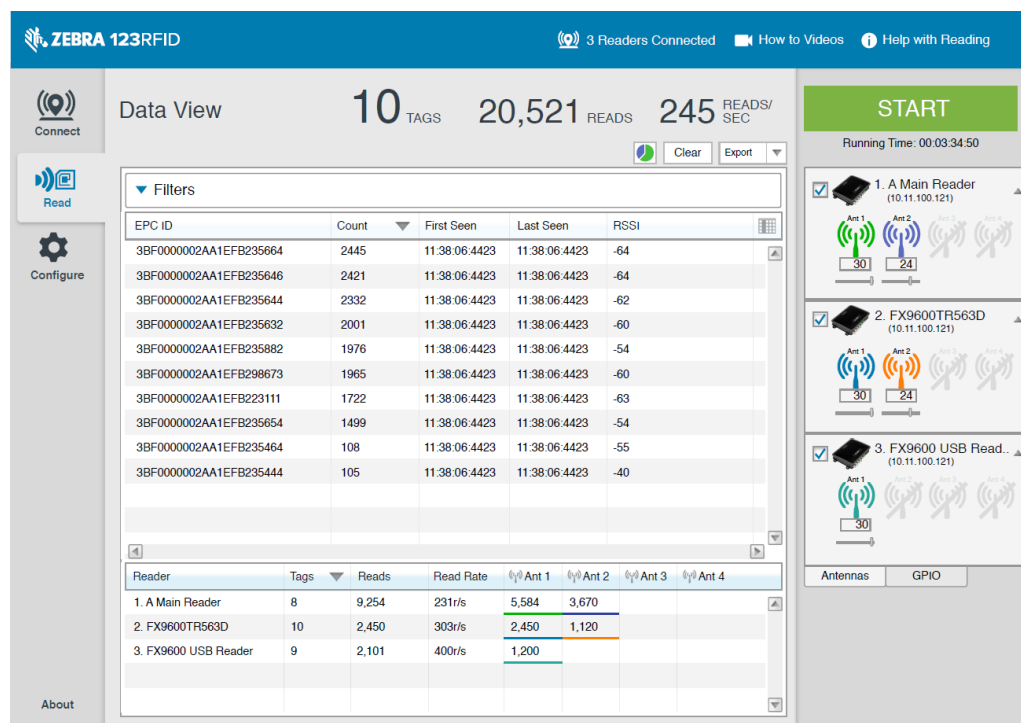
123RFID Desktop

Introduction

This chapter briefly describes 123RFID Desktop, the Zebra setup tool for fixed RFID readers.

For more information on 123RFID Desktop, go to www.zebra.com/123rfid.

Figure 20 123RFID Desktop Reader Screen



Features

123RFID Desktop is a software tool that simplifies reader setup.

Intuitive enough for first time users, 123RFID Desktop finds and connects to a reader with three simple clicks.

- Optimize the reader and its antenna settings using the easy-to-use configuration wizard. Settings are saved in a configuration file or can be printed as a report.
- Analyze tag data using filters, such as EPC or RSSI, and check system performance by looking at charts.

Through 123RFID Desktop a user can accomplish the following.

- Find, connect reader, and start reading tags with three simple mouse clicks.
- Streamline the optimization process using the intuitive configuration wizard
 - Save optimized settings to a file for later use.
 - Load an already saved configuration file to the connected reader.
 - Print a report of optimized settings.
- Analyze tag data using filtering tools
 - Use the Asset Tag List file to filter by known tags.
 - Filter by EPC or RSSI values.
- Check reader performance using charts
 - Charts that represent tag read counts by antennas.
 - Check RSSI signal on individual tags during an inventory.
- Program the GPIO accessory, for example to have a photo-eye sensor activate an inventory session.
- Built-in screen by screen help and How-To-Videos link to guide users through the tool.

For more information go to www.zebra.com/123rfid.

Communication with 123RFID Desktop

Connect a reader to a Windows PC over the local WiFi network or by USB cable.

123RFID Desktop Requirements

- Host computer running Windows 7 or Windows 10.
- A fixed reader.

Administrator Console

Introduction

This chapter describes the FX Series web-based **Reader Administrator Console** functions and procedures, and detailed information about FX Connect. 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.

TCP Port # 8001 is used for communication between the web console and reader. Access to this port is needed for the following web pages to function correctly.

- Advanced Antenna Configuration
- ReadTags
- Services
- Serial Port Communication
- FXConnect
- License Manager
- User Application
- Profiles
- File based firmware upload
- Syslog Export

Reader Administrator Console Selections

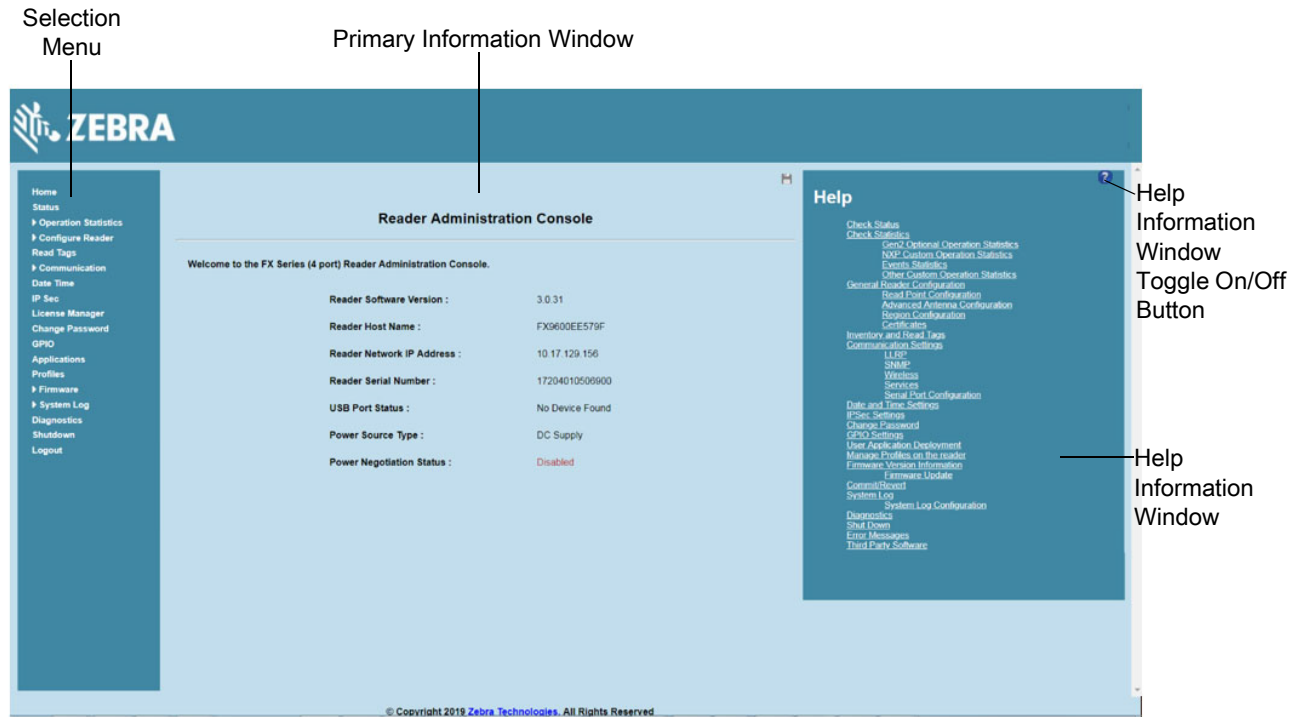
- **Selection Menu** - Selects the function for the primary information window.
- **Primary Information Window** - Provides the primary function information.
- **USB Port Status** - Provides details on the USB device connected to the USB host port. Hover the mouse pointer over the blue link, available 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



NOTE: It is recommended to clear the browser cache to ensure that the web pages pick up the latest frame content and functionality.

Figure 21 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 101](#).

Resetting the Reader

To reset the reader, press and hold the reset button for not more than 2 seconds. See [Figure 8 on page 19](#) for the reset button location. The reader reboots but retains the user ID and password. See [System Start-up/Boot LED Sequence on page 34](#).



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

Auto Discovery

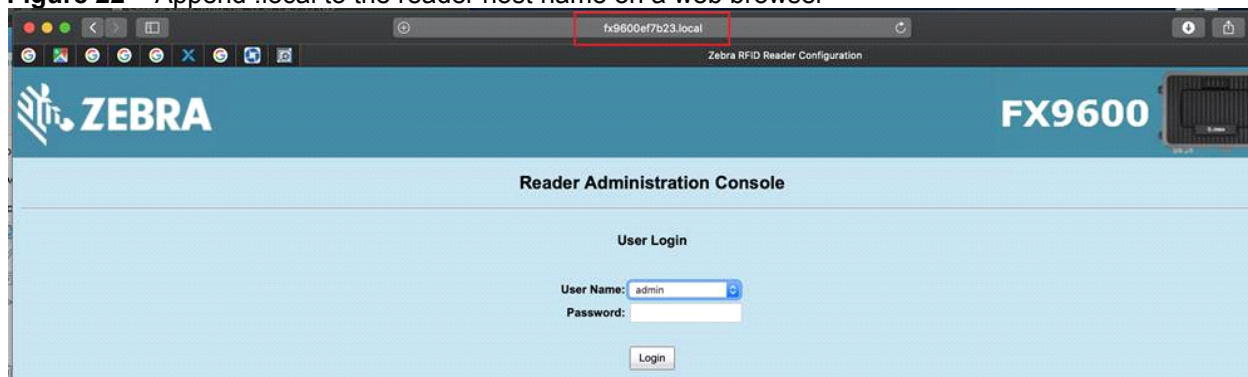
The FX7500 and FX9600 readers supports WS-Discovery and Bonjour (zero-configuration networking methods) to discovery readers in a subnet. The reader implements WS-Discovery conforming to RFID Reader Management Profile (RDMP) specification in ISO 24791-3. RDMP is based on an extension for Device Profile 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 host names. Because this feature is based on WS-Discovery, the readers can also be discovered in Windows Vista and Windows 7 computers by selecting the **Network** icon in a file browser.

Users of Linux, Windows and MAC OS PCs can discover FX Series readers in the subnet using Apple's Bonjour protocol.

- Windows users must download Bonjour Print Services first from https://support.apple.com/downloads/bonjour_for_windows.
- Linux users must install Avahi Service Discover from <https://www.avahi.org>.
- MAC OS has Bonjour support built in.

To discover FX Series readers, append **.local** to the reader host name (i.e. **FX75007F721E.local**) on a browser as shown in Figure 22.

Figure 22 Append .local to the reader host name on a web browser



In Windows and MAC OS, reader services can be discovered by using the command line as follows:

```
dns-sd -B _llrp._tcp
Browsing for _llrp._tcp
13:54:32.809 ...STARTING...
Timestamp      A/R    Flags   if     Domain Service Type      Instance Name
13:54:33.055    Add    2       4      local.  _llrp._tcp.             FX75007F721E
```

The command for HTTP service discovery is `dns-sd -B _http._tcp`.

Linux users can use the following command to list the services:

```
avahi-browse -a -k -d local
+ eth0 IPv6 FX75007F721E      _ssh._tcp      local
+ eth0 IPv4 FX75007F721E      _ssh._tcp      local
+ eth0 IPv6 FX75007F721E      _sftp-ssh._tcp local
+ eth0 IPv4 FX75007F721E      _sftp-ssh._tcp local
+ eth0 IPv6 FX75007F721E      _http._tcp     local
```

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 39](#).

Connect to the reader in one of two ways:

1. [Connecting via Host Name on page 42](#).
2. [Connecting via IP Address on page 42](#). (To obtain the IP address, see [Obtaining the IP Address via Command Prompt on page 41](#))

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 42](#).
3. Statically assigning an IP. See [Static IP Configuration on page 147](#).

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 42](#).



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 21 on page 39](#). 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 42](#).

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 43](#) 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 43](#) 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 select **Login**.

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

Setting the Region

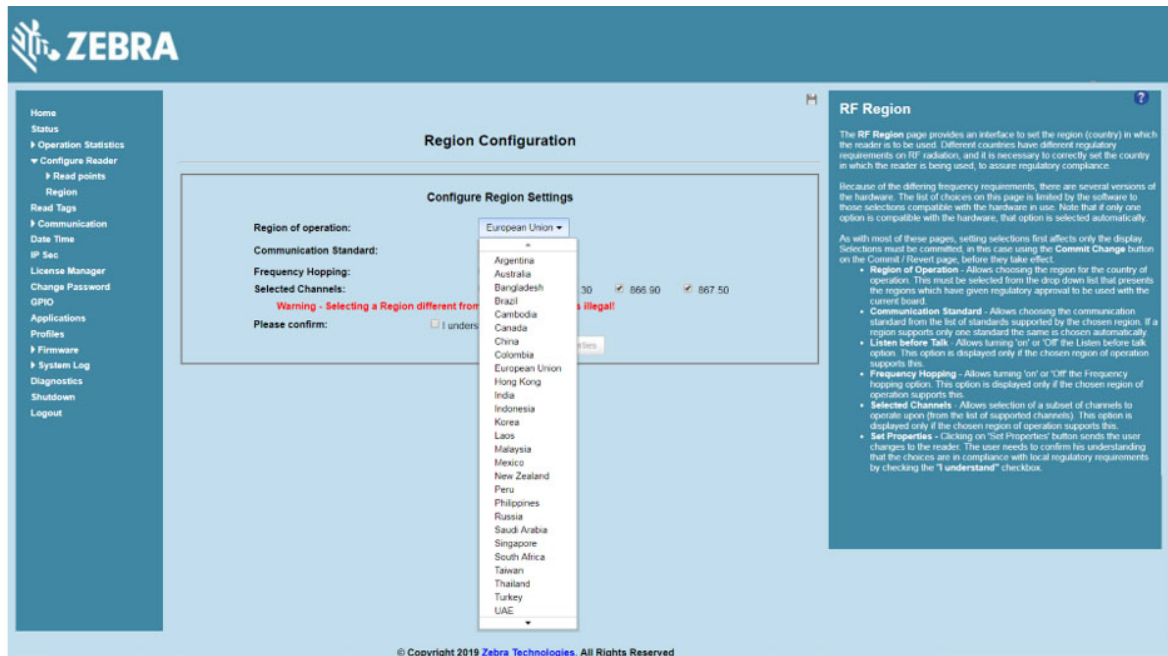
For global reader configurations, set the region of operation. **Setting the unit to a different region is illegal.**



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

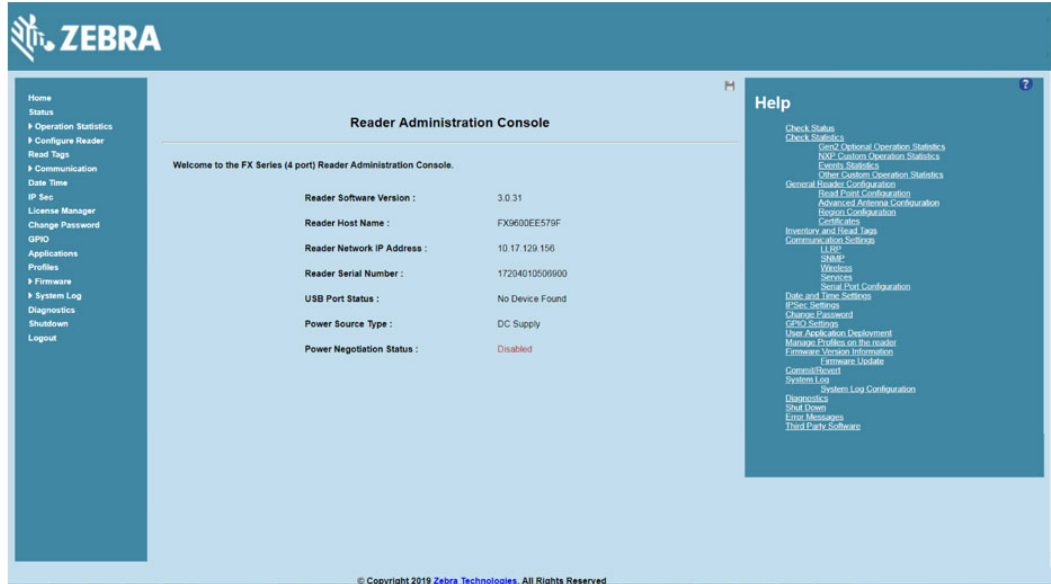


2. Select the **Communication Standard** if applicable.
3. Select **Frequency Hopping**, if applicable.
4. Select the appropriate channel(s), if applicable.
5. Select the **I understand** check box.
6. Select **Set Properties** to complete the region selection. The **Operation Successful** window appears. Commit step is no longer required to save configuration. See [Commit/Discard Functionality Changes on page 103](#).

Reader Administrator Console

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

Figure 26 Reader Administrator Console Main Window



Administrator Console Option Selections

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

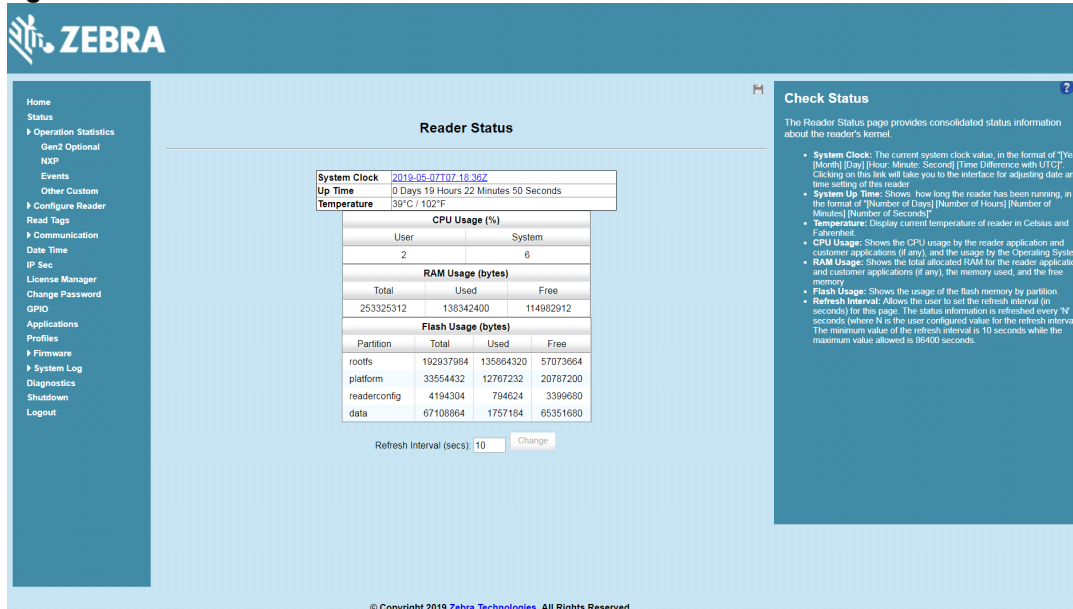
- **Status** - see [Status on page 47](#)
- **Operation Statistics** - see [Reader Statistics on page 48](#)
 - **Gen2 Optional** - see [Reader Gen2 Optional Operation Statistics on page 49](#)
 - **NXP** - see [NXP Custom Command Operation Statistics on page 50](#)
 - **Events** - see [Event Statistics on page 51](#)
 - **Other Custom** - see [Other Custom Command Operation Statistics on page 52](#)
- **Configure Reader** - see [Configure Reader on page 53](#)
 - **Read Points** - see [Read Points on page 54](#)
 - **Advanced** - see [Read Points - Advanced on page 55](#)
 - **Region** - see [Configure Region on page 56](#)
 - **Certificates** - see [Certificates on page 57](#)
- **Read Tags** - see [Read Tags on page 67](#)
- **Communication** - see [Communication Settings on page 68](#)
 - **LLRP** - see [Configure LLRP Settings on page 71](#)
 - **SNMP** - see [SNMP Settings on page 72](#)
 - **Wireless** - see [Wireless Settings on page 73](#)
 - **Services** - see [Network Services Settings on page 74](#)
- **Date/Time** - see [System Time Management on page 96](#)

- **IP Sec** - see [IPV6 IP Sec on page 97](#)
- **Change Password** - see [Change Password on page 98](#)
- **GPIO** - see [GPIO on page 99](#)
- **Applications** - see [Applications on page 100](#)
- **Profiles** - see [Reader Profiles on page 101](#)
- **Firmware** - see [Firmware Version/Update on page 102](#)
 - **Update** - see [Firmware Update on page 103](#)
- **System Log** - see [System Log on page 107](#)
 - **Configure** - see [Configure System Log on page 108](#)
- **Diagnostics** - see [Reader Diagnostics on page 109](#)
- **Shutdown** - see [Shutdown on page 110](#)
- **Logout** - select **Logout** to immediately log out of the **Administrator Console**.

Status

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

Figure 27 Reader Status Window



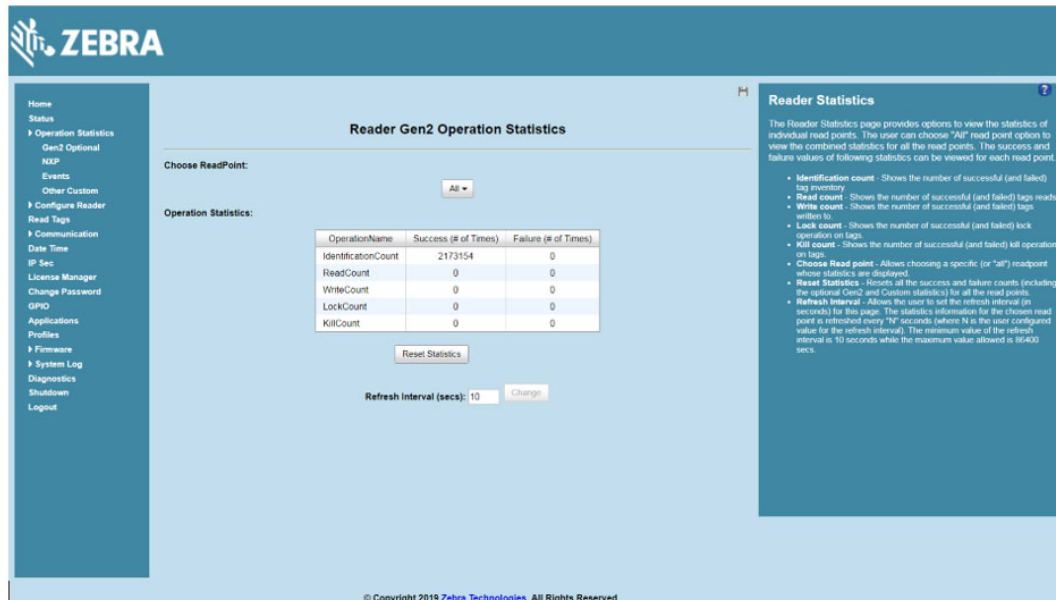
The **Reader Status** window provides consolidated reader status information:

- **System Clock:** The current system clock value, in the format of [Year] [Month] [Day] [Hour: Minute: Second] [Time Difference with UTC]. Select 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].
- **Temperature** - Displays current temperature of the reader in Celsius and Fahrenheit.
- **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 28 Reader Operation Statistics Window

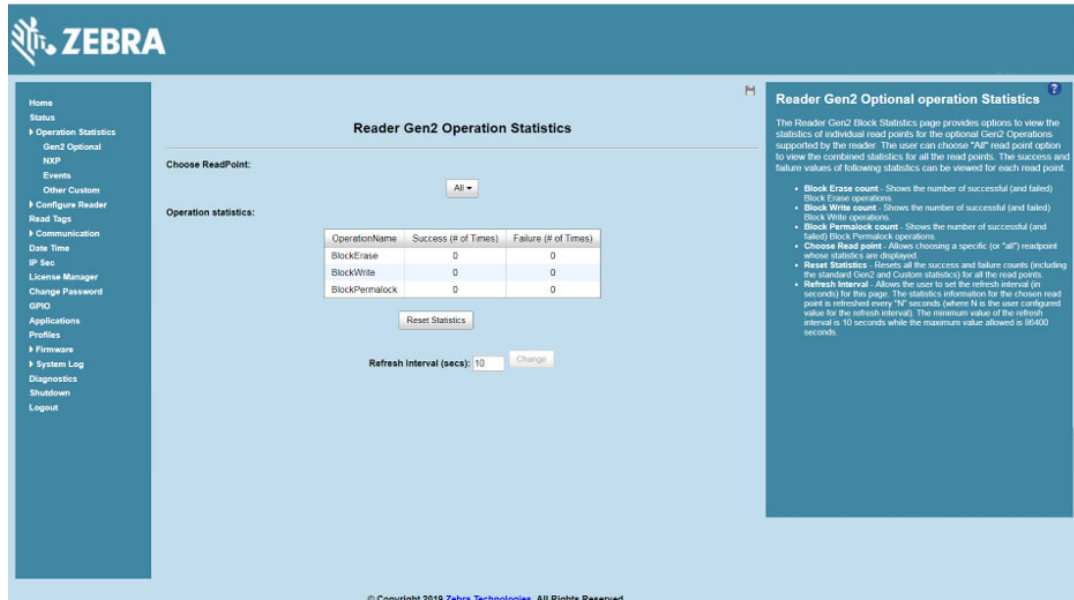


- **Choose ReadPoint** - Select a specific read point or select **All** from the drop-down list to display the statistics.
- **IdentificationCount** - Displays the number of successful (and failed) tag inventories.
- **ReadCount** - Displays the number of successful (and failed) tag reads.
- **WriteCount** - 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 select **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 29 Reader Gen2 Operation Statistics Window

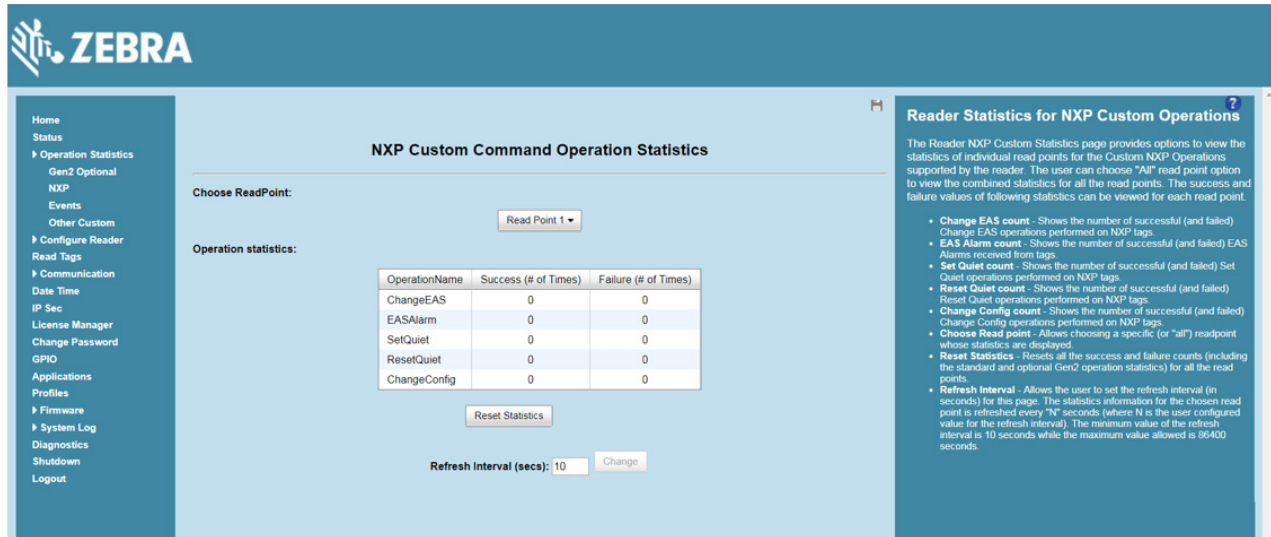


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **BlockErase** - Displays the number of successful (and failed) block erase operations.
- **BlockWrite** - Displays the number 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 select **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 30 NXP Custom Command Operation Statistics Window

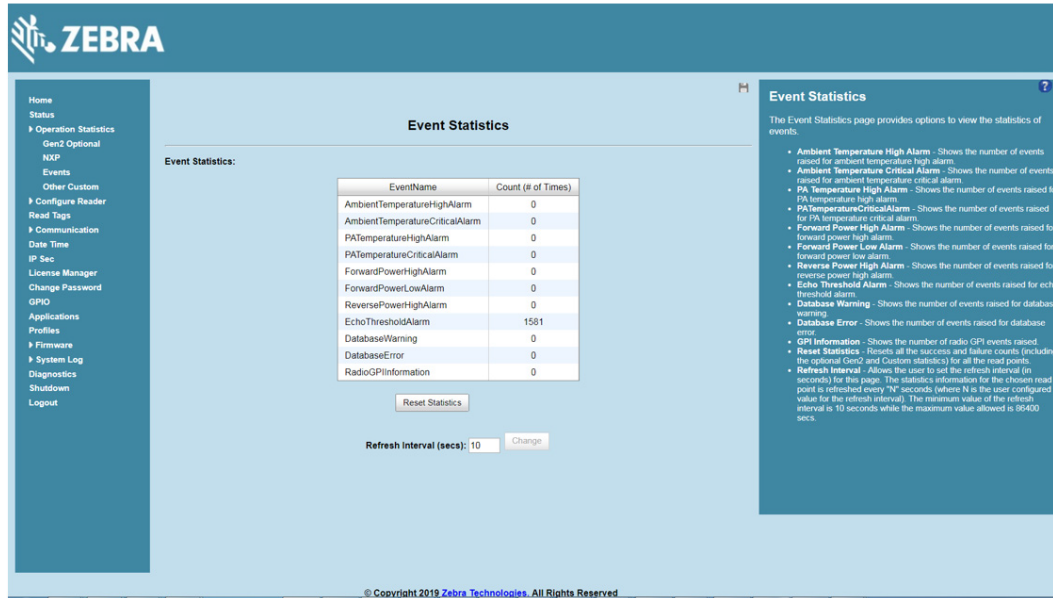


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **ChangeEAS** - Displays the number of successful (and failed) change EAS operations performed on NXP tags.
- **EASAlarm** - 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 select **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 31 Event Statistics Window

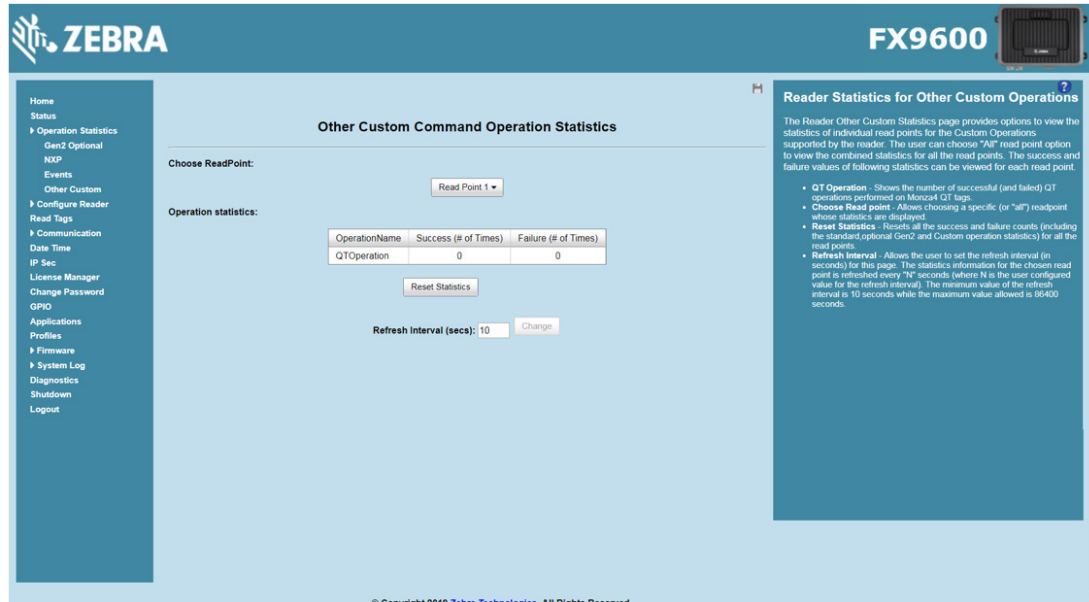


- **AmbientTemperatureHighAlarm** - Displays the number of events raised for ambient temperature high alarm.
- **AmbientTemperatureCriticalAlarm** - Displays the number of events raised for ambient temperature critical alarm.
- **PATemperatureHighAlarm** - Displays the number of events raised for PA 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 select **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 32 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 select **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 33 Reader Parameters

Reader Parameters

Zebra - FX9600 17204010506900

Configure Reader

Name: FX9600EE579F FX9600
 Description: FX9600EE579F 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
 Allow Guest User: ☒

Set Properties

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 PoE enabled Cisco switch and attempts to negotiate extra power so as to obtain power in the range of PoE+.
- Allow Guest User** - Option to control whether Guest User is allowed or not to access the reader using the web console. When Checked (default) this option is enabled and Guest user is allowed to login to view the reader settings. Disabling this option prevents Guest user login to the reader's web console.
- Set Properties** - Clicking on 'Set Properties' button sends the user changes to the reader.

© Copyright 2019 Zebra Technologies. All Rights Reserved

- **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.

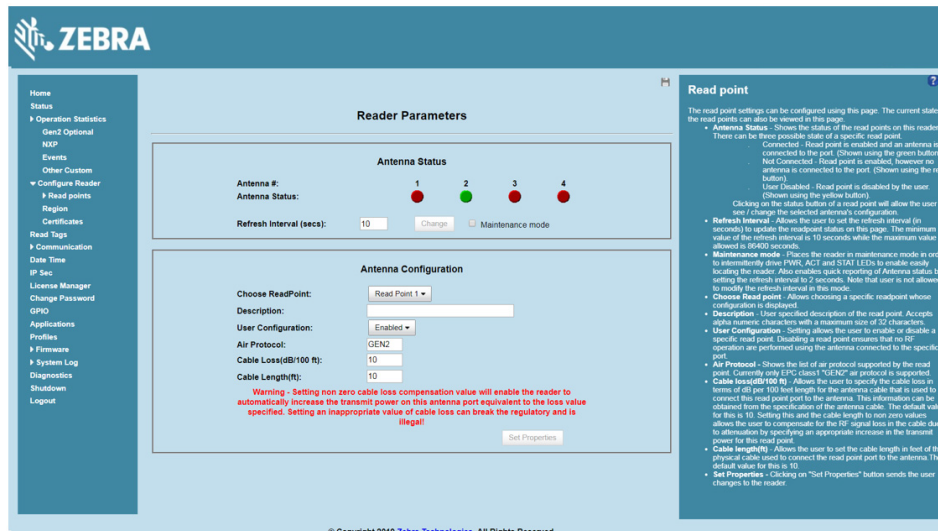
After power negotiation is enabled, and committed, it takes approximately 2 to 5 minutes to reach the PoE+ level. This is the time taken for LLDP packet exchange between the reader and the switch for power negotiation.

These settings only affect the display.

Read Points

Select **Configure Reader > Read points** in the selection menu to configure the read point settings and view the current read points state.

Figure 34 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.

Select 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 select **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.

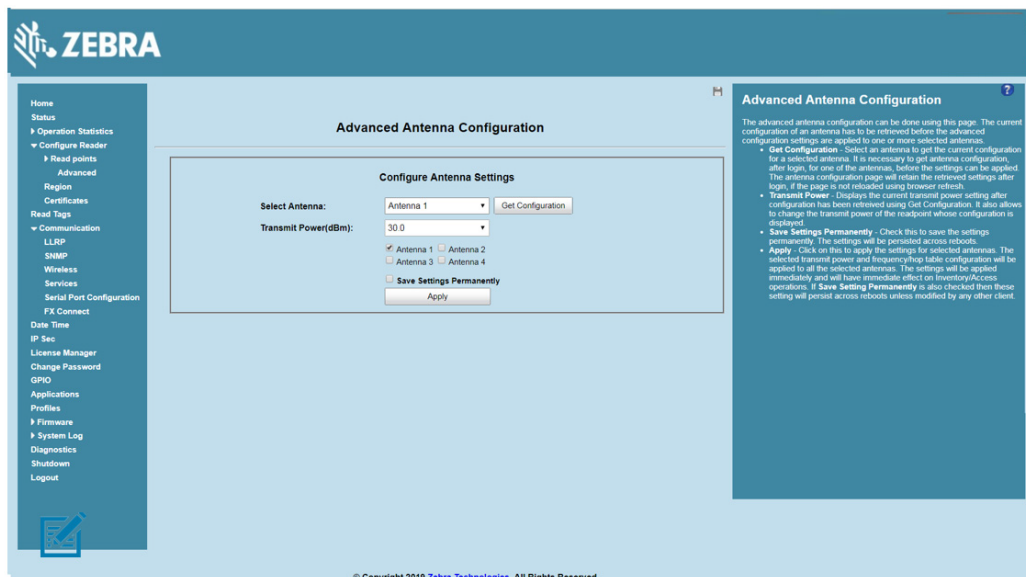
Antenna Configuration

- **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 **10**. 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. The default cable length is 10 feet.
- **Set Properties** - Select **Set Properties** to apply the changes.

Read Points - Advanced

Select **Configure Reader > Read points > Advanced** 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 35 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.
- **Save Settings Permanently** - Check this to save the settings permanently and persist them across reboots.
- **Apply** - Select 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

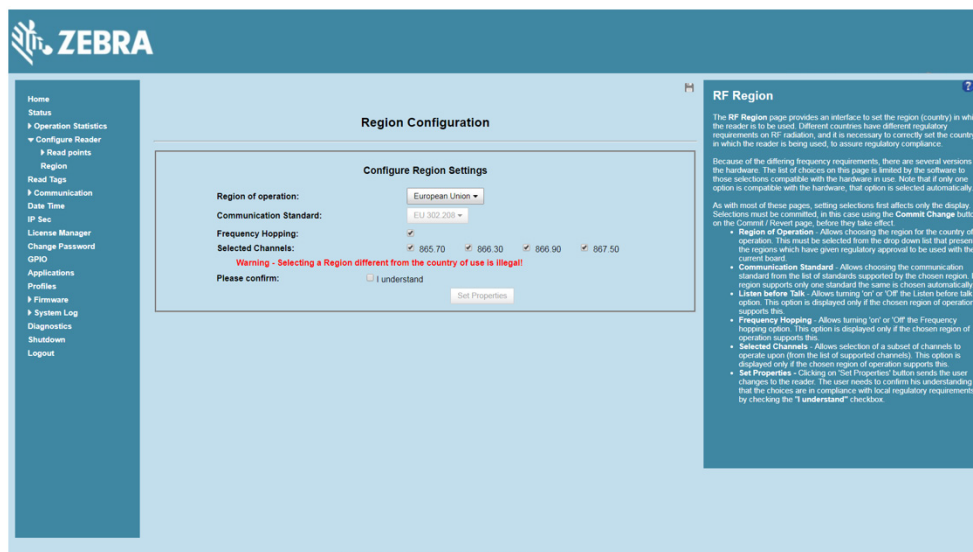
Different countries have different RF regulatory requirements. To assure regulatory compliance, select **Region** to set the reader for specific regulatory requirements in the country of reader operation using the **Configure Region Settings** window.



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 36 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** - Select to apply the changes.

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 74](#).
- File Transfer Service (FTPS - explicit SSL/TLS over FTP). See [Network Services Settings on page 74](#).
- 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 71](#).



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 71](#) 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.

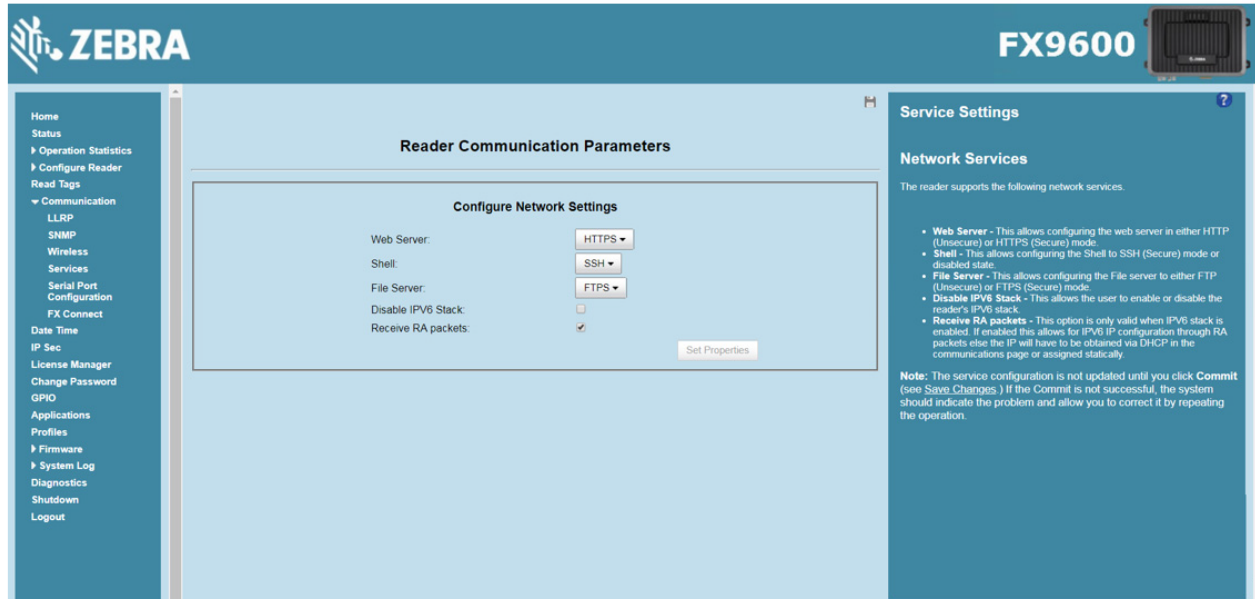
Certificate Configuration

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 37 Setting HTTPS Mode

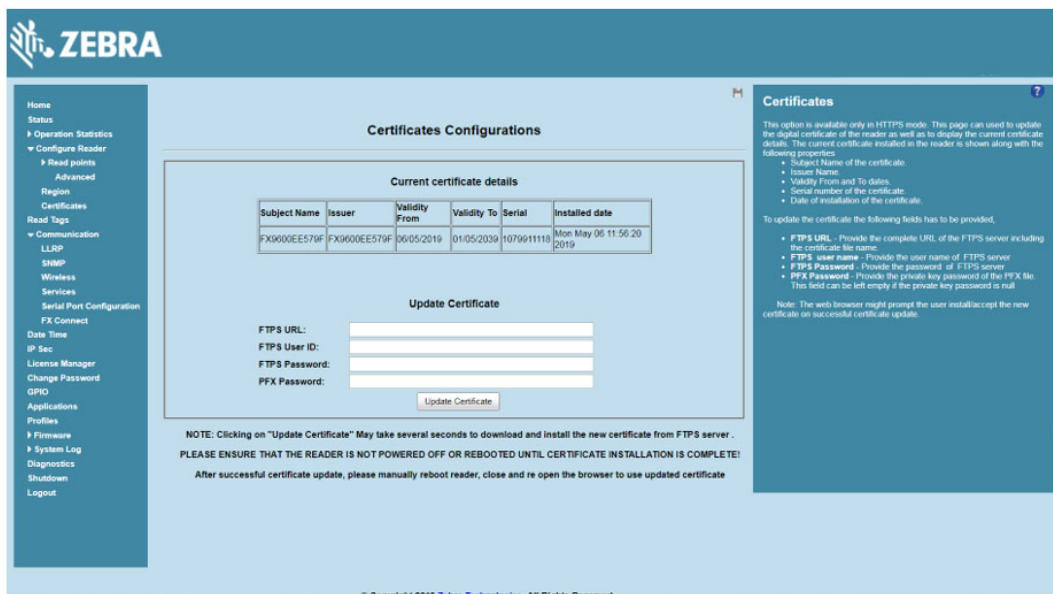


NOTE: The user cannot change Web Server mode if Inventory is in progress.



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

Figure 38 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 71](#).
- 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 74](#). 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.

(continued on next page)

#

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
```

```
(continued on next page)
```

```
#
```

```
#
```

```
# 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=$WORKSPACE_DIR/caconfig.cnf
openssl ca -in tempreq.pem -out client crt.pem -extensions ssl_client_server -passin
pass:$CA_KEY_PASSWORD -batch

rm -f tempreq.pem

echo 'Client key, certificate creation and signing completed. Use files client_key.pem and client crt.pem'
```

Script Usage

The following section illustrates how to use the previous scripts 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 **samplerereader.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: This page is not supported when LLRP is configured in secure mode.

Figure 39 Read Tags Window

Reader Operation

36 tags 27828 reads 00:01:04:150
456 reads/sec [Start] [Stop] [Clear]

EPC Id	Tag Seen Count	RSSI	Antenna Id	Seen Time
E2801160600002066680E3F9	788	-64	2	07/05/2019 06:23:17:371
E2801160600002066680FD09	1197	-53	2	07/05/2019 06:23:17:407
30380000033F10000000045	1126	-55	2	07/05/2019 06:23:17:406
8DF000000000000000007E02DC	1182	-53	2	07/05/2019 06:23:17:389
AD29190043ED8D835F00009E	1173	-55	2	07/05/2019 06:23:17:404
8DF000000000000000007E02D0	883	-62	2	07/05/2019 06:23:17:408
8DF000000000000000007E02CD	1122	-57	2	07/05/2019 06:23:17:383
8DF000000000000000007E02FB	581	-59	2	07/05/2019 06:23:17:397
E28011606000020E8A5AF45A	1067	-48	2	07/05/2019 06:23:17:391
E280A89400005017791EC74	1230	-53	2	07/05/2019 06:23:17:378
8DF000000000000000007E02D6	1190	-52	2	07/05/2019 06:23:17:398
E28011606000020E8A5AF44A	1137	-58	2	07/05/2019 06:23:17:382
E2806894000040177920874	350	-58	2	07/05/2019 06:23:16:204
30380000033F100000000001	1209	-52	2	07/05/2019 06:23:17:402
30380000033F100000000031	947	-58	2	07/05/2019 06:23:17:407
8DF000000000000000007E02FF	1170	-53	2	07/05/2019 06:23:17:376
8DF000000000000000007E02ED	1115	-59	2	07/05/2019 06:23:17:385
E280689400004017791EC74	748	-64	2	07/05/2019 06:23:17:394
E28011606000020E8A5AC81A	703	-64	2	07/05/2019 06:23:16:254
AD29190043EF4587D00000C1	1162	-55	2	07/05/2019 06:23:17:399

Read Tags

This page facilitates the user to perform inventory on the connected antennas and view the list of tags that are inventoried. The Read tags page also shows the read rate (in tags/second) along with the unique and total tags that have been read by the reader. The tag list and the statistics are updated once in every second.

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

Note: 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 for the tag.
- Antenna Id** - Antenna Id on which the tag has been seen last.
- Seen time** - UTC time at which the tag was first seen in time of day format.

© Copyright 2019 Zebra Technologies. All Rights Reserved

- **Start** - Select 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** - Stops the ongoing inventory operation.
- **Clear** - Clears the current tag list.

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

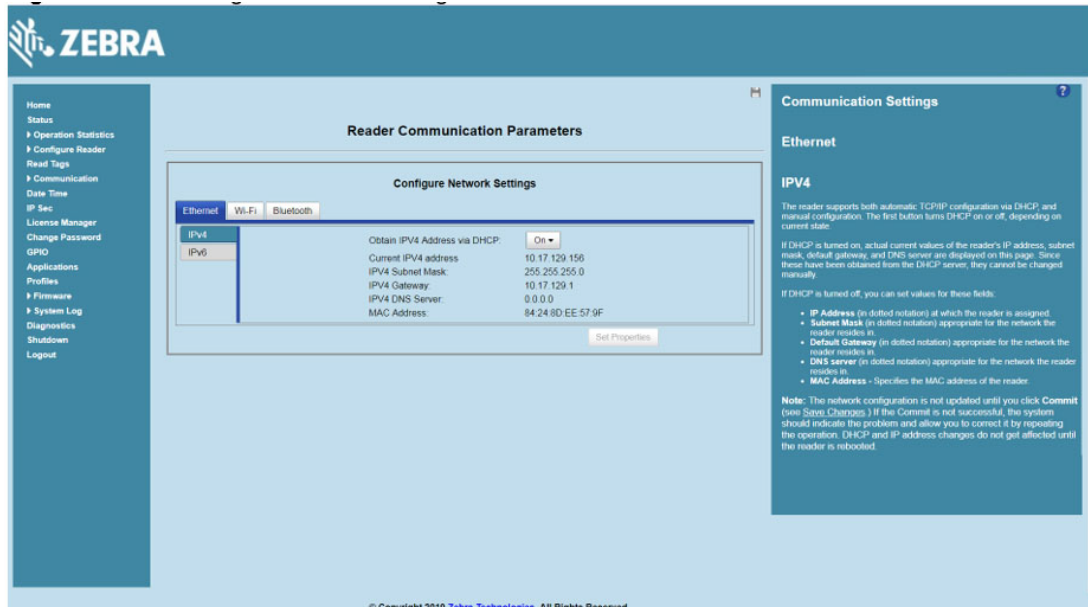
- **EPC Id** - Unique tag EPC ID.
- **Tag Seen Count** - Number of times the tag is identified on the specific antenna.
- **RSSI** - Received Signal Strength Indication.
- **Antenna Id** - Antenna ID on which the tag is seen.
- **Seen Time** - UTC time (in microseconds) showing when the tag was first 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 40 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 select **Set Properties** to update the network configuration. If saving changes is not successful, the system indicates the problem and allows correcting it by repeating the operation. DHCP and IP address updates do not 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.



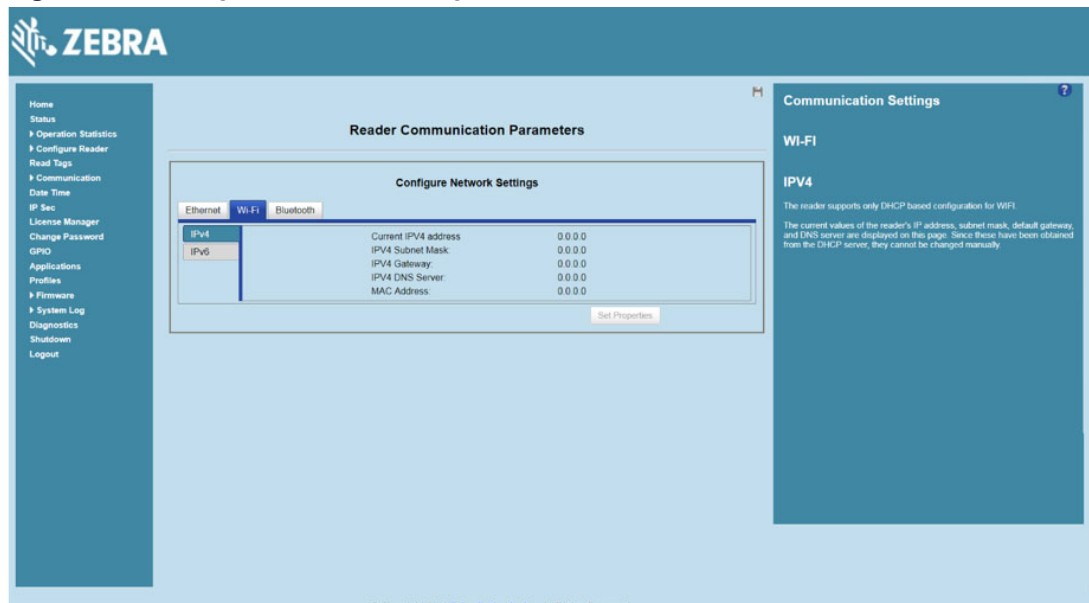
NOTE: You must select **Set Properties** to update the network configuration. If saving changes is not successful, the system indicates the problem and allows correcting it by repeating the operation. DHCP and IP address updates do apply until the reader is rebooted.



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 41 Configure Network Settings - Wi-Fi Tab



IPV4

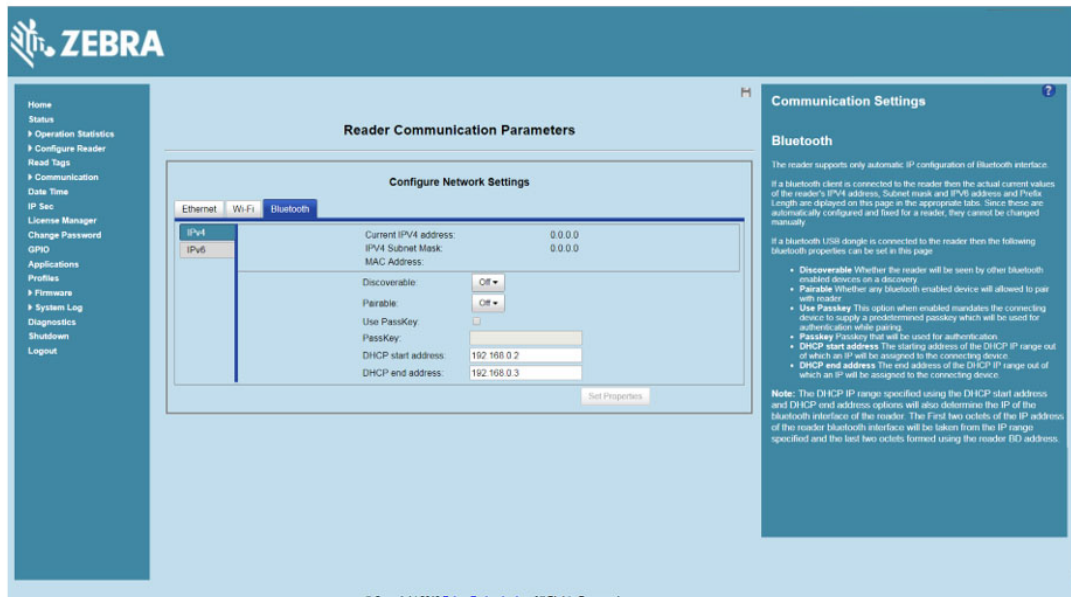
The reader supports only DHCP-based configuration for Wi-Fi. This window displays the current values of the reader's IP address, subnet mask, default gateway, and DNS server. Since these are obtained from the DHCP server, they cannot be changed manually.

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 42 Configure Network Settings - Bluetooth Tab



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

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

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

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

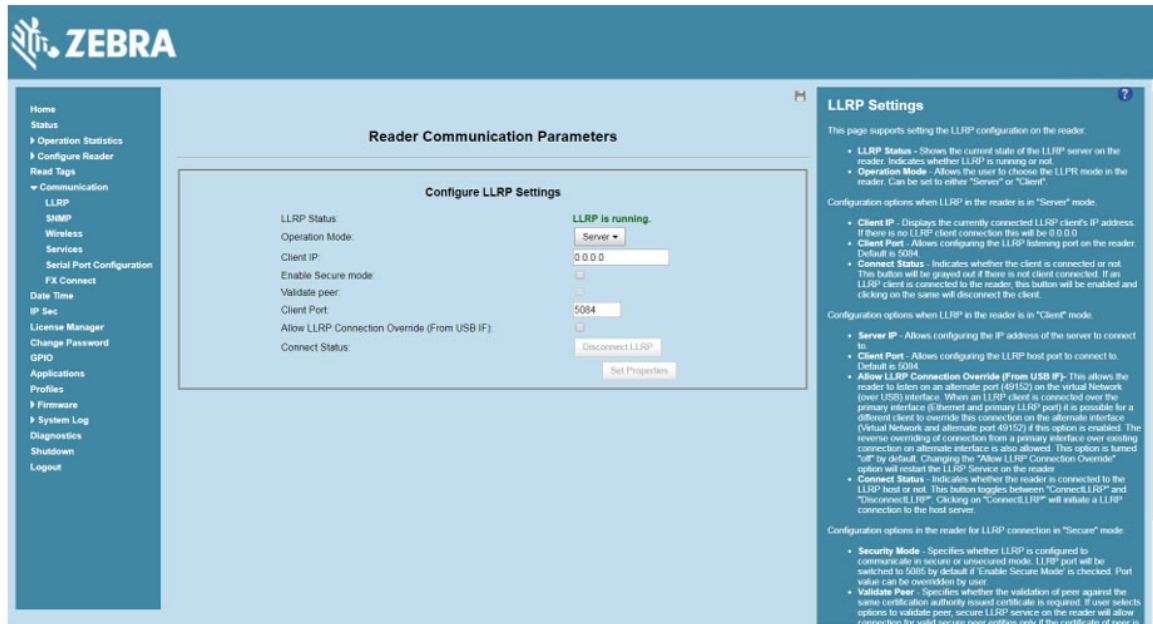


NOTE: The DHCP IP range specified using the DHCP start address and DHCP end address options also determine the IP of the Bluetooth interface of the reader. The first two octets of the IP address of the reader Bluetooth interface are taken from the IP range specified and the last two octets use the reader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

Configure LLRP Settings

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

Figure 43 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; select 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**. Selecting **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 44 Configure SNMP Settings Window

Reader Communication Parameters

Configure SNMP Settings

Send SNMP Trap To:

SNMP Community String:

SNMP Version:

Send Server Heartbeat: ☒

[Set Properties](#)

SNMP Settings

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

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

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

© Copyright 2019 Zebra Technologies. All Rights Reserved

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 selecting **Set Properties**. 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 45 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 were tested:

Table 7 Supported Wi-Fi Dongles

Dongle Model	Zebra FX7500	Zebra FX9600
TP-Link: AC 1200 Realtek RTL8812AU	Yes	Yes
ASUS: USB-AC56 Realtek RTL8812AU	Yes	Yes
Alfa Network Realtek RTL8812AU	Yes	Yes
Alfa AWUS036H	Yes	Yes
CCrane Versa Wifi USB Adapter II	Yes	Yes

The Wireless Settings window offers the following options:

- **Get Details** - Select to get details of the connected network, including the ESSID, signal strength, and connection status.
- **Disconnect** - Select to disconnect from a connected network.
- **Scan and Choose Network** - Scan the available networks. Selecting this lists the ESSID in the drop-down menu. If the ESSID is hidden (not broadcast), 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.

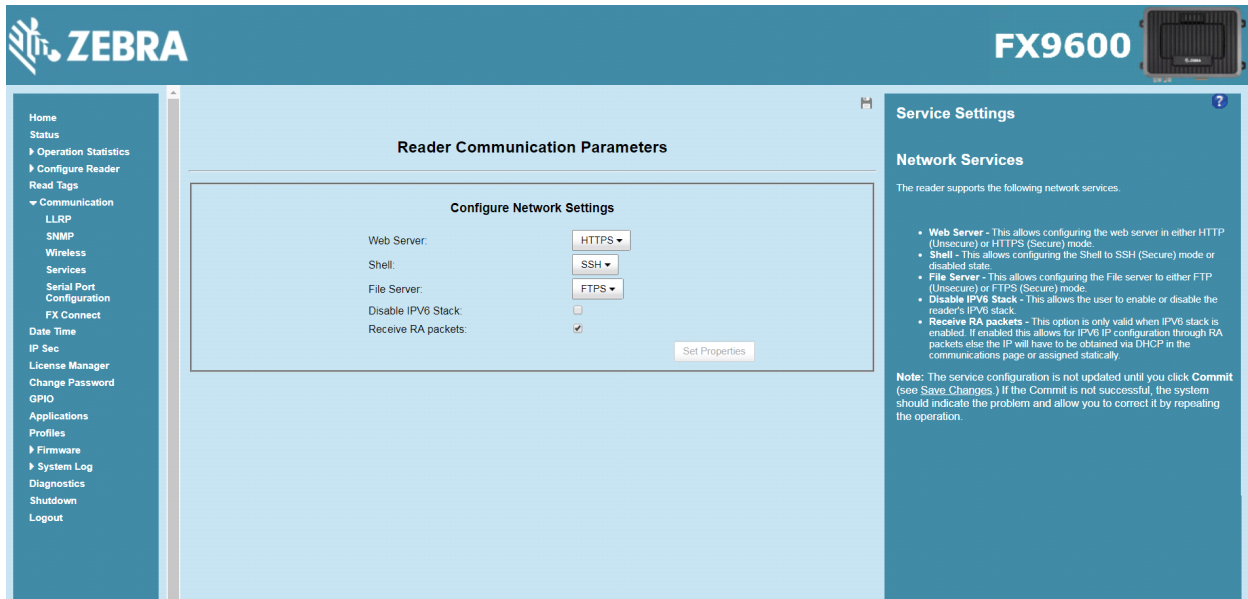
Network Services Settings

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

Figure 46 Configure Network Service Settings Window



NOTE: The user cannot change Web Server mode if Inventory is in progress.



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 select **Set Properties** to update the service configuration. If saving changes is not successful, the system indicates the problem and allows correcting it by repeating the operation.

FX9600 Serial Port Configuration

The external FX9600 serial port can be configured to one of the following three modes:

- Debug port (default).
- Push data - Allows a connected client to receive tag data when inventory starts from the web console.
- Free port - Supports user app to use serial port.

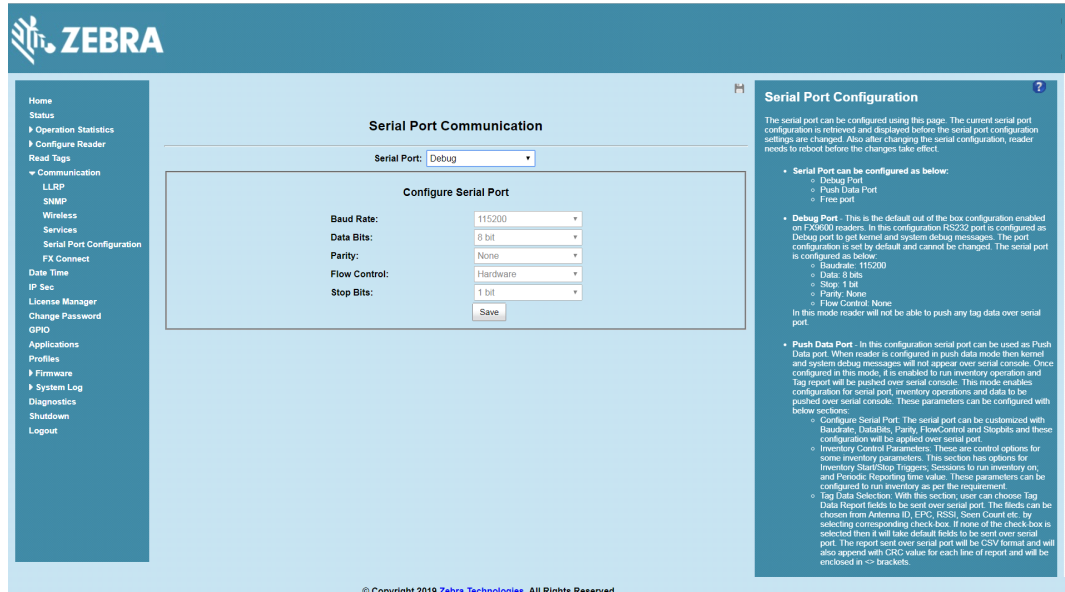


NOTE: Changing the serial port mode requires restart of the reader to take effect.

Debug Port

In this mode, the FX9600 serial console is used as the debug kernel port. The kernel uses this port for debug messages.

Figure 47 Serial Port Communication - Debug



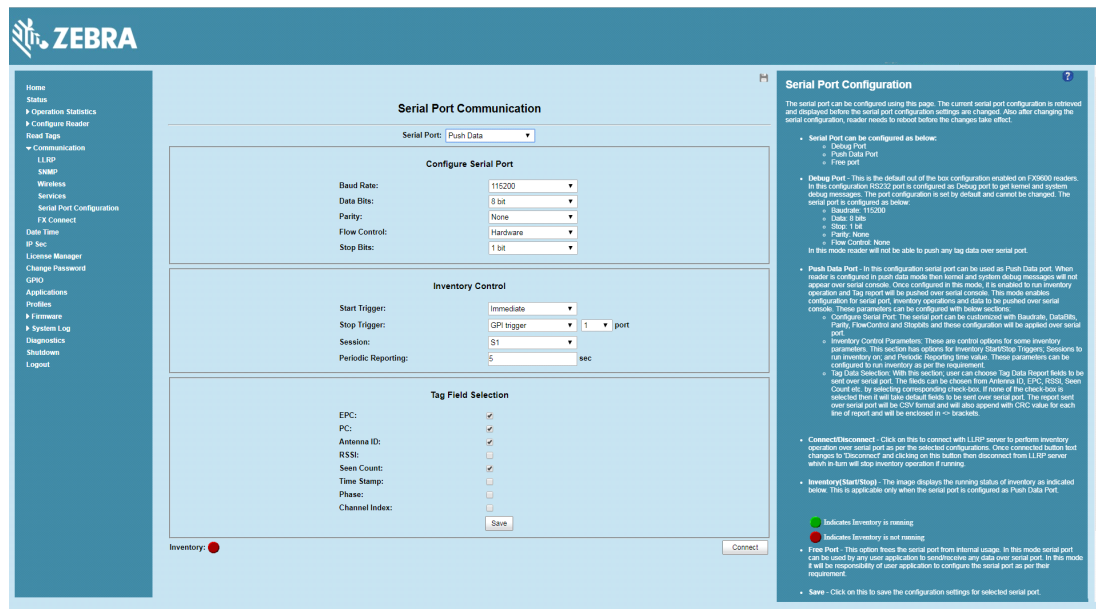
Push Data Port

In this mode, the FX9600 serial port is used as a push data port. The inventory operation can be performed and a TAG report is sent over the serial port with selected settings.

To configure Push Data:

1. Configure serial port communication fields (Figure 48).

Figure 48 Serial Port Communication - Push Data Configuration



2. Select **Save** to save the current settings.
3. Reboot the reader to implement the changes.

4. Select **Inventory (start/stop)**: to start inventory and report tags over the serial port.
5. The tag data can be seen on the serial port as shown in [Figure 50](#).

Figure 49 Serial Port Communication - Inventory Started

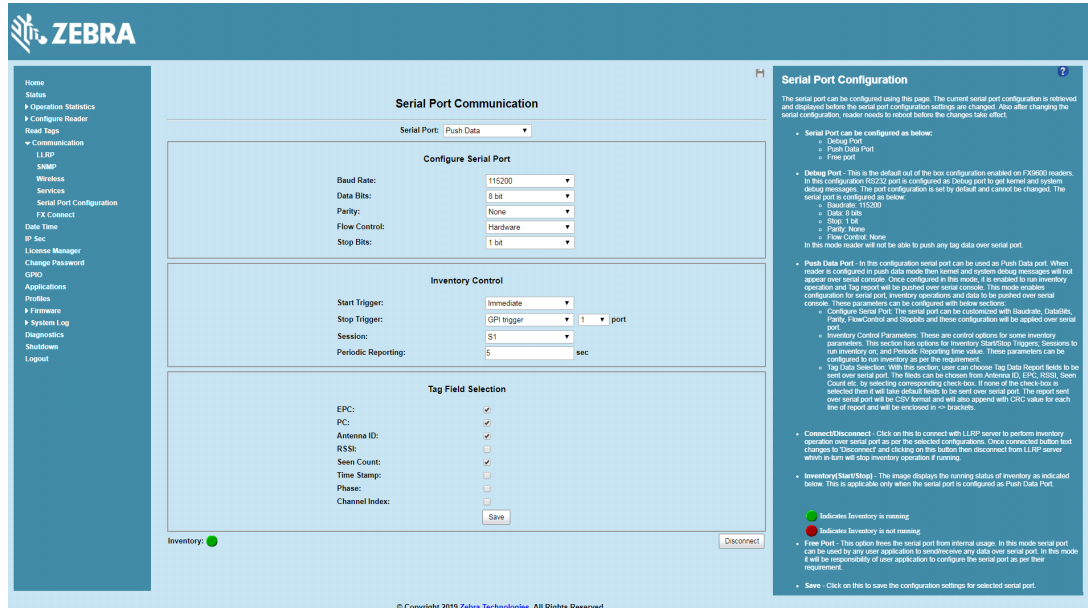
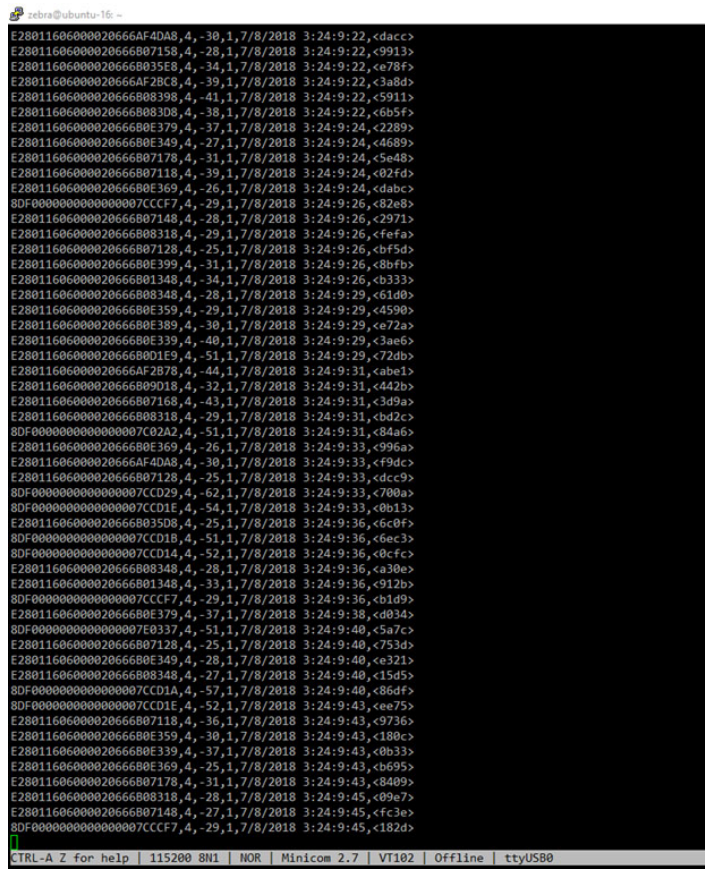


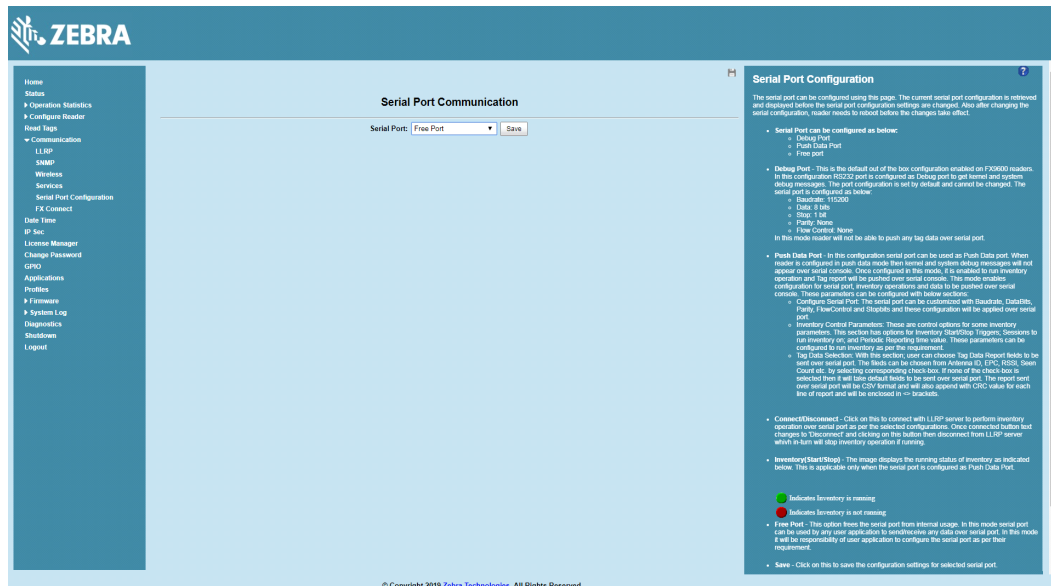
Figure 50 Tag Data



Free Port

When configured in Free Port mode, the serial port in the FX9600 can be used for the user application to perform any user specific operation. In this mode user app can perform open/read/write operation as per their requirement.

Figure 51 Serial Port Communication - Free Port



FX Connect

FX Connect is licensed feature which enables users to easily collect data from FX series RFID readers, namely the FX7500 and FX9600. Data is pushed to the host PC in keystrokes via USB-HID or HTTP POST in a hassle free manner. No knowledge of APIs or application development is required to receive RFID data from the reader. See [FX Connect Licensing Management on page 89](#) for detailed licensing information.

Using FX Connect

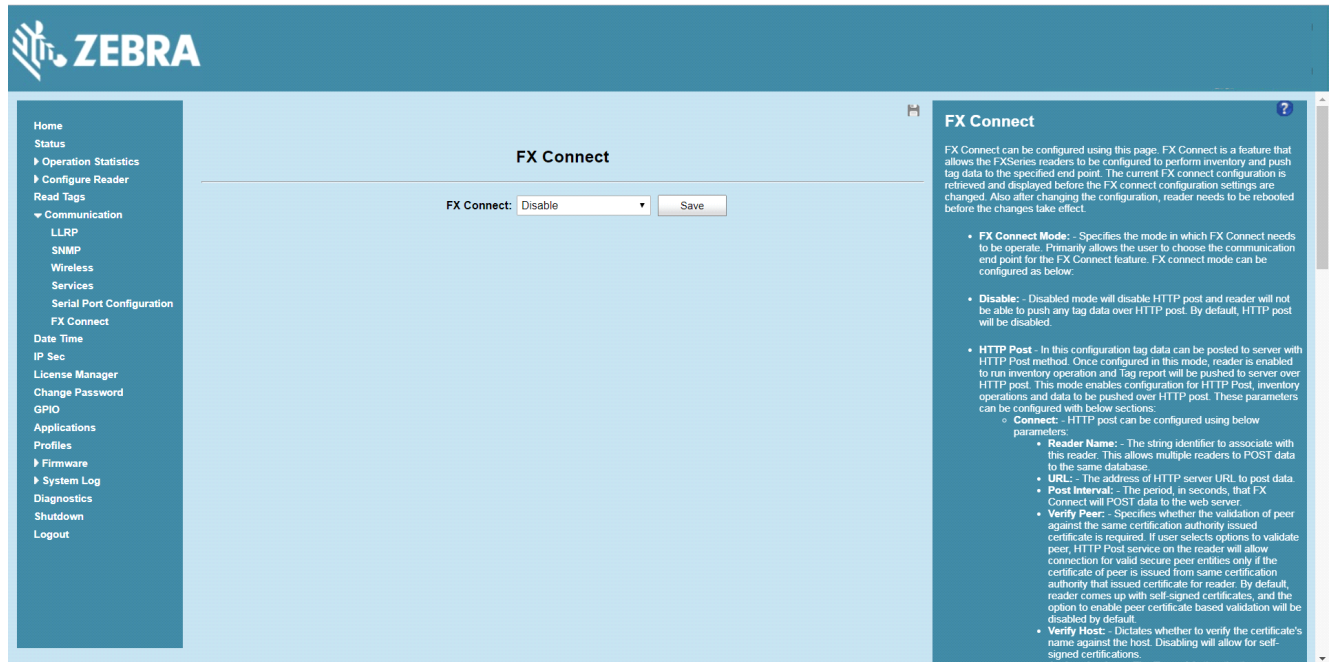
1. Open a web browser to connect to the FX reader using the host name or IP address. (See [Quick Start](#) for startup instructions.)
2. Click **Communication > FX Connect**.



NOTE If valid license is not already installed the screen displays information to obtain a valid license. See [FX Connect Licensing Management](#) for details on how to enable FX Connect via a license.

If a valid license is installed in the reader it displays in the FX Connect console.

Figure 52 FX Connect



3. Select the FX Connect drop-down arrow to select an option.
 - a. **Disable** - By default, FX Connect is disabled.
 - b. **HTTP Post** - This option enables the reader to push Inventory Tag data in JSON format to the web server using the HTTP Post method. The web server could be running on local network or in the cloud. See [Table 8](#) for field information.
 - c. **Keyboard Emulation** - This option allows the user to push data over USB HID. It enables the reader to send RFID data to an application running on a PC host connected to the reader via the USB client port. Any application that is able to receive keyboard input is able to receive RFID data from the reader in this mode because the reader uses Keyboard HID emulation to send data to the host PC. If this option is selected and the user starts the Inventory, tag data is shown in a key-value pair in the selected text editor (Notepad, MS Excel, etc.). See [Table 9](#) for field information.
 - d. **TCP/IP Socket** - As in HTTP POST, this option also enables the reader to push Inventory Tag data in JSON format to the defined TCP/IP socket port. Any client socket application connected to the reader with defined port can receive Tag data. See [Table 10](#) for field information.
 - e. **USB Flash Drive** - When this option is selected, the tag data is written to a specific file in attached USB Flash drive in Key Value Pair format. This mode does not have any specific configurable parameters. See [Table 11](#) for field information.
4. Select **Save** to save the configuration settings for FX Connect.

Figure 53 HTTP Post Screen

Table 8 HTTP Post Configurable Options

Option	Description
HTTP Post - This section displays the configurable parameters for the HTTP Post server.	
Reader Name	Reader name is the text string that appears in Post data to identify the reader. See Configuring the HTTP Post Server on page 84 for details on how to set up a web server to test this feature.
URL	HTTP Post Server URL to receive post data.
Post Interval	The period, in seconds, that FX Connect posts data to the web server.
Verify Peer	Specifies whether or not peer validation is required. If the user selects the option to validate peer, the HTTP Post service on the reader allows connection for valid secure peer entities only if the certificate of peer is issued from the same certification authority that issued the certificate for the reader. By default, the reader issues self-signed certificates and the option to enable peer certificate-based validation is disabled.
Verify Host	Dictates whether to verify the certificate's name against the host. Disabling this option allows self-signed certifications.

Table 8 HTTP Post Configurable Options (Continued)

Option	Description
Authentication	<p>The type of authentication to use when connecting to the remote or proxy server.</p> <ul style="list-style-type: none"> • NONE: No authentication at all. • BASIC: Sends the user name and password in plain text over the network. • DIGEST: RFC 2617. • DIGEST_IE: RFC 2617 but uses a special quirk that IE is known to have used before version 7 and some servers require. • NTLM: Challenge-response and hash concept similar to Digest. • ANY: FX Connect will automatically select the one it finds most secure. • ANYSAFE: FX Connect will automatically select any except BASIC that it finds most secure.
User Name	The user name required to connect to the Remote or Proxy Server for certain Authentication types.
Password	The password required to connect to the Remote or Proxy Server for certain Authentication types.
HTTP Post Proxy: If reader is behind a proxy server then select the check box. This provides proxy server related parameters. For more details on how to configure a proxy server see Configuring the HTTP Post Server on page 84 .	
Proxy Server	The Proxy Server Name or IP address with which to connect (when specified).
Proxy Port	The Proxy Server port to connect to.
Proxy Tunnel	Dictates whether to tunnel through HTTP Proxy.
Authentication	Same as HTTP Post Authentication but for the proxy server.
User Name	Same as HTTP Post User Name but for the proxy server.
Password	Same as HTTP Post Password but for the Proxy server.
Configure Antenna Power	Enables the user to select the transmit power level for particular antennas. By default, the maximum transmit power value supported by the reader is selected for each antenna.

Table 8 HTTP Post Configurable Options (Continued)

Option	Description
Inventory Control Parameters	These are control options for some inventory parameters. This section has options for inventory start/stop triggers, sessions on which to run inventory, and periodic reporting time value. These parameters can be configured to run inventory as per the requirement. If the user selects the auto start option, inventory starts automatically upon boot up (based on the start trigger chosen).
Tag Field Selection	<p>In this section the user can choose Tag Data Report fields to be sent over HTTP Post to the server. The available fields to be chosen are: EPC, PC, Antenna ID, RSSI, Seen Count, etc. by selecting the corresponding check-box. By default, EPC, PC, Antenna ID, and Seen Count are selected.</p> <p>Note: Heart Beat, when enabled, causes the reader to periodically send a heartbeat string (******) to indicate that the reader is up and running.</p> <p>The Period for heartbeat, in seconds, indicates the minimum delay before sending out another heartbeat string.</p>

Figure 54 Keyboard Emulation Screen

Table 9 Keyboard Emulation Configurable Options

Option	Description
Output Format - This section displays the configurable parameters for the Keyboard Emulation.	
Format	Output format that is supported with USB HID is key-value pairs.
Delimiter	The delimiter options are comma, space, and tab.
Line Ending	The line ending options are None, CRLF, and LF.
Timestamp Format	The timestamp format options are UTC and Unix.

Table 9 Keyboard Emulation Configurable Options (Continued)

Option	Description
Data Prefix/Data Suffix	The user can add a prefix and suffix for each tag read record. Note: Data Prefix and Data Suffix should be in a character sequence only.
Configure Antenna Power	See Table 8 .
Inventory Control Parameters	See Table 8 .
Tag Field Selection	See Table 8 (defaults vary).

Figure 55 TCP/IP Socket Screen

[illegible]

Table 10 TCP/IP Socket Configurable Options

Option	Description
TCP/IP - This section displays the configurable parameters for the TCP/IP.	
Port Number	This is the TCP/IP port number for which FX Connect will open TCP/IP socket and push data when inventory is running.
Configure Antenna Power	See Table 8 .
Inventory Control Parameters	See Table 8 .
Tag Field Selection	See Table 8 (defaults vary).

Figure 56 USB Flash Drive

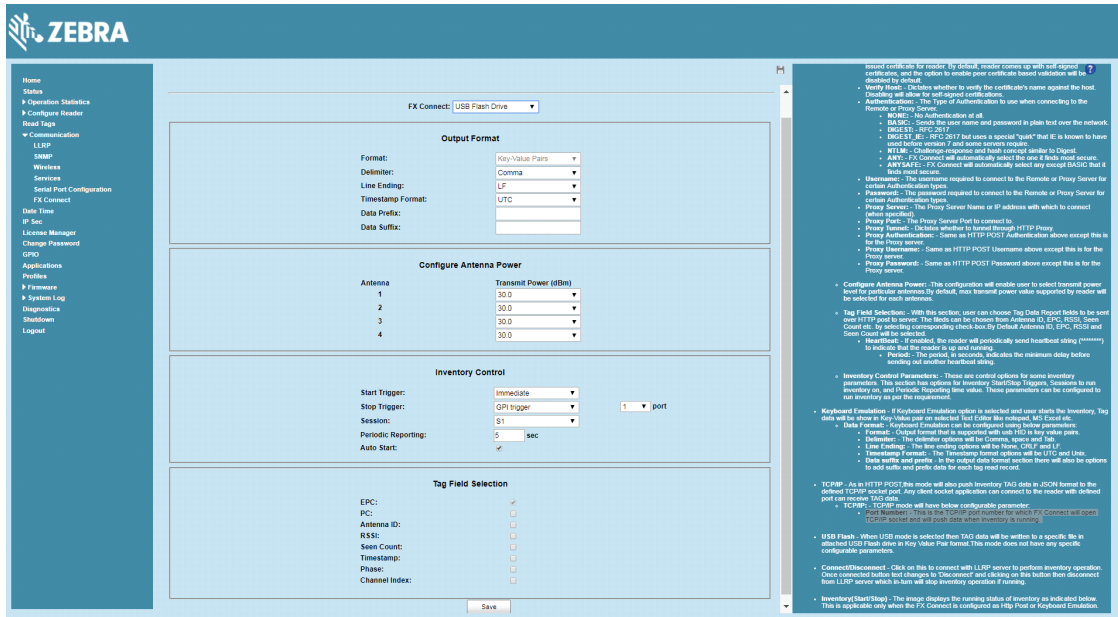


Table 11 USB Flash Drive Configurable Options

Option	Description
Output Format - This section displays the configurable parameters for the USB Flash Drive.	
Format	Output format that is supported with USB HID is key-value pairs.
Delimiter	The delimiter options are comma, space, and tab.
Line Ending	The line ending options are None, CRLF, and LF.
Timestamp Format	The timestamp format options are UTC and Unix.
Data Prefix/Data Suffix	The user can add a prefix and suffix for each tag read record. Note: Data Prefix and Data Suffix should be in a character sequence only.
Configure Antenna Power	See Table 8 .
Inventory Control Parameters	See Table 8 .
Tag Field Selection	See Table 8 (defaults vary).

Running Inventory on FX Connect

To start the inventory operation for the selected and configured Output mode:

- From the FX Connect console select **Connect**.



NOTE Connect appears after the user selects **Save**.

Connect changes to **Disconnect** after a successful connection.

- The inventory operation begins per the configured Start Trigger setting.

- b. The inventory status light turns green when inventory beings running. and turns red when inventory stops per the configured Stop Trigger setting.

2. Select **Disconnect**.



NOTE **Disconnect** changes to **Connect** after a successful disconnection.

Configuring the HTTP Post Server



NOTE You must have a valid license to run FX Connect. See [FX Connect Licensing Management](#) for more information.

To run the HTTP Server to receive tag data from FX Connect:

1. Open a web browser to connect to the FX reader using the host name or IP address. (See [Quick Start](#) for startup instructions.)
2. Click **Communication > FX Connect**.
3. Install Python 2.7 or greater.
4. Go to: github.com/BurntSushi/nfldb/wiki/Python-&-pip-Windows-installation and follow the instructions to install Python pip.

5. Open command shell.
6. Install Flask by typing the command: pip install Flask.
7. Save the text below as postServer.py.

```
from flask import Flask, request
app = Flask(__name__)

@app.route('/', methods = ['POST', 'GET'])

def message():
    if request.method == 'POST':
        app.logger.info('Request received.')
        app.logger.info('Url: %s', request.url)
        app.logger.info('Data: %s', (request.data).decode('utf-8'))
        app.logger.info('Is JSON: %s', request.is_json)
    else:
        app.logger.info('GET request received.')
    return 'OK\n'

if __name__ == '__main__':
    app.run(host='0.0.0.0', port='5001', debug=1)
```



NOTE The script above runs HTTP server on port 5001; if needed, change the port number.

- To see the HTTP Post output, run the command: `python postServer.py`. This starts the HTTP server which receives tag data from FX Connect and displays the data in the command shell.

Configuring the HTTP Proxy Server

To setup the Squid proxy server on an Ubuntu machine:

- Install, start, and enable Squid on the Ubuntu machine using the following commands.


```
$ sudo apt -y install squid
$ sudo systemctl start squid
$ sudo systemctl enable squid
```
- The `squid.conf` file is created in: `/etc/squid/squid.conf`.
- The default configuration file contains some configuration directives that affect the behavior of the Squid and they need to be configured.

Open the `squid.conf` file and update the lines below, the **Save**.

- Under **rule allowing access from your local networks** add the following statements:


```
acl all src 0.0.0.0/0.0.0.0
acl Safe_ports port 8081          # custom http
```
 - Under **access permission configuration** add the following statement:


```
http_access allow all
```
 - Under **access permission configuration** comment the statements:


```
#http_access allow localhost manager
#http_access deny manager
```
- Restart the Squid with the following command:


```
sudo systemctl restart squid
```
 - The proxy server is now ready.
 - Check the logs in the proxy server with the following command:


```
sudo tail -f /var/log/squid/access.log
```

Configuring USB HID



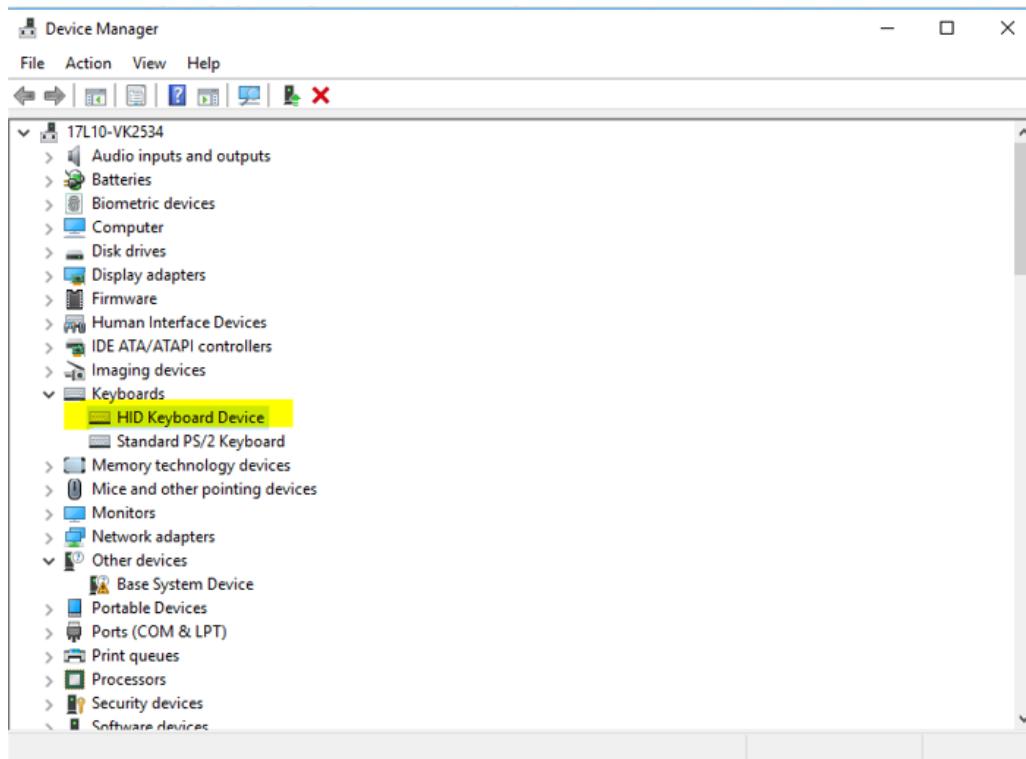
NOTE It is recommended to use two host PCs - one to control the reader through the web console and another to receive tag data.



NOTE Setting the reader to use USB HID disables RNDIS on the USB client port. The reader cannot be accessed using the RNDIS IP Address (169.254.10.1) in this scenario.

To run FX Connect in Keyboard Emulation:

- Open the reader web console to FX Connect (see [Figure 52 on page 78](#)).
- Connect the reader to the host machine through the USB Client port (same as RNDIS). See [Figure 7 on page 19](#) and [Figure 10 on page 21](#) for FX7500 and FX9600 USB Client ports. Windows automatically detects the reader as an HID device when inventory starts on FX Connect and enables the driver.

Figure 57 HID Device Detection

3. Open any text editor application or MS Excel to receive push data from the reader. Use your cursor to select the spot where you want to print the tag data.
4. Start the inventory by selecting **Connect** on reader web console.

Tag data is printed in the application at the selected spot.

Configuring the TCP/IP Socket

To use TCP/IP socket for receiving Tag data

1. Run TCP/IP socket client application on host machine. TCP/IP client will read the Tag data sent by the reader. Below is the simple TCP/IP client application which need to be compiled on host machine:

```
/*
 * tcpclient.c - A simple TCP client
 * usage: tcpclient <server IP> <port>
 */
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <sys/ioctl.h>
```

```

#define BUFSIZE 10240

/*
 * error - wrapper for perror
 */
void error(char *msg) {
    perror(msg);
    exit(0);
}

int main(int argc, char **argv) {
    int sockfd, portno, n;
    struct sockaddr_in serveraddr;
    struct hostent *server;
    char *hostname;
    char buf[BUFSIZE];
    struct timeval t;
    int iMode = 1;
    int count = 0;

    /* check command line arguments */
    if (argc != 3) {
        fprintf(stderr, "usage: %s <server IP> <port>\n", argv[0]);
        exit(0);
    }
    hostname = argv[1];
    portno = atoi(argv[2]);

    /* socket: create the socket */
    sockfd = socket(AF_INET, SOCK_STREAM, 0);
    if (sockfd < 0)
        error("ERROR opening socket");

    /* gethostbyname: get the server's DNS entry */
    server = gethostbyname(hostname);
    if (server == NULL) {
        fprintf(stderr, "ERROR, no such host as %s\n", hostname);
        exit(0);
    }

    printf("Connecting to server : %s\n", server->h_name);

```

```

/* build the server's Internet address */
bzero((char *) &serveraddr, sizeof(serveraddr));
serveraddr.sin_family = AF_INET;
bcopy((char *)server->h_addr,
      (char *)&serveraddr.sin_addr.s_addr, server->h_length);
serveraddr.sin_port = htons(portno);

/* connect: create a connection with the server */
if (connect(sockfd, (struct sockaddr *)&serveraddr, sizeof(serveraddr)) < 0){
    printf("Connecting to socket failed.\n");
    close(sockfd);
    error("ERROR connecting");
    return -1;
}
while(1){
    /* print the server's reply */
    bzero(buf, BUFSIZE);
    n = read(sockfd, buf, BUFSIZE);
    if (n < 0){
        error("ERROR reading from socket");
    } else if (n == 0){
        printf("Server Socket closed \n");
        break;
    } else {
        printf("\nMessage: %s", buf);
    }
    //if(count++ > 10)
    //    break;
}
close(sockfd);
return 0;
}

```

2. Once compiled, run this application with reader IP and PORT which is already configured on the reader.
3. After running the application, click on connect button on the reader web console to run inventory under FX Connect.
4. Application will print the received tag data on screen.

Configuring the USB Flash Drive

To get the tag data in USB drive there no configuration is required. The user just need to attach the USB flash drive in reader and click on **Connect** button at FX Connect web console.

The tag data will be pushed to USB flash drive in a file named as current timestamp.

FX Connect Licensing Management

This section explains, in detail, the licensing model and the licensing mechanism used in FX Connect (a feature available for FX7500 and FX9600 RFID readers). The following areas are discussed:

- The three different modes to acquire a license.
- How to return licenses.
- Setup and administration of the license server.

FX Connect Licensing Model

FX Connect features require a valid license installed in the reader. The FX Connect license purchased from Zebra determines the number of FX7500/FX9600 readers that can use FX Connect features. Only those readers that successfully acquired a license from the license server can read tags and output the RFID tag data to the designated output option on the FX Connect web page. There is also an option to acquire evaluation/trial licenses. The following sections explain where and how to procure the license. When you acquire the license, the user receives an Activation ID which is used to activate the license on the readers.

Acquiring Licenses

Trial and permanent licenses can be ordered from the Zebra ordering portal. For urgent trial version orders, contact the FX Series product manager or your local sales representative. An entitlement email is sent when the order is processed.

Types of Licenses

There are two types of FX Connect licenses.

- FX Connect Evaluation License
- FX Connect Perpetual

FX Connect Evaluation License

The evaluation license is a time bound license, based on the procurement type, and can be valid for 30, 60 or 90 days. The license is de-activated when the trial ends. Upon expiration of the trial term, the user is required to purchase a renewal license or switch to a permanent license.

FX Connect Perpetual

FX Connect perpetual is a permanent License and is available for the life of the reader.

Enabling a License

To enable an FX Connect license, acquire the appropriate license type (evaluation or perpetual) and then login to the reader web interface to configure and activate the license.

FX Connect Licensing Mechanism

License Acquisition Modes

FX Connect supports acquiring a license in one of three ways:

- From a Cloud based server (default).
- From a Local License Server (LLS) - see [page 91](#).
- From an off-line device - see [page 93](#).

Acquiring FX Connect License from Cloud Based Server

With this method of license acquisition, the license server is hosted on the cloud and the FX reader contacts the cloud-based license server to acquire licenses. This is the default mode for purchasing FX Connect licenses. It involves minimal setup and configuration.



IMPORTANT With this method, the FX reader(s) must be connected to the Internet to acquire license(s) from the cloud server and start operations.

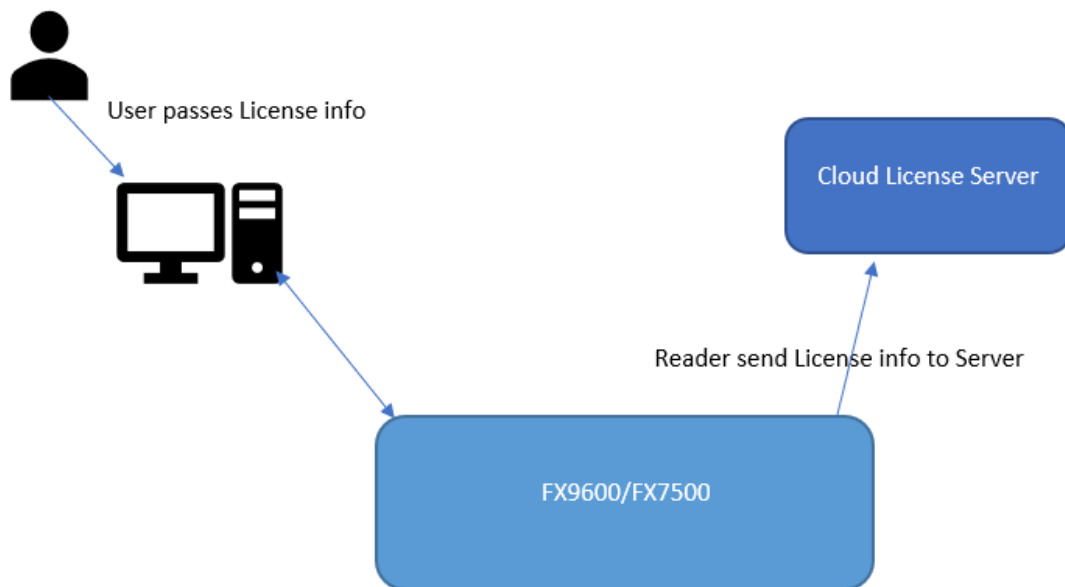
Copy and paste the following address of the cloud license server for FX Connect into a web browser.
zebra-licensing.flexnetoperations.com/flexnet/deviceservices.

The value of the **license_server_url** field must be set to this address.



NOTE To circumvent a firewall while contacting the cloud-based license server, set up a proxy server. To do this, go to:
https://supportcommunity.zebra.com/s/article/ZSL-Licensing-Server-Connectivity?language=en_US.

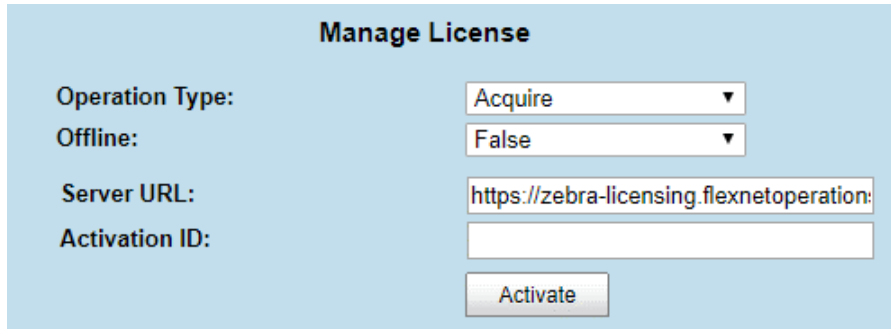
Figure 58 License Acquisition Process From The Cloud



Managing the License

Select the **License Manager UI** page on the reader.

Figure 59 License Manager UI - Acquire License



Manage License

Operation Type:

Offline:

Server URL:

Activation ID:

1. **Operation Type:** Use the drop-down arrow and select Acquire.
2. **Offline:** Use the drop-down arrow and select False.
3. **Server URL:** The cloud server URL (<https://zebra-licensing.flexnetoperations.com/flexnet/deviceservices>) should display. This is the default and should not be modified.
4. **Activation ID:** Enter the appropriate ID. (This is the ID received when you purchase the license.)
5. Select **Activate**.

Upon successful completion of the operation, license information displays on the **Available License** page (see [Available License Tab on page 94](#)).

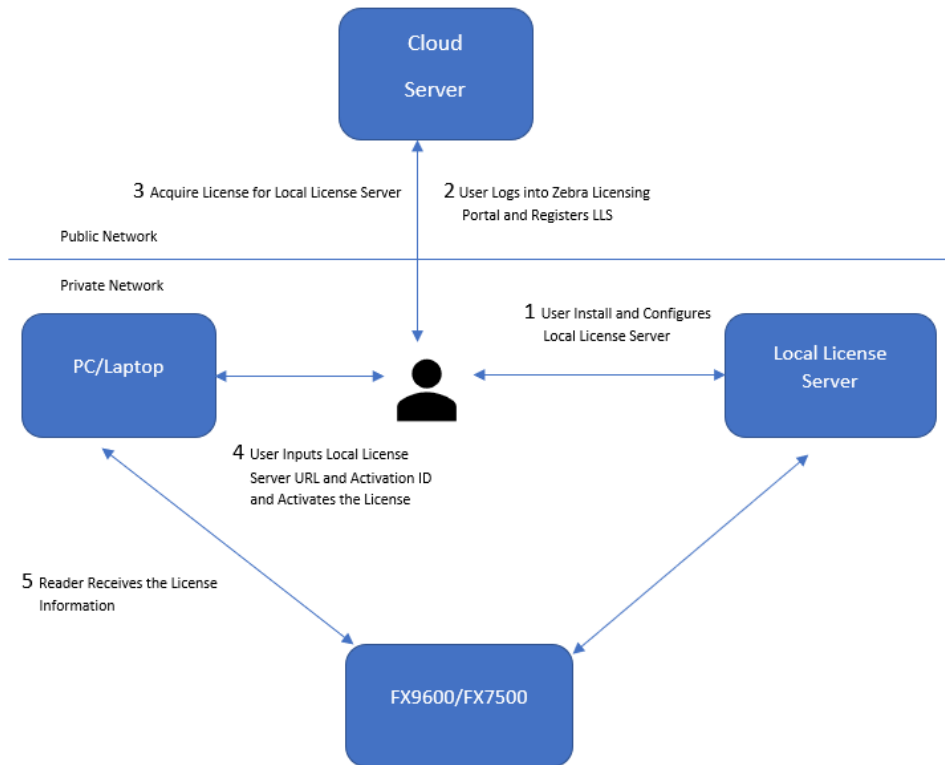
Acquiring FX Connect License from Local License Server (LLS)

With this license purchase method, the license server resides locally on the private network that is reachable from the reader(s). This method does not require Internet connectivity as license acquisition comes from local sever connectivity.

The local server must be setup before installing the FX Connect license and it must be registered in the Zebra end user licensing portal. For details, go to: www.zebra.com/us/en/support-downloads/software-licensing.html. and select the **Manuals** link to download the Local License Server Administration Guide for Windows (part number, MN-003302-xx).

[Figure 60](#) illustrates the process of license acquisition from a local license server.

Figure 60 Local License Server Acquisition



Setting Up a Local License Server



NOTE The following steps are described in detail in the Local License Server Administration Guide for Windows (part number, MN-003302-xx).

To setup a local license server:

1. Install the LLS.
2. Configure the LLS.
3. Login to the Zebra Licensing Portal and register the LLS.
4. Acquire a license(s) for the LLS (see [Acquiring Licenses on page 89](#)).
5. Input the LLS URL and Activation ID.
6. Activate the license.
7. The reader receives the license information, queries the LLS for the Activation ID, and acquires the license.

When all steps are complete, the FX reader must be setup to acquire licenses from the LLS. This is accomplished by changing the **license_server_url** field in HTML page file to the following `http://<license_server_ip_or_hostname>:7070`. The local license server by default listens on port 7070 which can be changed in the license server configuration. If a non-default port is configured in local license server, then be sure to update the **license_server_url** field in the HTML page to the same value. The **license_activation_id** field must be updated to the appropriate value provided by Zebra.

Acquiring an FX Connect License From an Off-line Device

The FX Connect license can be activated on a standalone device. The FX7500/FX9600 readers do not require an Internet or Local Area Network. However, the user must download the Capability Response (License.bin file) from the Zebra Licensing Server. For details, go to: www.zebra.com/us/en/support-downloads/software-licensing.html. and select the **Manuals** link to download the Software Licenses Portal For End Users Quick Reference Guide 2018.08 (part number, MN-123456-xx). Refer to the section Activating Licenses on an Off-line Device for a detailed explanation on downloading the Capability Response from the Zebra Licensing Server.

Requirements To Download the Capability Response

- Device ID - the unique identification number of the FX device on the Zebra Licensing Server. The Device ID must be in the following format:
 <Model Name>_<Mac_Address> i.e., FX9600_84_24_8D_EF_B2_BB
 where Model Name is the FX7500 or FX9600
 MAC/IEE address is a 12 digit number
 This information can be found on bottom of device.

Figure 61 Reader Label



- Activation ID - the unique 32-bit alpha-numeric number shared to the user when the license is purchased. This number acts a key to enable the FX reader to activate the license. The Activation ID is in the following format:
 8c88-d0e7-9f3c-435b-968b-69a8-7f8e-a302
- Downloading Capability Response - the user must login to the Zebra Licensing Server. Refer to the link shared via e-mail when the license is purchased or go to:
<https://zebra-licensing.flexnetoperations.com/flexnet/deviceservices>



NOTE The email received upon license purchase includes all necessary login information. When using the link above, the Activation ID is your password.

- Create the Device ID.
- Map the Activation ID to the Device ID.
- Click the Download Capability Response. The Lincense.bin file is loaded into the download folder in the format below:
 <Device ID>.bin file i.e., FX9600_84_24_8D_EF_B2_BB.bin

Activating the License on the Device

License manager has two functions:

- Manages the license.
- Displays the available licenses.

Managing the License

Managing the license allows the user to upload the License.bin and acquire a license. Select the **License Manager UI** page on the reader. The following page displays.

Figure 62 License Manager UI - Acquire License

Manage License

Operation Type: Acquire ▼

Offline: True ▼

Upload License: Choose File No file chosen

Activate

1. **Operation Type:** Use the drop-down arrow and select Acquire.
2. **Offline:** Use the drop-down arrow and select True.
3. **Upload License:** Select **Choose File** and browse to find the FX9600_84_24_8D_EF_B2_BB.bin file.
4. Select **OK**.
5. Select **Activate**.



NOTE The Capability Response downloads from the server and is only valid for five calendar day. The license.bin file uploads to the reader and is processed and validated.

Available License Tab

The **Available License** page is populated when the license is processed and validated.

Figure 63 Valid Licenses on the FX Connect Device

Available License(s)					
License Index	License Name	License Version	Expiry Date	License Count	Host ID
1	fx-feature-connect	1.0	permanent	1	FX9600_84_24_8D_EF_B2_BB
2	fx-feature-connect-eval	1.0	9-apr-2019	1	FX9600_84_24_8D_EF_B2_BB

The following license attributes are displayed.

- License Index
- License Name
- License Version
- Expiry Date
- License Count
- Device Host ID

Figure 63 shows two valid licenses on the FX Connect device.



NOTE Both Perpetual and Evaluation licenses can be mapped to same Device ID.

Returning a License



NOTE The FX reader must be connected to Internet to a return license.



IMPORTANT If the user is unable to login to the reader web console (for example, if the reader becomes defective), go to:
<https://www.zebra.com/us/en/about-zebra/contact-zebra/contact-tech-support.html> for Zebra Technical Support. At that time, the Zebra licensing team releases the license from the cloud server. The reader requires reboot upon online releasing of the license.

The license acquired using the steps above can be returned to the cloud server. Click on the License Manager UI page on the FX7500 or FX9600 device. The following page displays.

Figure 64 Return a License

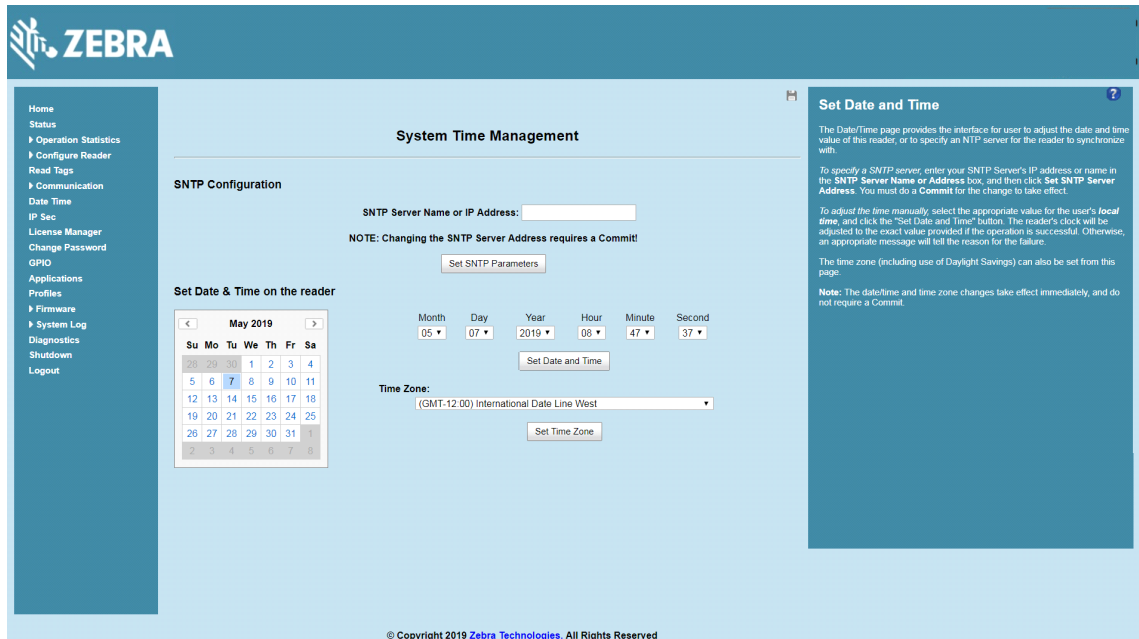
1. **Operation Type:** Use the drop-down arrow and select Return.
2. **Offline:** Use the drop-down arrow and select False.
3. **Server URL:** The cloud server URL (<https://zebra-licensing.flexnetoperations.com/flexnet/deviceservices>) should display. This is the default and should not be modified.
4. **Activation ID:** Enter the appropriate ID. (This is the ID received when you purchase the license.)
5. Select **Release**.
6. Upon successful release and completion of this operation, the license is removed from the reader and the reader reboots. License information is also deleted from the Available License page and the message below displays.

Figure 65 License

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 66 System Time Management Window



To specify an SNTP server, enter the SNTP server's IP address or name in the **SNTP Server Name or IP Address** box, and then select **Set SNTP Parameters**.

To adjust the time manually, select the appropriate value for the user's local time, and select 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.

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 67 IPv6 IP Sec Window

To add an IP Sec entry:

1. Select 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. Select the **Add IP Sec Entry** button.

To delete an IP Sec entry:

1. Select **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. Select 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 68 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. Select **Change Password**. The password changes immediately.

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.

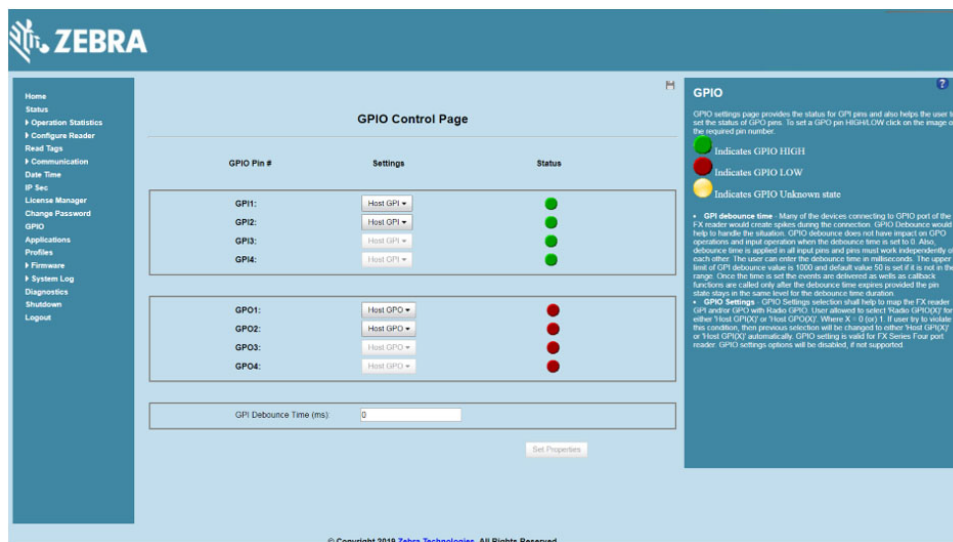
GPIO




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



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

Figure 69 FX7500 Example GPIO Control Page

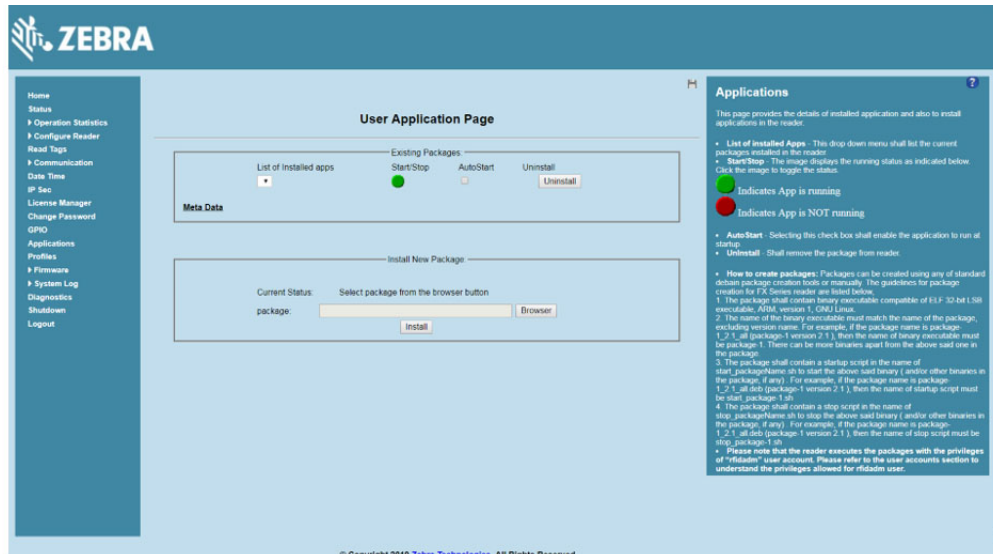


- Settings** - Map the reader GPI and/or GPO with the radio GPIO. Select either **Radio** or **Host** for **GPI_x** or **GPO_x** where $x = 0$ or 1 . An attempt to violate this condition changes the selection to either **Host GPI_x** or **Host GPO_x** automatically. The settings are disabled if a configuration is not supported.
- Status** - To set a GPO pin high or low, select 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** - Select 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 70 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. Select 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.
- **Install** - Installs a new package in 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.

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 71 Reader Profiles Window



NOTE The user cannot make profile active if inventory is in progress.



The **Reader Profiles** window functions are:

- **Available Profiles in the Reader** - Displays the available reader profiles.
- **Import** - Select 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 select **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 select **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 select **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 [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:

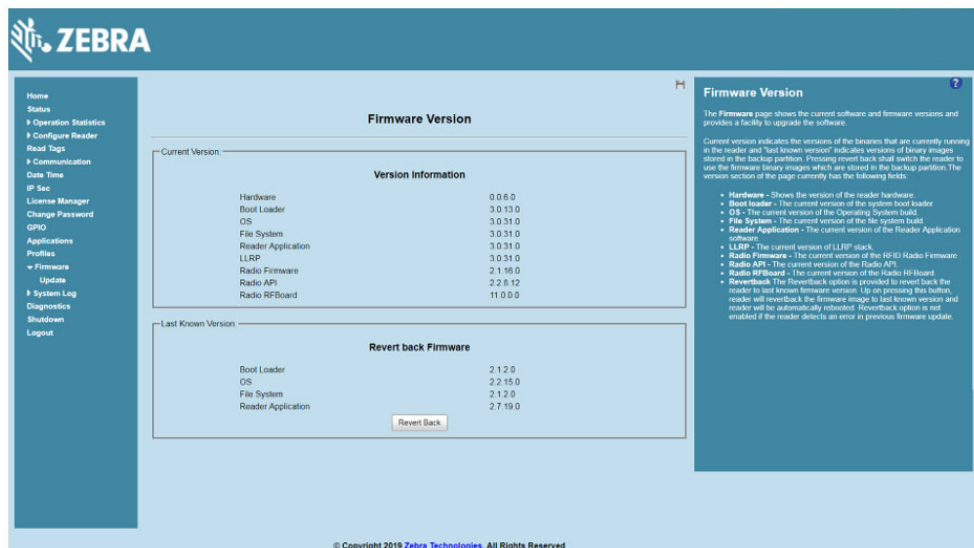
- HTTPS
- FTPS
- SSH
- LLRP Server
- IPSec

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, select **Firmware**.

Figure 72 Firmware Version



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

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

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

Firmware Update

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



NOTE: You must be logged in with Administrator privileges in order to access this window.
See [Change Password on page 98](#).

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 Functionality Changes

Firmware v3.0.35 or later includes a new auto commit functionality that no longer requires the user to manually commit changes. The **Commit/Discard** menu was removed.

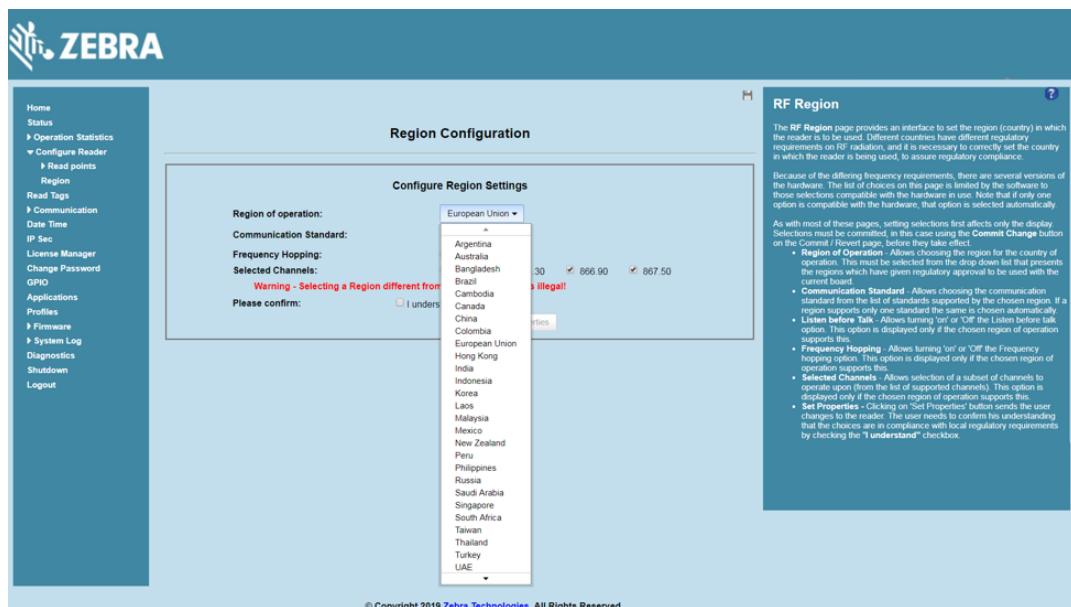
When the user changes any property and selects **Set Properties** on the web page, the commit function is automatically executed in the reader.

Region Configuration Commit

The following steps are an example of how the commit/discard functionality works.

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

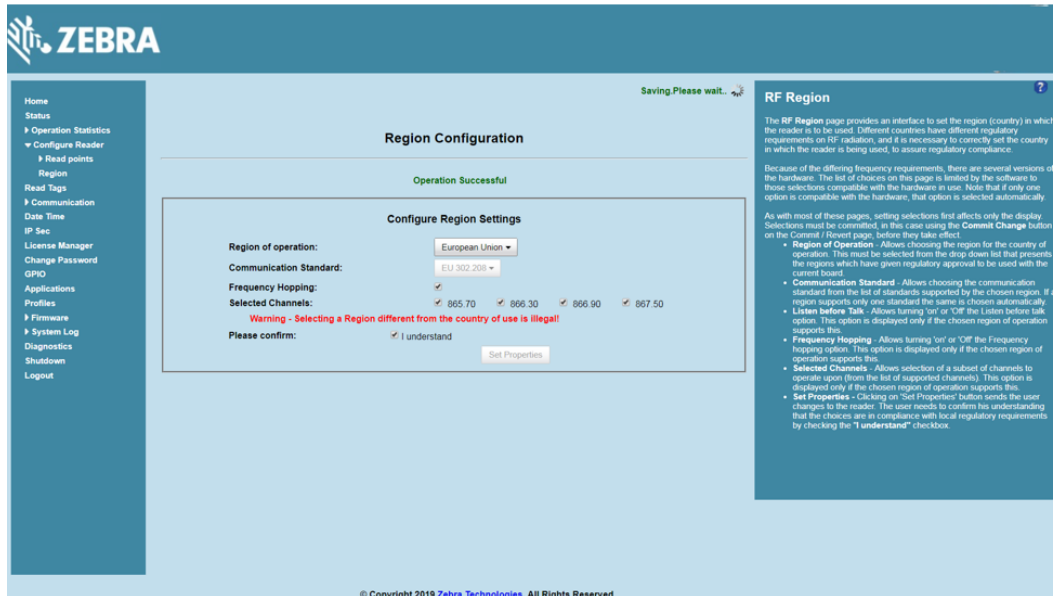
Figure 73 Configure Region Settings



2. Select the Communication Standard, if applicable.
3. Select Frequency Hopping, if applicable.

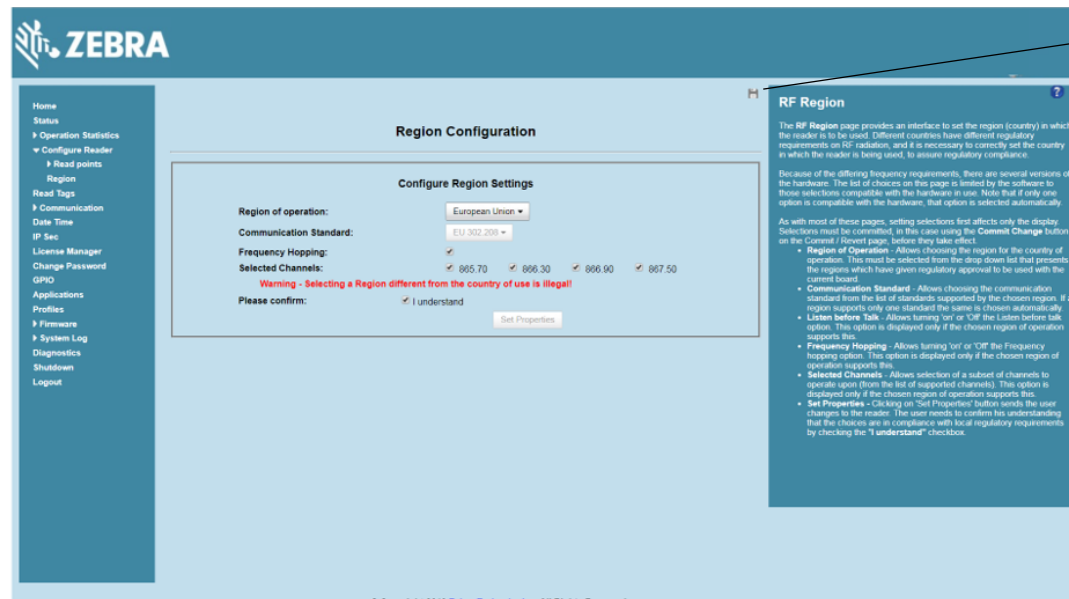
4. Select the appropriate channel(s), if applicable.
5. Select the **I understand** check box.
6. Select **Set Properties** to complete the region selection. The **Operation Successful** window displays a **Saving. Please wait...** message with a progress symbol until the commit completes.

Figure 74 Configure Region Settings, Operation Successful Window



7. When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully.

Figure 75 Commit Complete



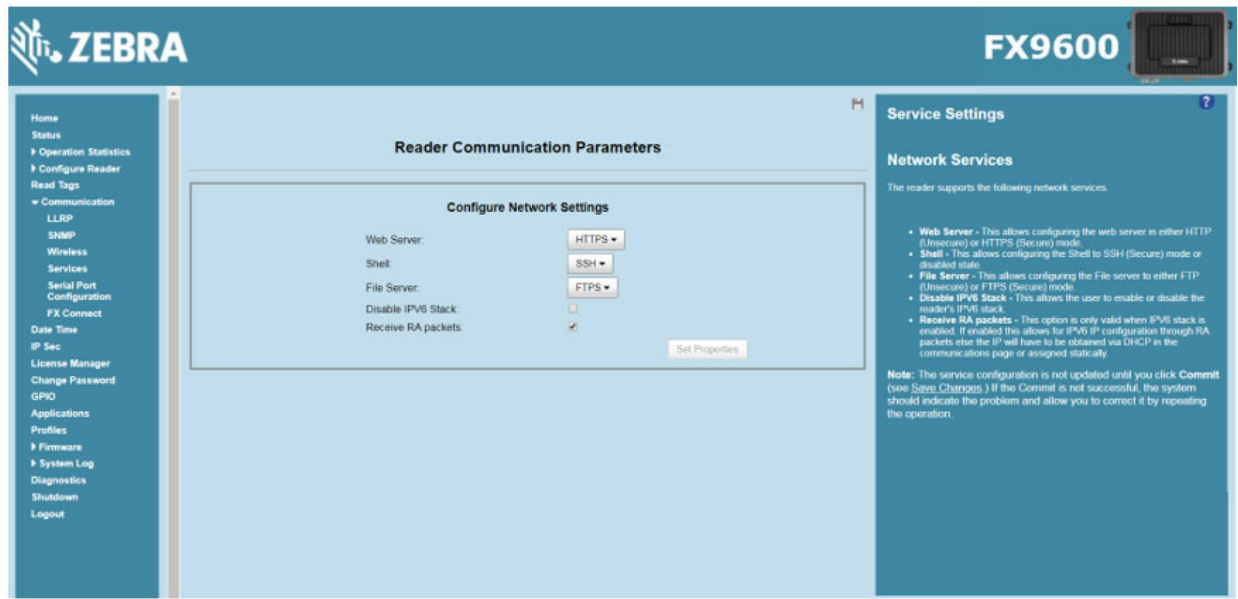
8. If after the successful completion of the commit any other action needs to be taken (for example, a reader reboot), the web page displays the appropriate message above the main setting tab.

New Property Change Work Flow

The following steps are an example of how the commit/discard functionality works when changing a property.

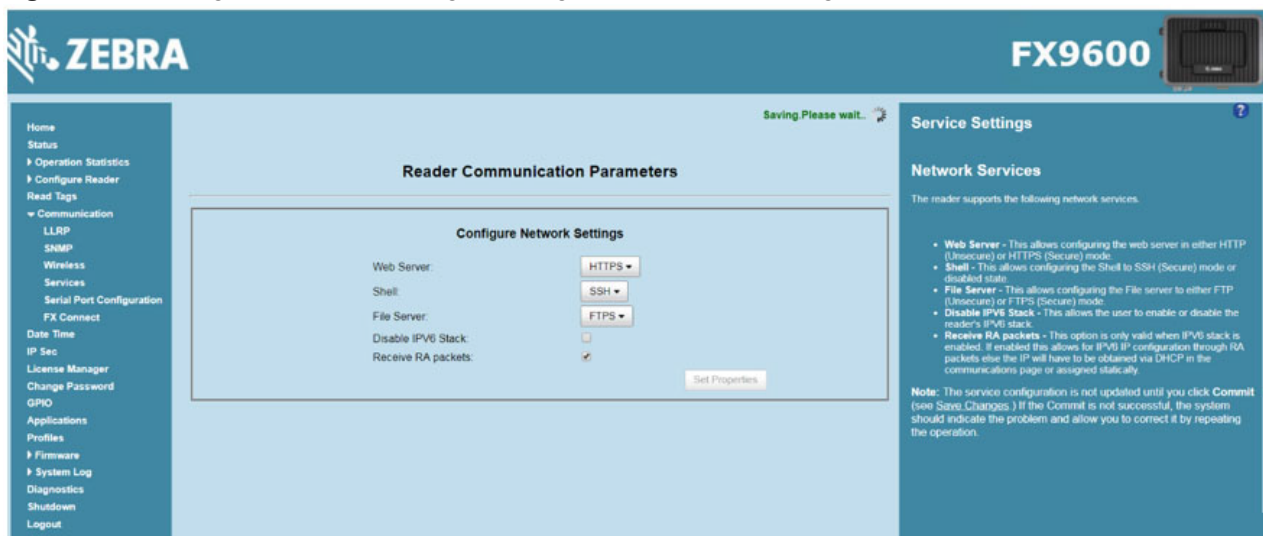
1. Select **Communication > Services**. On the **Configure Network Settings** screen, select a new Web Server or any other property from the appropriate drop-down menu.

Figure 76 Configure Network Settings



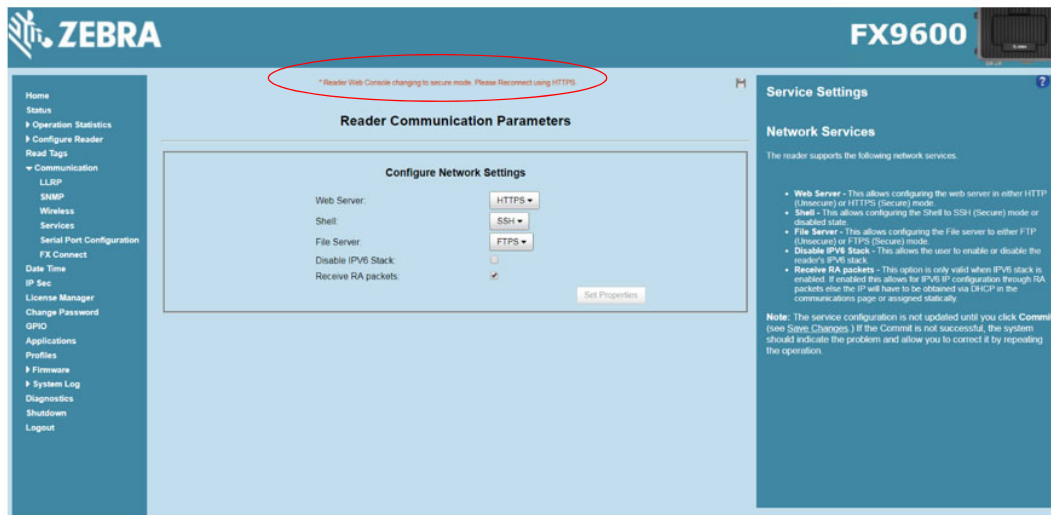
2. Select **Set Properties** to complete the new selection.
3. The message **Saving.Please wait...** displays with a progress symbol until the commit completes.

Figure 77 Configure Network Settings, Saving.Please wait... message Window



4. When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully.
5. If after the successful completion of the commit any other action needs to be taken (for example, a reader reboot), the web page displays the appropriate message above the main setting tab.

Figure 78 Action Message

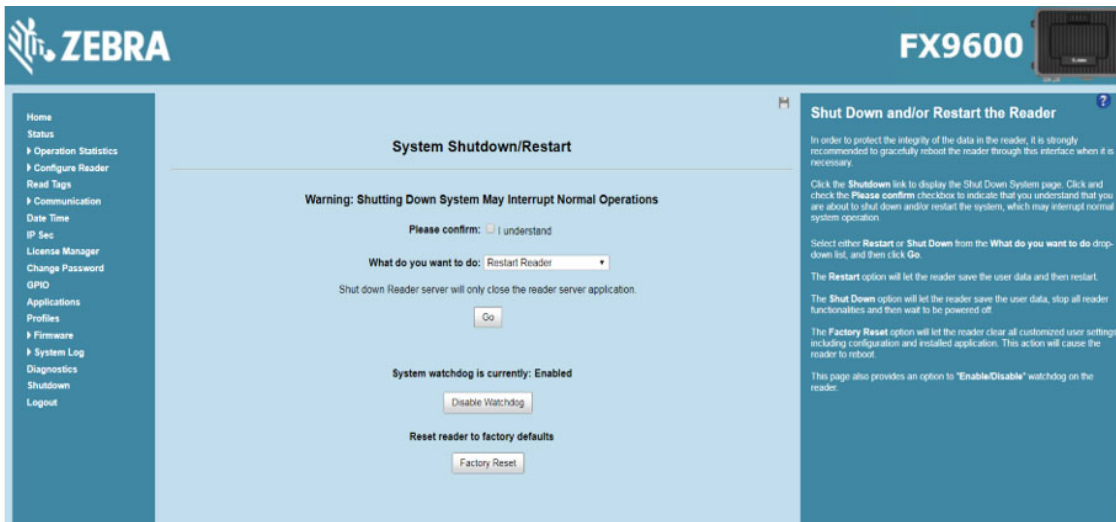


IMPORTANT

With the new version of software, the Discard Functionality option is no longer supported. Changes automatically commit to the reader.

In addition, the reset reader to factory defaults option was moved to the System Shutdown/Restart screen shown in [Figure 79](#).

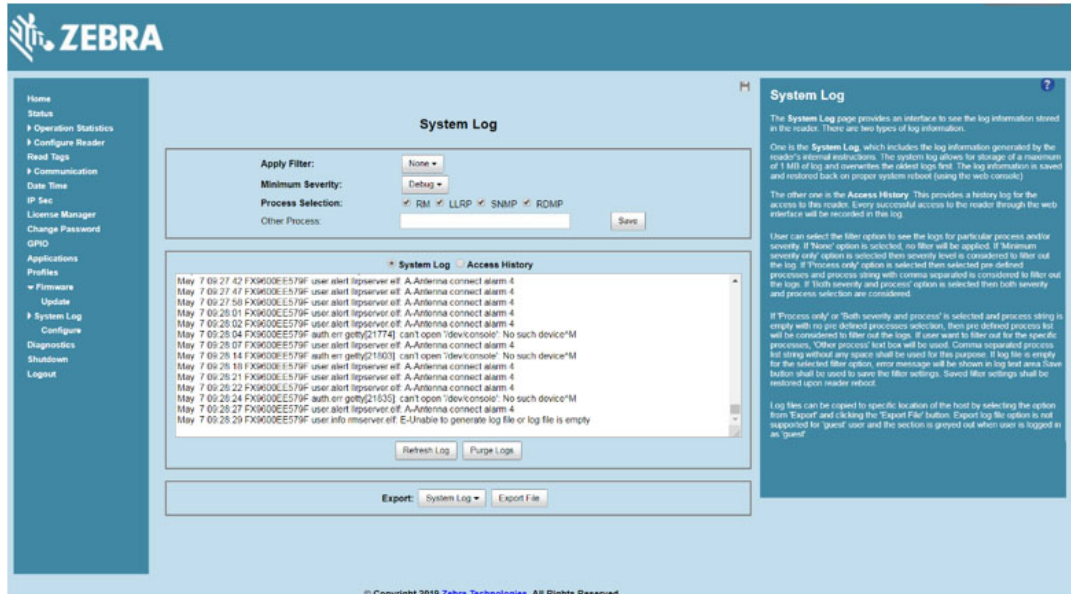
Figure 79 Reset Reader To Factory Defaults



System Log

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

Figure 80 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** - When this option is used, the log severity level filters the log content. Logs having severity levels equal or above the selected severity display.
 - **Process Selection** - When this option is used, only the logs for the selected process(es) display. More than one process can be listed, separated by a comma in the **Other Process** field.
 - **Minimum Severity & Process Selection** - When this option is used, both severity level and process are used to filter the logs. Only the logs that match the severity level filter and the process filter display.

When you select **Process Selection** only or **Minimum Severity** and **Process Selection** and no process is specified, by default, logs from RM, LLRP, SNMP, and RDMP are considered and display (severity level must match, if enabled).

- **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. Select **Save** to save the filter settings, which persist upon reader reboot.

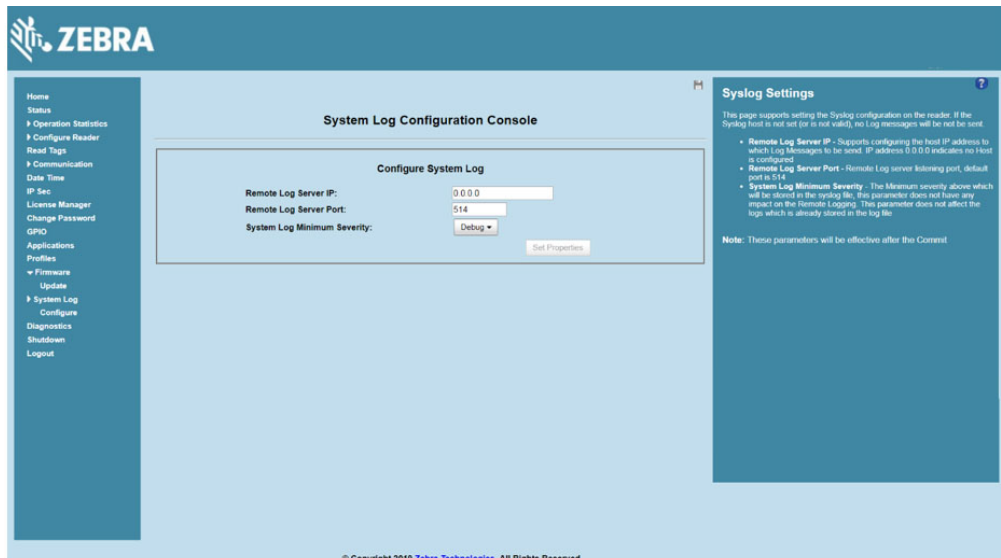
- **Log area** - Select a radio button for one of the two types of log information offered:
 - **System Log** - Includes the log information generated by the reader internal instructions. This stores up to 1 MB of log information, and overwrites the oldest logs first. The log information is saved and 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 **Refresh Log** to refresh the information in the log, or **Purge Logs** to clear the information.
- To export the system log select **System Log** from the **Export:** pull down menu, then select **Export File**. This saves the syslog file (and a zip file if there is more than one log file) in the **Downloads** folder on the PC.

To export the customer support data file select **Customer Support Data File** from the **Export:** pull down menu, then select **Export File**. This saves the data file in the **Downloads** folder on the PC.

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 81 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.

Select **Set Properties** to apply the changes. The **Operation Successful** window displays a **Saving. Please wait...** message with a progress symbol until the commit completes.

When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully. See [Commit/Discard Functionality Changes on page 103](#) for more information.

Reader Diagnostics

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

Figure 82 Reader Diagnostics Window

The screenshot shows the Zebra Administrator Console interface. On the left is a navigation menu with options like Home, Status, Operation Statistics, Configure Reader, Read Tags, Communication, Date Time, IP Sec, License Manager, Change Password, GPIO, Applications, Profiles, Firmware, Update, System Log, Configure, Diagnostics, Shutdown, and Logout. The main area is titled 'Reader Diagnostics Console' and contains a 'Start Diagnostics' button. Below the button is a log of system events. To the right of the log is a 'Reader Diagnostics' panel with instructions on how to use the diagnostics report.

Reader Diagnostics Console

Start Diagnostics

```
May 7 09:30:54 FX9600EE579F user notice root 13759 2 0 08:44 ? 00:00:12 [network2:0]
May 7 09:30:54 FX9600EE579F user notice root 21036 2 0 09:24 ? 00:00:01 [network2:1]
May 7 09:30:54 FX9600EE579F user notice root 22132 2 0 09:29 ? 00:00:00 [network2:2]
May 7 09:30:54 FX9600EE579F user notice root 22302 1602 0 09:30 ? 00:00:00 /bin/busybox.nosuid
/bin/sleep 10
May 7 09:30:54 FX9600EE579F user notice root 22308 827 0 09:30 ? 00:00:00 /bin/busybox.nosuid
/bin/sleep 1
May 7 09:30:54 FX9600EE579F user notice root 22310 934 0 09:30 ? 00:00:00 ps -ef
May 7 09:30:54 FX9600EE579F user notice ps -ef System Command completed with status Success
May 7 09:30:54 FX9600EE579F user notice System Running System Command top -n1b
May 7 09:30:54 FX9600EE579F user notice top -n1b System Command completed with status Success
May 7 09:30:54 FX9600EE579F user notice
=====
May 7 09:30:54 FX9600EE579F user notice System Diagnostics Finished successfully in 0 Seconds
May 7 09:30:54 FX9600EE579F user notice
=====
May 7 09:30:54 FX9600EE579F user notice Diagnostics --- Network ---
May 7 09:30:54 FX9600EE579F user notice
May 7 09:30:54 FX9600EE579F user notice Network Running System Command route
May 7 09:30:59 FX9600EE579F user notice Kernel IP routing table
May 7 09:30:59 FX9600EE579F user notice
Destination Gateway Genmask Flags Metric Ref
Use Iface
May 7 09:30:59 FX9600EE579F user notice default 10.17.129.1 0.0.0.0 UG 0 0 eth0
May 7 09:30:59 FX9600EE579F user notice 10.17.129.0 * 255.255.255.0 U 0 0 0 eth0
May 7 09:30:59 FX9600EE579F user notice 169.254.10.0 * 255.255.255.0 U 0 0 0 usb0
May 7 09:30:59 FX9600EE579F user notice 224.0.0.0 * 240.0.0.0 U 0 0 0 eth0
May 7 09:30:59 FX9600EE579F user notice route System Command completed with status Success
May 7 09:30:59 FX9600EE579F user notice Network Running System Command netstat -l -t
```

Reader Diagnostics

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

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

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

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

© Copyright 2019 Zebra Technologies. All Rights Reserved

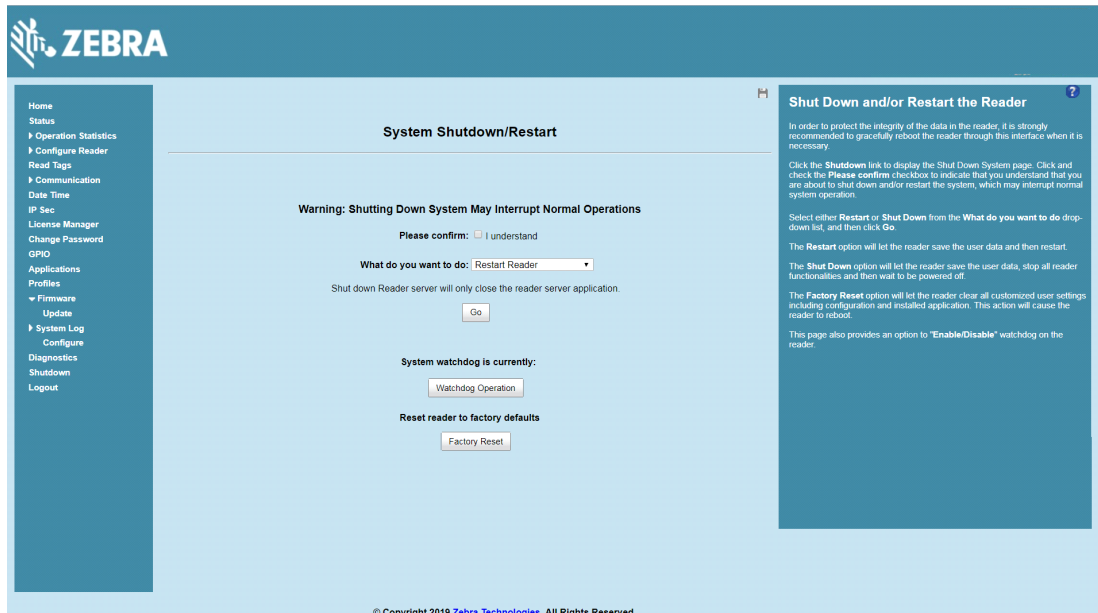
Selecting **Start Diagnostics** clears the system log and displays the diagnostics report. The reader reboots when the diagnostics completes. Return to the **Diagnostics** window to view the diagnostics report.

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,lrpserver.elf: N-D

Shutdown

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

Figure 83 System Shutdown/Restart Window



To shut down or restart the reader:

1. Select 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. Select **Go**.

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

The reset reader to factory defaults option is available in this window.

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 84 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.

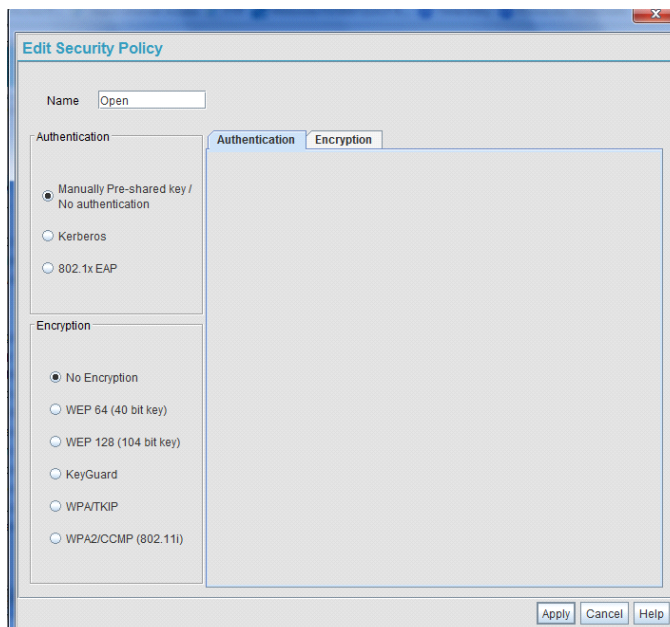
Preferred Configurations for Access Points

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 85 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 86 Open Network Configuration for Android Device

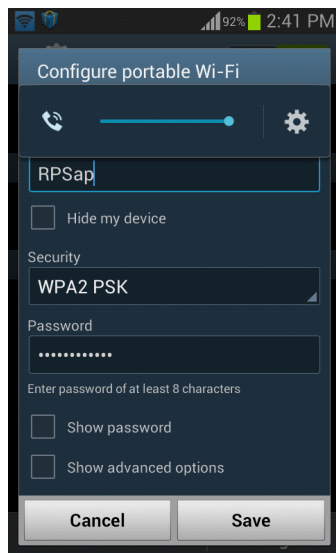


WPA2 PSK

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 87 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 88 WPA PSK Configuration for Android Device

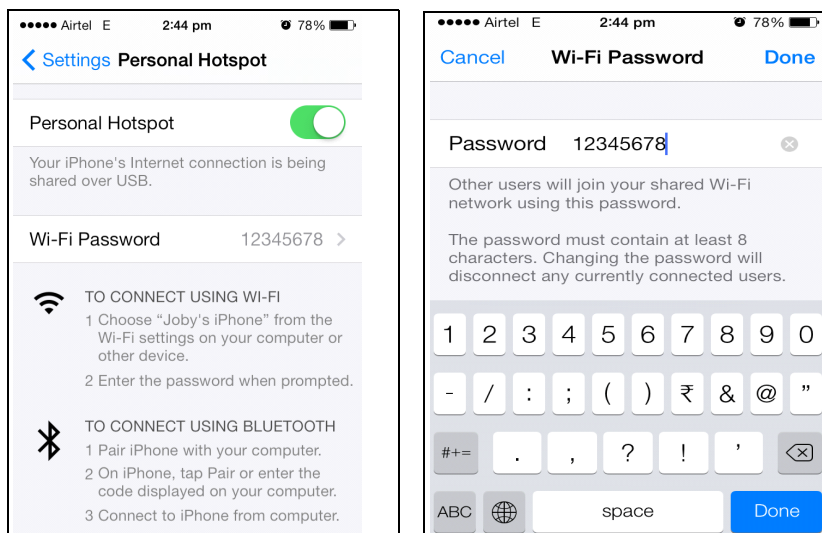


Internet Connection Configuration for iPhone

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 89 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 7 on page 73](#) for a list of supported Wi-Fi dongles.

Figure 90 FX7500 USB Host Port Location for Dongle

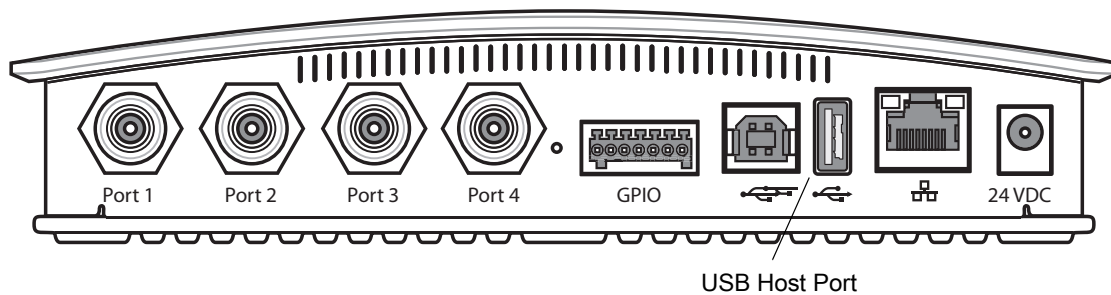
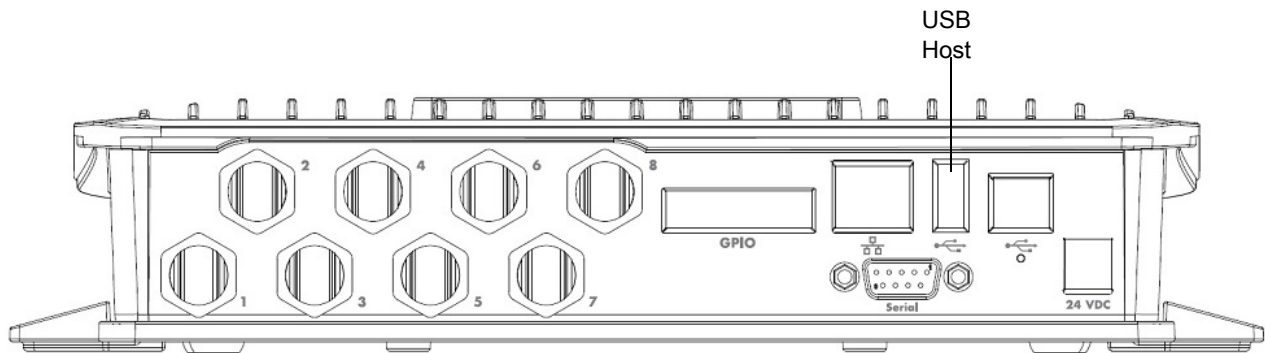
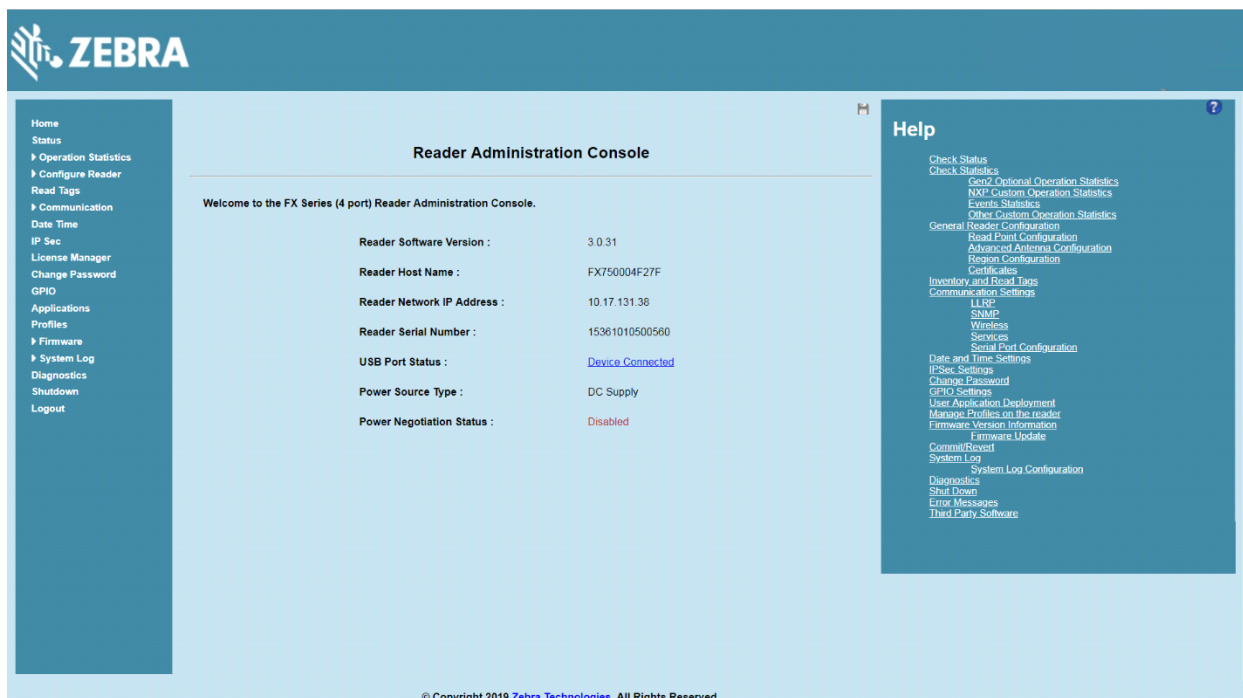


Figure 91 FX9600 USB Host Port Location for Dongle



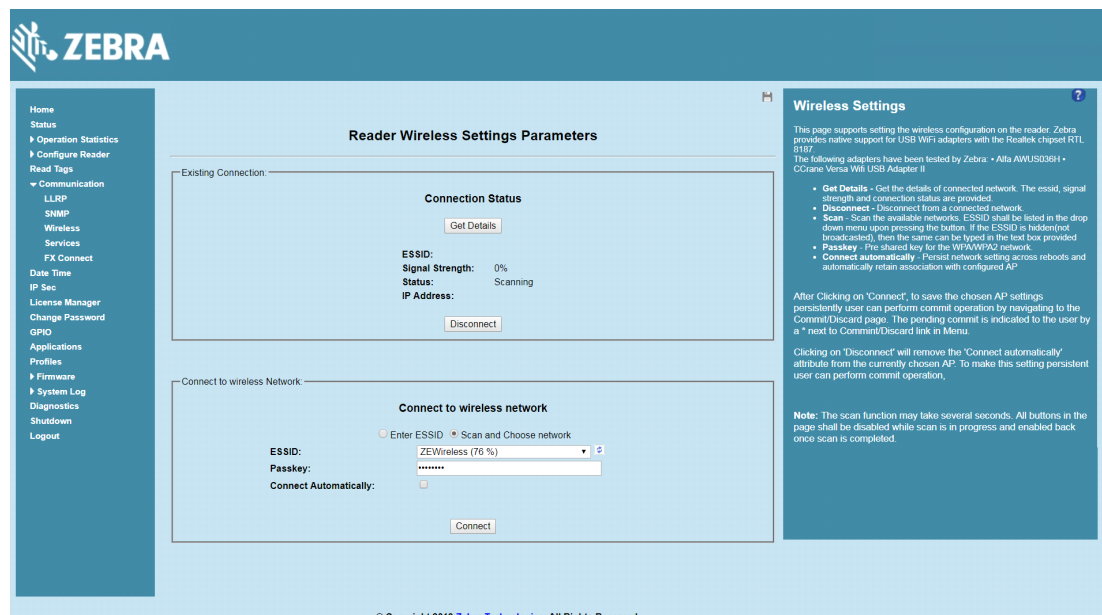
2. To confirm that the Wi-Fi dongle is detected properly, log in to the reader Administrator Console. On the Home page ensure the **USB Port Status** displays **Device Connected**. Hover the mouse pointer over this link to display the Wi-Fi dongle information shown in [Figure 92](#).

Figure 92 Wi-Fi Dongle Connected



3. Select **Communication > Wireless**.

Figure 93 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).

Figure 94 Entering Connect Information

The screenshot shows the Zebra Reader Wireless Settings Parameters page. The left sidebar contains navigation links: Home, Status, Operation Statistics, Configure Reader, Read Tags, Communication (LLRP, SNMP, Wireless, Services, FX Connect), Date Time, IP Sec, License Manager, Change Password, GPIO, Applications, Profiles, Firmware, System Log, 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 a 'Connection Status' table with fields for ESSID, Signal Strength, Status, and IP Address. The 'Connect to wireless Network' section has radio buttons for 'Enter ESSID' and 'Scan and Choose network'. The 'Scan and Choose network' option is selected, and a dropdown menu shows 'ZEWireless (76 %)' as the selected network. Below the dropdown are fields for 'Passkey' and 'Connect Automatically'. A 'Connect' button is at the bottom of this section. On the right, a 'Wireless Settings' sidebar provides additional information and instructions.

Reader Wireless Settings Parameters

Existing Connection:

Connection Status	
ESSID:	
Signal Strength:	0%
Status:	Scanning
IP Address:	

Connect to wireless Network:

☐ Enter ESSID
 ☒ Scan and Choose network

ESSID: ZEWireless (76 %)

Passkey: *****

Connect Automatically: ☐

Connect

Wireless Settings

This page supports setting the wireless configuration on the reader. Zebra provides native support for USB WiFi adapters with the Realtek chipset RTL 8187. The following adapters have been tested by Zebra: • Alfa AWUS036H • CCrane Vesta W6 USB Adapter II

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

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

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

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

© Copyright 2019 Zebra Technologies. All Rights Reserved

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

Figure 95 Assigned IP Address

The screenshot shows the Zebra Reader Wireless Settings Parameters page after a successful connection. The 'Connection Status' table now shows 'Signal Strength' as 100%, 'Status' as Completed, and 'IP Address' as 157.235.207.25. The 'Connect to wireless Network' section remains the same, but the 'Connect' button is no longer visible. The 'Wireless Settings' sidebar is also present.

Reader Wireless Settings Parameters

Existing Connection:

Connection Status	
ESSID:	ZEWireless
Signal Strength:	100%
Status:	Completed
IP Address:	157.235.207.25

Connect to wireless Network:

☐ Enter ESSID
 ☒ Scan and Choose network

ESSID: ZEWireless (76 %)

Passkey: *****

Connect Automatically: ☐

Connect

Wireless Settings

This page supports setting the wireless configuration on the reader. Zebra provides native support for USB WiFi adapters with the Realtek chipset RTL 8187. The following adapters have been tested by Zebra: • Alfa AWUS036H • CCrane Vesta W6 USB Adapter II

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

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

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

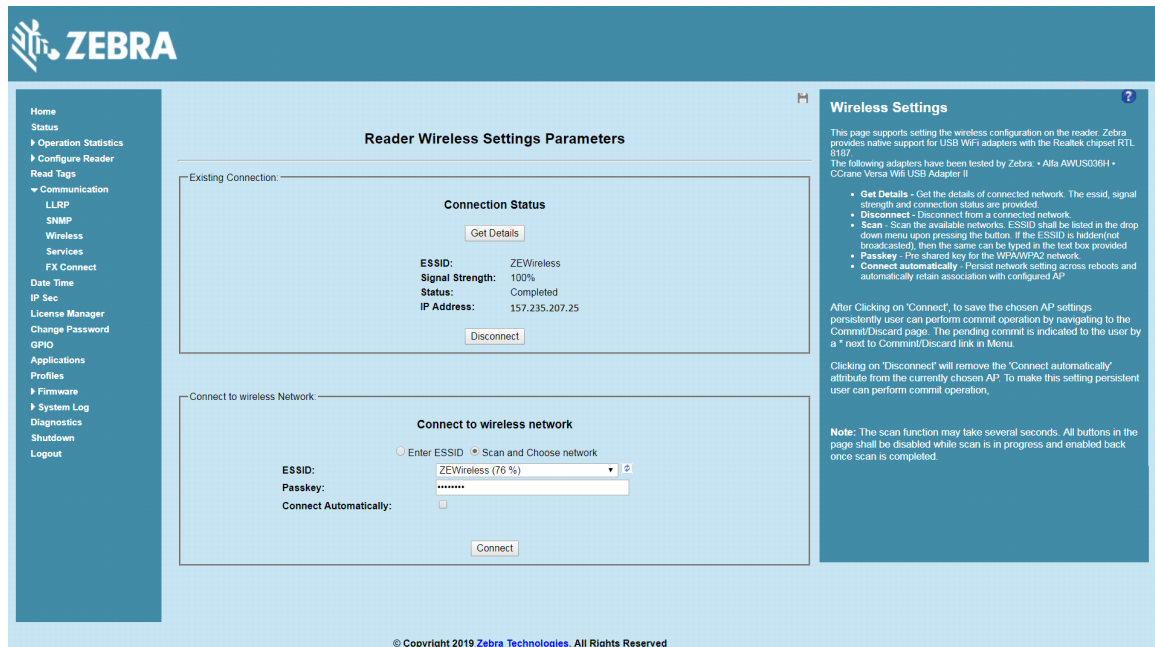
Note: The scan function may take several seconds. All buttons in the page shall be disabled while scan is in progress and enabled back once scan is completed.

© Copyright 2019 Zebra Technologies. All Rights Reserved

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.

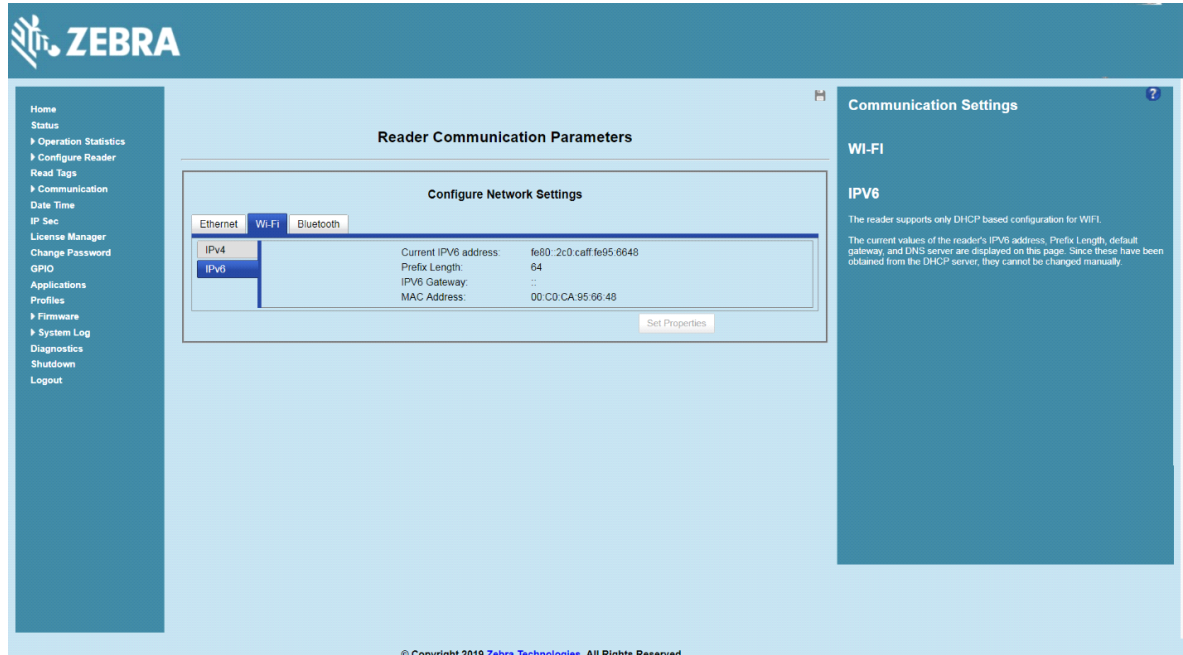
For wireless IP address details, select **Communication > Wi-Fi** tab.

Figure 96 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 97 Wi-Fi Tab - IPV6 Connecting 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:

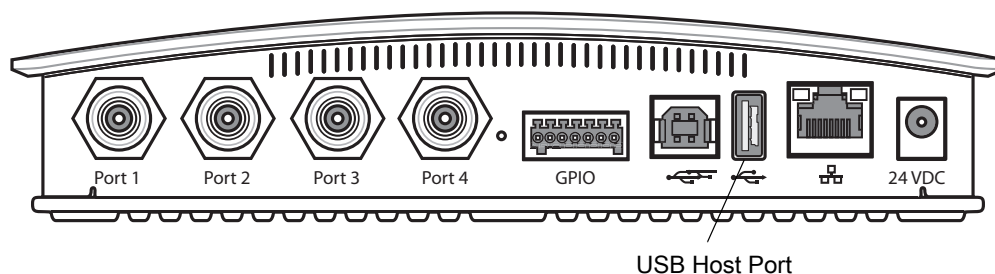
1. Plug the supported Bluetooth dongle into the USB host port on the FX Reader.

The Zebra FX9600 provides native support for USB Bluetooth dongles based on chipsets CSR8510 and RT5370L. The following dongles were tested:

Table 12 Supported Bluetooth Dongles

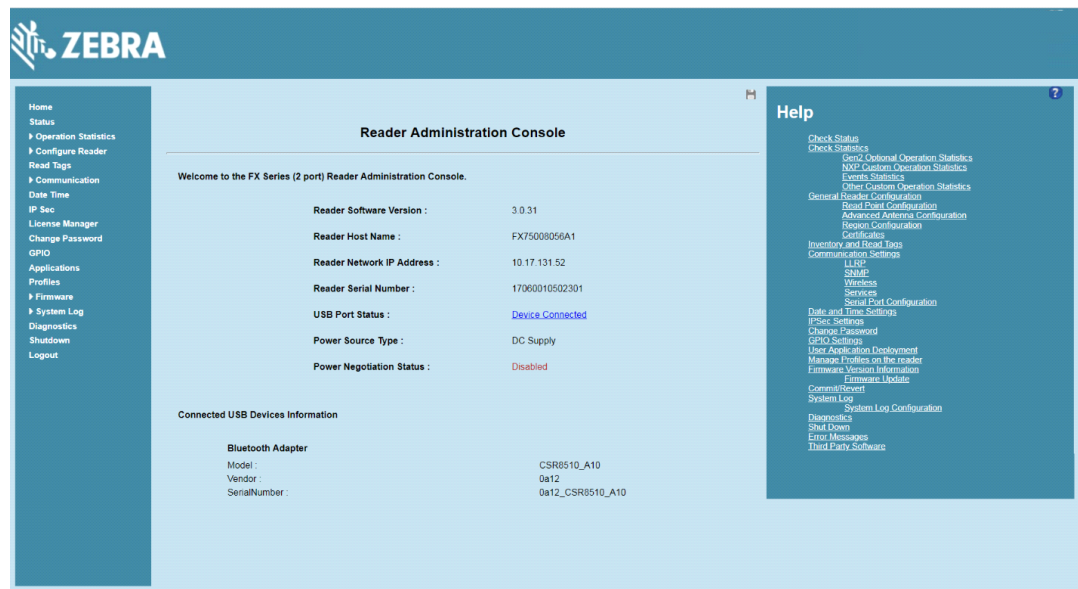
Dongle Model	Zebra FX7500	Zebra FX9600
Bluetooth CSR 4.0 dongle Qualcomm / Atheros CSR8510	Yes	Yes
Bluetooth 3.0+HS Ralink RT5370L	Yes	Yes
Asus Mini Bluetooth Dongle USB-BT211	Yes	Yes
MediaLink Bluetooth Dongle MUA-BA3	Yes	Yes

Figure 98 USB Host Port Location for Dongle



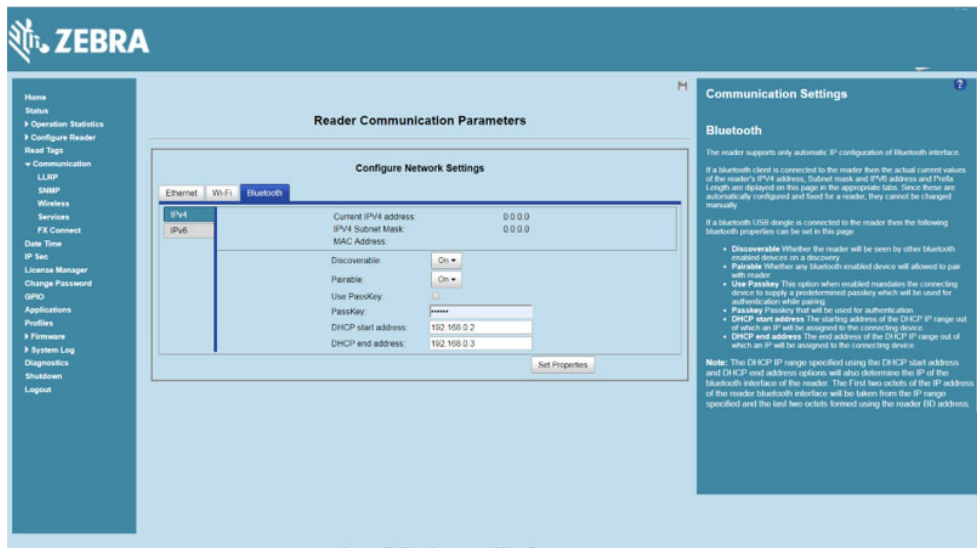
2. To confirm that the Bluetooth dongle is detected properly, log in to the reader Administrator Console. On the **Home** page ensure the **USB Port Status** displays **Device Connected**. Hover the mouse pointer over this link to display the Bluetooth dongle information.

Figure 99 Bluetooth Dongle Connected Select **Communication > Bluetooth**.



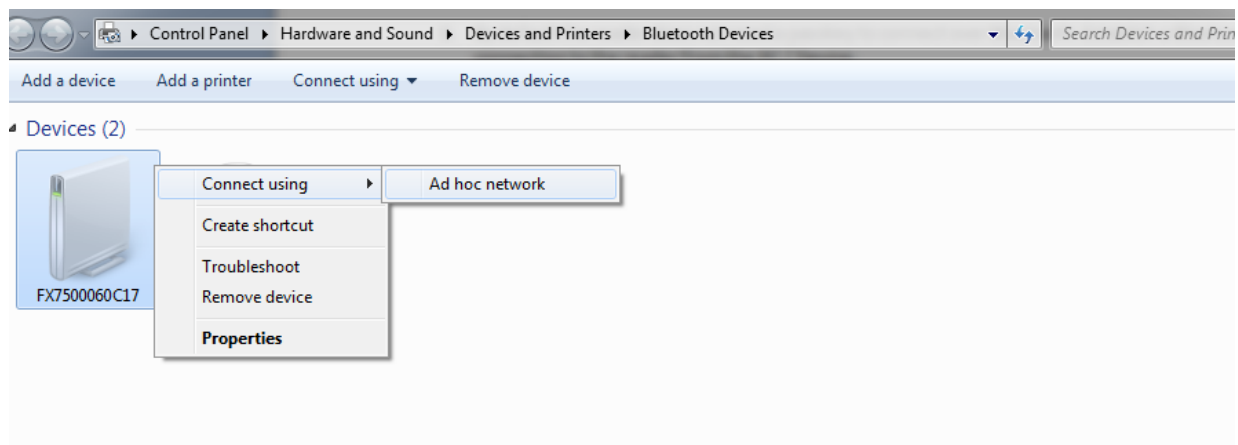
3. Change the **Discoverable** and **Pairable** properties to **On**.

Figure 100 Changing Discoverable and Pairable Properties



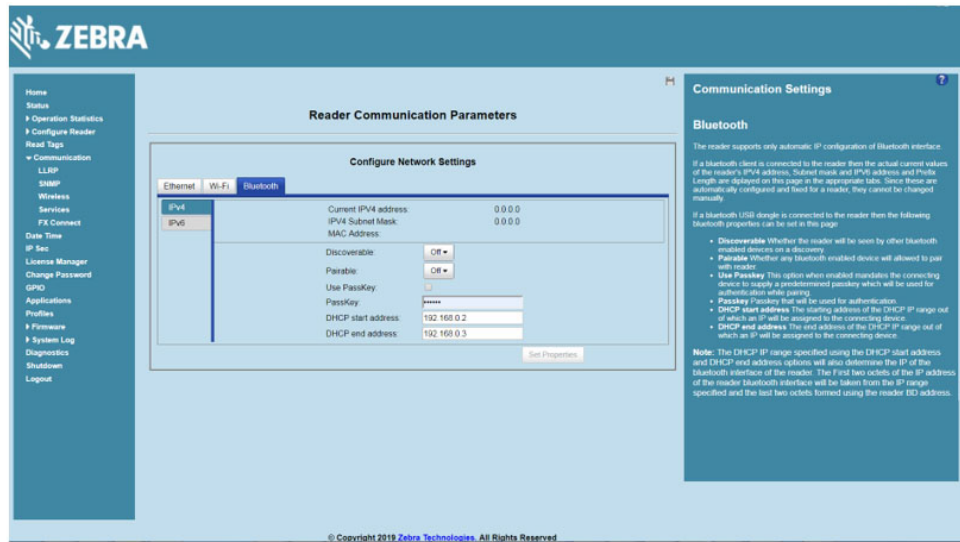
4. Optionally select **Use Passkey** and enter a passkey to validate the Bluetooth connection. The default passkey for the FX7500 and FX9600 is **0000**.
5. Discover the reader from a Bluetooth-enabled device (such as a laptop). Use the host name to identify the reader among the discovered devices (for 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 101 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 102 Communication Bluetooth Tab



Open the web page or sample application to connect to the Bluetooth IP (192.168.67.21 in [Figure 102](#)) 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 back-end 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.
- Zebra FX Series Embedded C/CPP SDK User Guide Linux provides instructions for using the FX Series Embedded native C/C++ SDK for Linux.
- Zebra FX Series Embedded Java SDK User Guide Linux explains how to use the FX Series Embedded Java SDK for Linux.
- Zebra FX Series Embedded Java SDK User Guide Windows describes instruction for using the FX Series Embedded Java SDK for Windows.
- 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.

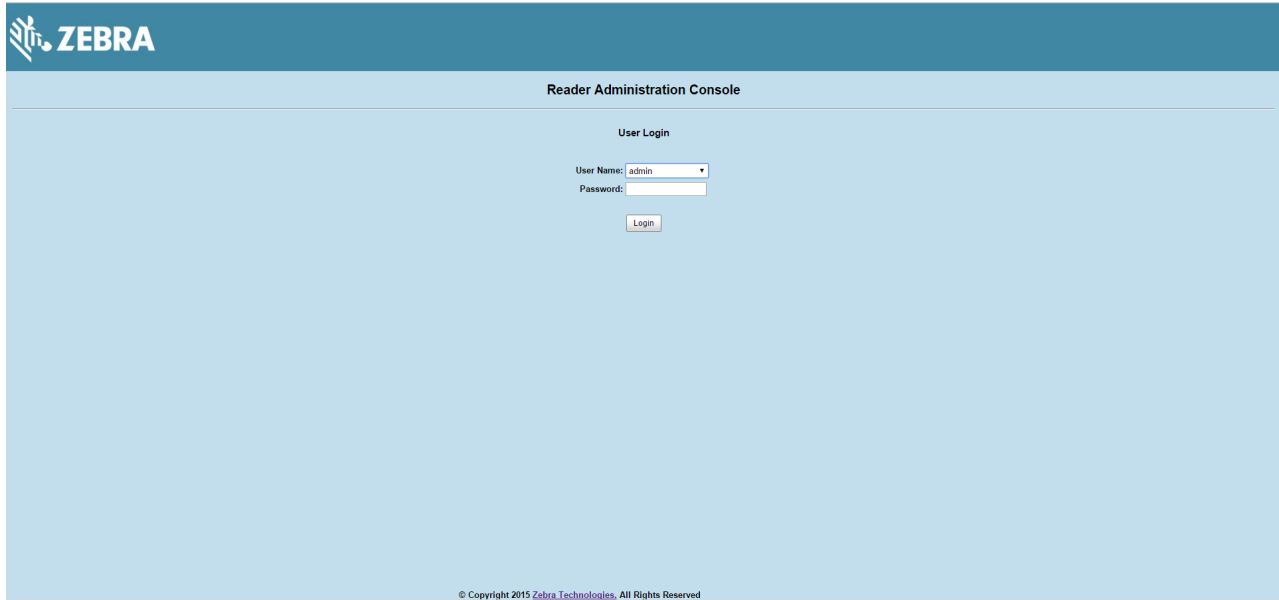
Updating FX Series Reader Software

Verifying Firmware Version

To verify that the FX7500 and FX9600 reader firmware is outdated:

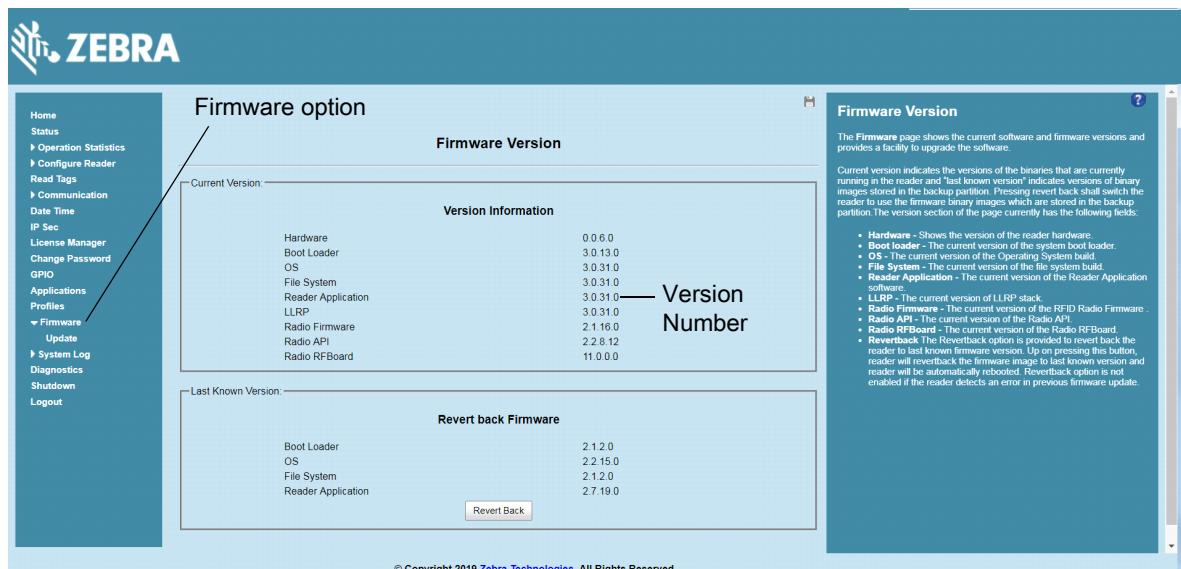
1. Log into the reader. In the **User Login** window, enter **admin** in the **User Name:** field and enter **change** in the **Password:** field.

Figure 103 User Login Window



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 104 Firmware Version Window



Updating Methods

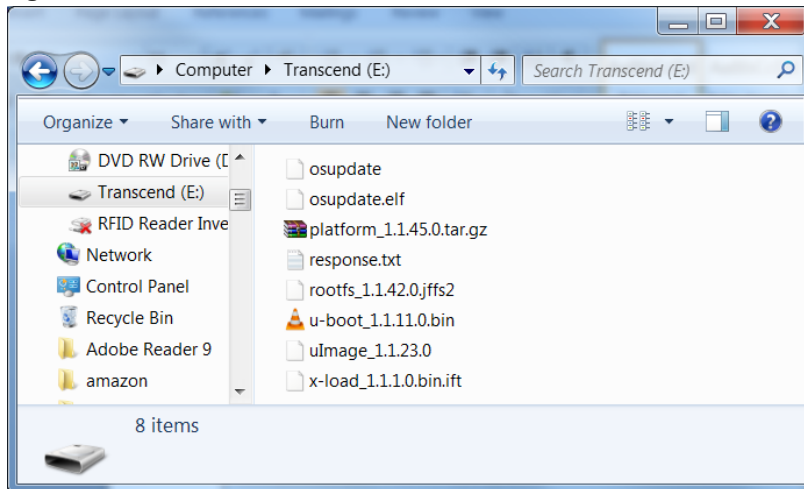
Download the reader update files from www.zebra.com/support, then use one of three methods to update the reader software to a later version, e.g., 1.1.45.0 or higher:

- [Update Using a USB Drive \(Recommended\)](#)
- [File-Based Update on page 128](#)
- [FTP-Based Update on page 131](#)

Update Using a USB Drive (Recommended)

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

Figure 105 USB Drive Root Folder



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

Figure 106 FX7500 USB Host Port Window

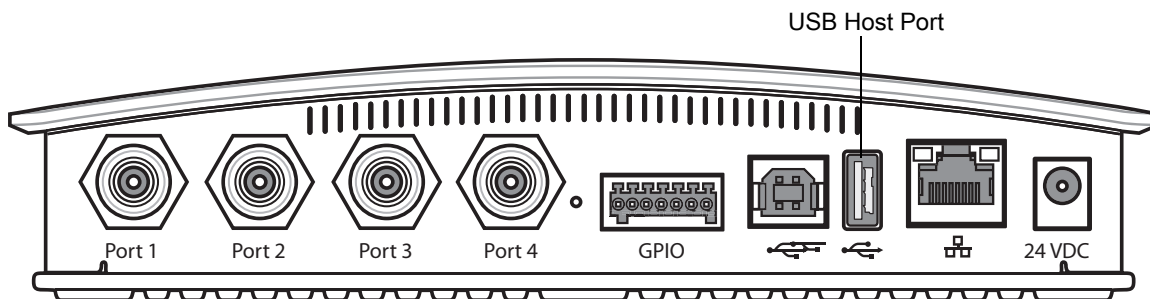
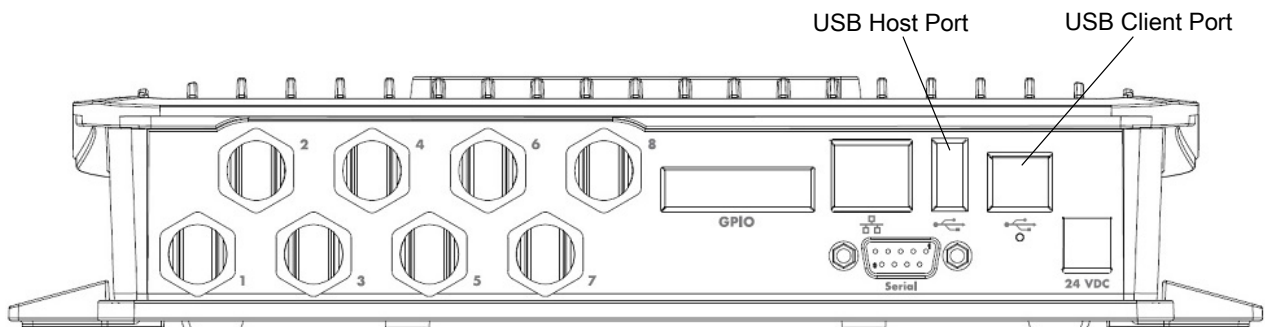


Figure 107 FX9600 USB Host Port Window



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 108 FX7500 Reader LEDs

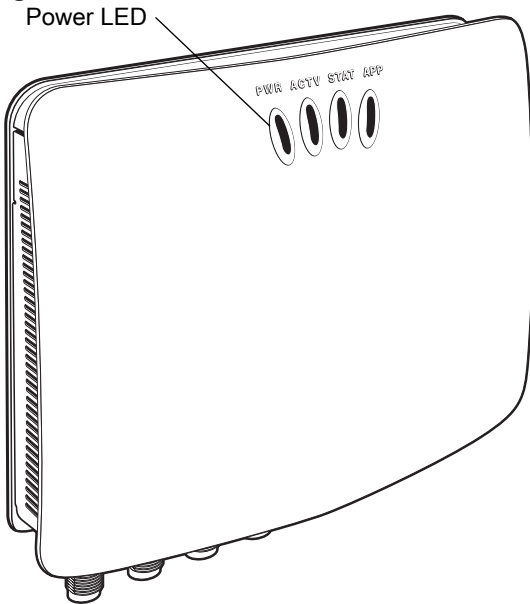
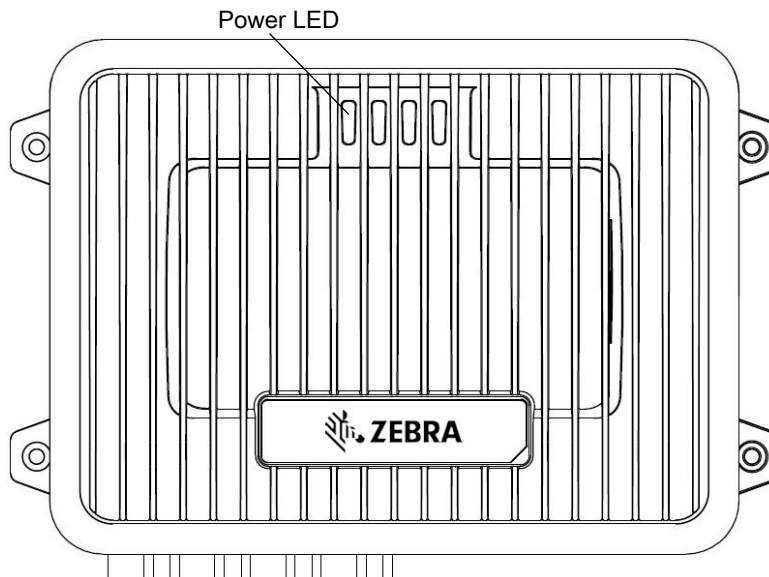


Figure 109 FX9600 Reader LEDs

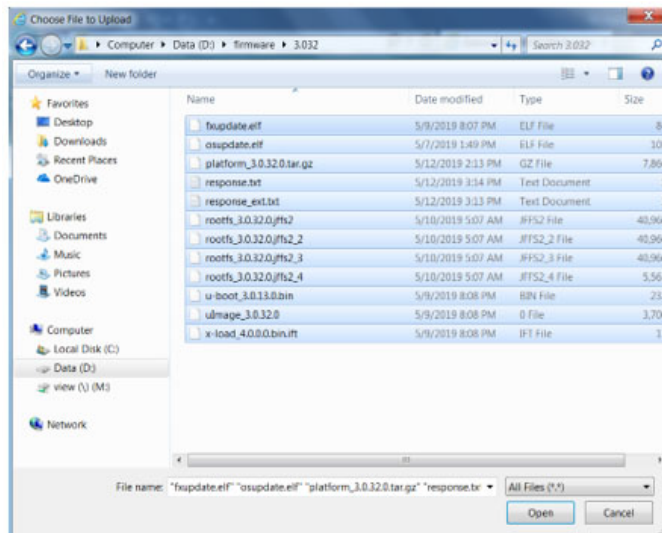


File-Based Update

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

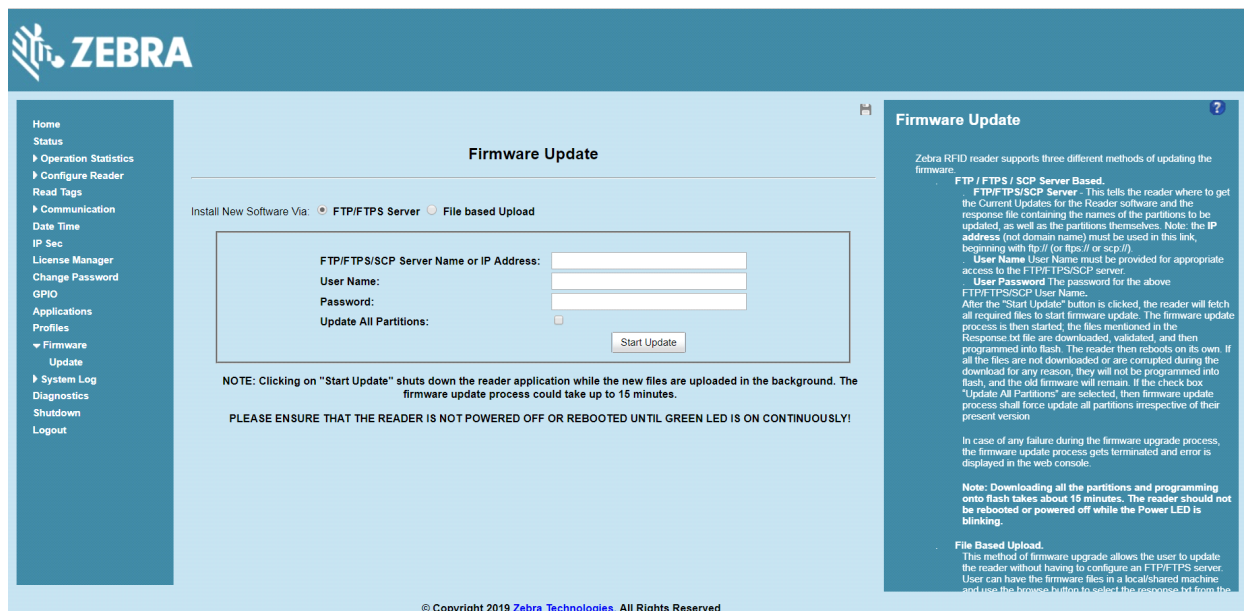
Firmware Upgrade

Figure 110 Host Computer Folder



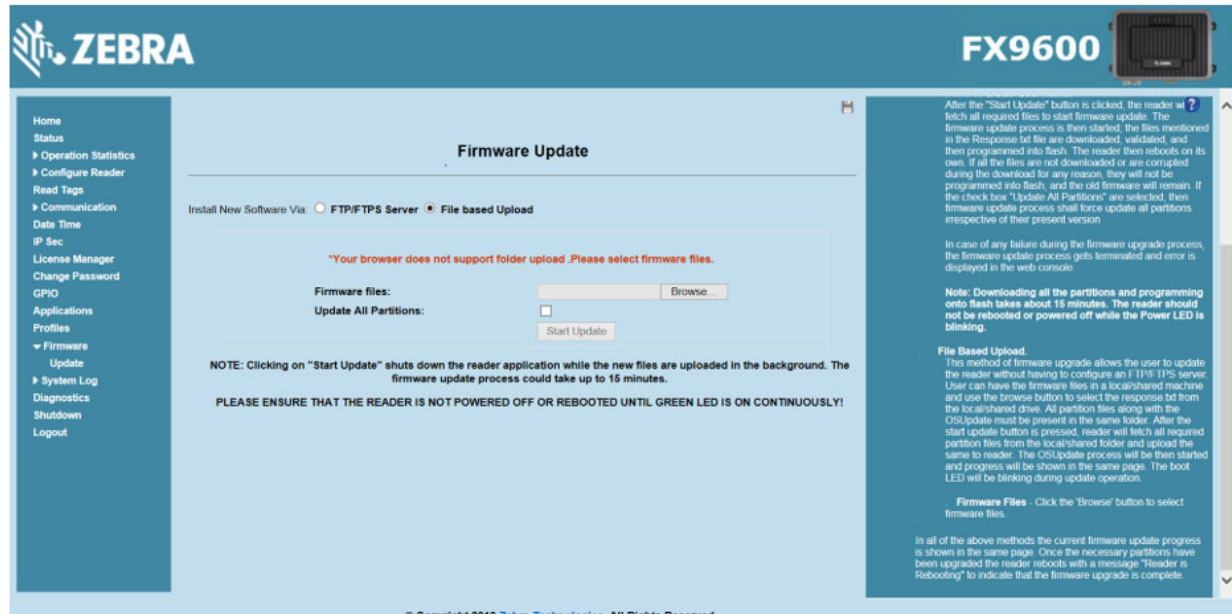
2. Log into the reader and navigate to the **Firmware Update** page.

Figure 111 Firmware Update Window



3. Select File based Upload.

Figure 112 Firmware Update Window



4. Select **Browse** and navigate to the folder or files that contains the firmware update files.

Figure 113 Browsing Update Folders

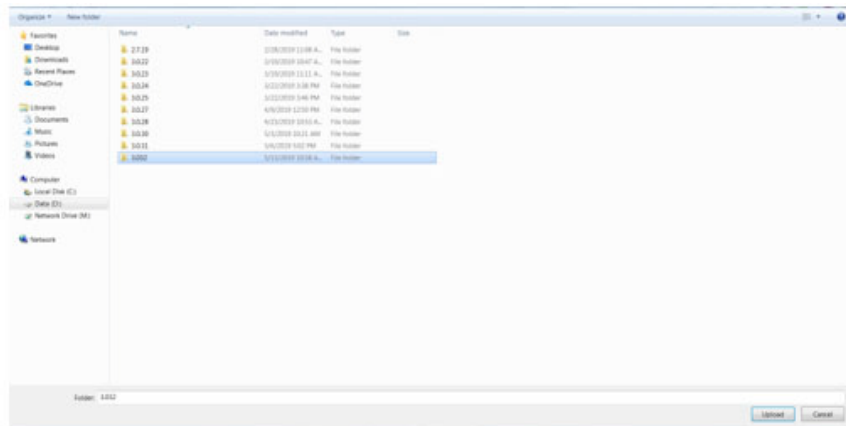
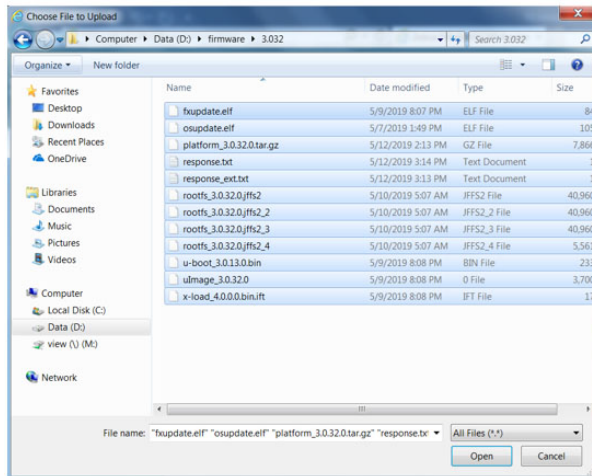


Figure 114 Browsing Update Files



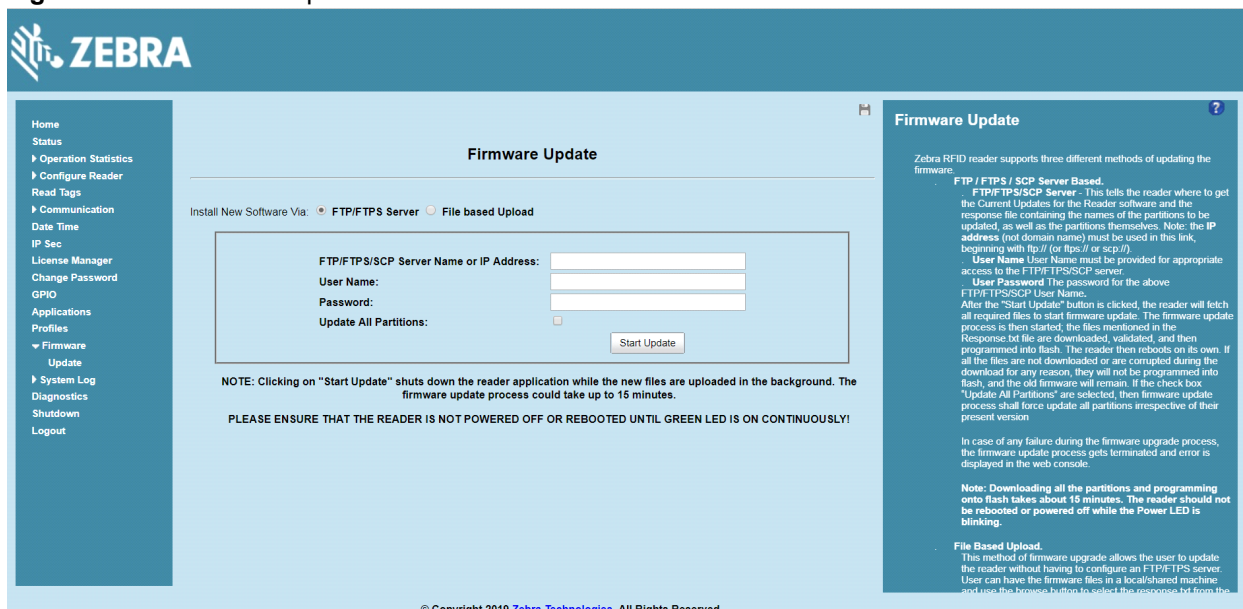
5. Select all the files.
6. Select **Start Update**. The reader starts the update process and displays the update status as follows:
 - The reader continuously blinks the power LED red.
 - The reader blinks all four LEDs orange, one time.
 - The reader power LED remains steady orange.
 - The reader power LED remains solid 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 115 Firmware Update Window



2. Select **FTP/FTPS Server**.

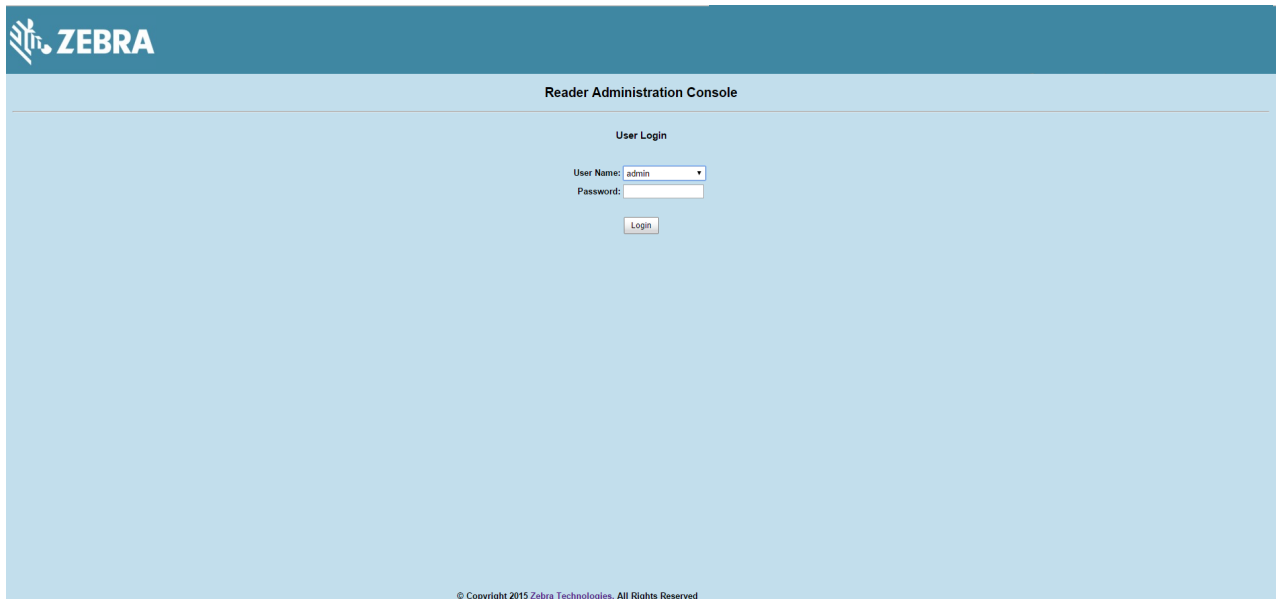
3. Enter the FTP location where the files are located.
4. Enter the **User Name** and **Password** for the FTP server login.
5. Select **Start Update**. The reader starts the update process and displays the update status as follows:
 - The reader continuously blinks the Power LED red.
 - The reader blinks 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 116 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 117 Firmware Version Window

The screenshot displays the Zebra Firmware Version window. On the left is a navigation menu with options: Home, Status, Operation Statistics, Configure Reader, Read Tags, Communication, Date Time, IP Sec, License Manager, Change Password, GPIO, Applications, Profiles, Firmware, System Log, Diagnostics, Shutdown, and Logout. The main content area is titled 'Firmware Version' and is divided into two sections: 'Current Version' and 'Last Known Version'. The 'Current Version' section contains a table of version information for various components. The 'Last Known Version' section contains a table of version information for the same components, along with a 'Revert Back' button. On the right side of the window, there is a 'Firmware Version' sidebar with a description of the page and a list of version information fields.

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:

- **Hardware** - Shows the version of the reader hardware.
- **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.
- **Radio RFBoard** - The current version of the Radio RFBoard.
- **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

Version Information	
Hardware	0.0.6.0
Boot Loader	3.0.13.0
OS	3.0.31.0
File System	3.0.31.0
Reader Application	3.0.31.0
LLRP	3.0.31.0
Radio Firmware	2.1.16.0
Radio API	2.2.8.12
Radio RFBoard	11.0.0.0

Last Known Version

Revert back Firmware	
Boot Loader	2.1.2.0
OS	2.2.15.0
File System	2.1.2.0
Reader Application	2.7.19.0

Revert Back

© Copyright 2019 Zebra Technologies. All Rights Reserved

Troubleshooting

Troubleshooting

Table 13 provides FX Series troubleshooting information.



NOTE: If problems still occur, contact the distributor or call the local contact. See [page 11](#) for contact information.

Table 13 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 29 .
Reader is not reading tags.	The tag is out of its read range.	Move the tag into read range. See Read Tags on page 67 .
	Antennas are not connected.	Connect antennas.
	Tags are damaged.	Confirm that tags are good.
	Tags are not EPCgen2.	Confirm that tags are EPCgen2.
Cannot connect to the reader.	The IP address is unknown.	See Communications and Power Connections on page 29 to view the IP address, or use the host name to connect to the reader.

Table 13 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 11 .
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 11 .
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 13 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: <ul style="list-style-type: none"> - 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 34 .
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 11 .
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 34 .
The name, serial number, or IP address entered already exists in the system.	The name, serial number, or IP address entered was already used.	Enter a unique value for the new name, serial number, or IP address.
Another administrator is currently logged in. Try again later.	The system does not allow more than one administrator to log in at a time.	Wait until the other administrator logs out (or times out) before logging in or override the current session with the new one.

Table 13 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
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 setting and storing the changes made during the session.	Select Set Properties to update the network configuration.
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 11 .
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 11
Request method was NULL. No query string was provided.	The system does not permit executing a proxy program from the command line rather than the web server.	No action required. The system is reporting that this action is not permitted.
Content length is unknown.	The system cannot accept an incorrectly formatted HTTP POST request (from an unsupported browser application).	Use a GET request instead, or update the software.
Couldn't read complete post message.	The system stopped a POST operation before completion.	Retry the operation, and allow it to complete.
Unhandled reply type.	The system generated an unexpected value.	Contact Zebra support. See Service Information on page 11 .
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 11 .

Table 13 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
Invalid Device Address.	The device address information (parent) is invalid, missing, or formatted inaccurately.	Contact Zebra support. See Service Information on page 11 .
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 11 .
The action must be confirmed.	The user must confirm the requested action before it is executed.	Select the confirmation option when issuing this request.
Invalid network adapter when navigating to the Bluetooth configuration page.	The Bluetooth dongle is not plugged in or not supported.	Plug in a supported Bluetooth dongle and refresh the browser.
Wireless scan error.	Wireless dongle is not plugged in or not supported.	Plug in a supported wireless dongle and repeat the wireless scan.
Unable to connect to the wireless network.	Access point is off or unreachable.	Turn on the access point and make sure it is accessible.
	Encryption type is not supported in the access point.	Use one of the following supported encryption types: WEP128, WPA/WPA2 and Open.
	The wireless page displays Adapter not found .	Connect the wireless adapter to the reader.
Wireless connection is complete, but no IP address.	No DHCP server is running in the network.	Add a DHCP server to the network.
OS update in progress.	Firmware update on the reader is ongoing. The current operation is not permitted.	Wait for the firmware update to complete and then retry the operation.

Table 13 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
Cannot change password.	Cannot change password for guest.	Guest does not need a password to log in to the Administrator Console.
<p>The following reader web console pages do not load correctly:</p> <ul style="list-style-type: none"> • Advanced Antenna Configuration • ReadTags • Services • Serial Port Communication • FXConnect • License Manager • User Application • Profiles • File based firmware upload • Syslog Export 	Port 8001 is not accessible.	<p>Allow port 8001 to be accessible across the networks.</p> <p>These web pages all use port 8001 to communicate to the reader and without this port the pages cannot function.</p>

Technical Specifications

Technical Specifications

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

Table 14 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

Table 14 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) FX9600-8: 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/IEC 18000-63
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

Table 14 Technical Specifications (Continued)

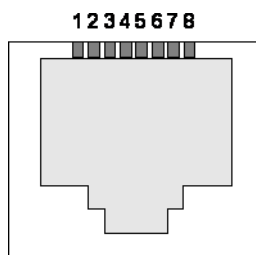
Item	Description
Transmit Power Output	
FX7500	10dBm to +31.5dBm (PoE+, 12V ~ 48V External DC, Universal 24 VDC Power Supply; +10dBm to +30.0dBm (PoE)
FX9600	0dBm to +33.0dBm (PoE+, 12V ~ 24V External DC, Universal 24 VDC Power Supply; +0dBm to +31.5dBm (PoE)
Max Receive Sensitivity	
FX7500	-82dBm
FX9600	-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 118 Ethernet Connections



USB Client Connector

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

Figure 119 USB Client Connector

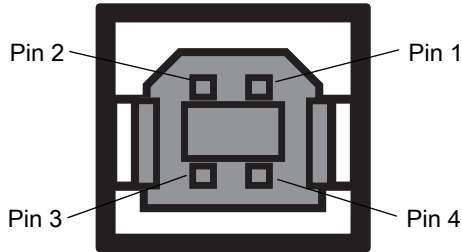


Table 15 USB Client Port Connector Pinout

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 120 USB Host Connector (J22)

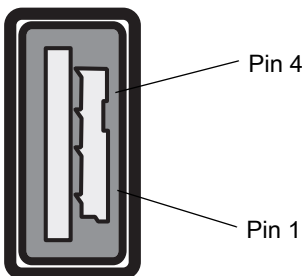


Table 16 USB Host Port Connector (J22) Pinout

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 121 FX7500 RFID Reader GPIO Connection

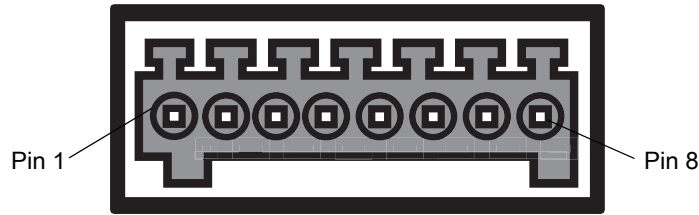


Table 17 FX7500 GPIO Pinouts

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 Connections

The FX9600 GPIO connector pinouts include the following:

Figure 122 FX9600 RFID Reader GPIO Connection



Table 18 FX9600 GPIO Pinouts

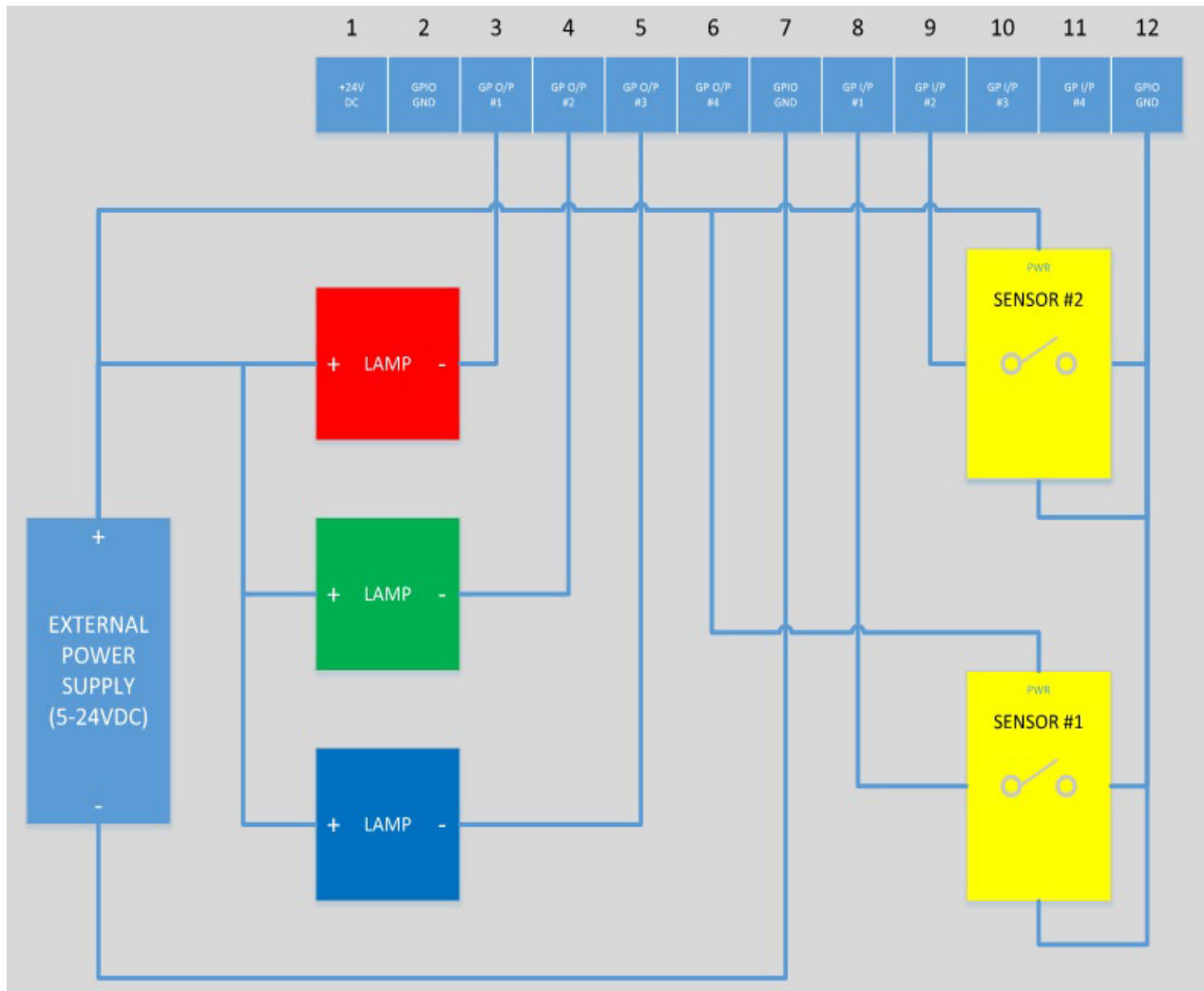
Pin #	Pin Name	Direction	Description
1	+24V DC Power	O	Supplies +24VDC At up to 1 Amp
2	GND	-	Ground connection
3	GP output #1	O	Signal for GP output #1
4	GP output #2	O	Signal for GP output #2
5	GP output #3	O	Signal for GP output #3

Table 18 FX9600 GPIO Pinouts (Continued)

Pin #	Pin Name	Direction	Description
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

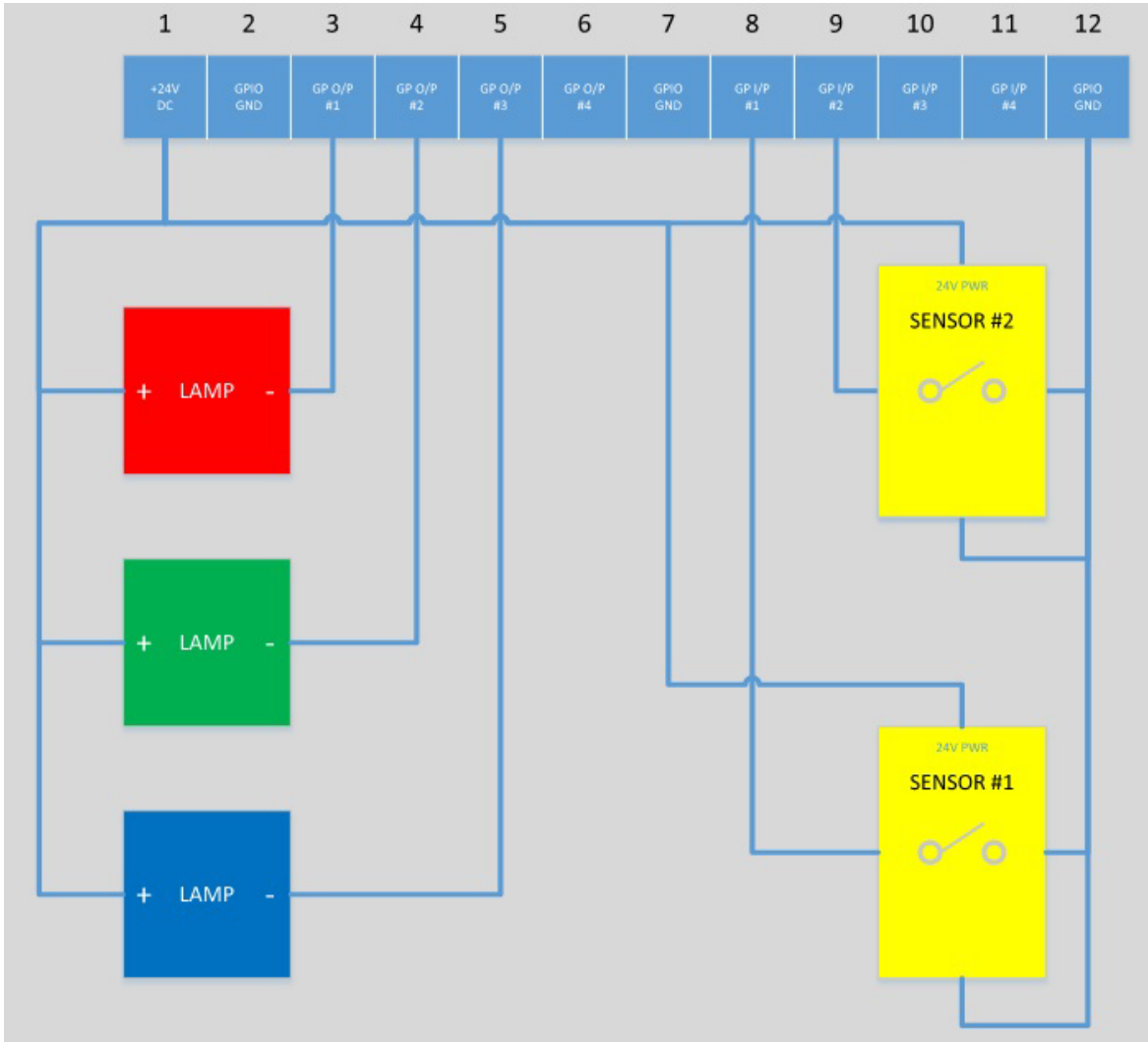
The [Figure 123](#) provides an example of a typical GPIO setup with the power derived from an external power supply.

Figure 123 FX9600 GPIO Setup Example with Power Derived from External Power Supply



The [Figure 124](#) provides an example of a typical GPIO setup with the power derived from GPIO 24V Pin.

Figure 124 *FX9600 GPIO Setup Example with Power Derived from GPIO 24V Pin*



Static IP Configuration

Introduction

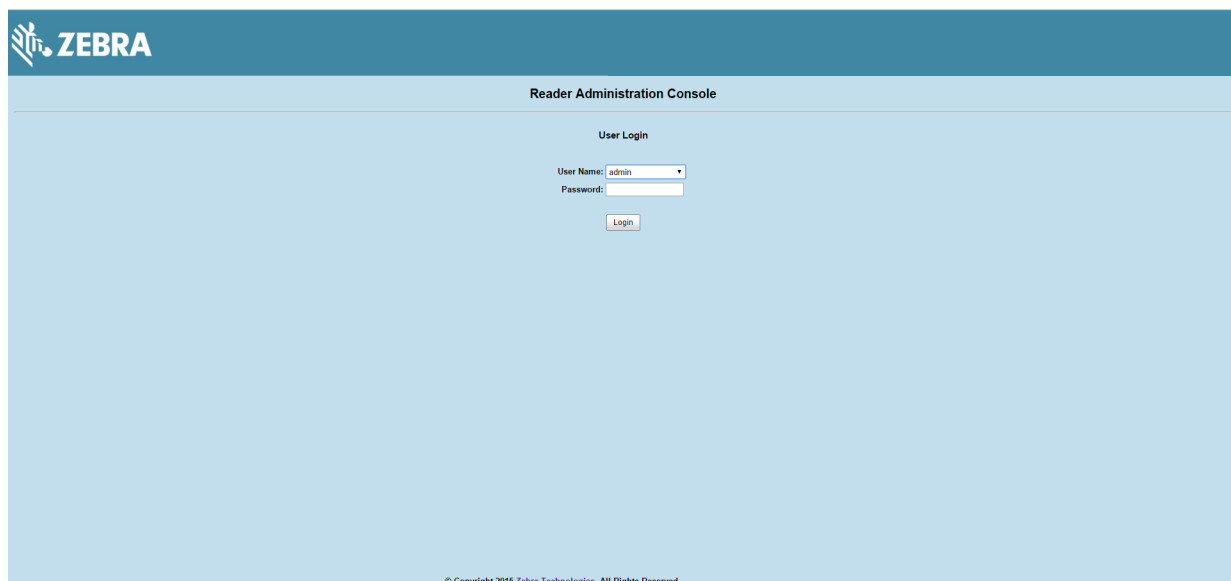
This chapter describes three methods of setting the static IP address on an FX7500 and FX9600 RFID Readers.

Reader IP Address or Host Name is Known

Set the Static IP Using the Web Console

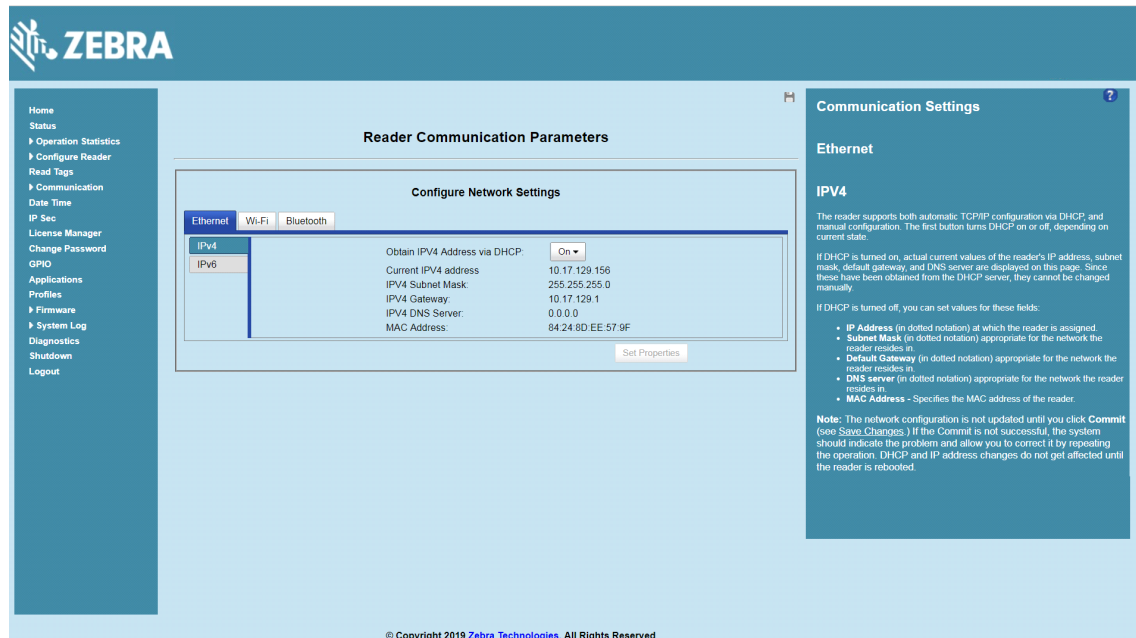
1. Browse the device using the host name, for example: FX7500CD3B1E.
2. Log onto the device.

Figure 125 Reader Administration Console Login Window



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

Figure 126 Reader Communication Parameters Window



5. Select **Set Properties**. You can set a static IP that doesn't belong to this DHCP network.
6. The window displays a **Saving. Please wait...** message with a progress symbol until the commit completes.
7. When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully. The new selection is now set and stored in the reader.
8. 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 127 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 128 Ping the Host Name

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

C:\Users\DRWH67>ping FX7500657E5

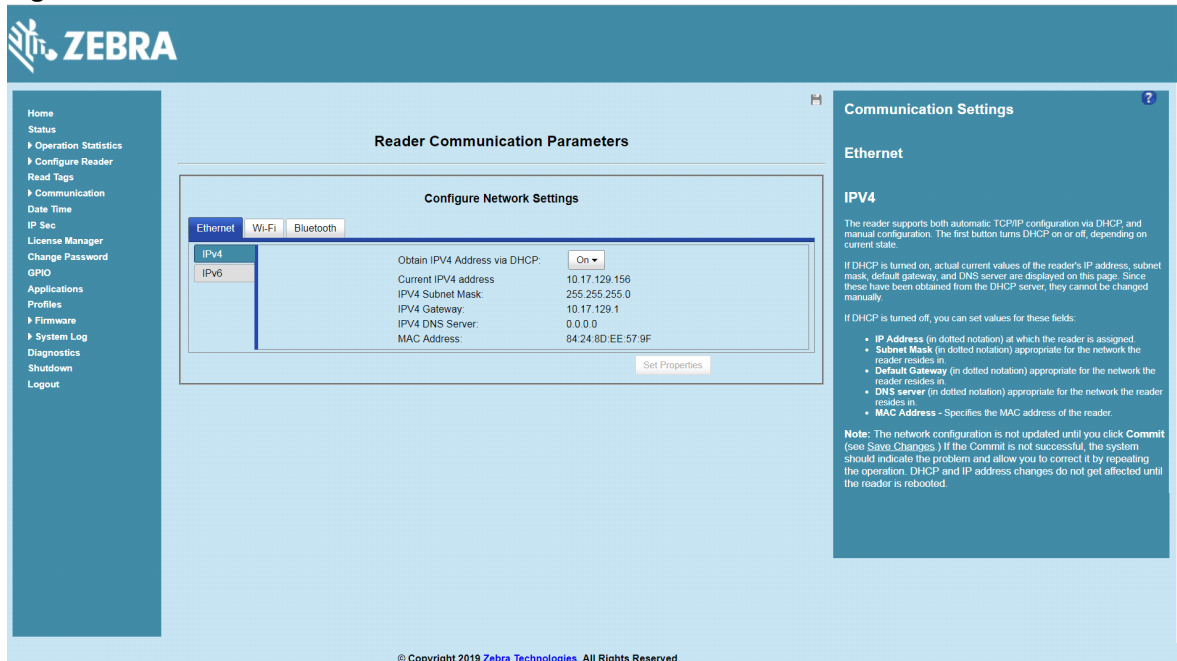
Pinging FX7500657E5.symbol.com [157.235.207.98] with 32 bytes of data:
Reply from 157.235.207.98: bytes=32 time=6ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64
Reply from 157.235.207.98: bytes=32 time<1ms TTL=64

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

Figure 129 Reader Communication Parameters Window



9. Select **Set Properties**.
10. The window displays a **Saving. Please wait...** message with a progress symbol until the commit completes.
11. When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully. The new selection is now set and stored in the reader.
12. 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 19](#) and [Table 20](#). The **Mode Index** column refers to the index used to walk the **C1G2UHFRFModeTable**. Refer to the EPCglobal *Low Level Reader Protocol (LLRP) Standard*.

Table 19 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.

Table 19 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.

Table 20 Radio Modes for ETSI Readers

RF Mode Index	Divide Ratio	BDR Value	M Value M2=2, FM0=1, M4=4, M8=8	FLM Value	PIE Value	Min Tari	Max Tari	Step Tari	Spectral Mask Indicator**	EPC HAG T&C Conformance
1	64/3	120000	2	PR_ASK	1500	25000	25000	0	Dense	false
2	64/3	120000	2	PR_ASK	1500	12500	23000	2100	Dense	false
3	64/3	120000	2	PR_ASK	2000	25000	25000	0	Dense	false
4	64/3	120000	2	PR_ASK	2000	12500	23000	2100	Dense	false
5	64/3	128000	2	PR_ASK	1500	25000	25000	0	Dense	false
6	64/3	128000	2	PR_ASK	1500	12500	23000	2100	Dense	false
7	64/3	128000	2	PR_ASK	2000	25000	25000	0	Dense	false
8	64/3	128000	2	PR_ASK	2000	12500	23000	2100	Dense	false
9	64/3	160000	2	PR_ASK	1500	12500	18800	2100	Dense	false
10	64/3	160000	2	PR_ASK	2000	12500	18800	2100	Dense	false
11	64/3	60000	4	PR_ASK	1500	25000	25000	0	Dense	false
12	64/3	60000	4	PR_ASK	1500	12500	23000	2100	Dense	false
13	64/3	60000	4	PR_ASK	2000	25000	25000	0	Dense	false
14	64/3	60000	4	PR_ASK	2000	12500	23000	2100	Dense	false
15	64/3	64000	4	PR_ASK	1500	25000	25000	0	Dense	false
16	64/3	64000	4	PR_ASK	1500	12500	23000	2100	Dense	false
17	64/3	64000	4	PR_ASK	2000	25000	25000	0	Dense	false
18	64/3	64000	4	PR_ASK	2000	12500	23000	2100	Dense	false
19	64/3	80000	4	PR_ASK	1500	12500	18800	2100	Dense	false
20	64/3	80000	4	PR_ASK	2000	12500	18800	2100	Dense	false
*21	64/3	variable	variable	PR_ASK	variable	12500	25000	variable	variable	false
22	64/3	320000	1	PR_ASK	1500	12500	18800	2100	Dense	false
23	64/3	320000	1	PR_ASK	2000	12500	18800	2100	Dense	false
24	64/3	30000	8	PR_ASK	1500	25000	25000	0	Dense	false
25	64/3	30000	8	PR_ASK	1500	12500	23000	2100	Dense	false
26	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
27	64/3	30000	8	PR_ASK	2000	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.

Table 20 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
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	13, 19, 20, 21, 23
123RFID Desktop	
features	37
requirements	37

A

administrator console	38
applications	100
committing changes	103
communication settings	68
configure network services	74
configure network settings	68, 69, 70
configuring system log	108
discarding changes	103
firmware version	102, 103
GPIO	99
IPV6 sec	97
login	43
main screen	45
managing login	99
reader diagnostics	109
reader profiles	101
scan control	17, 67
set password	98
setting date and time	96
shutting down	110
status	47
system log	107
air link	151
antennas	
configuring	55
installing	28
ports	13, 19, 20, 21, 22
applications	100

B

bluetooth	119, 120
connecting	119, 120

C

cable pinouts	
ethernet	142
GPIO	144
USB	143
USB client	143
USB host	143
chapter descriptions	10
commit region change	15
committing changes	103
communication	20, 22
ethernet, wired	29
communication settings	68
configure	
antenna	55
LLRP	71
read points	54, 55
reader	53
region	56
SNMP	72
static IP	147
static IP via web console	147, 149
wireless	73
configuring network	
bluetooth	70
ethernet	68
services	74
wi-fi	69
connecting	
to reader	41
via bluetooth	119, 120
via host name	42
via IP address	42
via wi-fi	116
connection	
antennas	28
communication	29
port diagram	22
ports	19, 21
wired ethernet	29
conventions	

notational 11
 copying files 122, 155
 country list 15

D

data protection 156
 date 96
 deployments 39
 discarding changes 103

E

ethernet
 pinouts 142
 POE 30
 port 20, 23
 setup 29, 30
 wired 29
 event statistics 51

F

files
 copying 122, 155
 firmware
 version 102, 103
 firmware update 102, 103, 126
 prerequisites 124
 first time login 14, 43
 FTP
 copying files 122, 155
 FTPS
 copying files 155
 FX Connect
 http proxy server 85
 licensing
 acquisition modes 90
 activating 94
 cloud acquisition 90
 download capability response 93
 local license server acquisition 91
 managing license 91, 94
 off-line acquisition 93
 licensing evaluation
 enabling license 89
 perpetual license 89
 licensing model 89
 running inventory 83
 USB HID 85
 using 77

G

GPIO 13, 19, 21

GPIO connections 144
 pinouts 144
 port 20, 22
 GPIO control 99

H

host communication
 ethernet, wired 29
 host name connect 14

I

information, service 11
 initiating reads 17, 67
 installation
 antennas 28
 communication connection 29
 mounting 25
 IP address 41
 IP ping 41

L

LEDs 20, 23
 LLRP
 configure 71
 radio modes 151, 153
 log 107
 configuring 108
 login 43
 first time 43
 managing 99

M

mounting 25, 27
 concrete wall mounting 27
 drywall mounting 27
 wood or metal wall mounting 27
 mounting plate 25
 multiple reader deployments 39

N

NXP
 statistics 50, 52

O

obtain reader IP address 41

P

Password 14, 126, 132

password 14, 43, 126, 132
 changing 98
 pinouts
 ethernet 142
 GPIO 144
 USB 143
 USB client 143
 USB host 143
 POE 13, 19, 20, 21, 23, 30, 142
 ports 19, 21
 descriptions 20, 22
 ethernet 29
 power 13, 19, 21
 POE 30
 port 20, 23
 profiles 101

R

read points 54, 55
 reader
 configuration 53
 connecting 41
 GEN2 statistics 49
 profiles 101
 statistics 48
 event 51
 NXP 50, 52
 status 47
 reading tags 35
 initiating 17, 67
 rear panel 13, 22
 reboot 39
 region 44
 region configuration 56
 region control 44
 region setting 15
 region settings 15
 reset 13, 19, 20, 21, 22
 RFID
 FX reader 18, 21
 RJ45 20, 23

S

SCP
 copying files 122, 155
 service information 11
 set region 15, 44
 setting date 96
 setting time 96
 setup
 wired ethernet 29
 wired ethernet AC outlet 29
 wired ethernet, power-over 30

shutdown 110
 SNMP
 configure 72
 software update 126
 specifications 140
 start-up 14
 static IP configuration 147
 via web console 147, 149
 Statistics 51
 statistics 48
 event 51
 GEN2 49
 NXP 50, 52
 status 47
 system log 107
 configuring 108
 system time 96

T

tags
 reading 35, 67
 technical specifications 140
 time 96
 tool for RFID readers - 123RFID Desktop 36
 troubleshooting 134

U

unpacking 24
 updating firmware 102, 103, 126
 prerequisites 124
 updating software 126
 USB 13, 19, 21, 116, 127
 client pinouts 143
 host pinouts 143
 pinouts 143
 user ID 43
 user name 14, 126, 132
 user password 43

V

version control 102, 103

W

wi-fi 116
 connecting 116
 wired ethernet 29
 wireless
 configure 73

Z

zero-configuration networking42

