FX SERIES RFID FIXED READER

Integration Guide

ZEBRA

MN-000026-17EN Rev. A

FX SERIES RFID READER INTEGRATION GUIDE

MN-000026-17EN

Revision A

JAN 2026

Copyright

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: 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: - 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. - 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: - FX9600 Bluetooth dongle support information. - Air Protocol ISO/IEC 18000-63.
-09 Rev A	9/2018	Added: - "Requirements" section to "Quick Start". - "Install" below Applications. - FX9600 Serial Port Data Configuration. Updated: - "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: - 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	Added: - FX Connect information. - New troubleshooting information. - New Important statement in the Connecting FX7500 and FX9600 RFID Reader Antennas section. Updated: - 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
-11EN Rev A	4/2020	Updated: - FX series operating system - Network Services Settings section - FX Series Licensing Management section - Reader Profile section - Reader Configuration via USB Thumb Drive section. Added: - Example JSON format of Tag Data section - Example Key-Value Pair format of Tag Data section - Licensing errors troubleshooting - 2-step firmware update - Ethernet/IP section - Cellular Connectivity with Sierra Modem section - SOTI MOBI Client section - Moving vs Stationary section - REST RCI Support section.
-12EN Rev A	4/2020	- Updated the Procuring Licenses section. - Added notes that mentioned the FX7500 Reader does not support Network Connect (EtherNet/IP). - Updated Table 12. - Updated Figure 12.
-13EN Rev A	9/2020	Added: - An important note at the FX Series Licensing Management introduction section. - A note in the Acquiring License from Production Server (ON-Line) section. - Licensing Error Logs. Updated the Troubleshooting section.
-14EN Rev A	5/2021	Updated the SFDC Forms link in the Procuring Licenses section.

Change	Date	Description
-15EN Rev A	3/2022	Updated: - Changed Zero-Configuration to Link Local - Certificate Configuration - Configure LLRP Settings Window - Supported Wi-Fi Dongles in Wireless Settings - Defaults in FX9600 Serial Port Configuration - FX Connect - Modified Reset Reader to Factory Defaults to Enterprise Reset the Reader - Supported Bluetooth Dongles in Connecting to a Peer Device Over Bluetooth Using a Bluetooth Dongle - Cellular Connectivity with Sierra Modem - Header in Cellular Connectivity with Sierra Modem - Moving and Stationary Tags Added: - Section NTP Statistics - Bullets for the following in Administrator Console Option Selections: Zebra IoT Connector Configuration Connection 802.1x EAP - Reconnect to Server bullet in Configure LLRP Settings - 802.1x EAP Configuration in Administrator Console
-16EN Rev A	12/2024	- Removed FX Connect section and REST RCI Support section. - Updated: Table 21: Radio Modes for ETSI Readers and FTP/SCP-Based Update. - Added SSH Key Management and Security Recommendations.
-17EN Rev A	1/2026	- Removed license manager components - Eliminated all license manager functionality and related details - Updated web UI screenshots - Replaced all user interface images to reflect the application without license manager features - Added updates featuring EU-RED changes New section: - Compliance and Implications of EU RED for the FX7500/FX9600

Table of Contents

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.
- *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.
- *Firmware Upgrade* provides reader firmware upgrade information on using the web-based **Administrator Console** and an FTP or FTPS server running a host computer.
- *EtherNet/IP* provides the overview of EtherNet/IP for FX Series RFID reader.
- *Cellular Connectivity with Sierra Modem* includes the information on how to configure the Sierra Modem RV50X to provide cellular connectivity for the FX9600 RFID Reader.
- *SOTI MOBI Client* provides information on SOTI Mobicontrol and includes references to the appropriate guides.
- *Gen2 V2 Enhancement* describes the Gen2V2 commands supported by the FX Series RFID Reader and includes the reference to the appropriate guide.
- *Reader Configuration via USB Thumb Drive* includes the steps to transfer a reader configuration to another reader via a USB thumb drive.
- *GPS and Triggers for Trucking and Delivery* provides information on the GPS feature and three new triggers for trucking and delivery.

- *Moving and Stationary Tags* recommends the LLRP and RFID3 APIs configurations to read the moving and stationary tags.
- *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 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 (for example, 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 (describes Low Level Reader Protocol (LLRP) and Reader Management (RM) extensions for the reader), p/n 72E-131718-xx
- RFID Demo Applications User Guide (provides instructions for using sample applications which demonstrate how to use Zebra RFID readers), p/n 72E-160038-xx
- 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)
- Programmer's Guide provided with the Zebra RFID SDK (this introductory guide describes how to perform various functions using the RFID3 API set)
- RFID3 API
- EPCglobal Low Level Reader Protocol (LLRP) Standard.

For the latest version of these guides and software, visit: 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: 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

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

1. Unpack the reader. See Unpacking the Reader on page 32.
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 42 for boot-up details.

Figure 1 FX7500 RFID Fixed Reader Rear Panel Connections

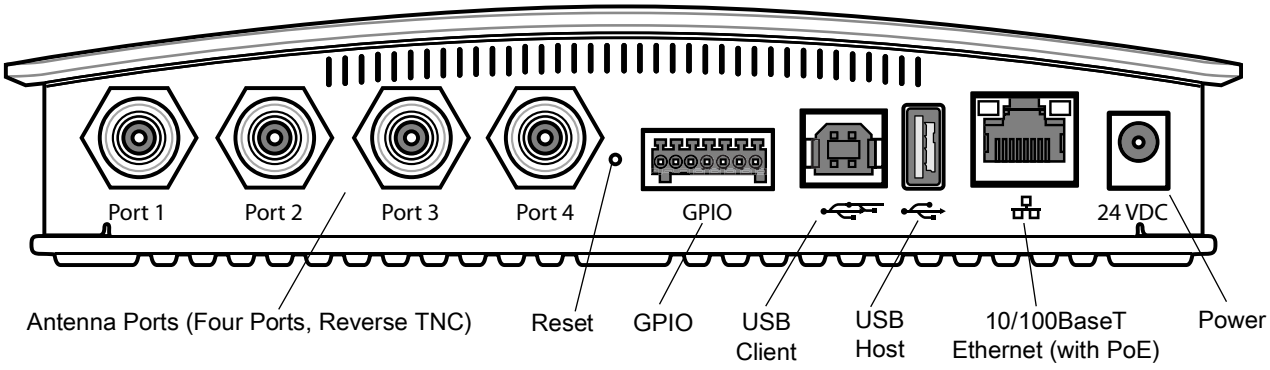
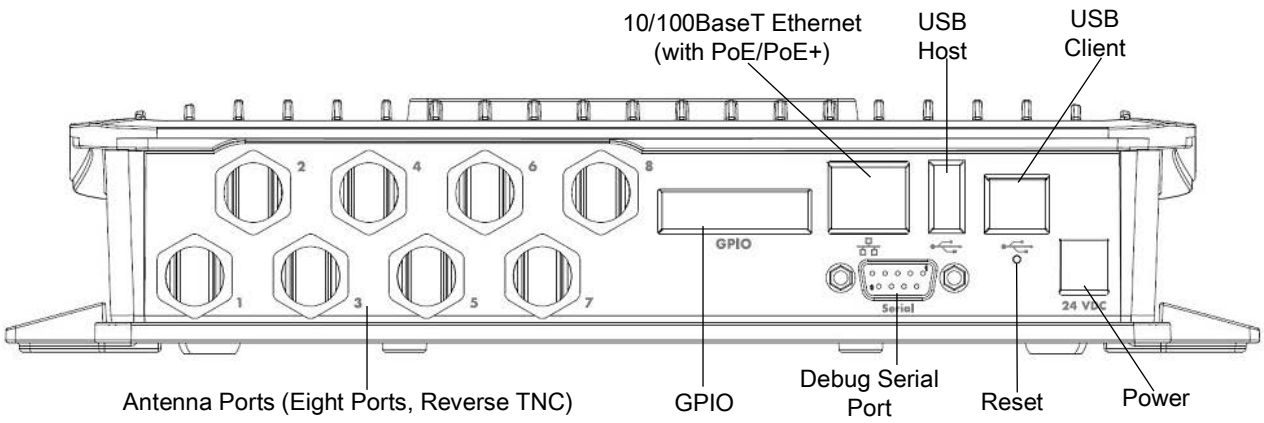


Figure 2 FX9600 RFID Fixed Reader Rear Panel Connections



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.

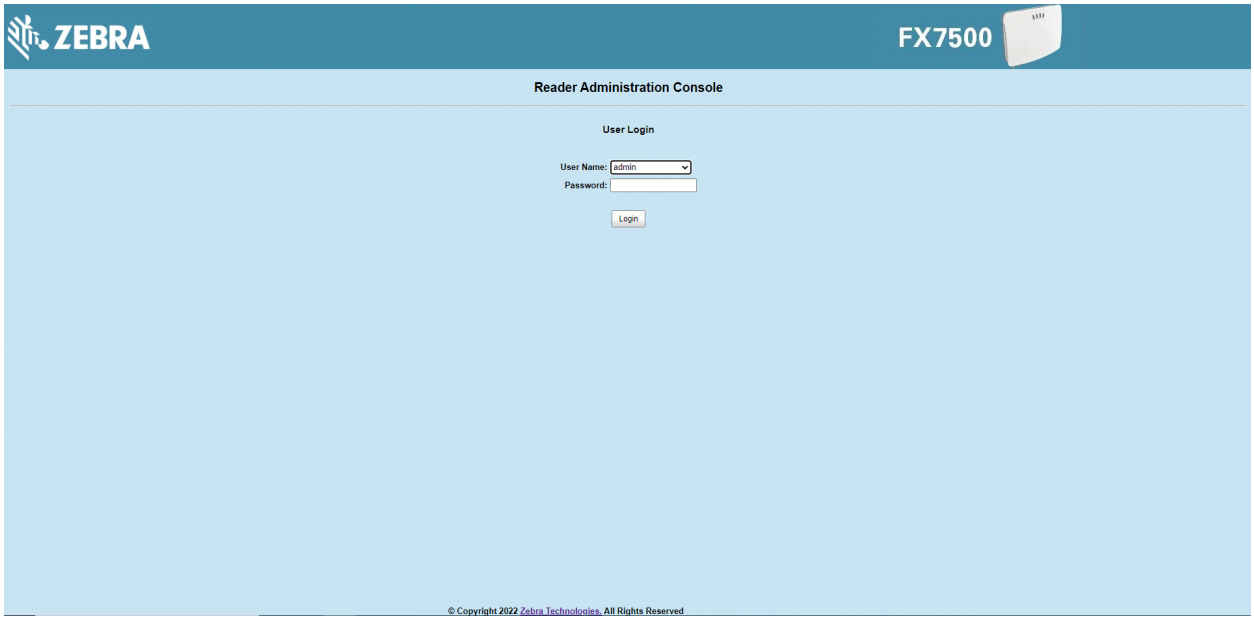
NOTE: Connect the reader to a network that supports host name registration and lookup to ensure the network can access the reader using the host name. For instance, some networks can register host names through DHCP. When first connecting to the reader, it is recommended to keep DHCP enabled in both 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 or Start-Up Login

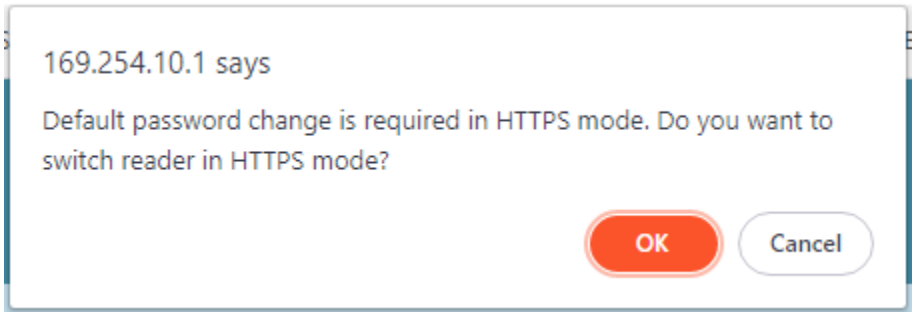
When starting the reader for the first time the reader will force the user to change the admin password. To log in for the first time, and change the password, follow the steps below:

1. In the **User Login** window, select admin in the **User Name** drop-down menus and enter **change** in the **Password** field and click **Login**.

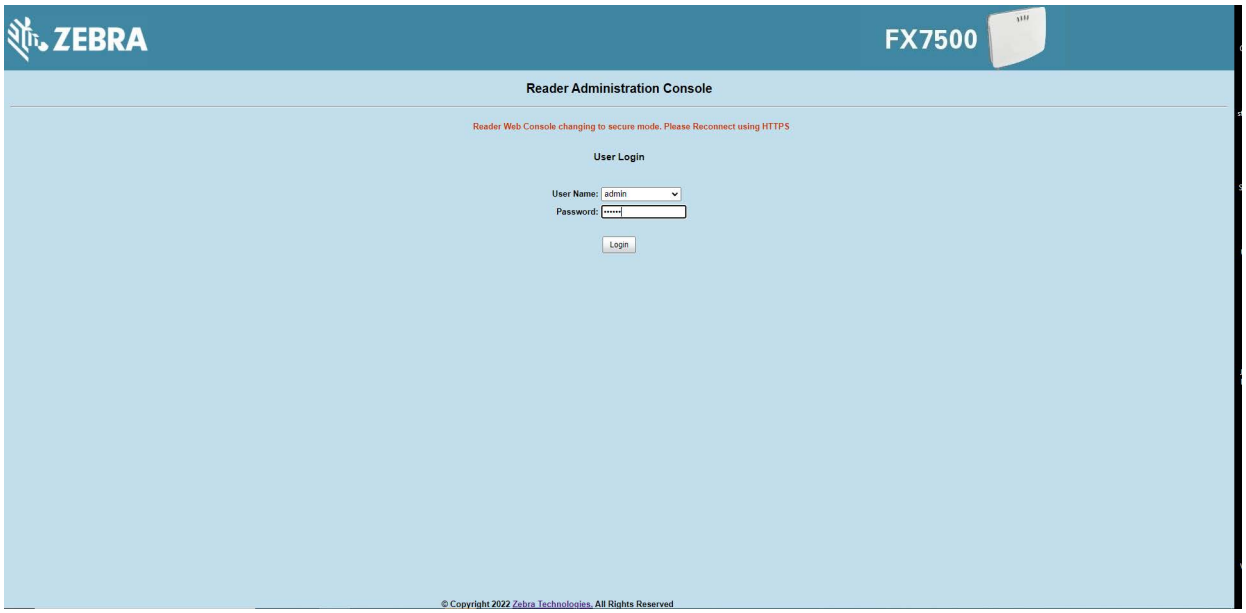
Figure 3 User Login Window



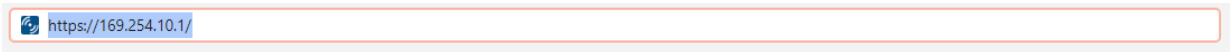
2. A dialog will appear, indicating that the reader login is performed using the default password and the reader needs to switch to HTTPS mode to allow the user to change the password. Click **OK**.



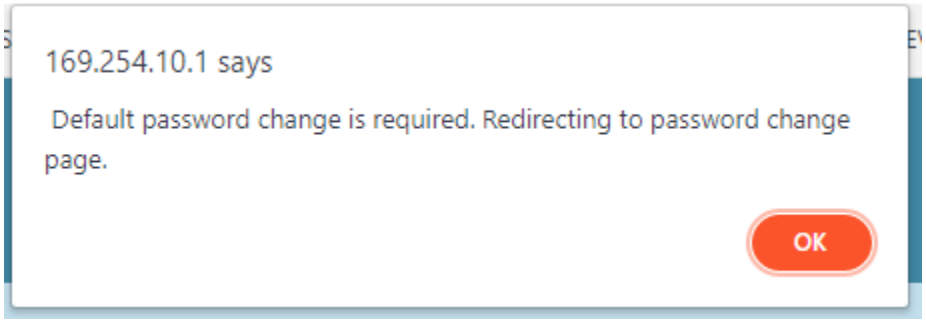
3. Reader will now switch to HTTPS mode and display the message asking the user to log in again using HTTPS mode.



4. Change the URL in the browser address box to use HTTPS instead of HTTP and press Enter. Since the reader starts up with a self signed certificate, the browser might issue a warning about it not being able to verify the certificate. Accept any risks and continue.



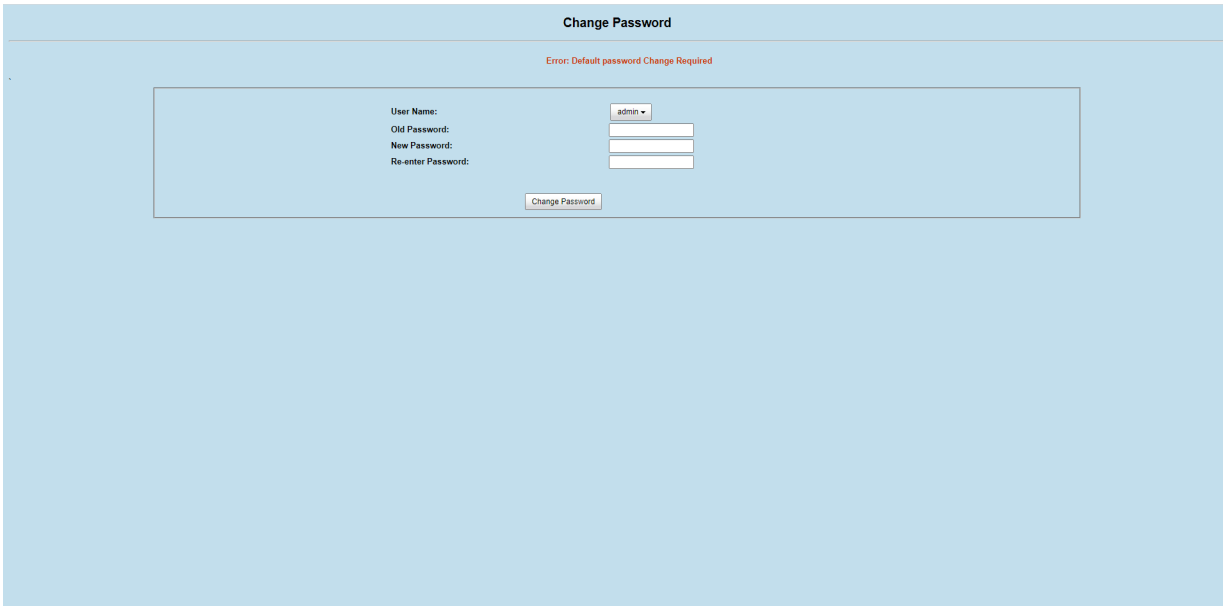
5. Type **change** in the **Password** field again and click on Login. Click **OK** on the web dialog, when it says that it will redirect you to change password page.



6. A Change Password page will appear. Enter the **Old Password** as **change** and enter the **New Password.** **Re-enter new password** to confirm.

Enter your password that should satisfy the following criteria:

- Should contain minimum of 8 and maximum of 15 characters
- English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)
  - A password must be at least 8 characters and no more than 32 characters in length.
  - Should not use previously used five passwords



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. On the **Configure Region Settings** window (see Figure 4):
   a. Select the region from the drop-down menu.
   b. Select the **Communication Standard**, if applicable.
   c. Select **Frequency Hopping**, if applicable.
   d. Select the appropriate channel(s), if applicable.
   e. Select the **I understand** check box.
2. 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.
3. When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully. See Commit/Discard Functionality Changes on page 106 for more information.

Figure 4 Selecting the Region

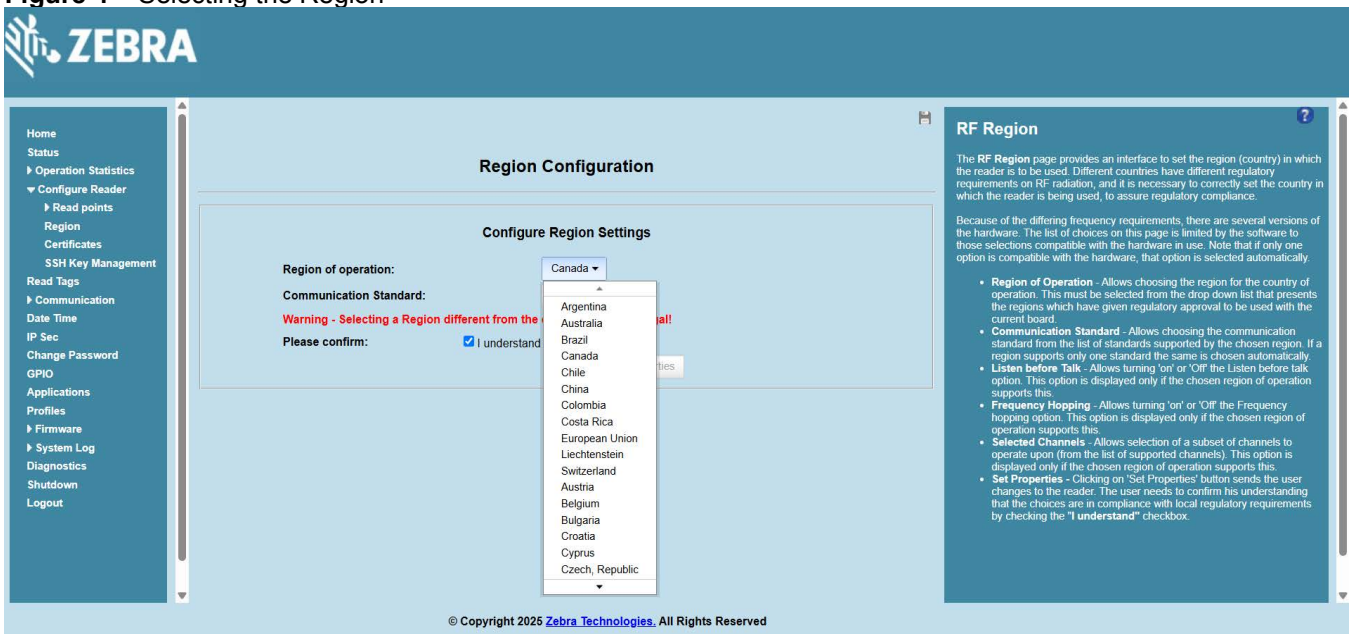
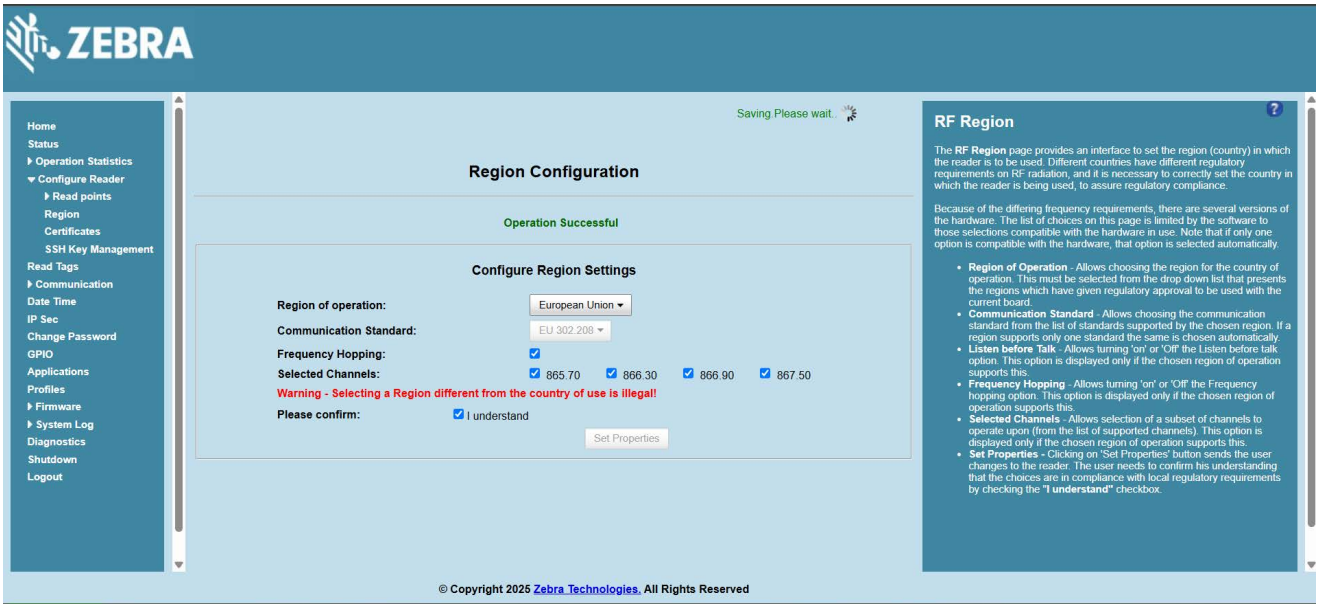
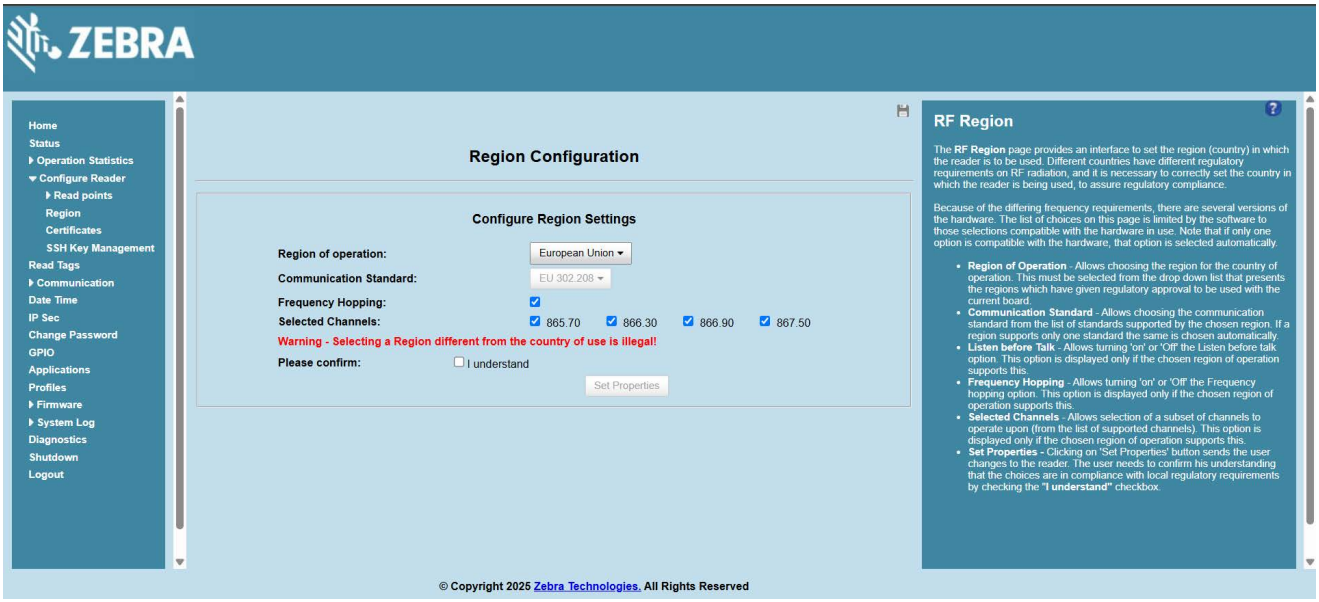


Figure 5 Region Configuration, Operation Successful Window

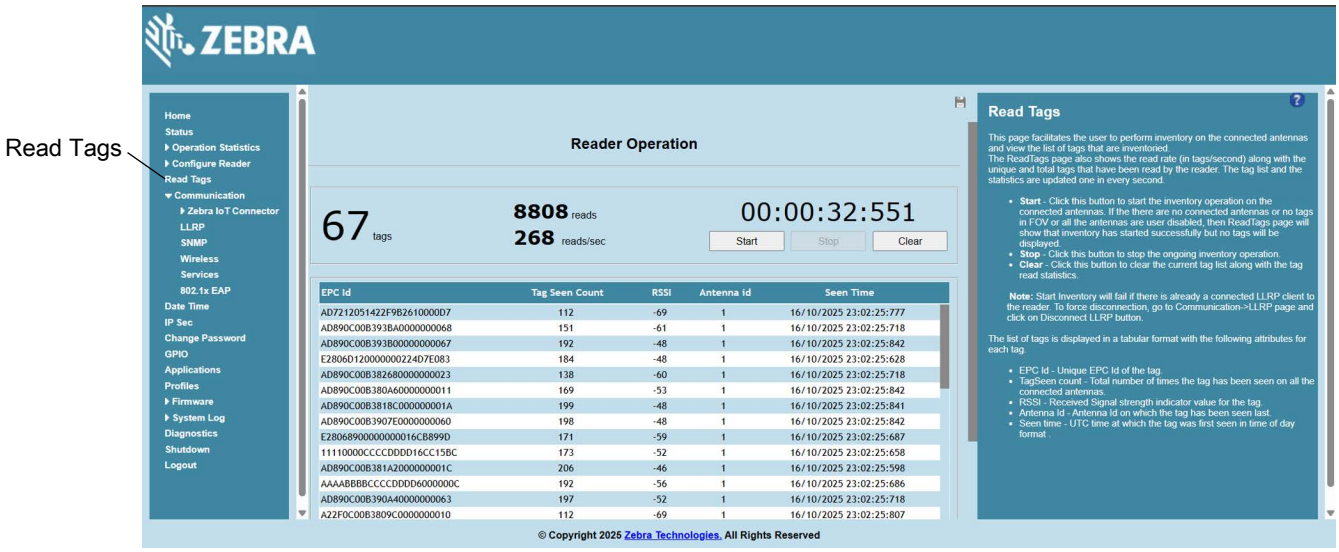




Step 5, Read Tags

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

Figure 6 Read Tags Window



On the Reader Operation window (see Figure 6):

- 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 is 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[1]	Linux v4.9	Linux v4.9
Java	OpenJDK Run time v1.8 JVM OpenJDK Zero build 25.102-b14	Run time v1.8 JVM OpenJDK Zero build 25.102-b14
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

[1]The Linux kernel and tool chain for embedded application development have been updated starting with version 3.0.35. Applications created with older tool chain need to be recompiled with new embedded SDK. If recompiling is not an option, please see note on reverting back to older firmware version in Firmware Update section.

Table 1 FX Series RFID Reader Features (Continued)

Feature	Zebra FX7500	Zebra FX9600
RX Sensitivity	-82 dBm	-86 dBm
IP Sealing	IP40	IP53
Power-Over-Ethernet	Yes	Yes
Embedded Applications	Yes	Yes
SDKs Embedded[1] Applications: Host Based Applications:	 C, Java C, Java, .Net	 C, Java C, Java, .Net
Wi-Fi/Bluetooth Dongle Support	Yes	**Yes**
[1]The Linux kernel and tool chain for embedded application development have been updated starting with version 3.0.35. Applications created with older tool chain need to be recompiled with new embedded SDK. If recompiling is not an option, please see note on reverting back to older firmware version in Firmware Update section.		

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

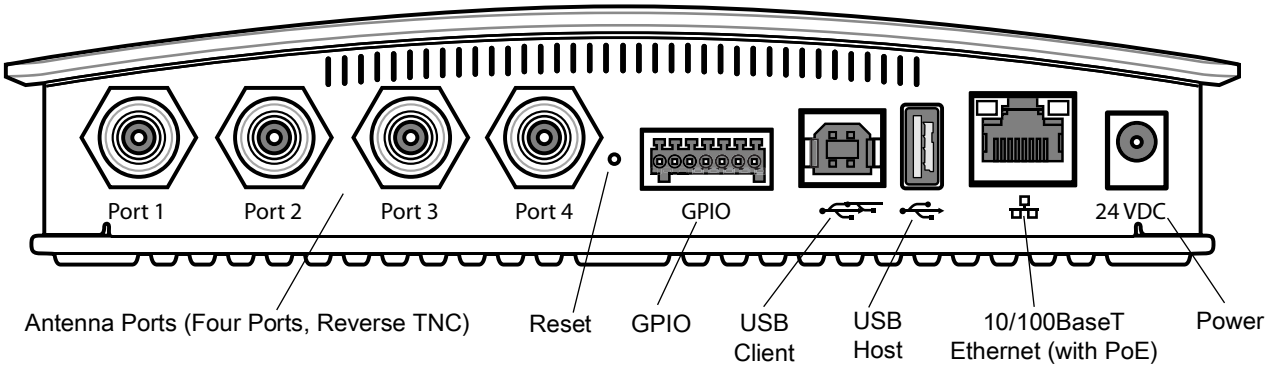
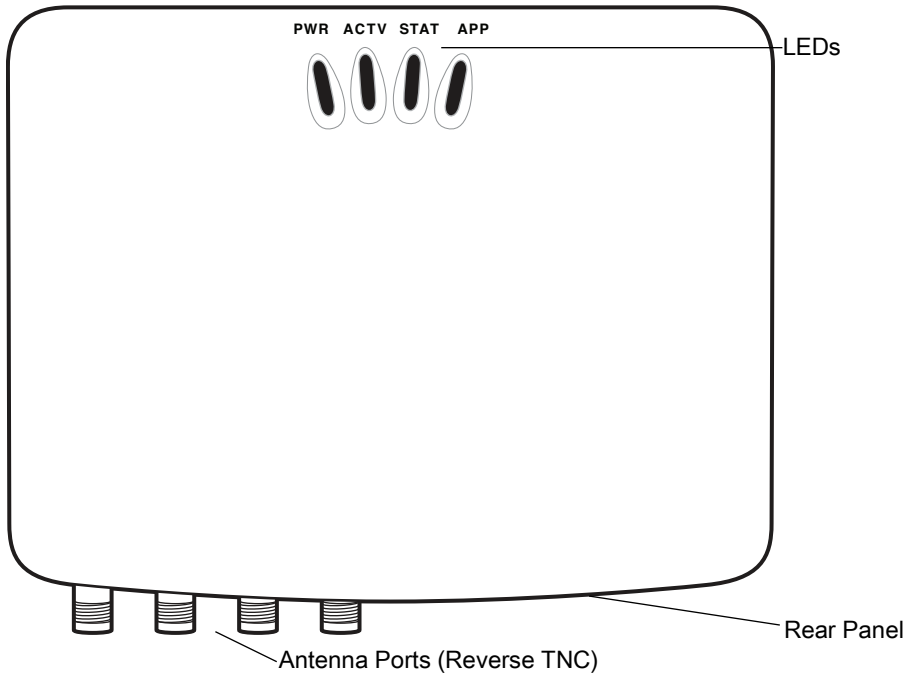


Figure 8 FX7500 RFID Reader



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 184 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 36 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 41 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 38 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.

Table 2 Rear Panel Descriptions

Port	Description
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 37 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 42.

Figure 9 FX7500 RFID Readers LEDs

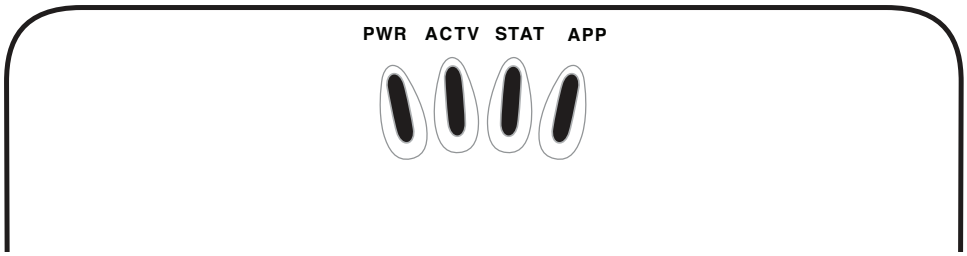


Table 3 FX7500 LED Indications

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 Red 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 On for 2 seconds indicates IoT connector connects and disconnects
APP	Application	Green/Red/Amber	Controlled through RM

FX9600 Parts

Figure 10 FX9600 RFID Reader Rear Panel Connections

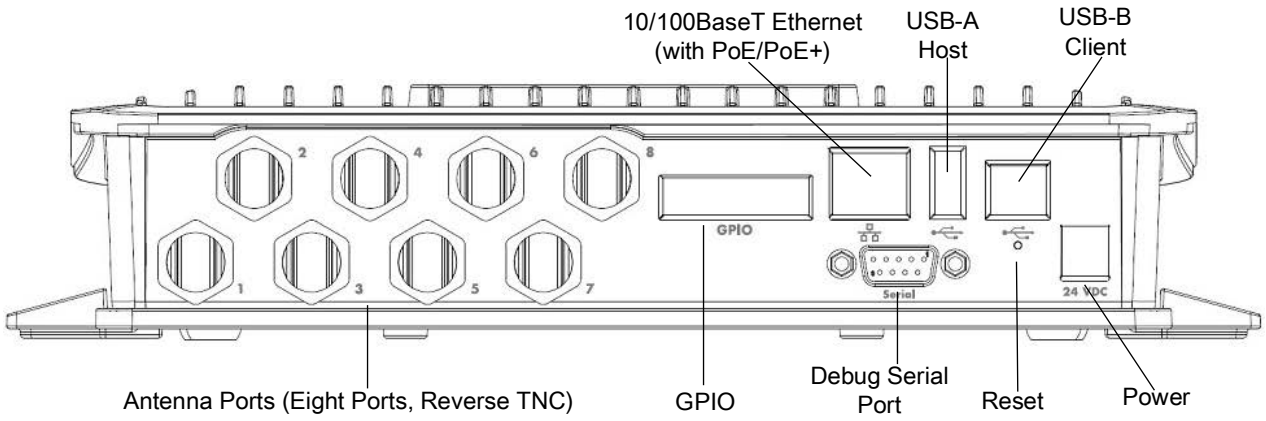
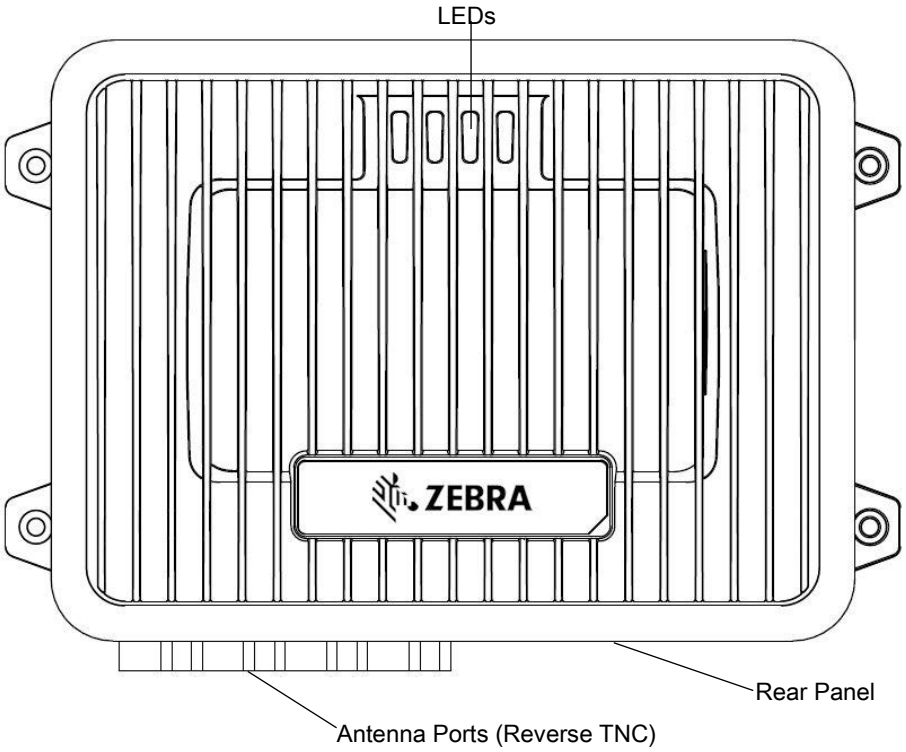


Figure 11 FX9600 RFID Reader



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)	Four port version: Connect up to four antennas. Eight port version: Connect up to eight antennas. See Table 14 on page 184 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 36 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 41 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 38 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.
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 37 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 42.

Figure 12 FX9600 RFID Readers LEDs

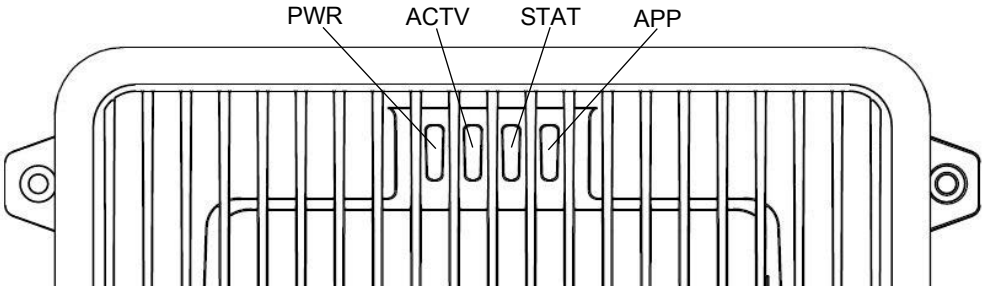


Table 5 FX9600 LED Indications

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:

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

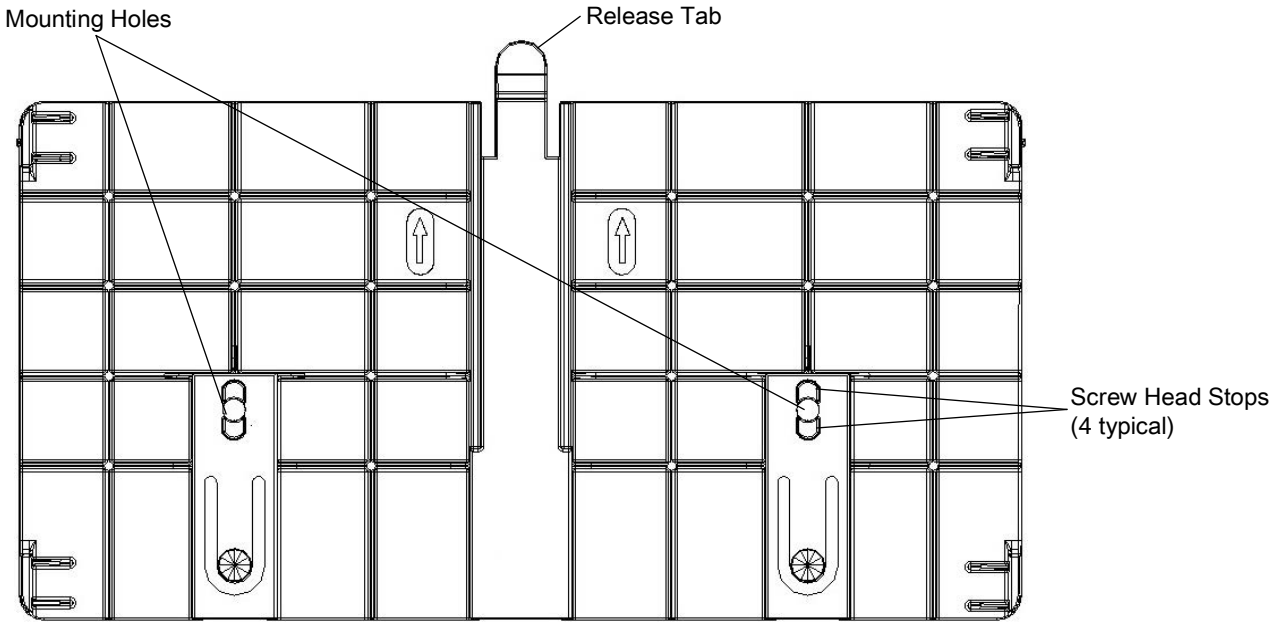
WARNING: For Mounting in Environmental Air Handling Space (EAHS): Do not install the Bracket, Cables in the EAHS unless they are suitable for use in EAHS per UL 2043.

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 on page 34.
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 in. diameter by 7/8 in. deep holes. For drywall/masonry surfaces, drill two 3/16 in. diameter by 7/8 in. 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:

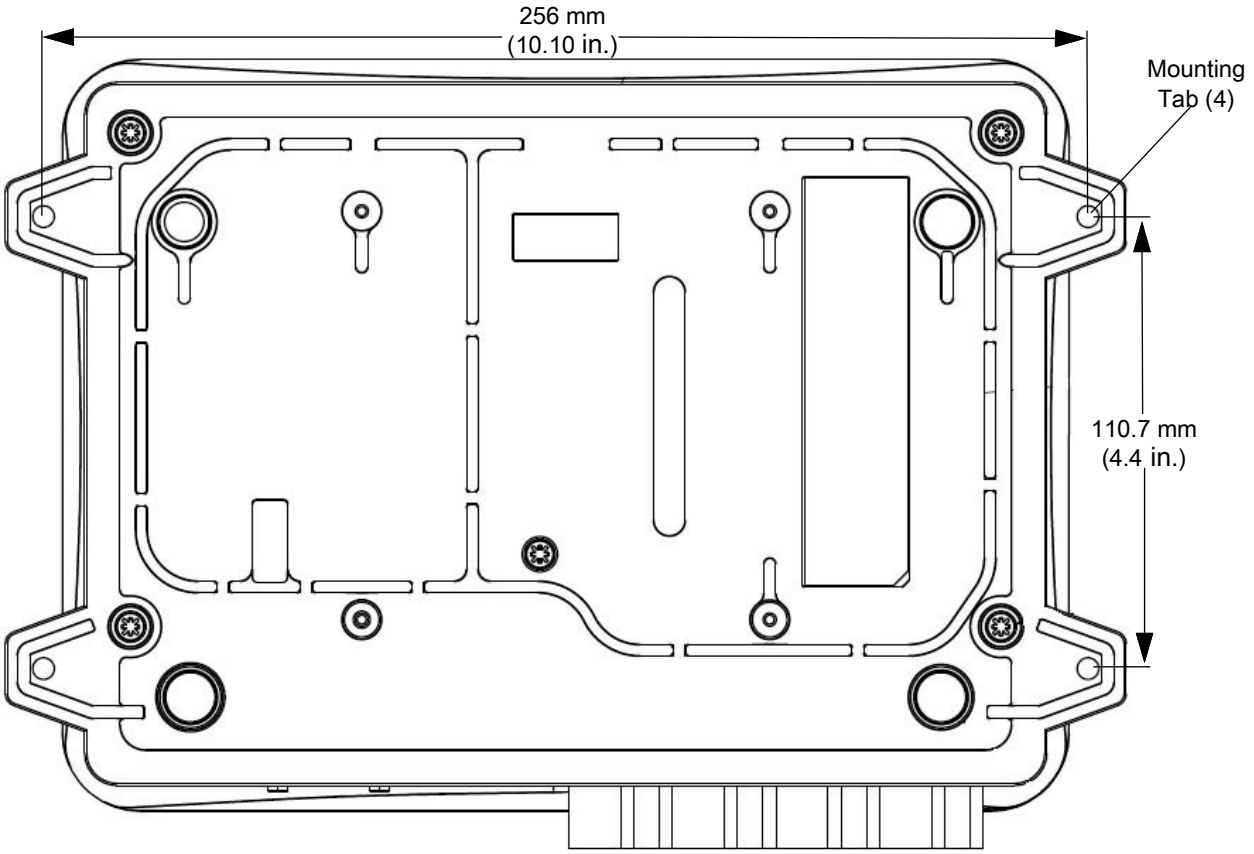
1. Use the mounting bracket as a template to locate the holes, or locate and mark the holes on 4 3/16 in. centers, +/- 1/32 in.
2. For wood surfaces, drill two 1/8 in. diameter by 7/8 in. deep holes on 4.192 in. centers. For drywall/masonry surfaces, drill two 3/16 in. diameter by 7/8 in. deep (min) holes on 4.192 in. 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 on page 37):

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

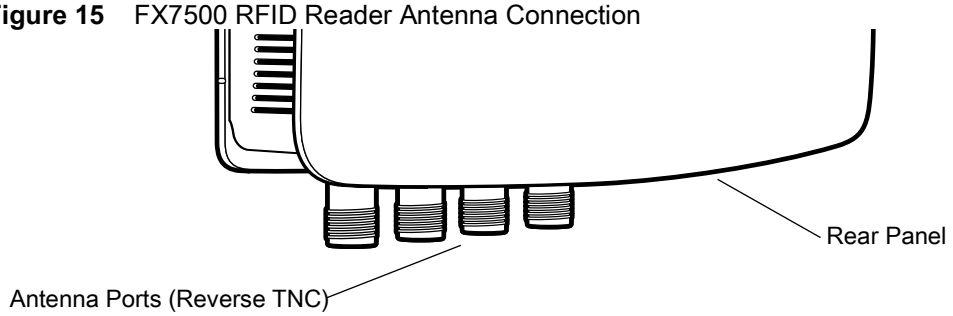
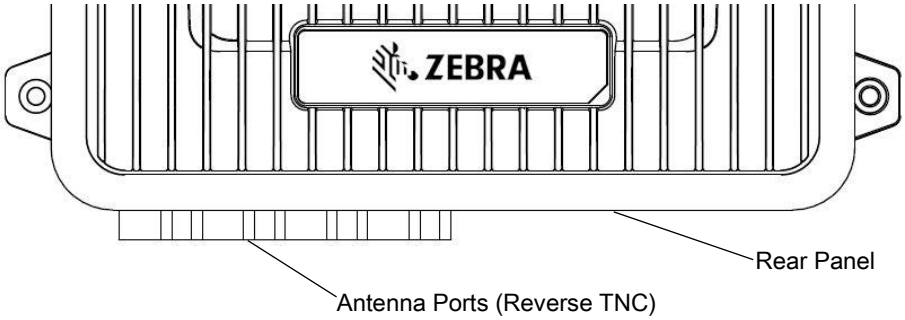


Figure 16 FX9600 RFID Reader Antenna Connection



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 26) or FX9600 reader (see Figure 10 on page 29).
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 42.

9. On a networked computer, open an Internet browser and connect to the reader. See Connecting to the Reader on page 49.
10. Log in to the **Administrator Console**. See Administrator Console Login on page 51.

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 26 or Figure 10 on page 29.
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 42.
4. On a networked computer, open an Internet browser and connect to the reader. See Connecting to the Reader on page 49.
5. Log in to the **Administrator Console**. See Administrator Console Login on page 51.

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 40 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 26 or for the FX9600, see Figure 10 on page 29. 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 39).

To install the RNDIS driver on the host.

1. Download the installer file **Zebra RNDIS.msi** from 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**.

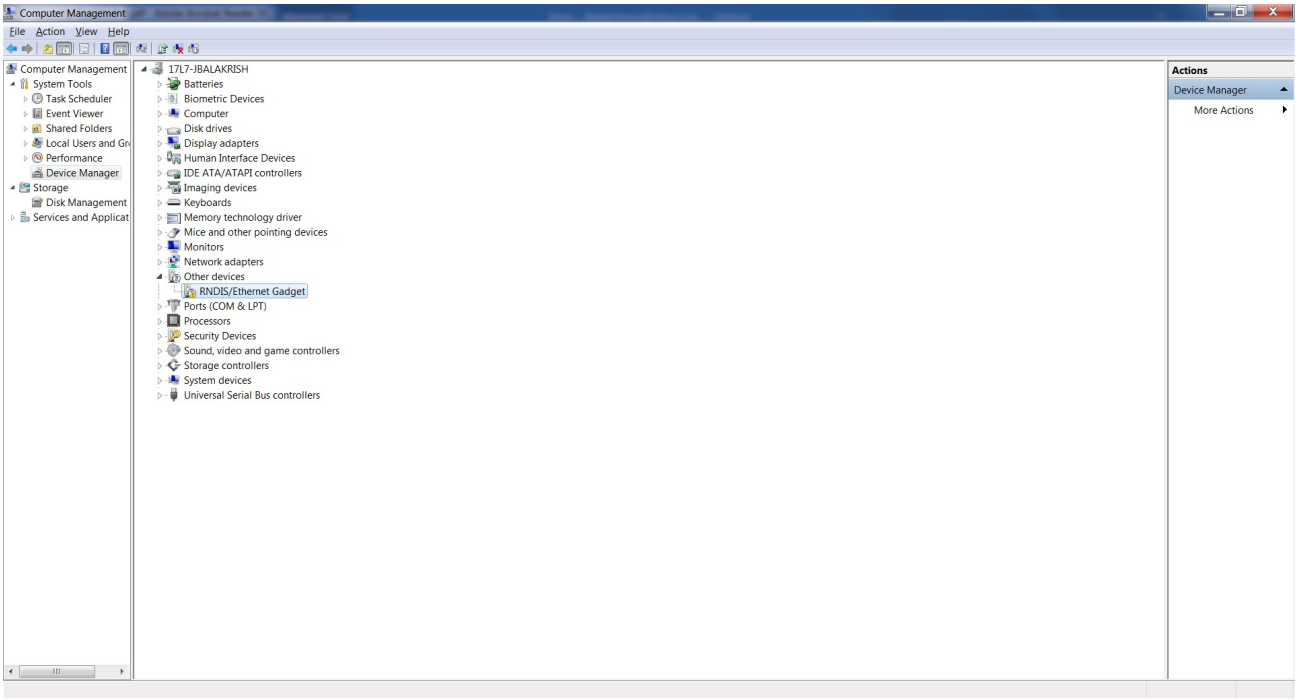
7. Select **Finish** to complete the installation. This assigns the host an auto-configured IP address. The network is now ready to use and the reader's IP address is fixed to 169.254.10.1.

Microsoft RNDIS Driver for Windows 7

The following steps are the recommended procedure for Windows 7:

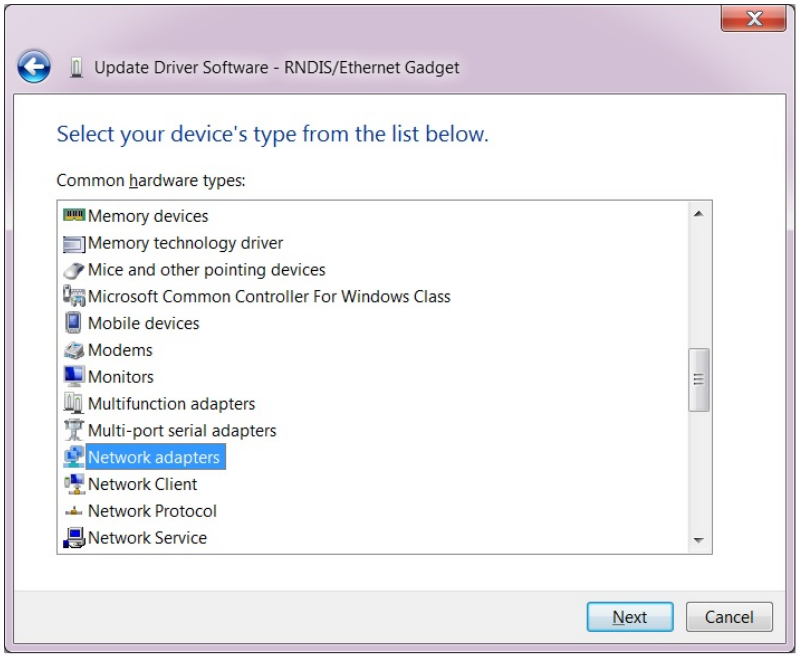
1. After connecting a USB cable between the PC and reader, the RNDIS driver automatically installs. If it does not, right-click on **Computer** and select **Manage**. From **System Tools**, select **Device Manager**. Under **Other Devices**, look for an entry for RNDIS with an exclamation icon indicating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

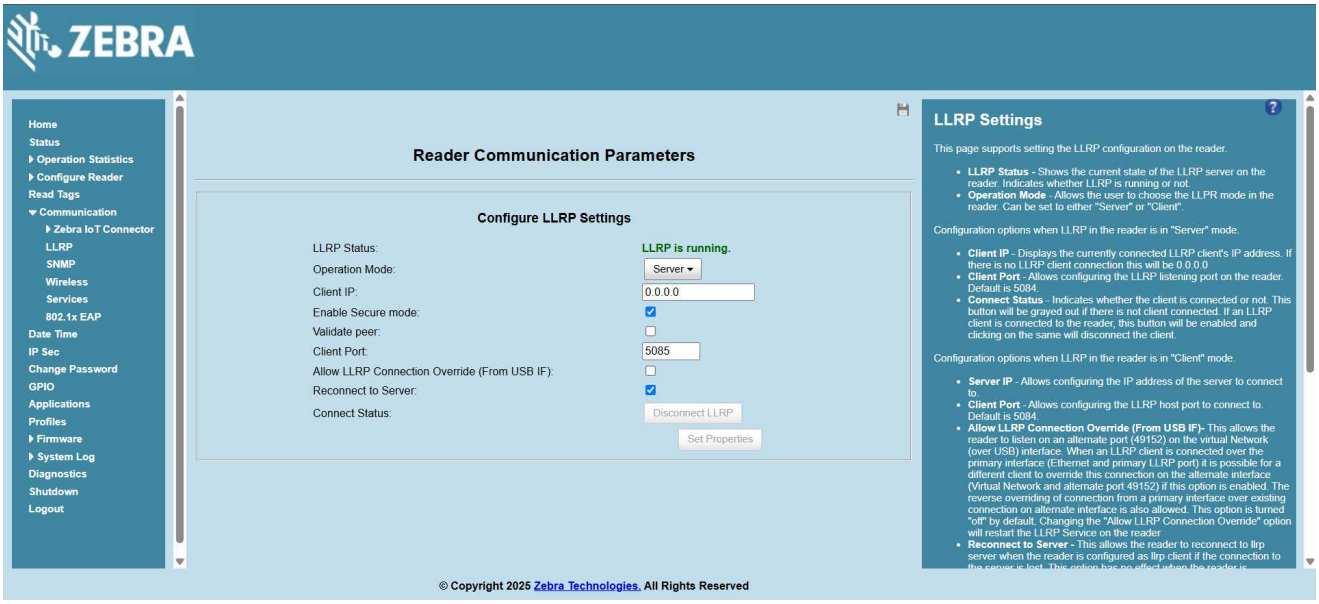
Sample Implementation

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.

By default, LLRP will use a secure connection.

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 188 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 28 for the FX7500 and Figure 12 on page 31 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 Link Local 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

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.

After the reader powers up, test the reader. See System Start-up/Boot LED Sequence on page 42.

1. Enable tag reading using the web-based **Administrator Console** (see Read Tags on page 79) 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 28. The distance between the tag and the antenna is the approximate read range.

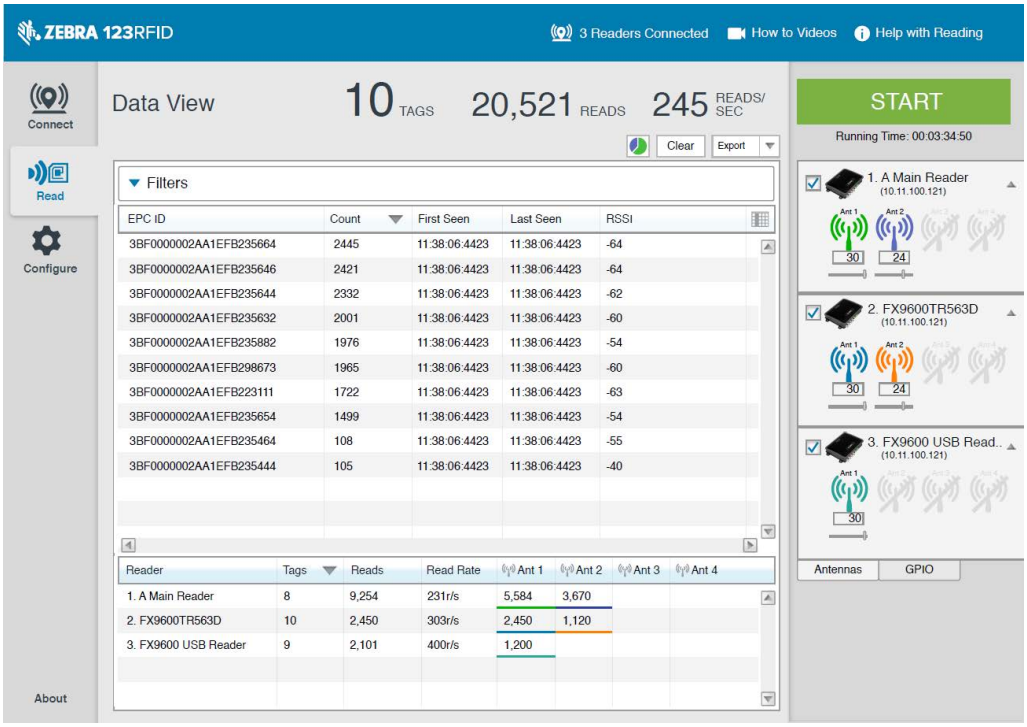
123RFID Desktop

Introduction

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

For more information on 123RFID Desktop, go to 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 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. 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.

By default, 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
- User Application
- Profiles
- File based firmware upload
- Syslog Export.

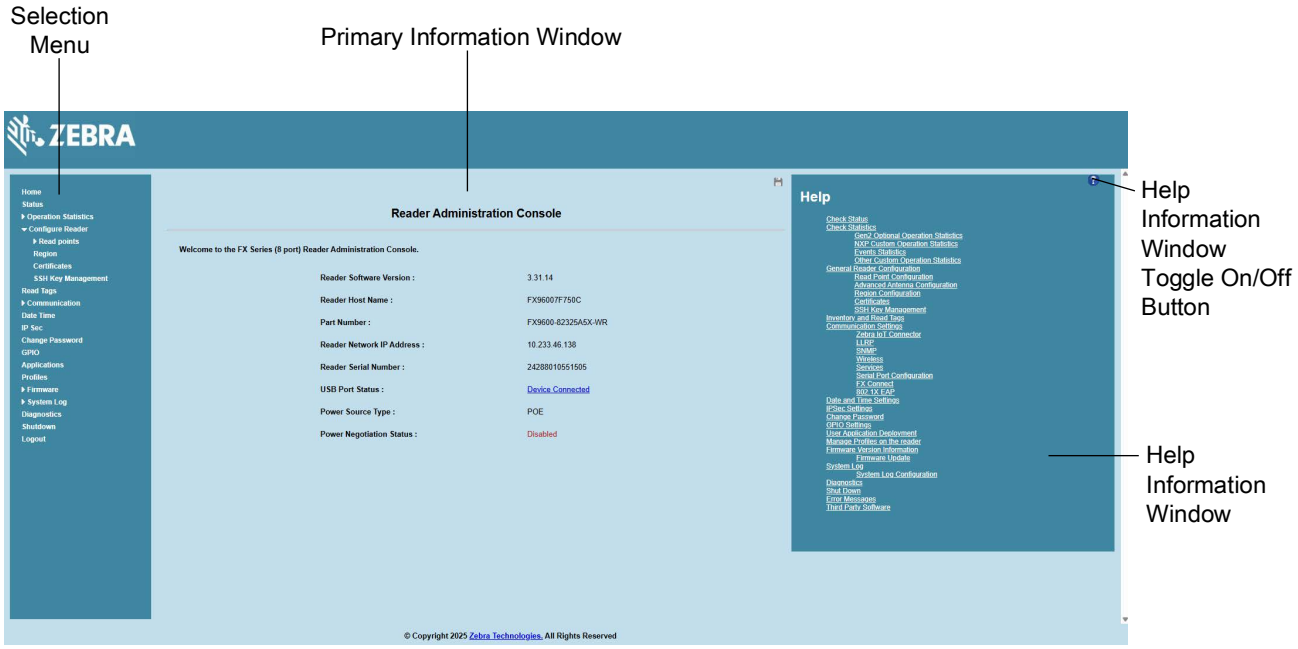
Reader Administrator Console Selections

- **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 102.

Resetting the Reader

To reset the reader, press and hold the reset button for not more than 2 seconds. See Figure 8 on page 27 for the reset button location. The reader reboots but retains the user ID and password.
See System Start-up/Boot LED Sequence on page 42.

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

Auto Discovery

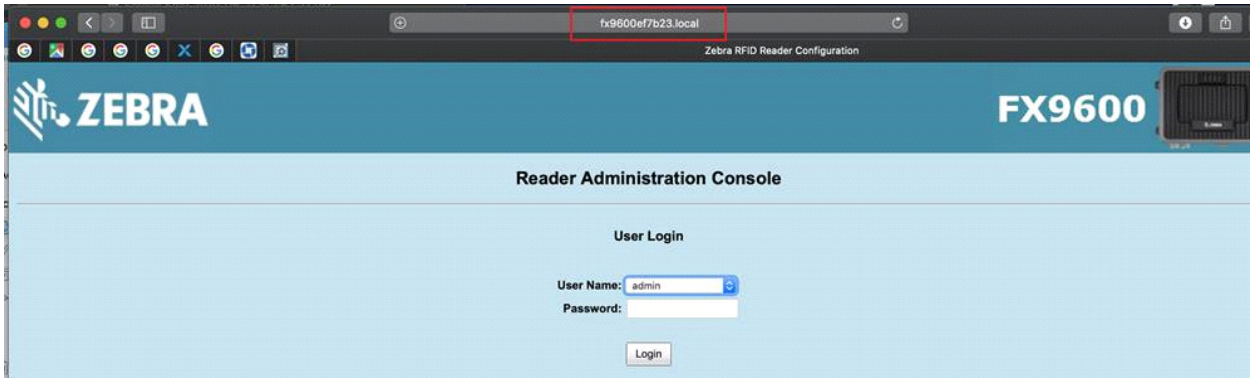
The FX7500 and FX9600 readers supports WS-Discovery and Bonjour (Link Local networking methods) to discovery readers in a subnet. The reader implements WS-Discovery conforming to RFID Reader Management Profile (RDMP) specification in ISO 24791-3. RDMP is based on an extension for Device Profile for Web 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 support.apple.com/downloads/bonjour_for_windows.
- Linux users must install Avahi Service Discover from avahi.org.
- MAC OS has Bonjour support built in.

To discover FX Series readers, append **.local** to the reader host name (for example, **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 HTPP 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, 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 47.

Connect to the reader in one of two ways:

1. Connecting via Host Name on page 50.
2. Connecting via IP Address on page 50. (To obtain the IP address, see Obtaining the IP Address via Command Prompt on page 49)

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

1. Using DHCP on the network.
2. Using Link Local Networking when DHCP Server is Not Available on page 50.
3. Statically assigning an IP. See Static IP Configuration on page 191.

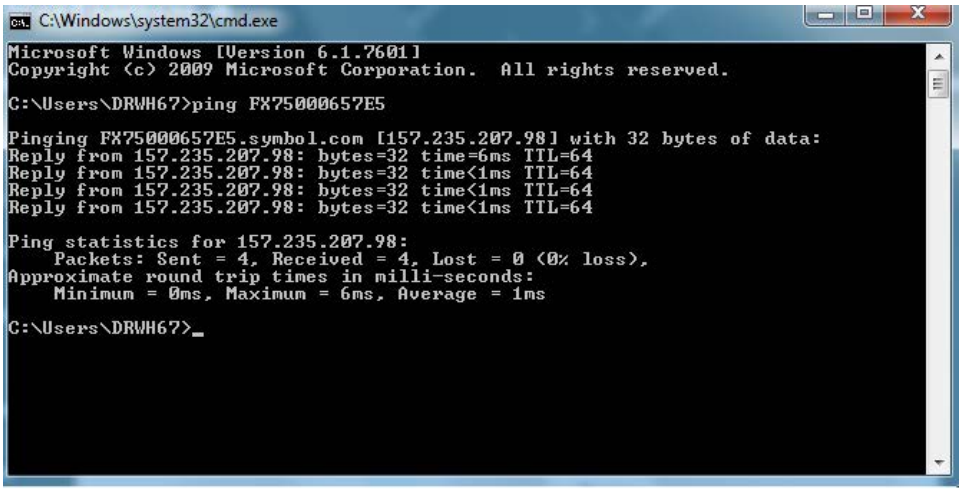
Any method of assigning the IP supports connection using host name or IP address. Alternatively, connect the reader directly to a local computer using zero-configuration networking. See Using Link Local Networking when DHCP Server is Not Available on page 50.

NOTE: When using Link Local 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 47. 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 50.

Figure 23 IP Ping Window



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. The 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 51 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 recommended browsers are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54.
2. Enter the IP address in the browser (for example, 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 51 to login to the reader.

Using Link Local Networking when DHCP Server is Not Available

If a DHCP server is not available, the FX7500 and FX9600 readers can use Link Local networking to automatically provide a unique network IP address. The reader can then use TCP/IP to communicate with other computers also using a Link Local networking-generated IP address.

NOTE: When using Link Local 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 Link Local 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 Link Local 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 Link Local algorithm is **169.254.85.148**.

Windows-based computers support APIPA/Link Local networking by default when DHCP fails. To enable APIPA for a Windows PC, go to 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.

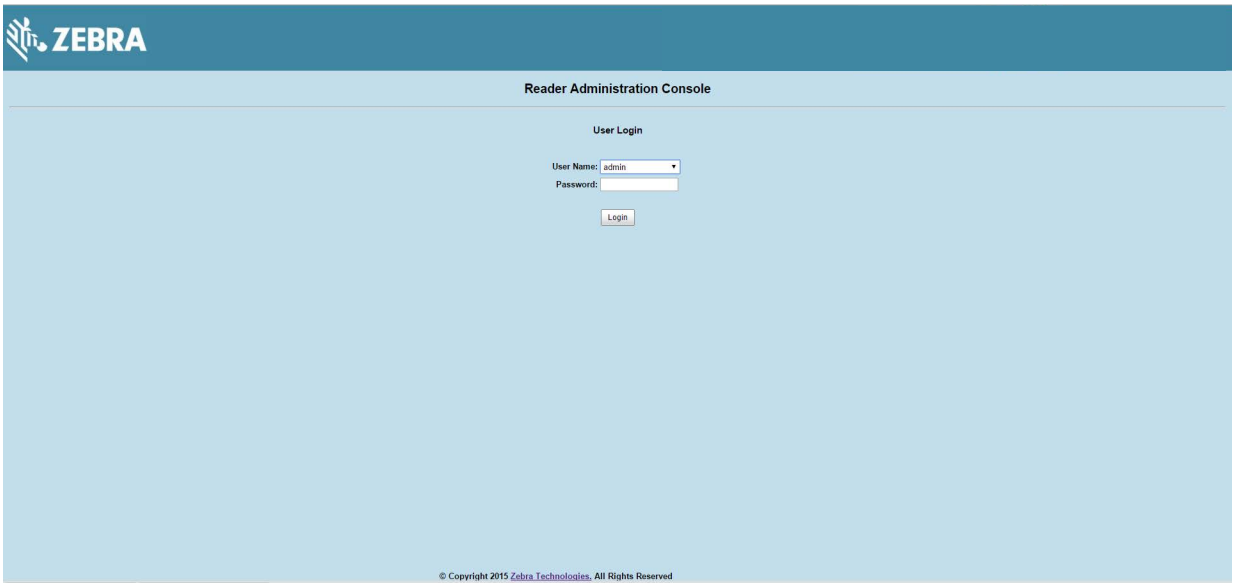
Logging In with Default User ID and Password

Upon connecting to the reader with a web browser, the **User Login** window appears as shown in Figure 24.

In the **User Login** window, select **admin** in the **User Name** drop-down menus and enter **change** in the **Password** field.

- For global reader configurations, the **Configure Region Settings** window appears (see Figure 25 on page 52).
- For the US reader configurations, the **Reader Administration Console** main window appears (see Figure 26 on page 53).

Figure 24 User Login Window



Setting the Region

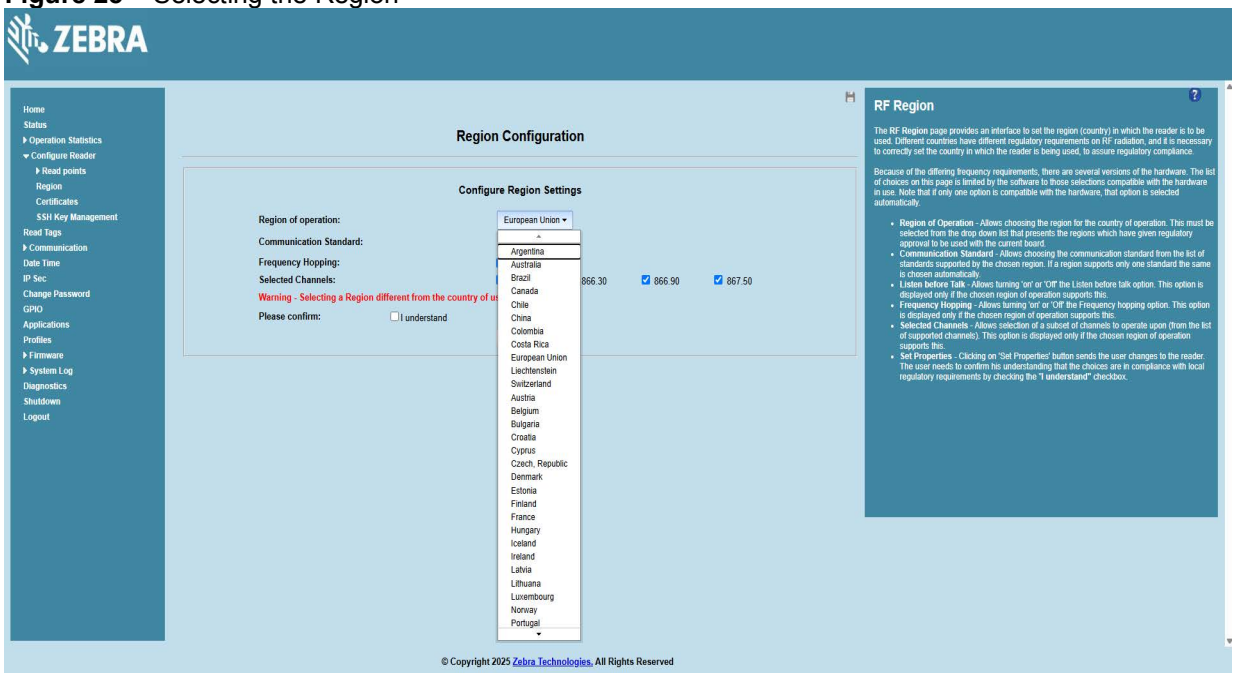
For the global reader configurations, set the **region of operation**.

IMPORTANT: Setting the unit to a different region is illegal.

NOTE: Region configuration is not available for the readers to operate in the United States (under FCC rules). Skip this step if you are configuring the readers to be used in the US.

1. On the **Configure Region Settings** window:
   a. Select the region from the **Region of operation** drop-down menu.
   b. Select the **Communication Standard**, if applicable.
   c. Select **Frequency Hopping**, if applicable.
   d. Select the appropriate channel(s), if applicable.
   e. Select the **I understand** check box.
2. Select **Set Properties**. The **Operation Successful** window appears. Commit step is no longer required to save configuration. See Commit/Discard Functionality Changes on page 106.

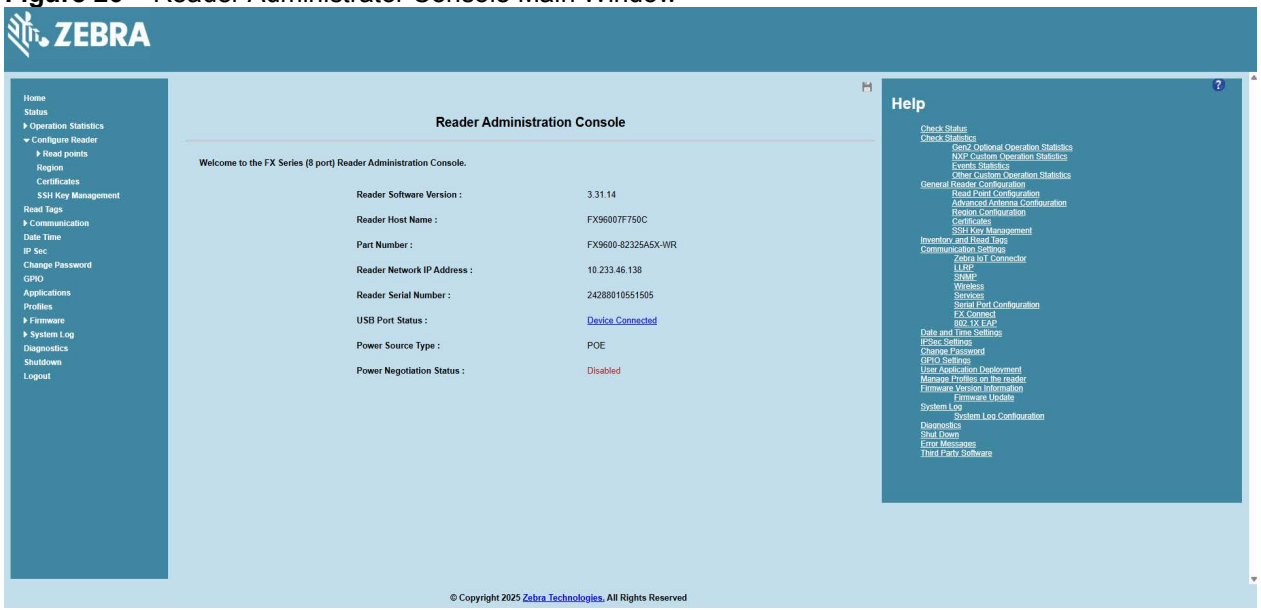
Figure 25 Selecting the Region



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

NOTE: When the reader firmware is updated, the outdated web page may display due to cache. Refresh the browser to update the browser web page.

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

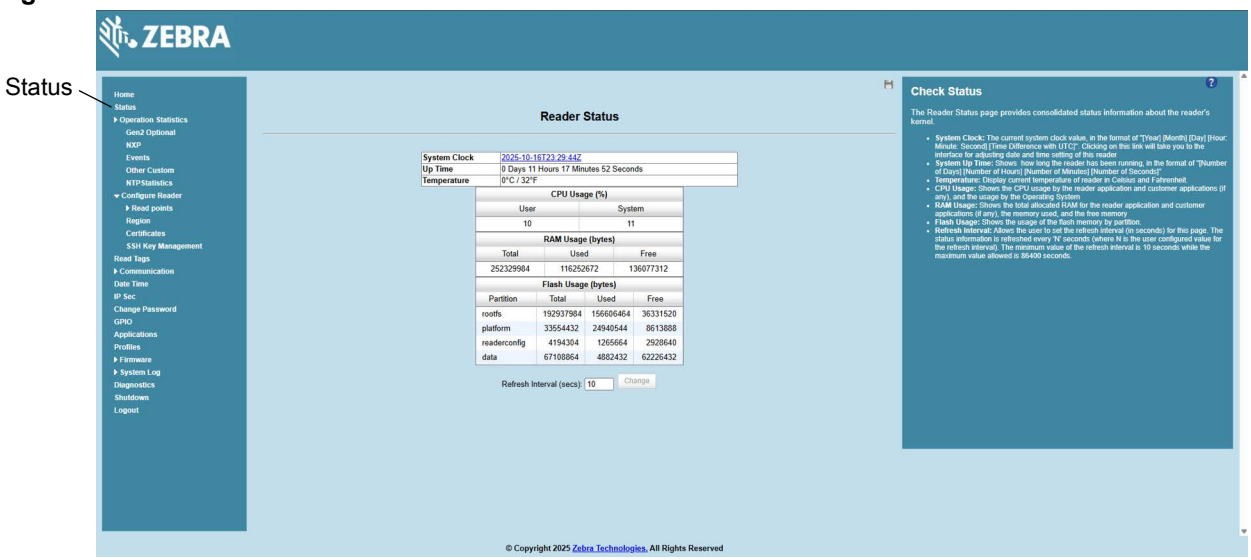
- **Status** - see Status on page 55
- **Operation Statistics** - see Reader Statistics on page 56
  - **Gen2 Optional** - see Reader Gen2 Optional Operation Statistics on page 57
  - **NXP** - see NXP Custom Command Operation Statistics on page 58
  - **Events** - see Event Statistics on page 59
  - **Other Custom** - see Other Custom Command Operation Statistics on page 60
  - **NTP Statistics** - see NTP Statistics on page 61
- **Configure Reader** - see Configure Reader on page 62
  - **Read Points** - see Read Points on page 63
    - **Advanced** - see Read Points - Advanced on page 64
  - **Region** - see Configure Region on page 65
  - **Certificates** - see Certificates on page 66
- **Read Tags** - see Read Tags on page 79

- **Communication** - see Communication Settings on page 80
  - **LLRP** - see Configure LLRP Settings on page 83
  - **SNMP** - see SNMP Settings on page 84
  - **Wireless** - see Wireless Settings on page 85
  - **Serial Port Configuration** - see FX9600 Serial Port Configuration on page 90
  - **Services** - see Network Services Settings on page 86
- **Zebra IoT Connector**
  - **Configuration**
  - **Connection**
- **802.1x EAP**
- **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 101
- **Profiles** - see Reader Profiles on page 102
- **Firmware** - see Firmware Version and Update on page 105
  - **Update** - see Firmware Update on page 106
- **System Log** - see System Log on page 111
  - **Configure** - see Configure System Log on page 112
- **Diagnostics** - see Reader Diagnostics on page 113
- **Shutdown** - see Shutdown on page 114
- **Logout** - select **Logout** to log out from the **Administrator Console.**

Status

Select **Status** from 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



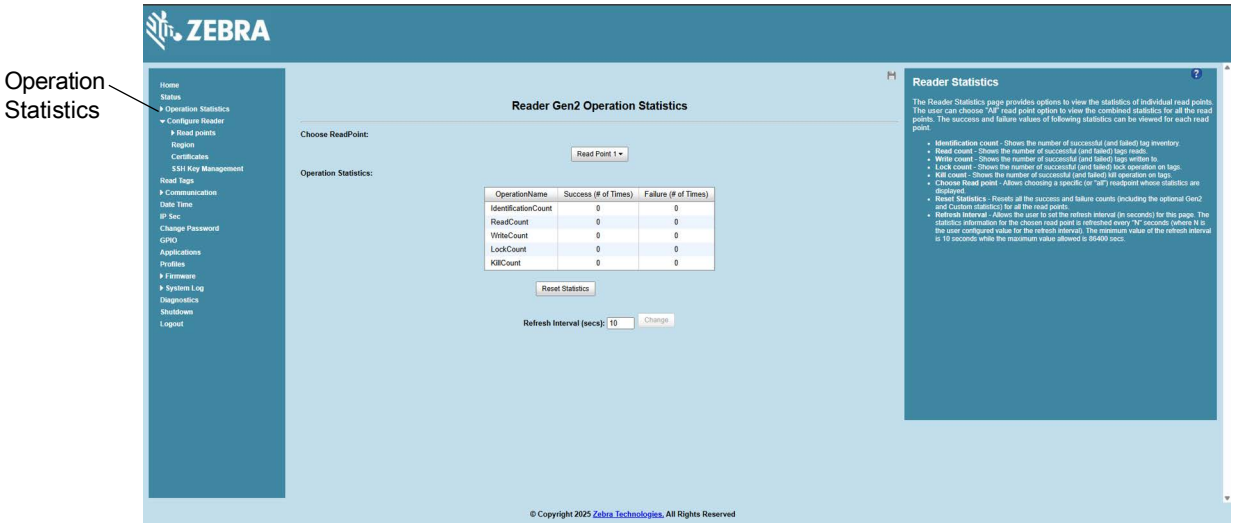
The **Reader Status** window provides consolidated reader status information:

- **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

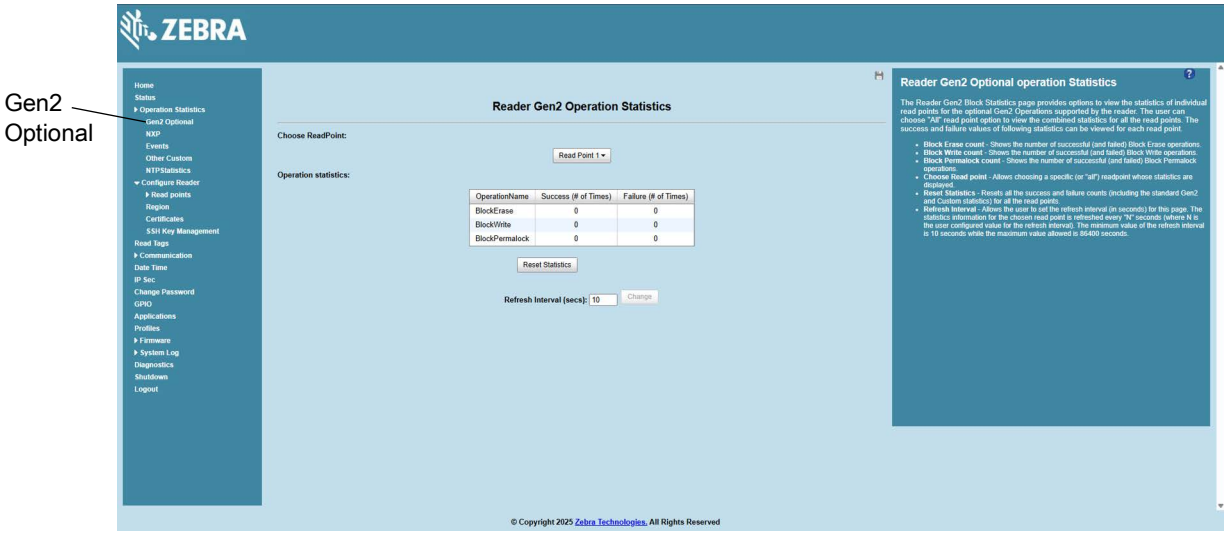


- **Choose ReadPoint** - Select a specific read point or select **All** from the drop-down list to display the statistics.
- **IdentificationCount** - Displays the number of successful (and failed) tag inventories.
- **ReadCount** - Displays the number of successful (and failed) tag reads.
- **WriteCount**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

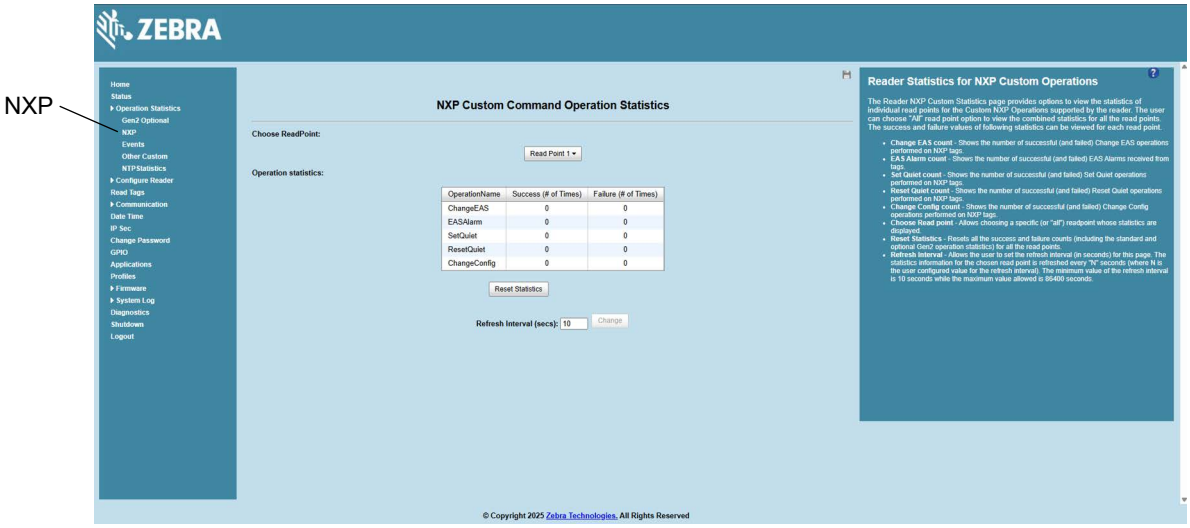


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **BlockErase** - Displays the number of successful (and failed) block erase operations.
- **BlockWrite** - Displays the number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

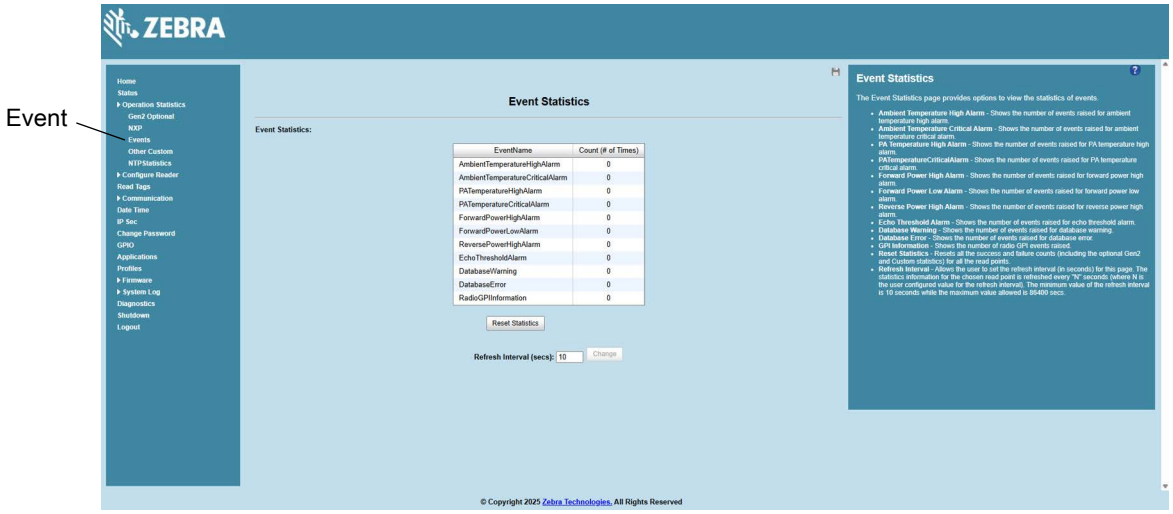


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **ChangeEAS** - Displays the number of successful (and failed) change EAS operations performed on NXP tags.
- **EASAlarm**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

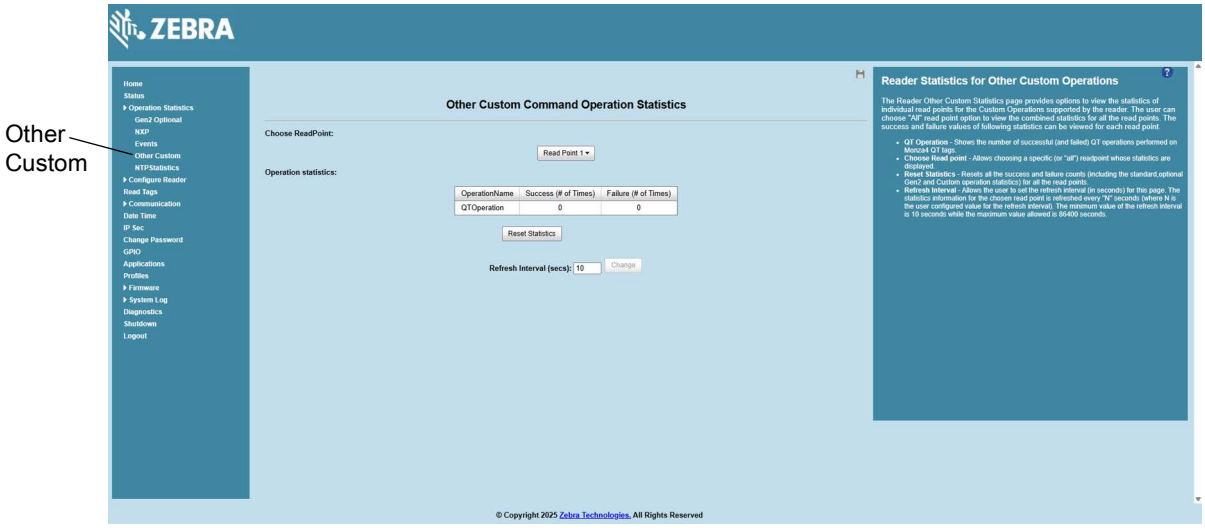


- **AmbientTemperatureHighAlarm** - Displays the number of events raised for ambient temperature high alarm.
- **AmbientTemperatureCriticalAlarm** - Displays the number of events raised for ambient temperature critical alarm.
- **PATemperatureHighAlarm** - Displays the number of events raised for PA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

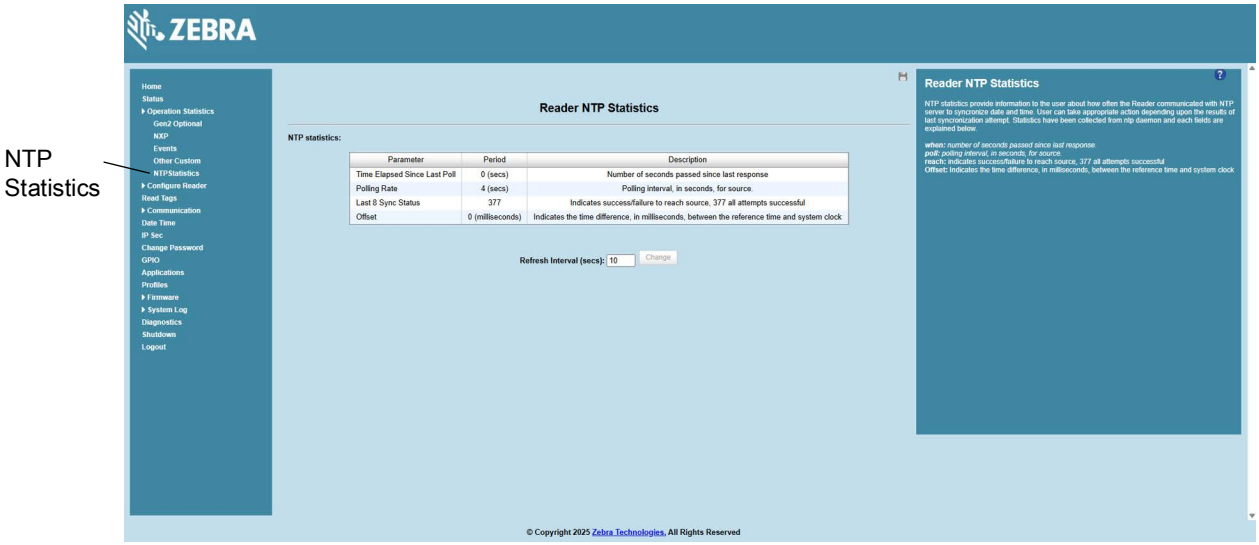


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **QTOperation** - Displays the number of successful (and failed) QT operations performed on Monza4 QT tags.
- **Reset Statistics** - 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.

NTP Statistics

Select **NTP Statistics** to view the **NTP Statistics** window. This window provides options to view the reader NTP statistics.

Figure 33 NTP Statistics Window



NTP statistics provide information to the user about how often the Reader communicated with NTP server to synchronize date and time. User can take appropriate action depending upon the results of last synchronization attempt.

Time Elapsed Since Last Poll: This value indicates the time that has elapsed since the reader last attempted to sync its time from the NTP server.

Polling Rate: This Values indicates the frequency at which the reader is polling the NTP Server.

Last 8 Sync Status: This Value indicates the status (success/failure) to reach source of the last 8 attempts. A value of 0 indicates a failure for sync time on all of the last 8 attempts. And a value of 377 indicates success on all of the last 8 attempts.

Offset: Indicates the time difference, in milliseconds, between the reference time and system clock.

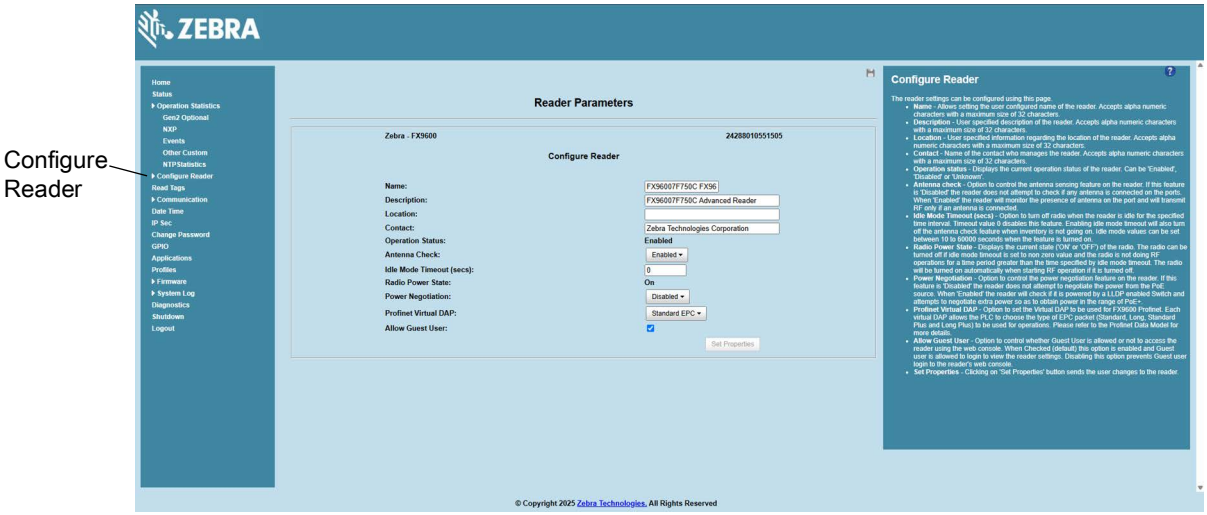
Configure Reader

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

Reader Parameters

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

Figure 34 Reader Parameters



- **Name** - Sets the user-configured reader name. Accepts up to 32 alphanumeric characters.
- **Description** - Sets a user-configured reader description. Accepts up to 32 alphanumeric characters.
- **Location** - Enter information on the reader location. Accepts up to 32 alphanumeric characters.
- **Contact** - Enter the name of the reader manager contact. Accepts up to 32 alphanumeric characters.
- **GPI Debounce Time** - Delays input events up to this time, and delivers these events only if the PIN states remains on the same level.
- **Operation Status** - Displays the current operation status of the reader (**Enabled**, **Disabled**, or **Unknown**).
- **Antenna Check** - Controls the antenna sensing feature on the reader. **Disabled** indicates that the reader does not attempt to check if an antenna is connected on the ports. When **Enabled**, the reader monitors the presence of an antenna on the port and only transmits RF if an antenna is connected.
- **Idle Mode Timeout (secs)** - Set this turn off the radio and the antenna-check feature when the reader is idle for the specified time interval. Set **0** to disable this feature. The default value is zero.

NOTE: Set a non-zero value to enable this feature for the following purposes:

- To save the battery capacity when charging the reader with a vehicle power outlet.
- To lower the reader temperature by turning off the radio function.

- **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.

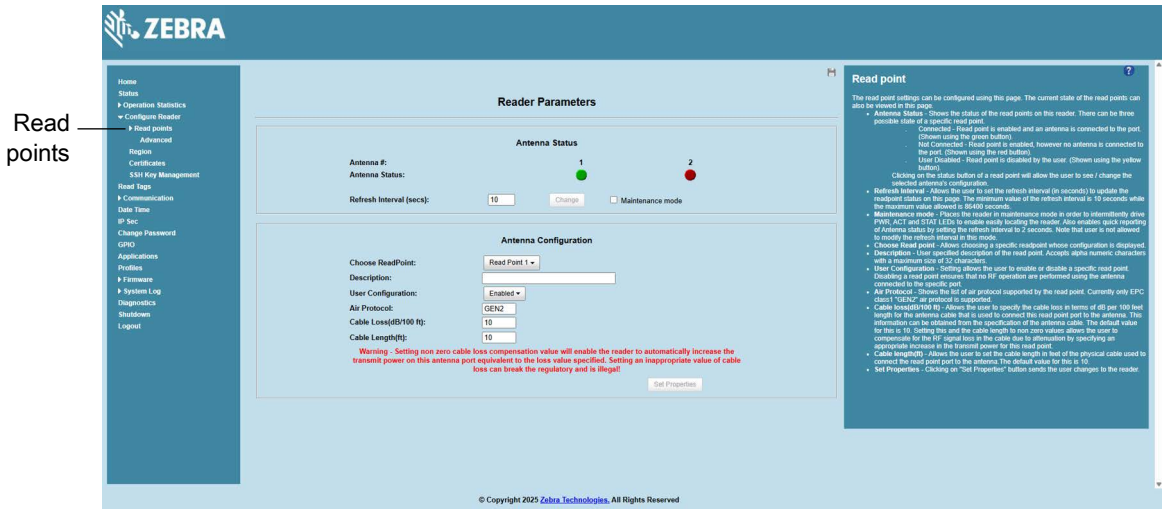
  After power negotiation is enabled, and committed, it takes few seconds for the negotiation to complete and power to reach the PoE+ level. This is the time taken for LLDP packet exchange between the reader and the switch for power negotiation.
- **Allow Guest User** - This option controls if a guest user can access the reader using the web console. The default setting is Enabled. When this option is enabled, a guest user can log in and view the reader settings. Disabling this option prevents a guest user to access the reader's web console.

These settings only affect the display.

Read Points

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

Figure 35 Configure Read Points



Antenna Status

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

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.

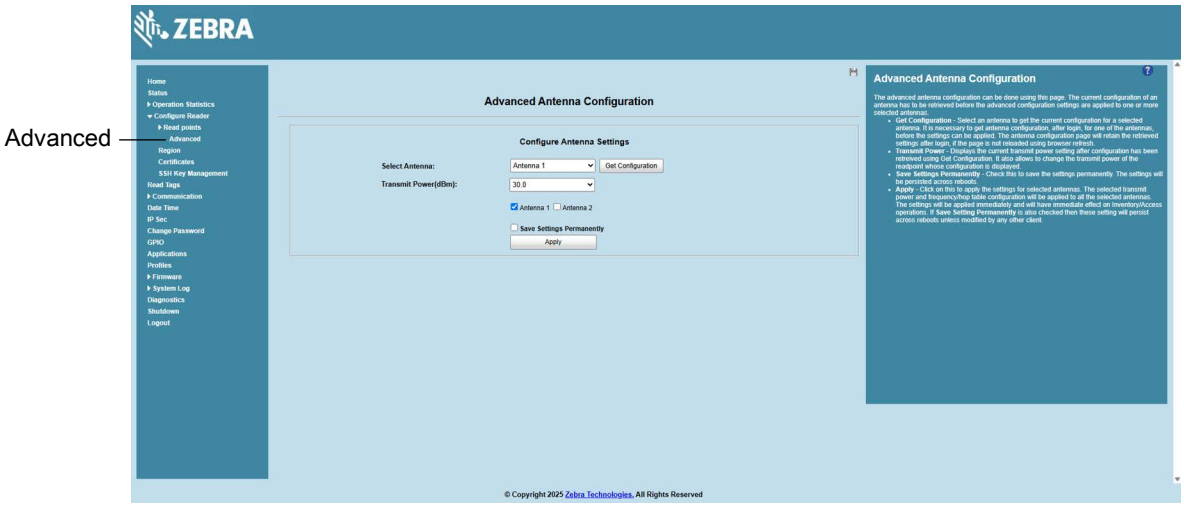
Antenna Configuration

- **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 36 Advanced Antenna Configuration



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

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

- **Get Configuration** - Select an antenna to get the current configuration for that antenna. After login, you must get the antenna configuration for an antenna before settings can be applied. The antenna configuration page retains the retrieved settings after login if you do not refresh the page using browser refresh.
- **Transmit Power** - Displays the current transmit power setting after selecting **Get Configuration**, and allows changing the transmit power for that antenna. This transmit power level does not include cable loss compensation.
- **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.

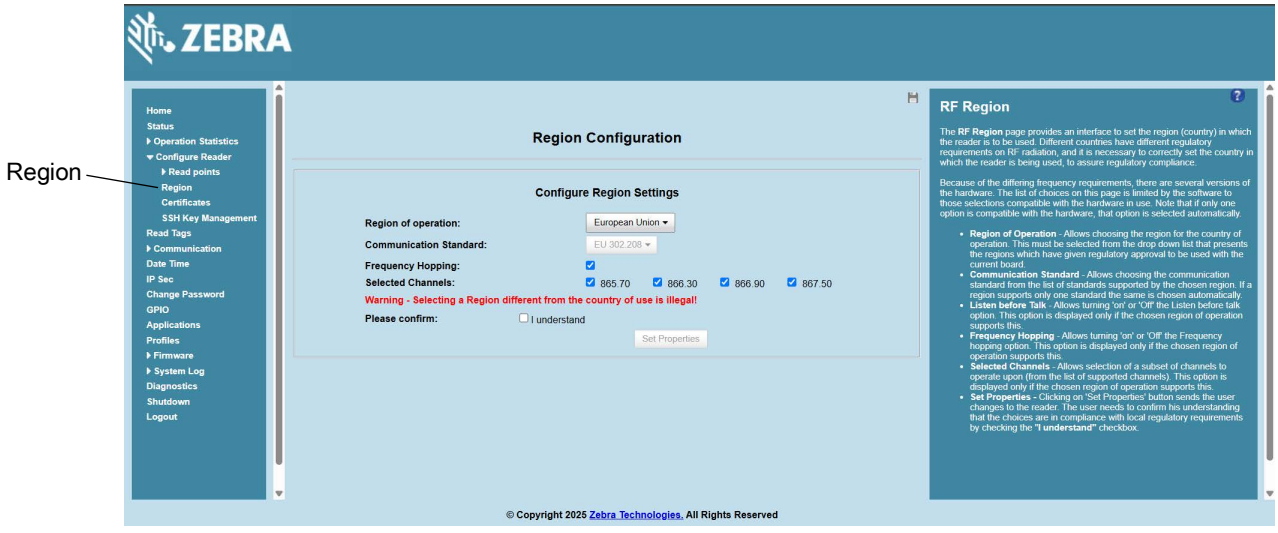
Configure Region

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 37 Configure Region Settings Window



- **Region of Operation** - Select the region for the country of operation from the drop-down list. This list includes regions which have regulatory approval to use with the current board.
- **Communication Standard** - Select the communication standard from the list of standards that the chosen region supports. If a region supports only one standard, it is automatically selected.

- **Frequency Hopping** - Check to select frequency hopping. This option appears only if the chosen region of operation supports this.
- **Selected Channels** - Select a subset of channels on which to operate (from the list of supported channels). This option appears only if the chosen region of operation supports this.
- **Please confirm** - Check the **I understand** check box to confirm your understanding that the choices are in compliance with local regulatory requirements.
- **Set Properties** - 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 86.
- 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 83.

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 83 for details. Services other than Secure LLRP rely on password-based authentication.

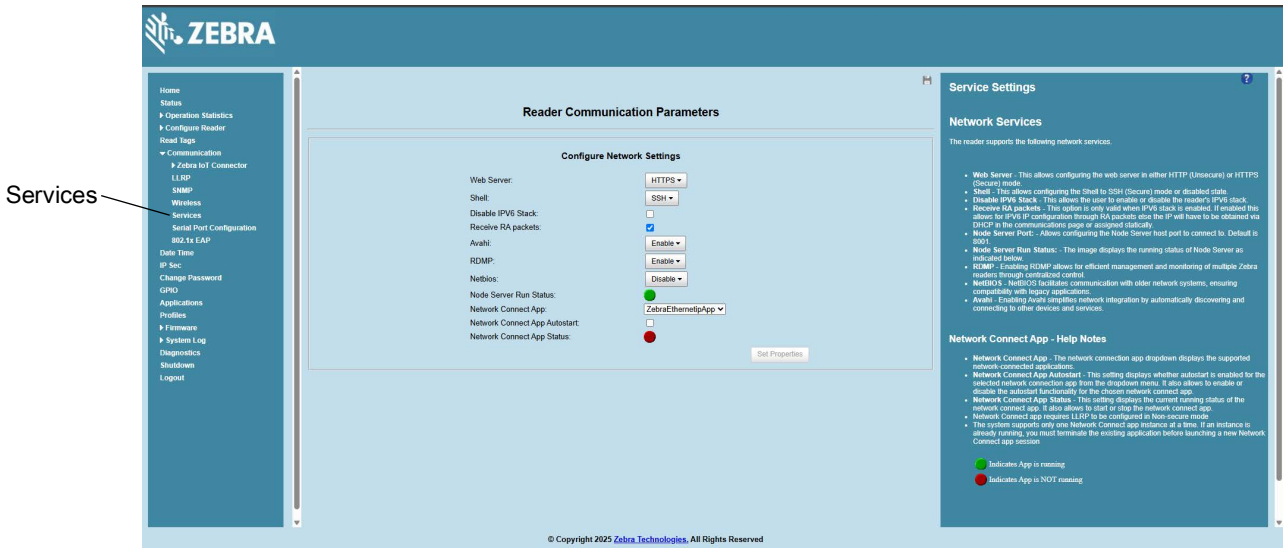
NOTE: The SNMP service on the reader supports SNMP v2c and does not support security.

Certificate Configuration

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

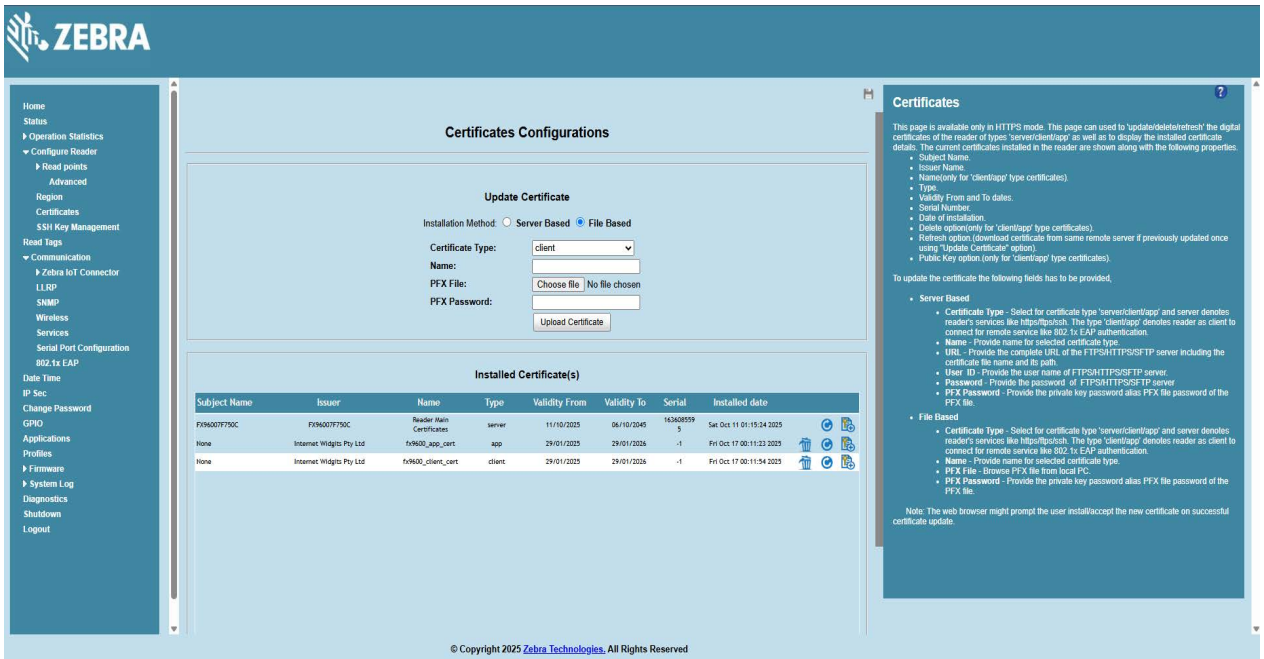
Figure 38 Setting HTTPS Mode

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



Select **Configure Reader > Certificates**. The **Certificate Configuration** page provides the details of certificates and an option to download custom certificates.

Figure 39 Certificate Configuration Page



FX readers allow the user to import and install multiple certificates on the reader. The reader makes a distinction between three kinds of certificates.

- Server
- Client
- App

Server Certificate

Reader allows installation of only one server certificate. The installed Certificate is used on the reader for securing communication interfaces like HTTPS, FTPS Secure LLRP and Secured Shell.

Server certificate can undergo certificate operations like refresh/view public key. Delete operation is not applicable.

update

Client Certificate

Reader allows installation of a multiple client certificates. For example, one such installed Certificate can be used by the reader to connect to 802.1x networks if configured with RADIUS server.

Client certificate can undergo certificate operations like update/refresh/delete/view public key.

App Certificate

Reader allows installation of multiple app certificates. The installed app Certificates can be used by any installed user app for its own purposes.

App certificate can undergo certificate operations like update/refresh/delete/view public key.

By default, the reader uses self-signed certificates for server certificate (characterized by Subject name and Issuer in Installed Certificates(s) section) 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 83.
- 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 86. 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 Installed Certificates(s) section displays the details of installed certificates such as issuer, serial number, type, name, and validity information.

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), Root CA bundled into a single file. The certificate must be hosted on a secure FTPS/HTTPS/SFTP server. The following options are used to perform the update:**FTPS URL**: Full path to server, including ftps:// prefix, where the **.pfx** file is hosted.

Certificate Type: Type of the Certificate being installed.

Name: A friendly name for the Certificate.

URL: URL from where to pull the certificate. HTTPS/FTPS/SFTP URLs are supported.

User ID: The user name to be used for authenticating to the server hosting the certificate.

Password: The password for the above mentioned user name.

PFX Password: The password to the imported PFX f il e

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

The 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** (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** (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_crt.pem -passin pass:$CA_KEY_PASSWORD -batch

rm -f tempreq.pem

echo 'Exporting reader certificate and key to PKCS#12 format....'

openssl pkcs12 -export -out reader.pfx -inkey reader_key.pem -in reader_crt.pem -certfile cacert.crt -passin pass:$GENERATED_CERT_KEY_PASSWORD -passout pass:$GENERATED_CERT_KEY_PASSWORD

echo 'Reader certificate, key and export to PKCS#12 format (.pfx) completed.'

echo 'Note: PFX protected with password: '$GENERATED_CERT_KEY_PASSWORD
```

CreateClientCert.sh

```
#Initialize from current directory

#Enable definition for environment variable OPENSSL_FIPS to execute in FIPS mode on system with FIPS compliant OpenSSL build

#export OPENSSL_FIPS=1

export WORKSPACE_DIR=$( cd "$( dirname "$0" )" && pwd )

#Make sure passwords are unique and secret

export CA_KEY_PASSWORD=CA-abcd12345

export GENERATED_CERT_KEY_PASSWORD=abcd12345

cd $WORKSPACE_DIR/CA-Certs/myCA

echo 'Current dir:'$( cd "$( dirname "$0" )" && pwd )

#Create sample client key and certificate

export OPENSSL_CONF=$WORKSPACE_DIR/samplehost.cnf

echo 'Creating client key and certificate with its signing request ....'

openssl req -newkey rsa:1024 -keyout client_key.pem -keyform PEM -out tempreq.pem -outform PEM -passout pass:$GENERATED_CERT_KEY_PASSWORD

#CA now signs client certificate by processing its certificate sigining request

echo 'CA Signing client certificate....'

export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf

openssl ca -in tempreq.pem -out client_crt.pem -extensions ssl_client_server -passin pass:$CA_KEY_PASSWORD -batch

rm -f tempreq.pem

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

Script Usage

The following section illustrates how to use the previous scripts 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 **samplereader.cnf** to update any configuration such as **hostname** if necessary.
- Execute **CreateReaderCert.sh** by invoking **./CreateReaderCert.sh**.

Issue Client certificate:

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

SSH Key Management

Users can import SSH keys into the reader to establish remote connections. SSH keys provide a secure method for logging into remote servers.

Generating a New SSH Key Pair

Before importing SSH keys into the reader, you need to generate them. These steps create a pair of cryptographic keys: a public key (shared with the remote server) and a private key (kept secure on your local machine).

1. Open a terminal on a local machine.
2. Run the following command to create an SSH key pair:

   $ssh-keygen -t rsa -b 4096

   - -t rsa specifies the type of encryption (RSA).
   - -b 4096 specifies the bit length of the key (higher is more secure).

NOTE: FX readers currently support 2048-bit and 4096-bit RSA ssh keys only.

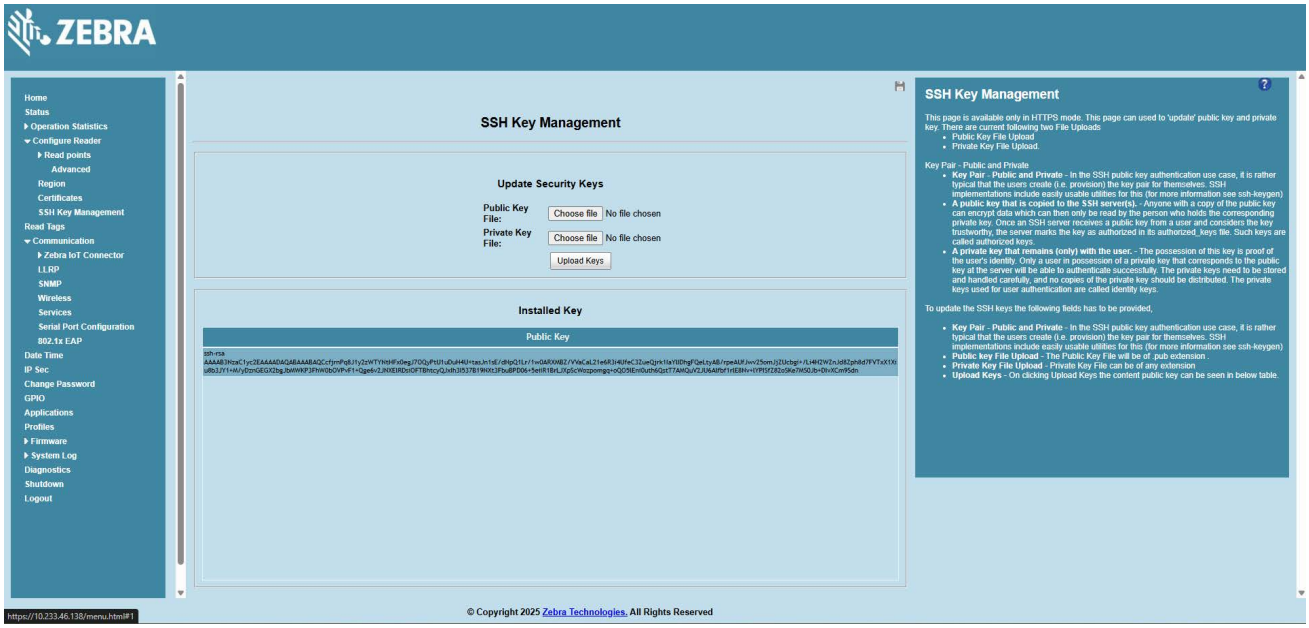
3. When prompted to enter a file in which to save the key, enter the desired location or press **Enter** to accept the default location (~/.ssh/id_rsa).
4. When prompted to enter a passphrase, press **Enter** to leave it empty. (FX readers do not support SSH keys with passphrases)

After done, there will be two files: one private key file (containing a key beginning with '-----BEGIN OPENSSH PRIVATE KEY-----') and another public key file (with a .pub extension containing a key beginning with 'ssh-rsa').

Importing SSH Keys

Import the SSH keys into the reader by navigating to **Configure Reader > SSH Key Management**.

Figure 40 SSH Key Management



NOTE: The current public key is displayed under the "**Installed Key**" section.
Import both the public and private keys into the reader by selecting the '**Public Key File**' and the '**Private Key File**' and navigating to the appropriate location on your local machine. After selected, click the '**Upload Keys**' to upload the files onto the reader and replace its existing keys.

NOTE: The reader can possess only a single active public SSH key at any instance.
The new public key displays under the '**Installed Key**' section.

Adding SSH Key to Remote Server

The remote server allows login from your FX reader, which holds the matching private key.

1. Log in to the remote server using a password:
   ssh user@remote_server_ip
2. After logged in, append your public key to the server's ~/.ssh/authorized_keys file:
   echo "your_public_key_here" >> ~/.ssh/authorized_keys

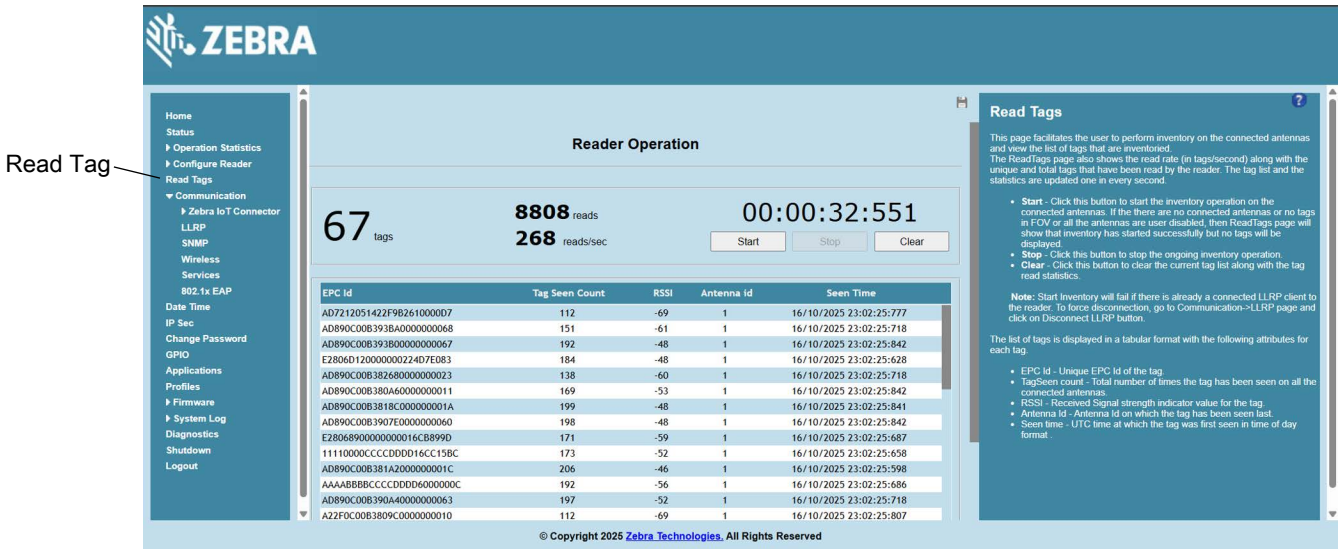
NOTE: The public key begins with 'ssh-rsa'. Ensure the entire content of the file is copied.

3. Ensure the permissions on the ~/.ssh/ directory and the authorized_keys file are correct:
   chmod 700 ~/.ssh
   chmod 600 ~/.ssh/authorized_keys

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.

Figure 41 Read Tags Window



- **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:

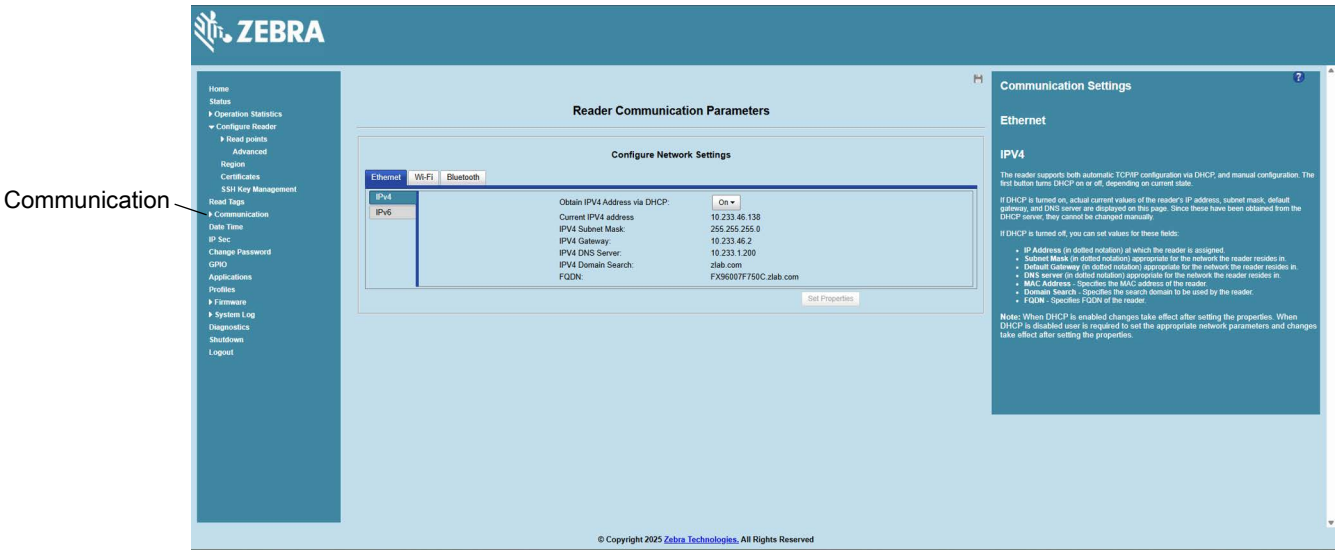
- **EPC Id** - Unique tag EPC ID.
- **Tag Seen Count** - Number of times the tag is identified on the specific antenna.
- **RSSI** - Received Signal Strength Indication.
- **Antenna Id** - Antenna ID on which the tag is seen.
- **Seen Time**: UTC time (in microseconds) showing when the tag is first seen.

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 42 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.
- **IPV4 Domain Search:** Specifies the search domain to be used by the reader.
- **FQDN:** Specifies FQDN 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.

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.

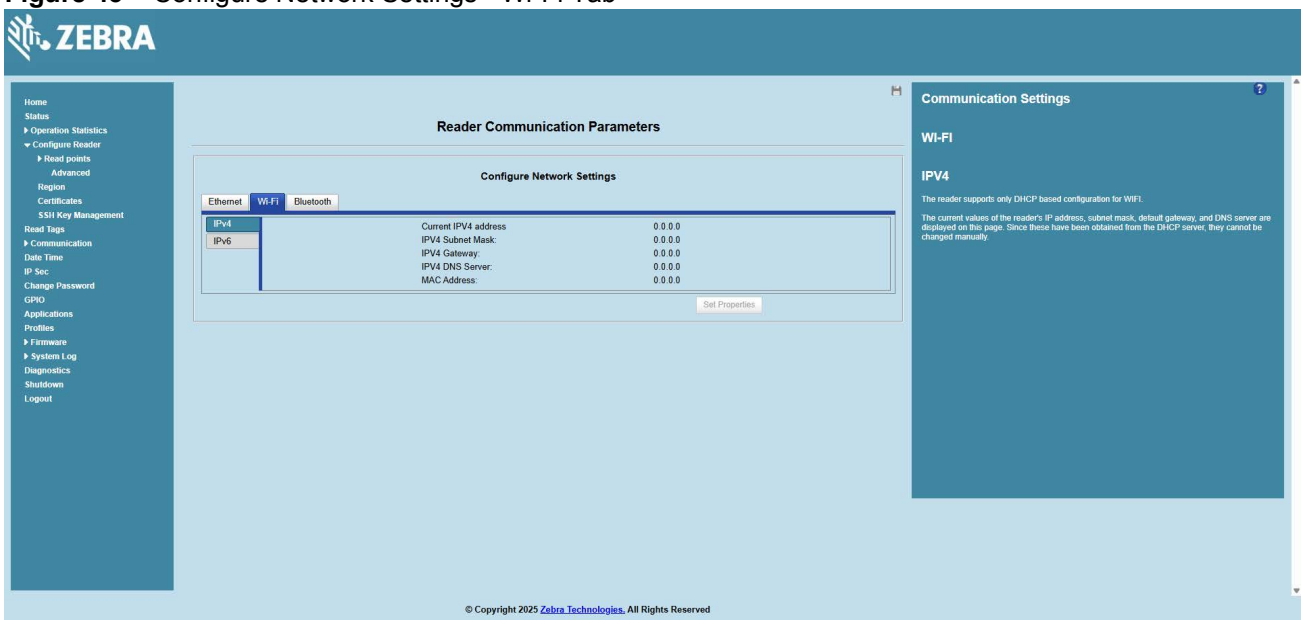
  If DHCP is turned off, you can set the following values for these fields.
- **Current IPV6 Address** - IP address (in dotted notation) at which the reader is assigned.
- **Prefix Length** - Prefix length appropriate for the network in which the reader resides.
- **IPV6 Default Gateway** - Default gateway (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 43 Configure Network Settings - Wi-Fi Tab



IPV4

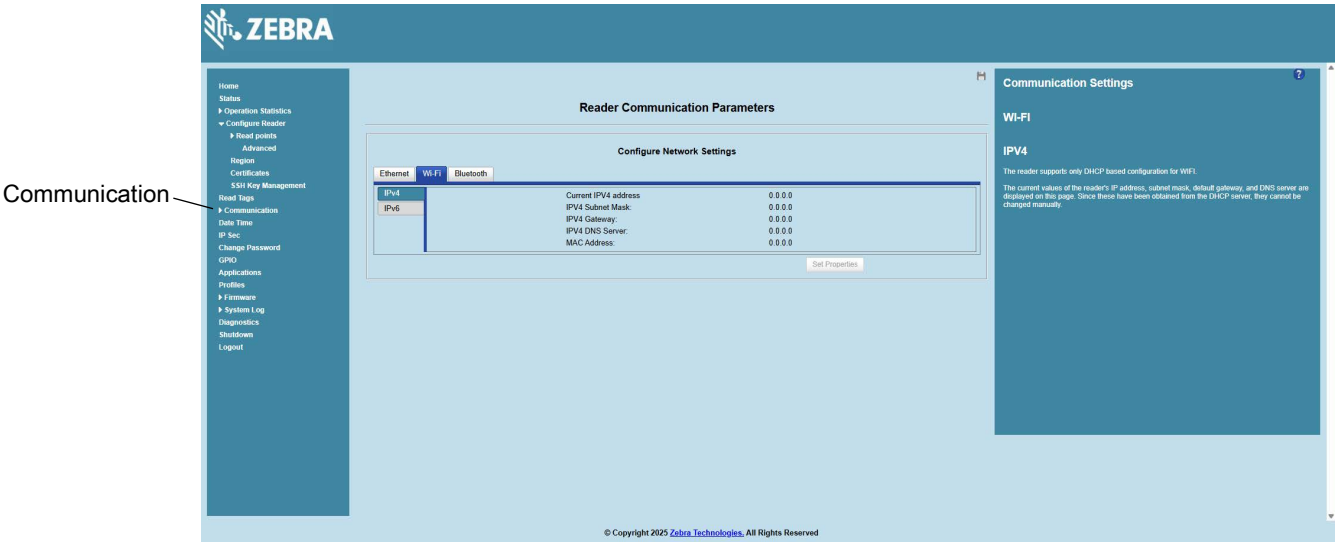
The reader supports only DHCP-based configuration for Wi-Fi. This window displays the current values of the reader's IP address, subnet mask, default gateway, and DNS server. Since these are obtained from the DHCP server, they cannot be changed manually.

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 44 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:

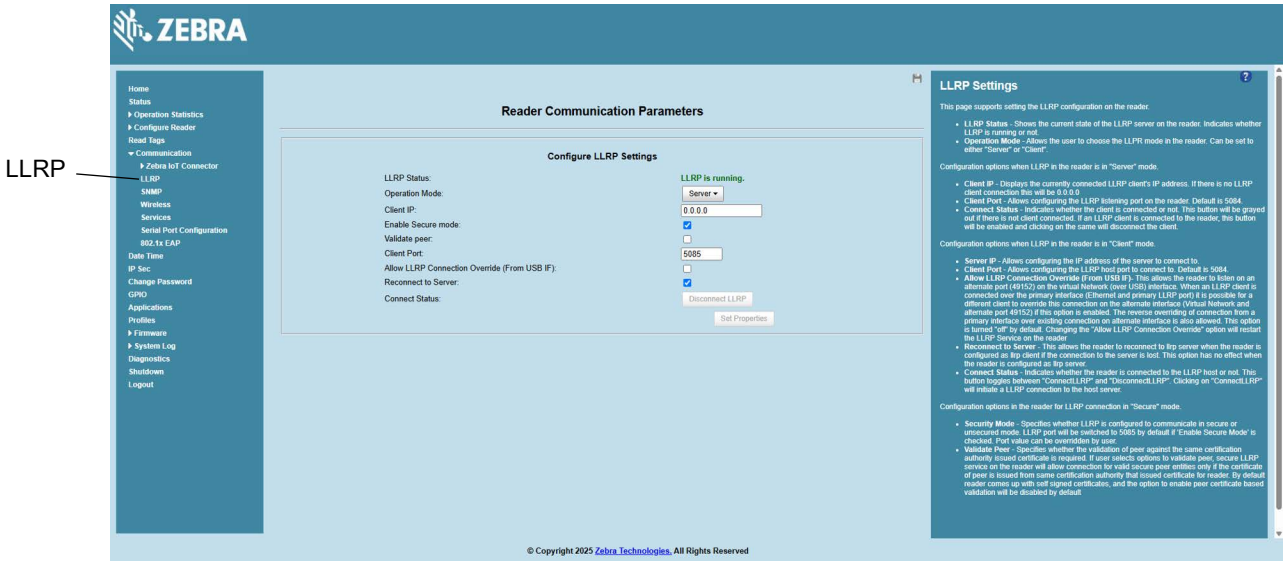
- **Discoverable** - Select whether the reader is seen by other Bluetooth-enabled devices on discovery.
- **Pairable** - Select whether any Bluetooth-enabled device can pair with reader.
- **Use Passkey** - Enable this option to mandate the connecting device to supply a pre-determined passkey to use 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 operates in server mode with a secure connection enabled, where LLRP clients can connect to the reader using the port number specified in the **Client** port field. You can also configure the reader in LLRP client mode. In this case, configure the LLRP server address in this web page as well. LLRP cannot be disabled since it is the primary native protocol for RFID for the reader.

Figure 45 Configure LLRP Settings Window



This window offers the following fields:

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

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

- **Client IP** - Displays the currently connected LLRP client's IP address. If there is no LLRP client connection, this is 0.0.0.0.
- **Client Port** - Configures the LLRP listening port on the reader. The default is 5085.
- **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.

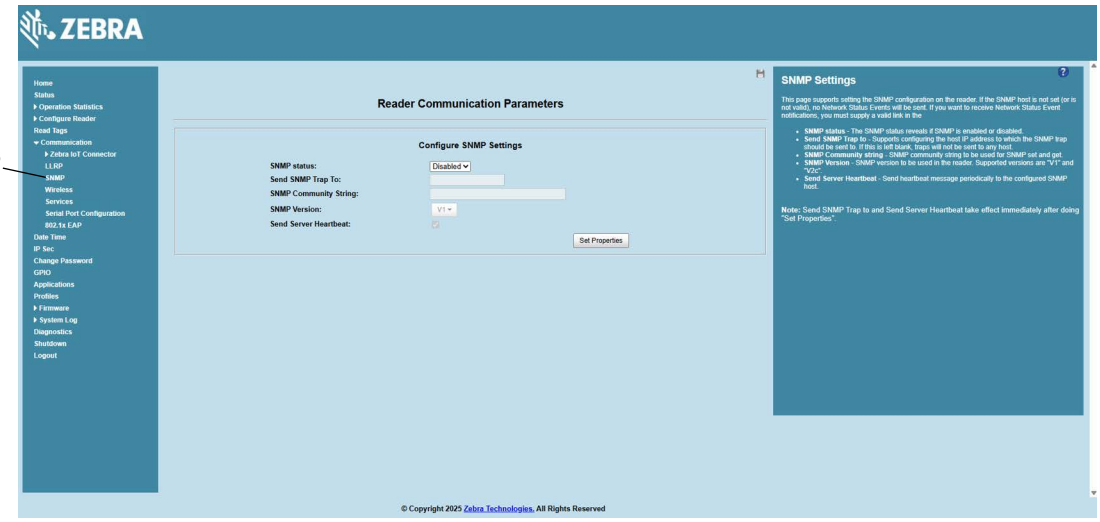
LLRP configuration options when the reader is in **Secure** mode:

- **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.
- **Reconnect to Server:** This allows the reader to reconnect to llrp server when the reader is configured as llrp client if the connection to the server is lost. This option has no effect when the reader is configured as llrp server.

SNMP Settings

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

Figure 46 Configure SNMP Settings Window



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

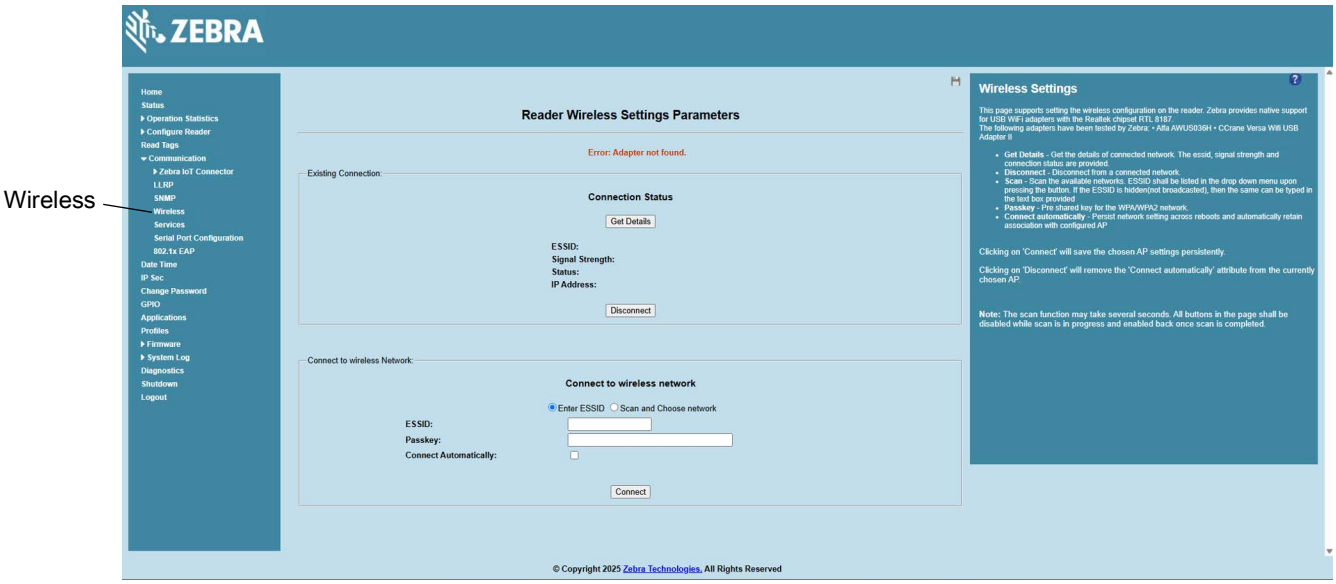
- **SNMP Status -** The SNMP status reveals if SNMP is enabled or disabled. By default, SNMP will be disabled. Enable it to configure the SNMP fields.
- **Send SNMP Trap To** - Configures the host IP address to which the SNMP trap is sent. Leave this blank to send no traps to any host.
- **SNMP Community 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 47 Wireless Settings Window



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

Table 7 Supported Wi-Fi Dongles

Dongle Model	Zebra FX7500	Zebra FX9600
BELKIN F7D2102 N300 MICRO WIRELESS N USB ADAPTER	Yes	Yes
PANDA WIRELESS PAU06 300MBPS WIRELESS N USB ADAPTER	Yes	Yes
ASUS (USB-AC56) DUAL-BAND WIRELESSAC1300 USB 3.0 WI-FI ADAPTER	Yes	Yes
TP-Link TLWN821N N300 USB Wireless Netgear Nighthawk AC1900 Wi-Fi USB Adapter (A7000)	Yes	Yes
TP-Link Nano USB Wifi Dongle 150Mbps (TLWN772N)	Yes	Yes
TP-Link Archer T2U 11AC USB WiFi Adapter - AC600	Yes	Yes
AC1750 Dual-Band Wi-Fi USB 3.0 Adapter	Yes	Yes
TP-Link AC 1200 - Alfa Network AWUS036H(Realtek	Yes	Yes
RTL8187L chipset)	Yes	Yes
CCrane Versa Wifi	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.

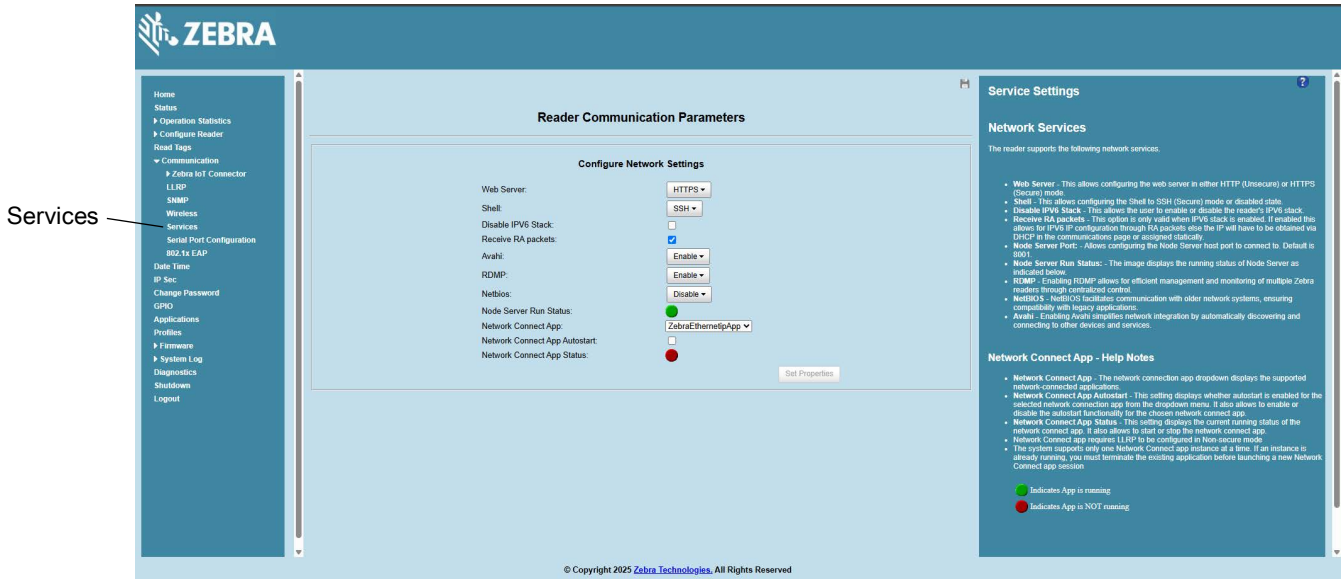
NOTE: The scan function can take several seconds. All buttons on the page are disabled while the scan is in progress, and re-enabled when the scan completes.

Network Services Settings

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

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

Figure 48 Configure Network Service Settings Window



The reader supports the following network services.

- **Web Server** - Configures the web server in either HTTP (unsecure) or HTTPS (secure) mode.
- **Shell** - Sets the shell to SSH (secure) mode or a disabled state. By default, SSH will be disabled.
- **Enable SSH by setting the rfidadm password from the change password page.** Setting the rfidadm should satisfy the following criteria:
  - Should contain a minimum of 8 and a maximum of 32 characters.
  - English uppercase characters (A through Z).
  - English lowercase characters (a through z).
  - Base 10 digits (0 through 9).
  - Non-alphabetic characters (for example: !, $, #, %).
  - Should not use previously used five passwords.
- **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.
- **Node Server Port** - Set the Node Server host connection port. The default value is 8001.
- **Node Server Run Status** - Displays the Node Server status:
- **Network Connect App** - The network connection app dropdown displays the supported network-connected applications.
- **Network Connect App Autostart** - This setting displays whether the autostart is enabled for the selected network connection app from the dropdown menu. It also allows to enable or disable the autostart functionality for the chosen network connect app.
- **Network Connect App Status** - This setting displays the current running status of the network connect app. It also allows to start or stop the network connect app.
  - Green - App is running.
  - Red - App is not running.

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.

802.1x EAP Configuration

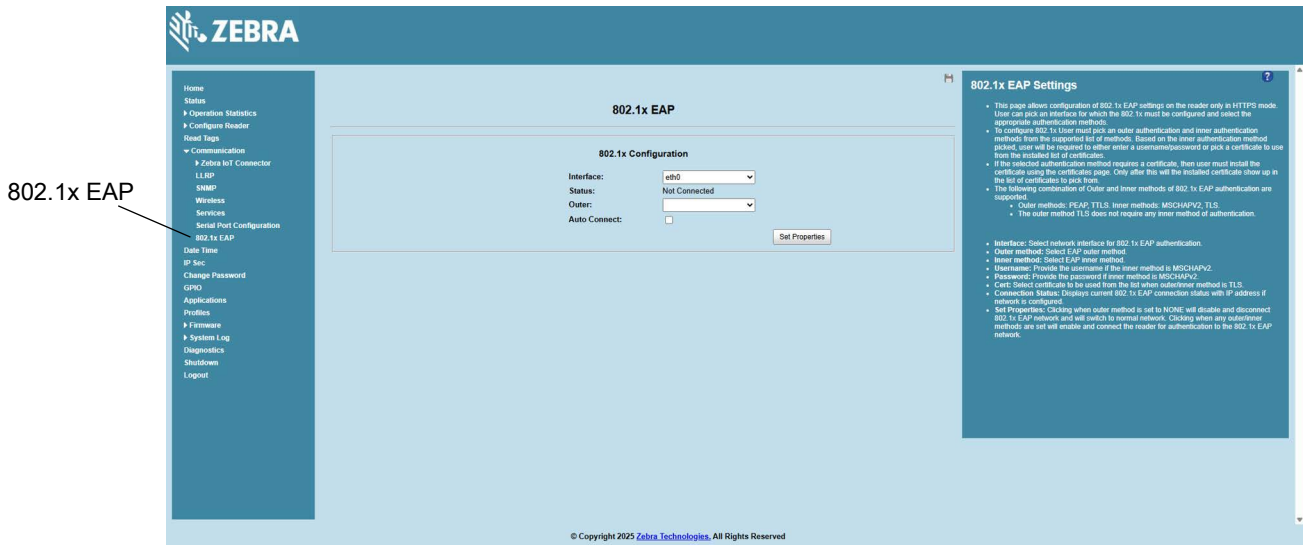
Select **802.1x EAP** to view the 802.1x EAP configuration.

NOTE: The FX Series readers support 802.1x over Ethernet interface only.

NOTE: 802.1x Configuration is allowed in HTTPS mode only.

To configure 802.1x User must pick an outer authentication and inner authentication method from the supported list of methods. Based on the inner authentication method picked, user will be required to either enter a username/password or pick a certificate to use from the installed list of certificates. To install a certificate from the reader, please refer to the Certificates section of this document.

Figure 49 Configure 802.1x Window



The reader supports the following combinations for the inner and outer methods of authentication for 802.1x EAP.

Outer Method	Inner Method
PEAP	TLS, MSCHAPV2
TTLS	TLS, MSCHAPV2
TLS	NA

The following configuration options are available:

- **Interface:** Selects network interface for 802.1x EAP authentication. Currently 802.1x is supported on Ethernet interface only.
- **Status:** Indicates the current 802.1x connection status.
- **Outer:** The Outer method of authentication to be used.
- **Inner:** The Inner method of authentication to be used.
- **UserName:** provide username if the inner method selected in MSCHAPV2.
- **Password:** provide password if the inner method selected is MSCHAPV2
- **Cert:** Select the cert to be used from the list of installed certificates on the reader.
- **Auto Connect:** Enabling Auto Connect will ensure the reader connects back to 802.1x network on reboot.

FX Series Reader 802.1x EAP configuration/Testing with FreeRADIUS

This section is for configuring and testing Fx Reader 802.1x EAP authentication with FreeRADIUS server.

RADIUS Server (FreeRADIUS) Configuration

Install FreeRADIUS on Ubuntu x86_64 host.

```
$ sudo apt-get install freeradius
```

1. Add sample user ‘user1’ with password ‘user123’ like below at file ‘/etc/freeraidus/3.0/users’:

   "User1" Cleartext-Password := "password123"

   Reply-Message = "Hello, %{User-Name}"

   NOTE: The username ‘user1’ and password ‘password123’ is given for inner method ‘MSCHAPV2’ of outer method ‘PEAP/TTLS’. See 802.1x EAP Configuration on page 87.

2. Update IP address and secret password of Cisco switch at file ‘/etc/freeradius/3.0/clients.conf’ under section ‘client localhost’ as below:

   client localhost {

   ipaddr = 192.168.1.100

   secret = testing123

   }

3. Modify the following lines change at file ‘/etc/freeradius/3.0/mods-enabled/eap’ by uncommenting or apply the changes wherever are possible.

   eap

   {

   default_eap_type = peap

   tls-config tls-common

```
        {
            private_key_file = ${certdir}/server.key
            certificate_file = ${certdir}/server.pem
            ca_file = ${certdir}/ca.pem
            disable_tlsv1_2 = no
            dh_file = ${certdir}/dh
            tls_min_version = "1.0"
            tls_max_version = "1.2"
        }
    }
```

4. Create Signed Certificates.
   a. Change to directory '/etc/freeradius/3.0/certs/' and remove existing certificates.

      $ sudo -i; cd /etc/freeradius/3.0/certs/

      $ rm -f *.pem *.der *.csr *.crt *.key *.p12 serial* index.txt*

   b. Execute following commands for creating Root CA, server and client certificates

      $ sudo make ca.pem

      $ sudo make server.pem

      $ sudo make client.pem

      $ chown freerd:freerd server.key server.pem client.pem ca.pem

   c. Execute the below command for generating PFX file 'client.pfx'.

      $ openssl pkcs12 -export -out client.pfx -inkey client.key -in client.pem -certfile ca.pem -passin pass:whatever -passout pass:whatever

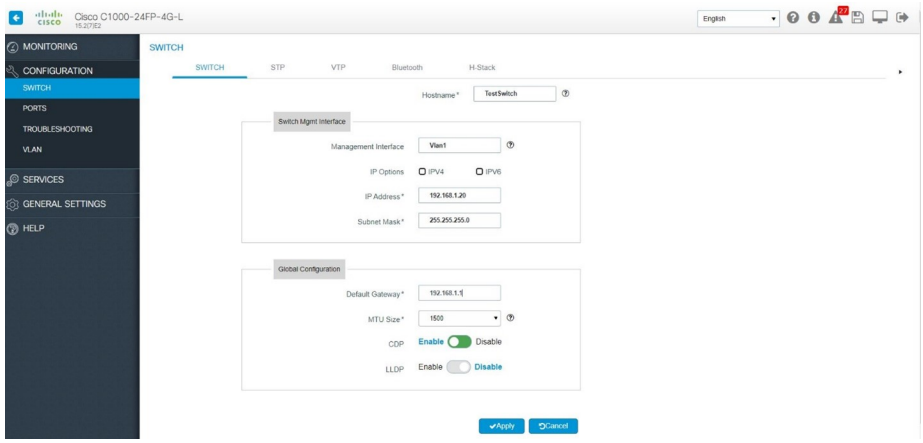
      NOTE: The sample password 'whatever' provided here is given for PFX password during update certificate. See Certificate Configuration on page 67.

5. Start FreeRADIUS server.

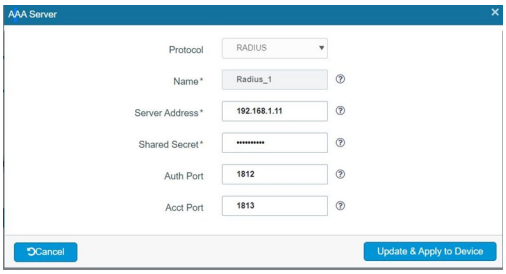
   $ sudo freeradius -X

Cisco Switch (Cisco C1000-24FP-4G-L) Configuration

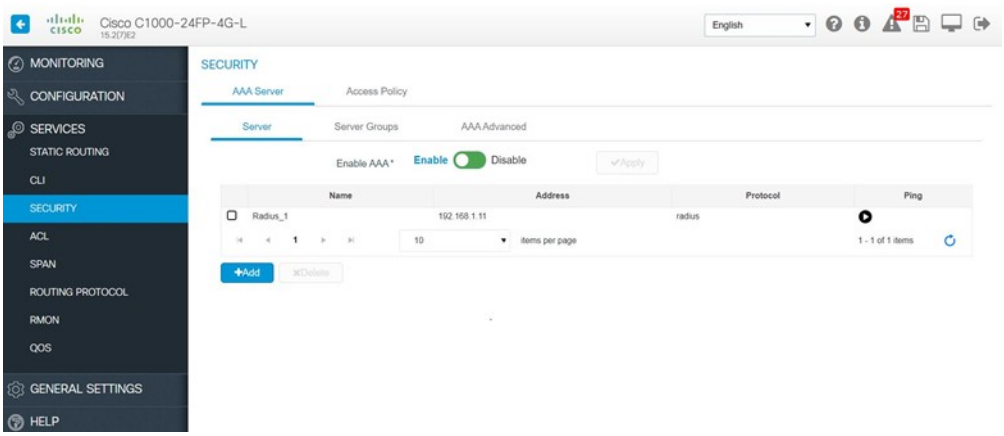
1. Below figure show configuring switch with IP address details under menu "Configuration→Switch→Switch":



2. Below figures show con figuring Radius server details in switch under menu “service→security→AAA Server→Server→Add”:



NOTE: For “Server Address” add IP address of FreeRADIUS and Shared Secret “testing123” with port details as above. The shared secret is already mentioned in file ‘/etc/freeradius/3.0/clients.conf’ under se ction “client localhost” while configuring FreeRADIUS at Ubuntu 18.04 x86_64 host.



Cisco C1000-24FP-4G-L

Fx Reader 802.1 EAP authentication testing with RADIUS server (FreeRADIUS)

1. Install the generated PFX file at Fx Reader. See Certificate Configuration on page 67.
2. Connect Fx Reader at dotx (not MAB) configured network port through ethernet of Cisco switch.
3. Connect DSL Modem with DHCP server running to yet another ethernet network port of Cisco switch.
4. Connect Ubuntu 18.04 host (which has FreeRADIUS configured) ethernet into yet another network port of Cisco switch.
5. Connect to 802.1x EAP network authentication. See 802.1x EAP Configuration on page 87.

NOTE: - Both Fx Reader and FreeRADIUS server must be synchronized for date and ti me for cer ti fica te base 802.1x authent ic ati on li ke TLS for to work and on generating certificate at Ubuntu x86_64 h

- Following 802.1x EAP outer/inner authent ic ati ons are successful with Fr eeRADIUS server
  1. PEAP/MACHAPv2
  2. TTLS/MSCHAPv2
  3. TLS
  4. TTLS/TLS

FX9600 Serial Port Configuration

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

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

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

Serial Port Configuration - 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 50 Serial Port Communication - Debug

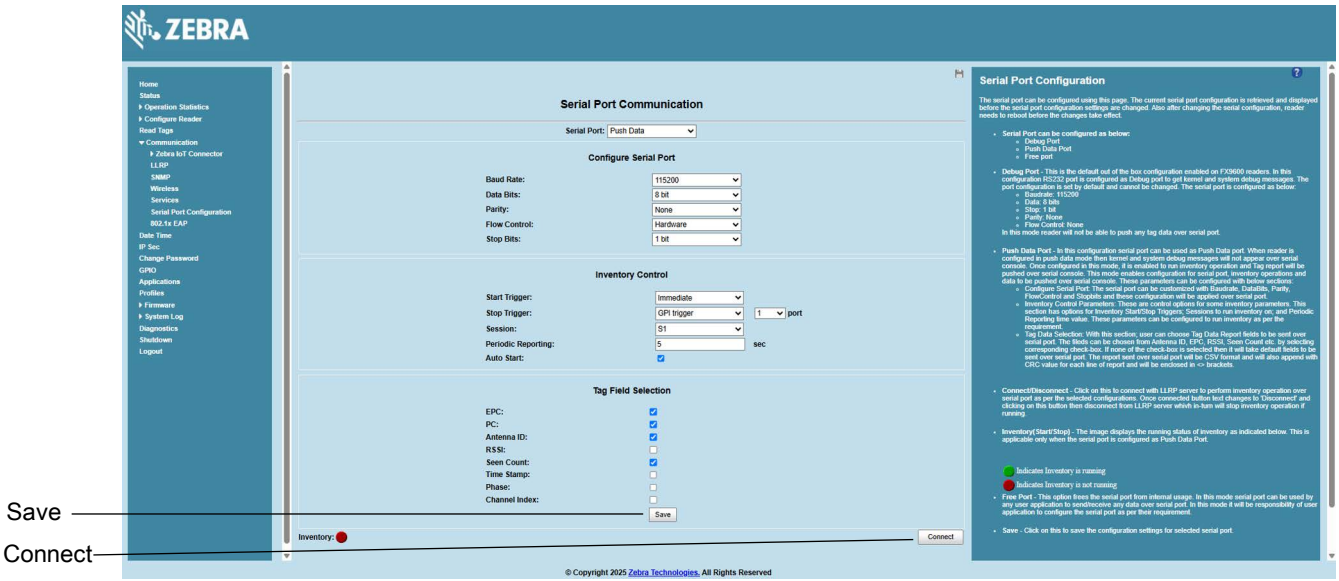
Serial Port Configuration - Push Data Port

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 the serial port communication fields (see Figure 51).

Figure 51 Serial Port Communication - Push Data Configuration



2. Select **Save** to save the current settings.
3. Reboot the reader to implement the changes.
4. Select **Connect** to connect to LLRP. If **Auto Start** is selected in **Inventory Control** options, the reader is set to connect to LLRP upon boot up. Once connected, the inventory starts as per the Inventory Control configuration and report tags over the serial port.
5. The tag data can be seen on the serial port as shown in Figure 53.

Figure 52 Serial Port Communication - Push Data Inventory Started

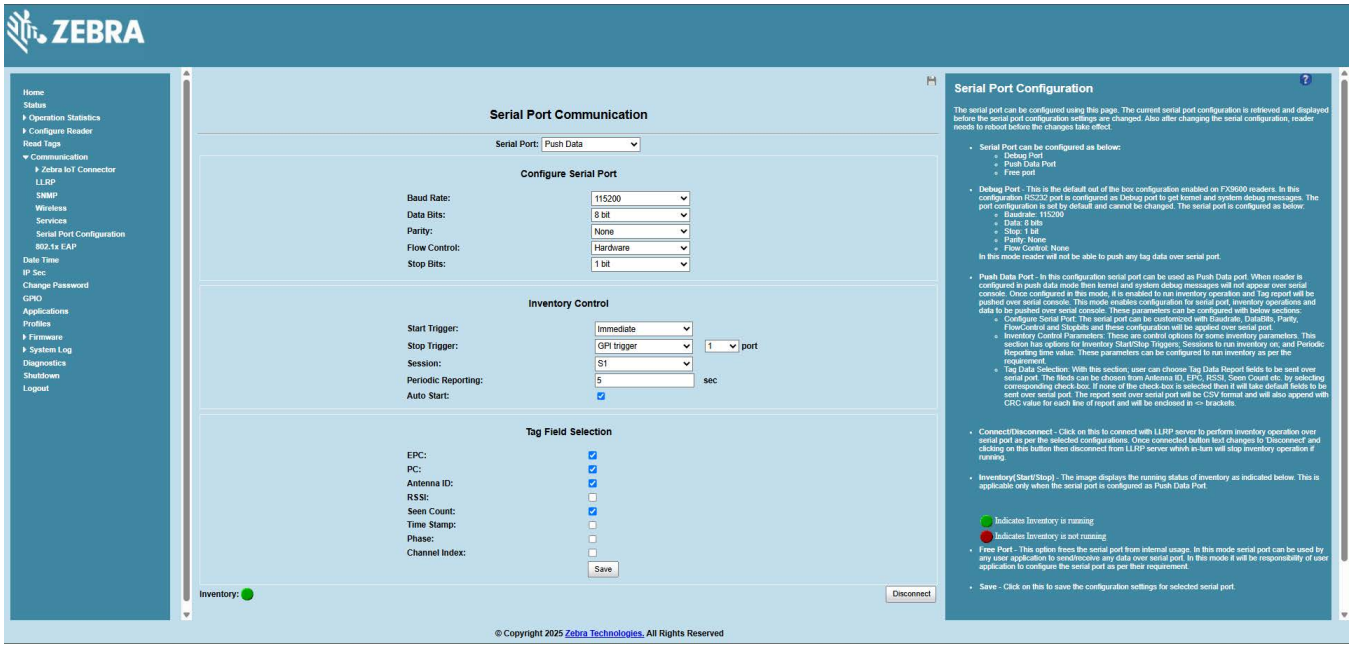
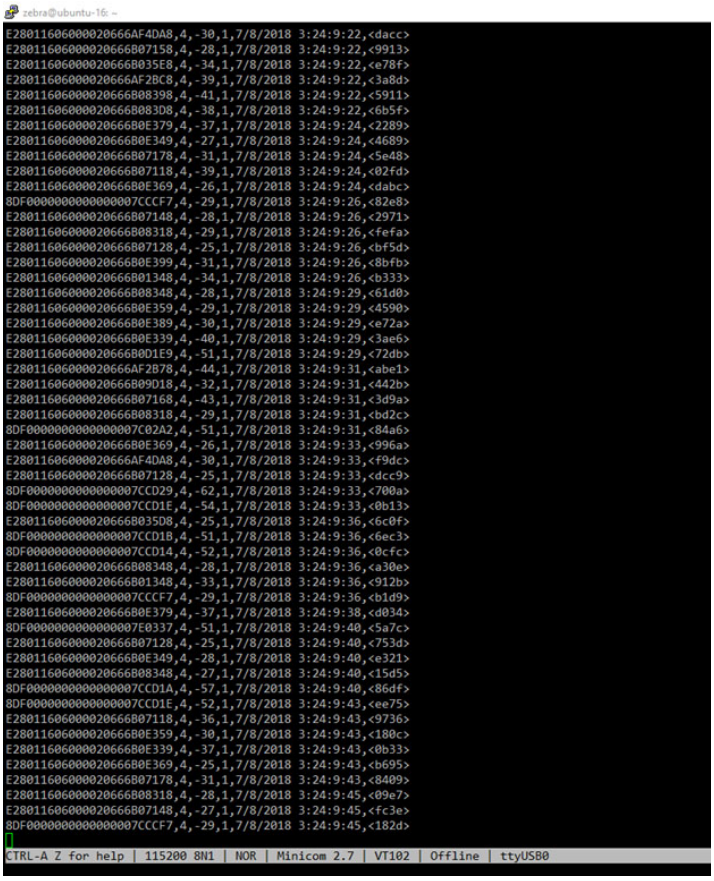


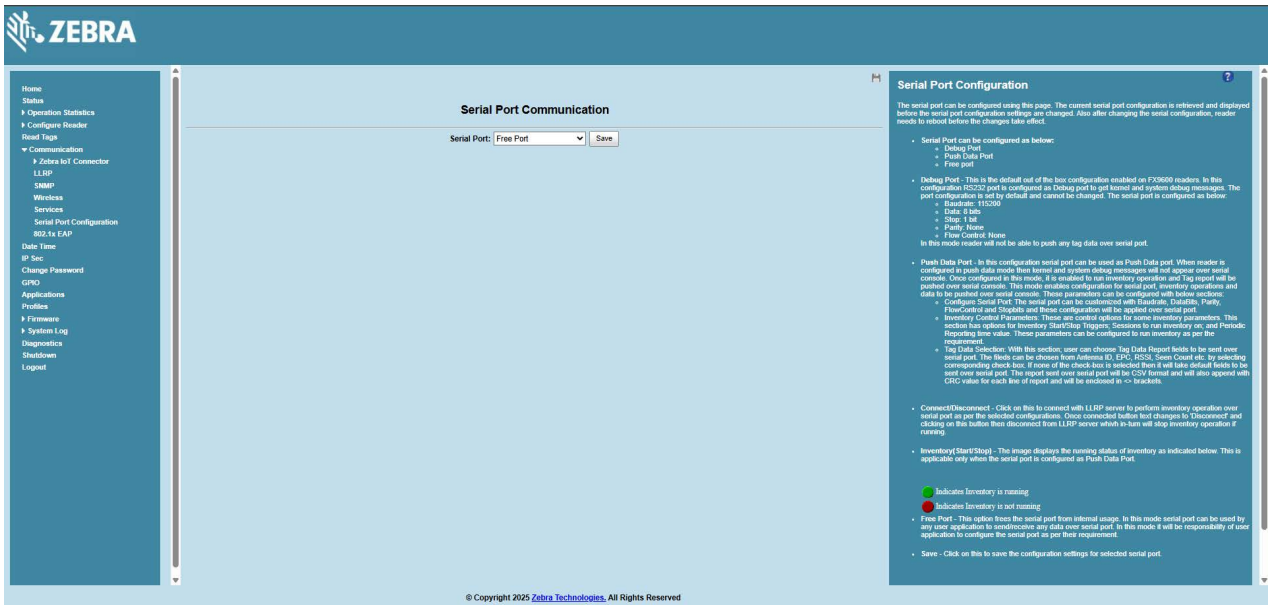
Figure 53 Tag Data



Serial Port Configuration - Free Port

When the FX9600 is the Free Port mode, the serial port in the FX9600 is able to perform operations such as open, read, and write as per the user requirement.

Figure 54 Serial Port Communication - Free Port

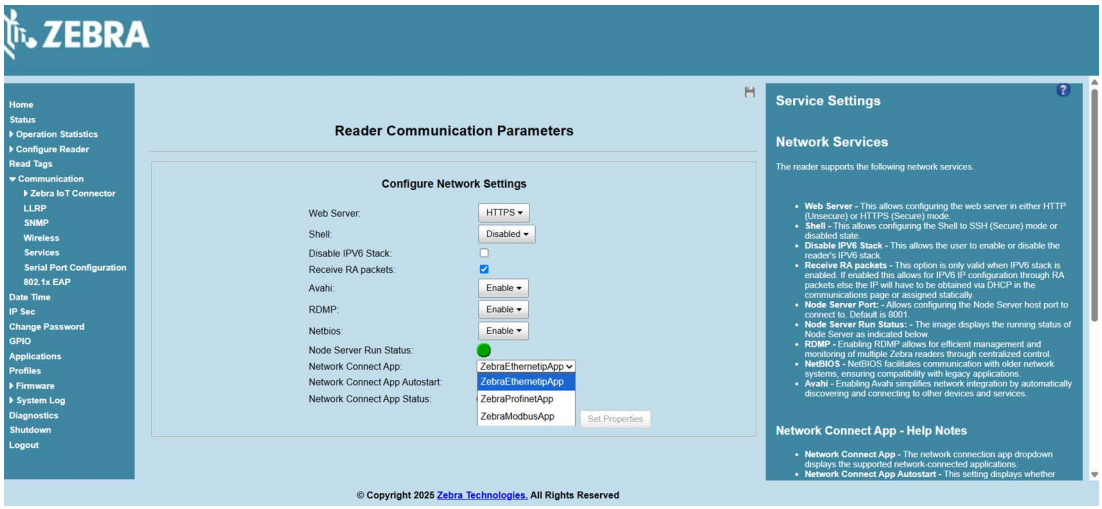


Network Connect App Configuration

Network connect apps can be configured on the service page. There are three available network connect apps:

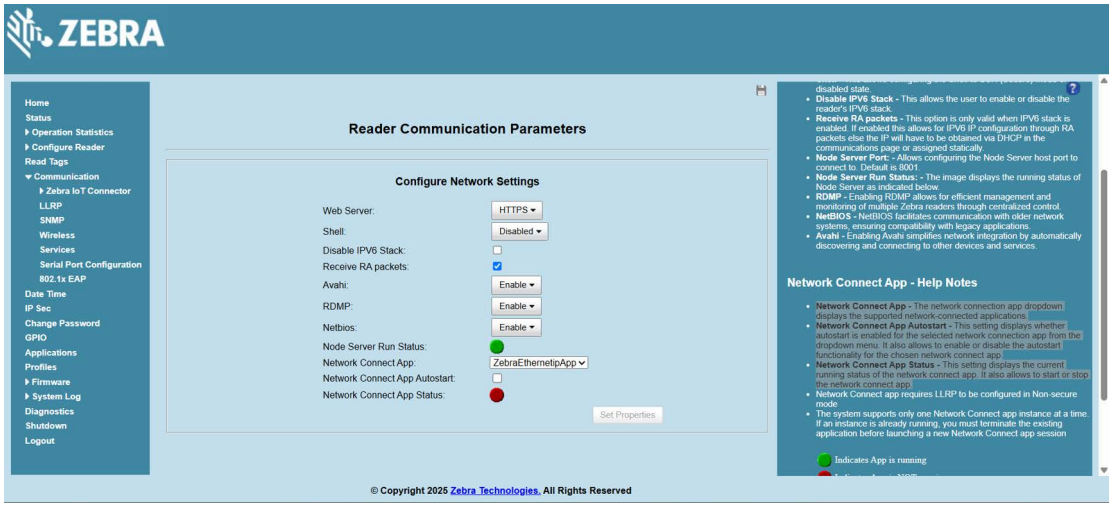
1. ZebraEthernetIPApp
2. ZebraProfiNetApp
3. ZebraModbusApp

Figure 55 Network Connect App Dropdown



- Network Connect App - The network connection app dropdown displays the supported network-connected applications.
- Network Connect App Autostart - This setting displays whether autostart is enabled for the selected network connection app from the dropdown menu. It also allows to enable or disable the autostart functionality for the chosen network connect app.
- Network Connect App Status - This setting displays the current running status of the network connect app. It also allows to start or stop the network connect app.

Figure 56 Start Network Connect App



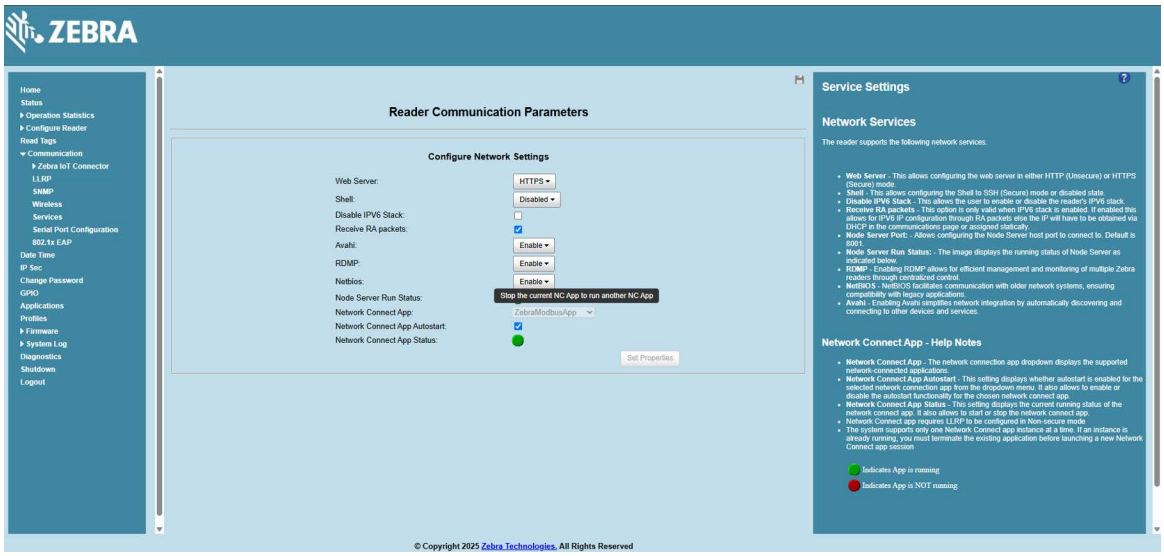
Procedure to Start a Network Connect App

The following procedure describes how to start a network connect app.

1. Select one of the network connect apps from the dropdown menu.
2. If you want the application to start automatically after a reboot, check the autostart option.
3. Click the Start button and ensure its status turns green.
4. Proceed to set properties.

1. The Network Connect app is supported only on the FX9600 and is not available on the FX7500 or ATR7000.
2. Network Connect app requires LLRP to be configured in Non-secure mode.
3. The system supports only one Network Connect app instance at a time. If an instance is already running, you must terminate the existing application before launching a new Network Connect app session.

Figure 57 After Network Connect App Is Started

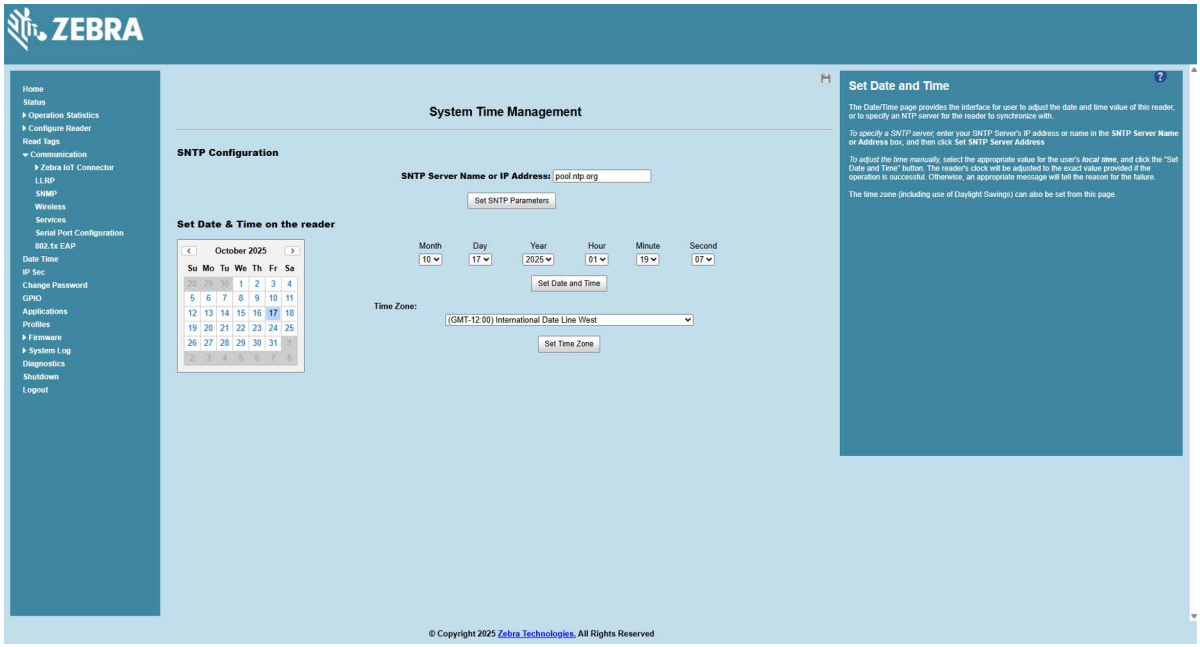


- After starting the Network Connect app and setting the properties, the web page will log out.
- The user must log in again and navigate to the service page.
- The Network Connect App status will show:
  - Green: The app has started successfully and is running.
  - Red: The app is not running.
- If autostart is enabled, this will be indicated.
- The Network Connect App selection will be greyed out, as only one app can run at a time.
- Hovering over the Network Connect App will display a message: "Stop the current running network connect app to run another NC app."
- To stop the currently running app, click the Network Connect App status button to change it to red, then set the properties.
- Once the operation is successful, the dropdown will be enabled, allowing you to start another Network Connect app.

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 58 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.

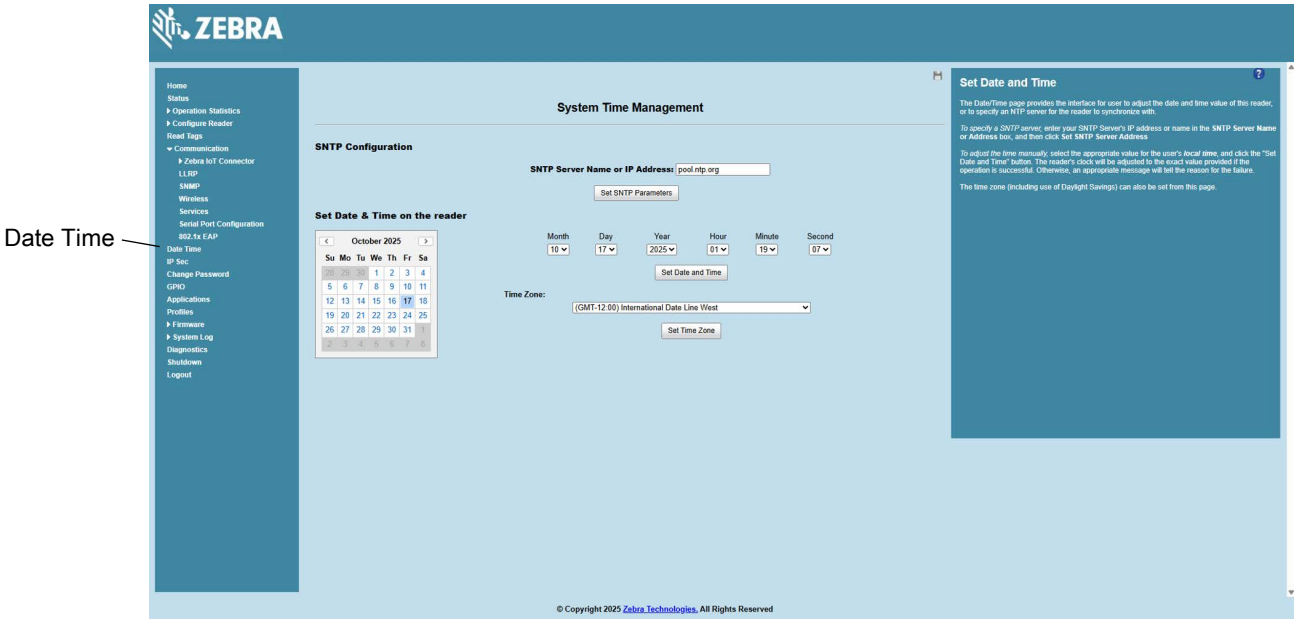
You can also set the **Time Zone** (including use of Daylight Savings) using the drop-down menu.

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 59 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:

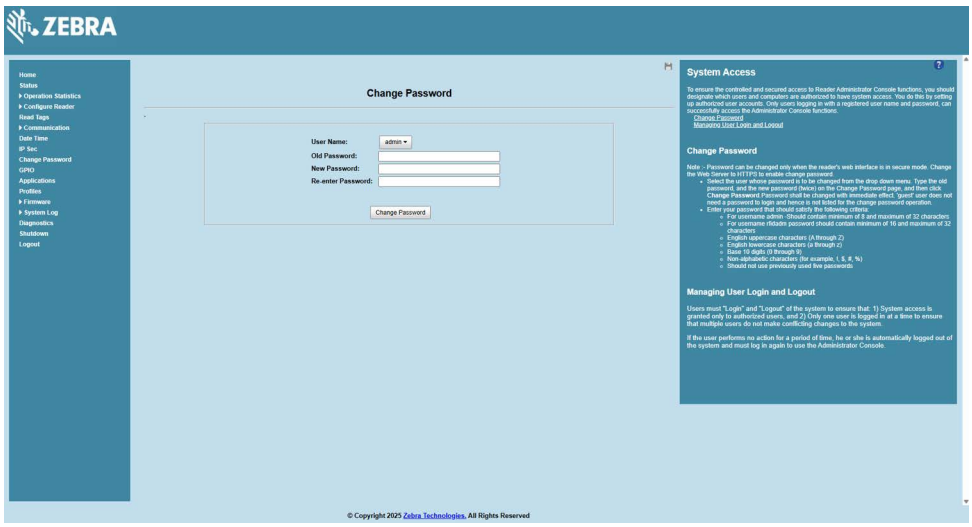
- **admin** - This user has web access but no shell access, with full privileges to make changes on the reader using the Administrator Console interface and to access to the reader using the FTP interface.
- **guest** - This user has web access but no shell access, with read-only privileges in the Administrator Console and can not make configuration changes. To log in as a guest user, the admin must first log in and set a password for the guest account by navigating to change password. After the password is set, the guest user can log in using those credentials.
- To set the guest password, ensure it meets the following requirements:
  - Minimum length: 8 characters
  - Maximum length: 32 characters
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example: !, $, #, %)

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

- **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 60 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.

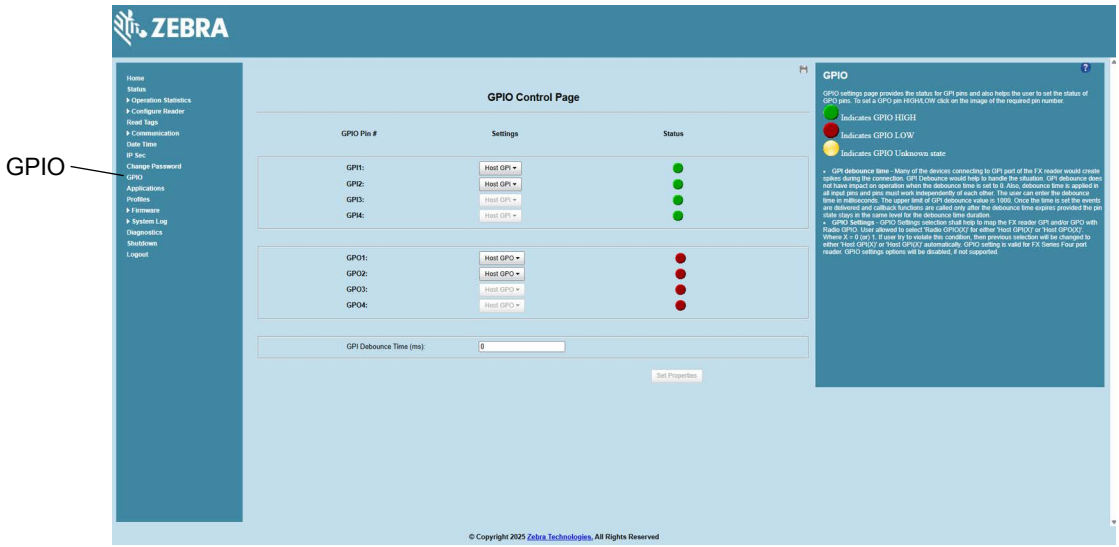
If the user performs no action for a period of time, the system automatically logs him or her out. The user must log in again to use the Administrator Console.

GPIO

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

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

Figure 61 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 62 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 the **rfidadm** user privileges.

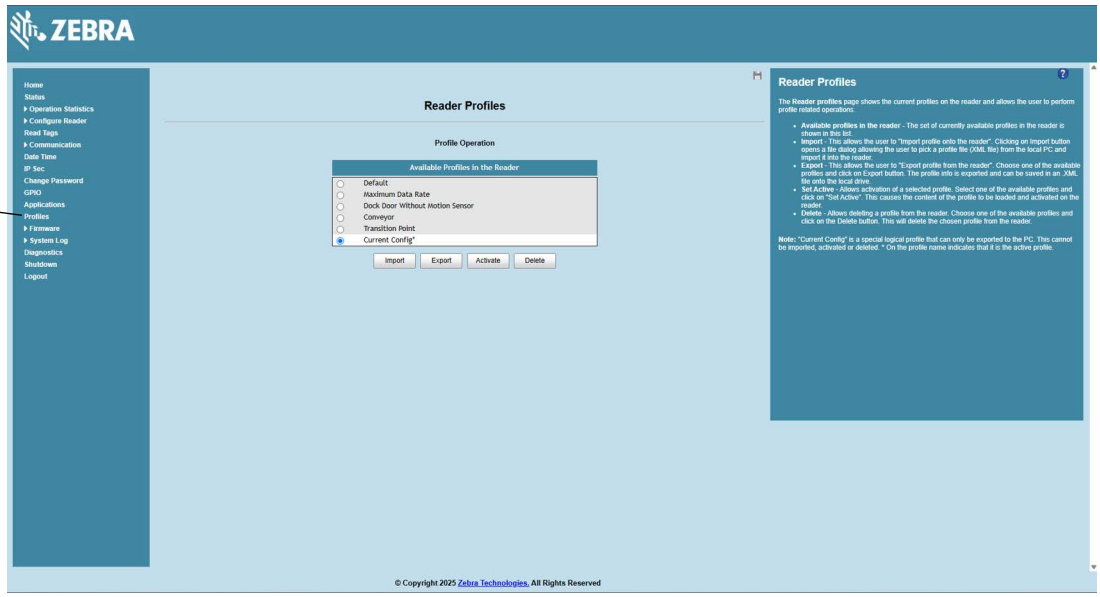
Reader Profiles

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

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.

NOTE: You cannot activate any profiles if the inventory is in progress.

Figure 63 Reader Profiles Window



The reader profile with the asterisk at the end is the active profile.

Out of the box, the Current Config profile is active.

The Current Config profile is the same as the Default profile until the user starts configuring the reader. When the user overwrites the out of box configuration, the reader still shows Current Config as the active profile, however at that point Current Config is not the same as the Default profile.

The **Reader Profiles** includes 5 build-in profiles:

- Default:
  - Use this profile to return the reader to the out-of-box RFID configuration.
  - The reader default settings in use include Session (S0), Target(A), Sel(SL All), Tag, and Population (100).
  - The RF mode is set to AutoMAC. In this RF mode, the radio scans RF environment to determine the best RF link settings so that the reader is interference tolerant while at the same time maximizes unique tag throughput.

- Maximum Data Rate:
  - This profile demonstrates maximum tag read rate in low interference environments.
  - The RF mode is set based on the reader module (see Table 8).
  - Other parameters used in this mode are Session (S0), Target(A/B), Sel(SL All), and Tag Population (300).
  - This profile can be used to stress test the application ability to process large data rates.
- Dock Door with Motion Sensor:
  - This profile can be used to monitor tag passing through the dock door.
  - The RF mode is set based on the reader module (see Table 8).
  - Other Parameters used in this mode are Session (S2), Target(A), Sel(SL All), and Tag Population (300).
  - This profile can be customized to include the additional GPI trigger to link door open/close.
- Conveyor:
  - This profile can be used to detect single tag passing reading field on the conveyor.
  - The RF mode is set based on the reader module (see Table 8).
  - The tag population is set to 5 due to few tag in FOV.
  - The antenna dwell time is set to 25 ms per antenna.
  - Other parameters used in this mode are Session (S2), Target(A), and Sel(SL All).
- Transition Point:
  - This profile can be used to detect tag status such as moving tag and stationary tag.
  - It works with applications such as autonomous event mode or portal directionality.
  - The RF mode is set based on reader module (see Table 8).
  - Other parameters used in this mode are Session (S2), Target(A), Sel(SL All), and Tag Population (300).

Table 8 lists the parameter setting of build-in profiles.

NOTE: Refer to Table 19 on page 195, Table 20 on page 197, and Table 21 on page 199 for RF mode index definitions.

Table 8 Parameter Settings of Build-in Profiles

Profile Name	RF Mode Index				Session	Target	Sel	Tag Population
	US-FCC	EU-ETSI	JP-FX9600	JP-FX7500				
Default	23	21	11	5	S0	A	SL ALL	100
Maximum Data Rate	1	10	21	3	S0	A/B	SL ALL	300
Dock Door with Motion Sensor	1	10	21	3	S2	A	SL ALL	300
Conveyor	1	10	21	3	S2	A	SL ALL	5
Transition Point	1	10	21	3	S2	A	SL ALL	300

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:

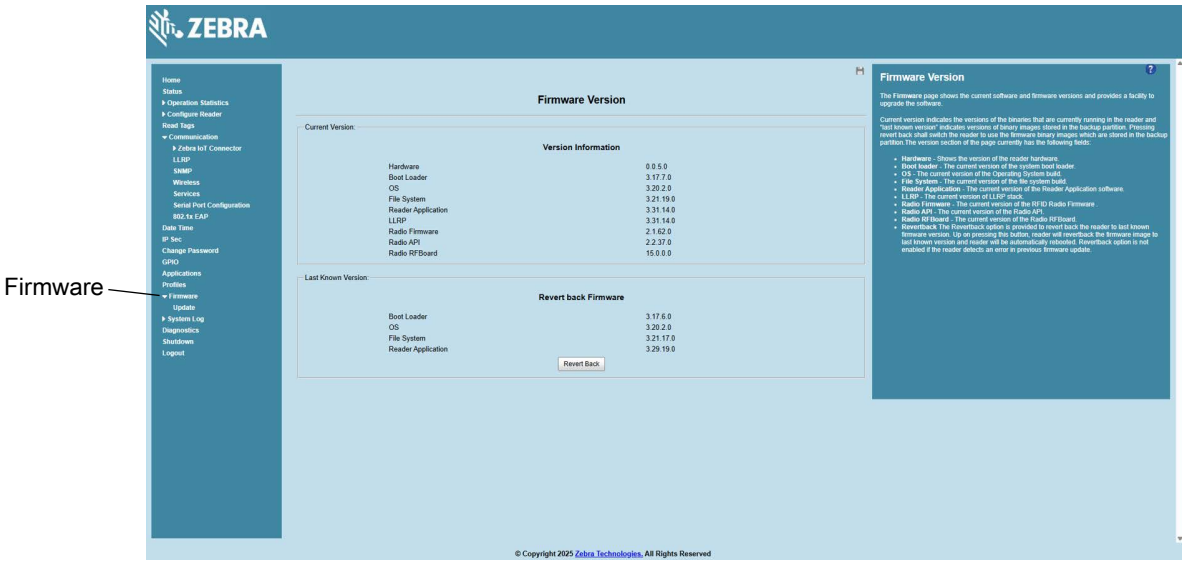
- HTTPS
- SSH
- LLRP Server
- IPSec.

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 and Update

Select **Firmware** from the selection menu to view **Firmware Version** window. This window displays the current software and firmware versions and allows users to upgrade the firmware.

Figure 64 Firmware Version



Current Version displays the binary versions currently running in the reader. **Last Known Version** displays the 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.

NOTE: If an embedded application no longer runs due to the new tool chain and Linux kernel, recompile the application with new embedded SDK or revert the reader to the older firmware which supports older embedded applications.

Firmware Update

Select **Update** from the selection menu to view **Firmware Update** window. This window allows users to upgrade the firmware of the readers.

NOTE: You must log in as Administrator to have the access to this window.
See Change Password on page 98.

The FX readers support three firmware update methods:

- 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, or SCP server-based update.

To upgrade the firmware of the readers, see Firmware Upgrade.

Commit/Discard Functionality Changes

The **Commit/Discard** menu is removed in the firmware version 3.0.35 or newer. After making changes to the reader configuration, you must select **Set Properties** for the changes to take effect.

This sections includes two examples on how to save the changes to the reader configuration.

Region Configuration Commit

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

1. On the **Configure Region Settings** window (see Figure 65 on page 107):
   a. Select the region from the **Region of operation** drop-down menu.
   b. Select the Communication Standard, if applicable.
   c. Select Frequency Hopping, if applicable.
   d. Select the appropriate channel(s), if applicable.
   e. Select the **I understand** check box.
2. Select **Set Properties** to save the new region configuration. The **Operation Successful** window displays a **Saving. Please wait...** message with a progress symbol (see Figure 66 on page 107).
3. When the commit completes, the page displays a gray floppy disk icon (see Figure 67 on page 108). The settings are now set and stored in the reader. If other actions are required to complete the changes (for example, a reader reboot), the action message displays at the top of the window.

Figure 65 Configure Region Settings

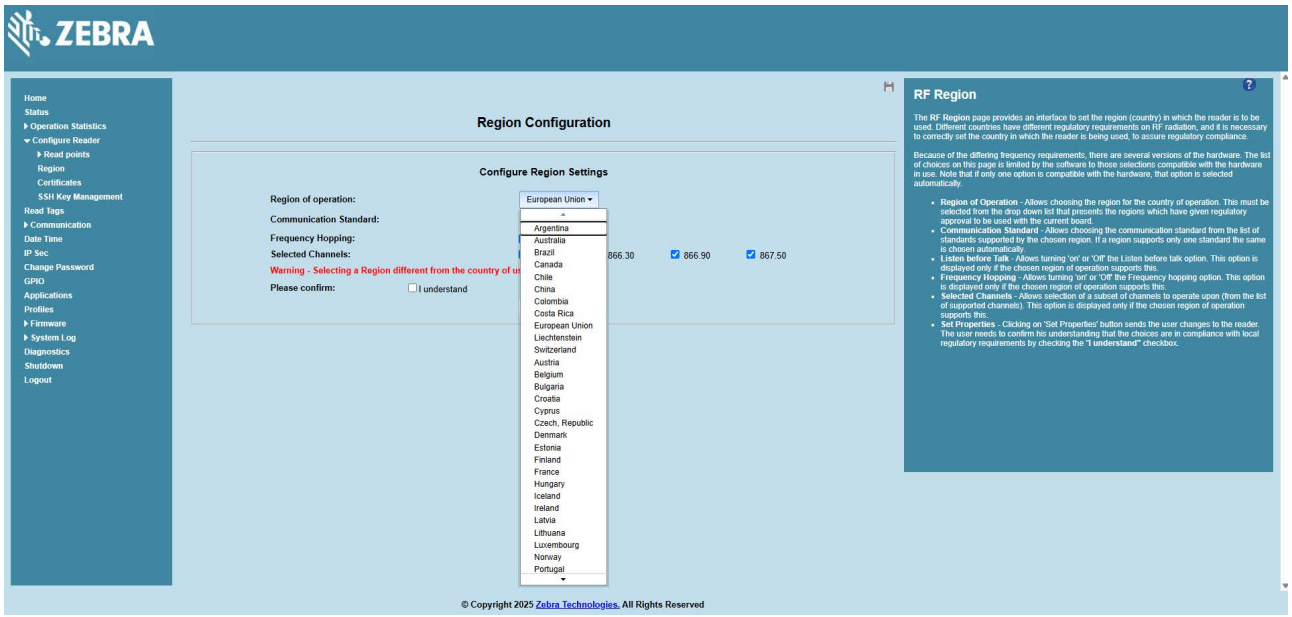


Figure 66 Configure Region Settings - Saving Message

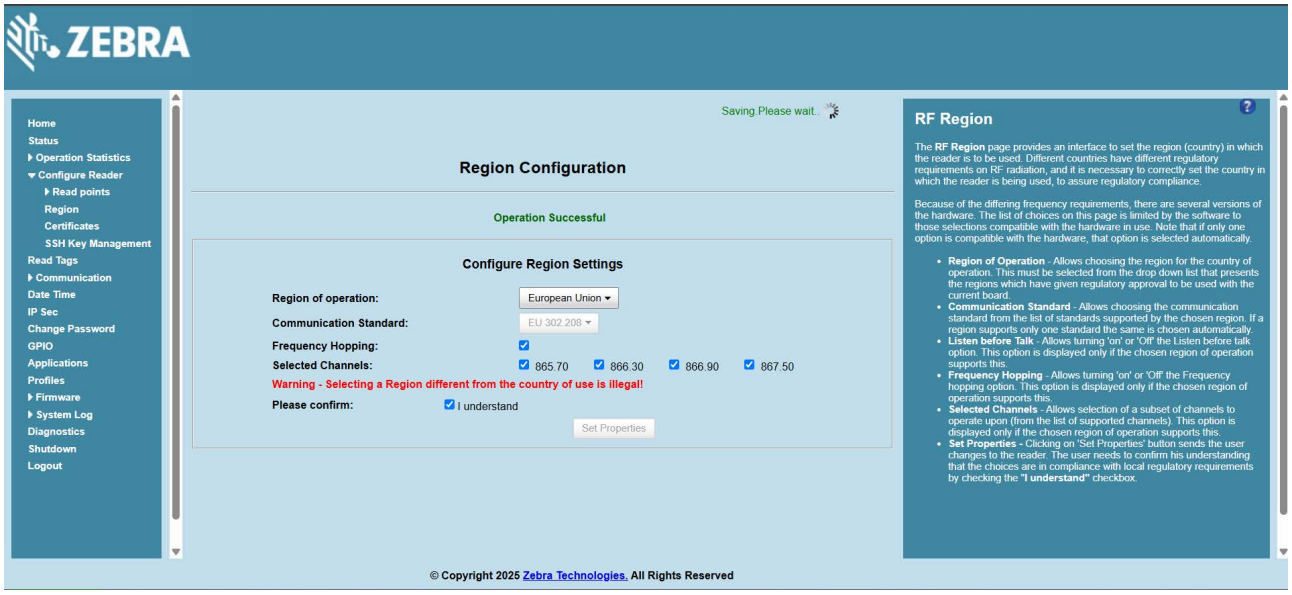
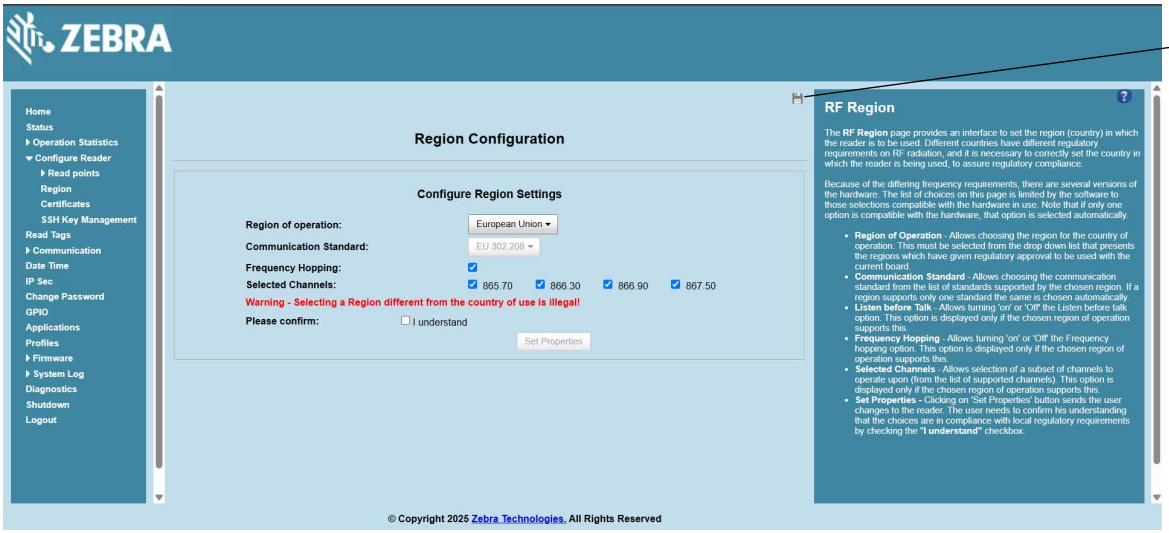


Figure 67 Configure Region Settings - Commit Complete

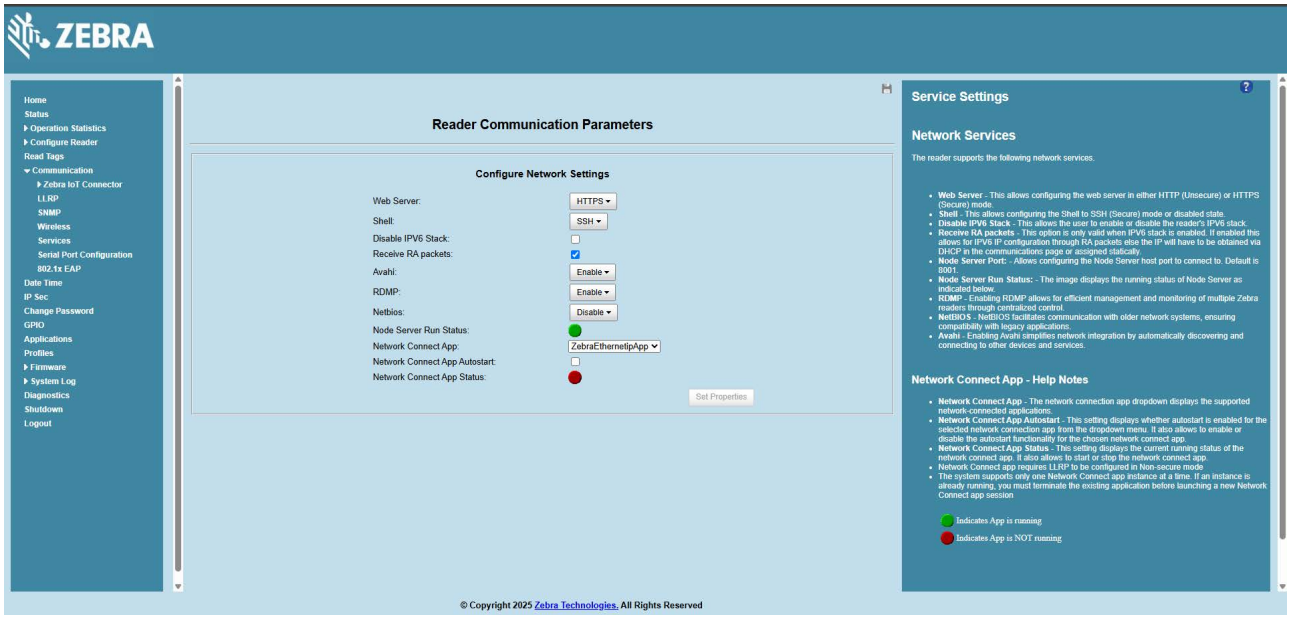


New Property Change Work Flow

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

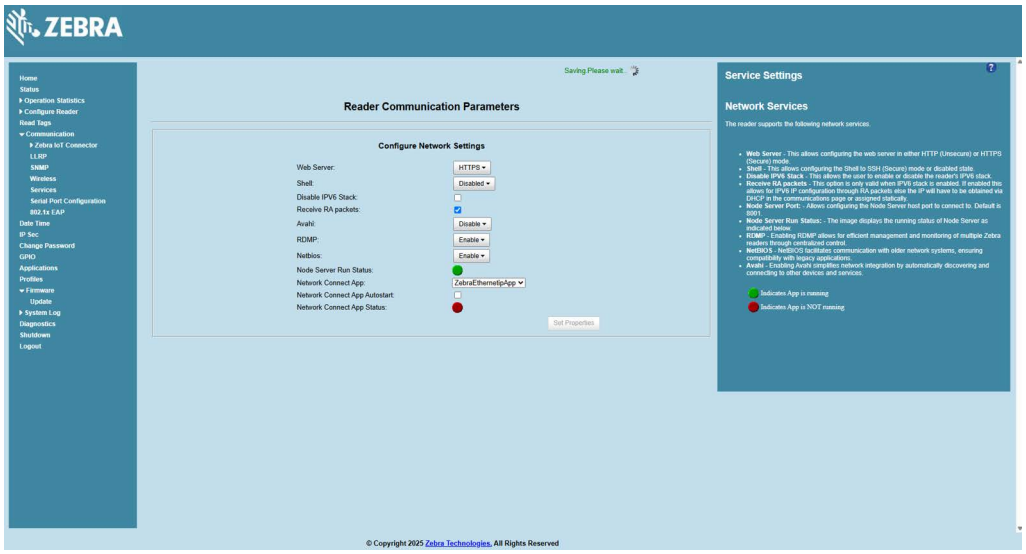
1. On the **Configure Network Settings** screen, select the appropriate options from the drop-down menus as shown in Figure 68.

Figure 68 Configure Network Settings



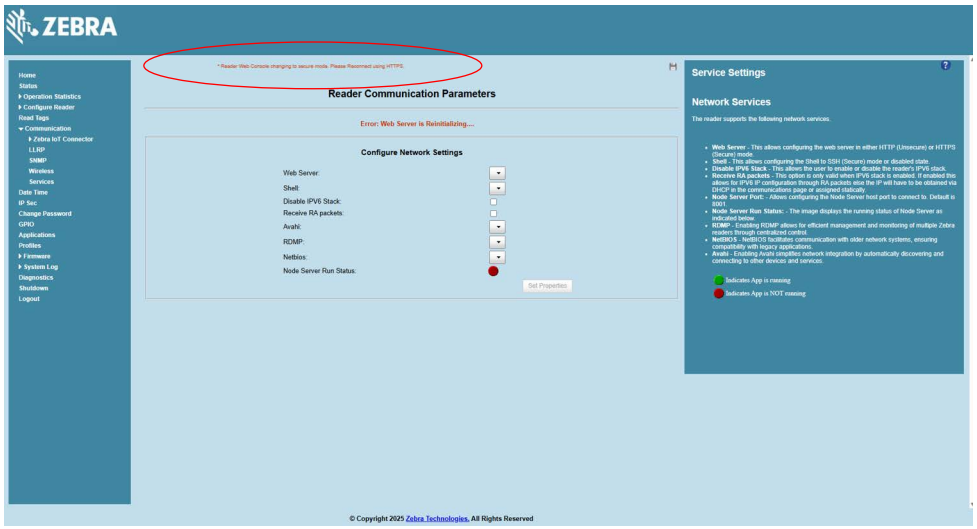
2. Select **Set Properties**. The message **Saving.Please wait...** displays with a progress symbol (see Figure 69 on page 109).

Figure 69 Configure Network Settings - Saving Message



3. When the commit completes, the page displays a gray floppy disk icon. The settings are now set and stored in the reader. If other actions are required to complete the changes (for example, a reader reboot), the action message displays at the top of the window (see Figure 70 on page 109).

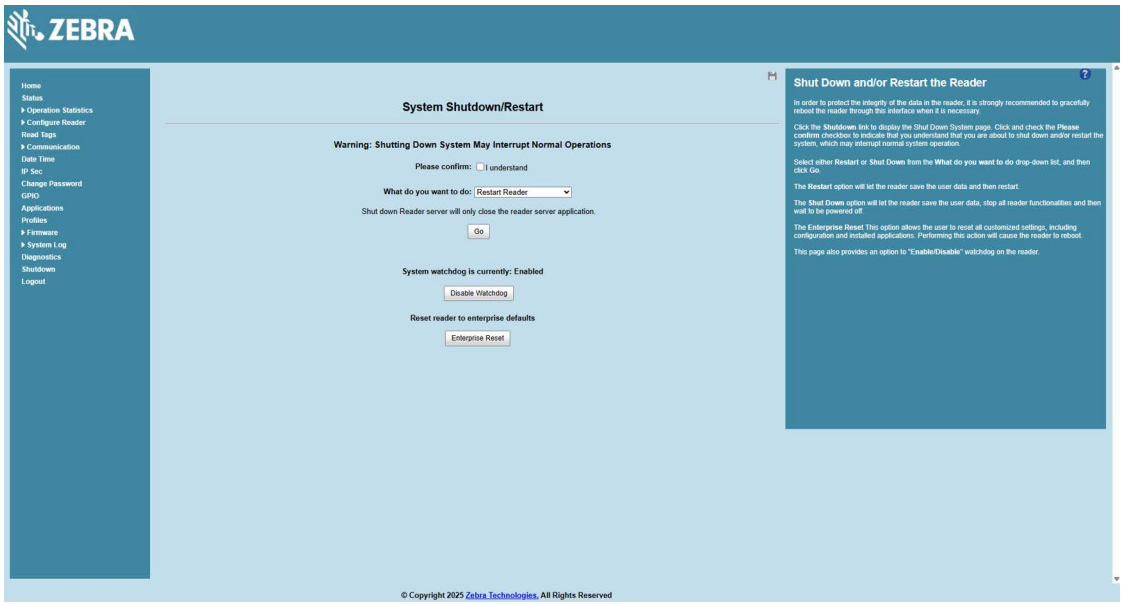
Figure 70 Action Message



IMPORTANT: With the new software version, the Discard Functionality option is no longer supported. Changes are automatically commit to the reader after selecting **Set Properties**.

The reset reader to factory defaults option is on the System Shutdown/Restart screen (see Figure 71).

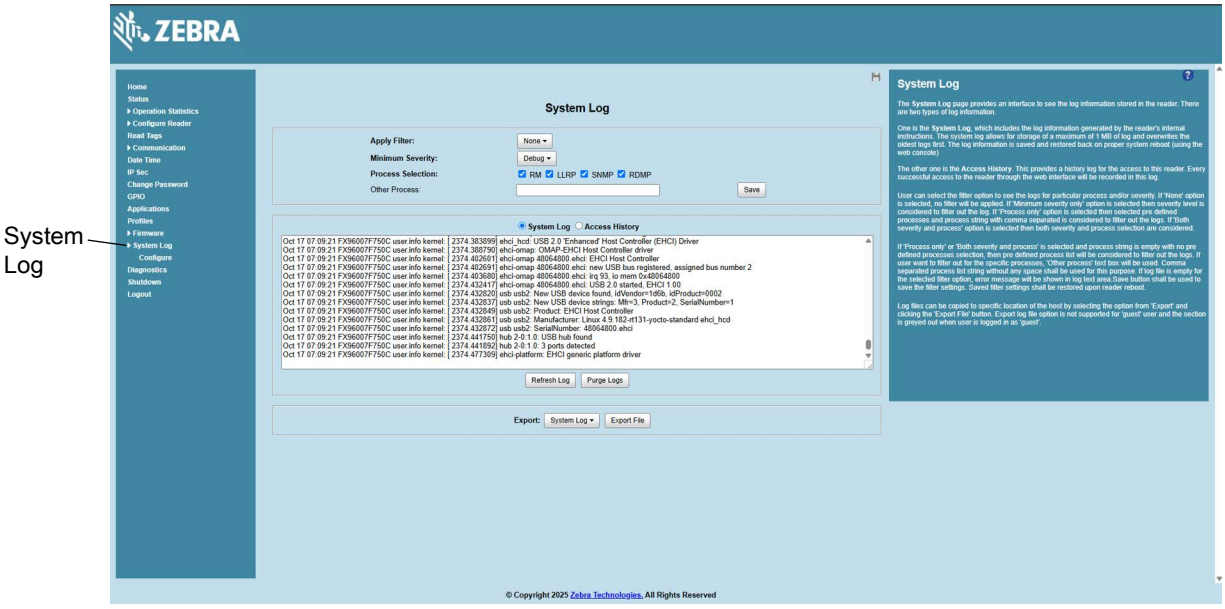
Figure 71 Enterprise Reset the Reader



System Log

Select **System Log** from the selection menu to view the **System Log** window. This window lists the reader log information.

Figure 72 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 selected, the log severity level filters the log content. Logs that have severity levels equal or above the selected severity display.
  - **Process Selection** - When this option is selected, 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 selected, 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.

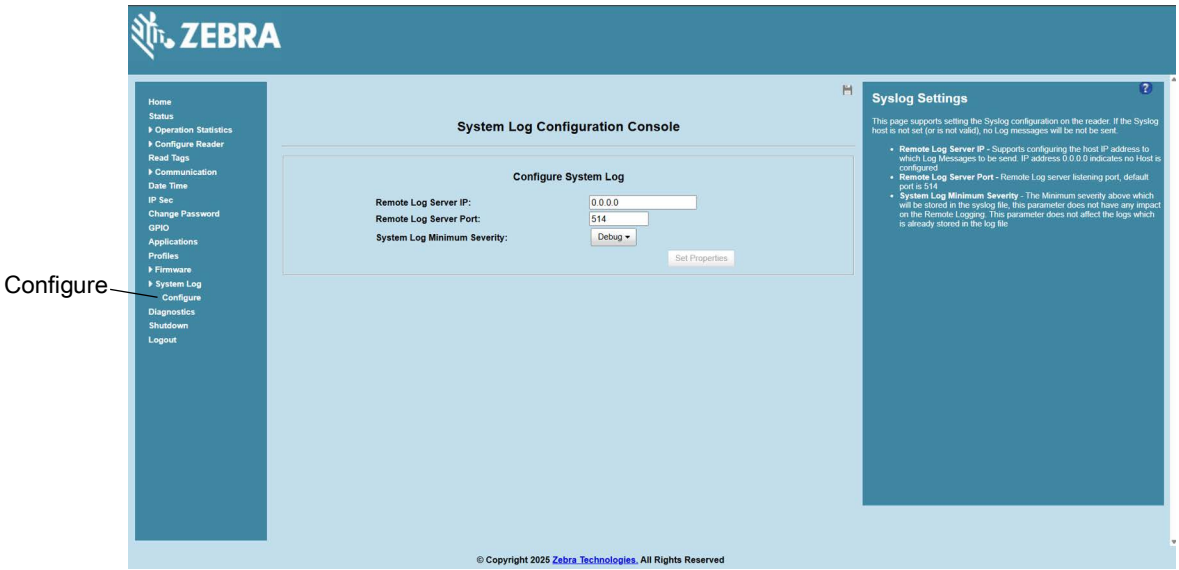
- **Log area** - Select a radio button for one of the two types of log information offered:
  - **System Log** - Includes the log information generated by the reader internal instructions. This stores up to 1 MB of log information, and overwrites the oldest logs first. The log information is saved and 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** drop-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** drop-down menu, then select **Export File**. This saves the data file in the **Downloads** folder on the PC.

Configure System Log

Select **System Log > Configure** to view **Configure System Log** window. This window configures system log settings. If the system log host is not set (or is not valid), log messages are not sent.

Figure 73 Configure System Log Window



This window includes 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.

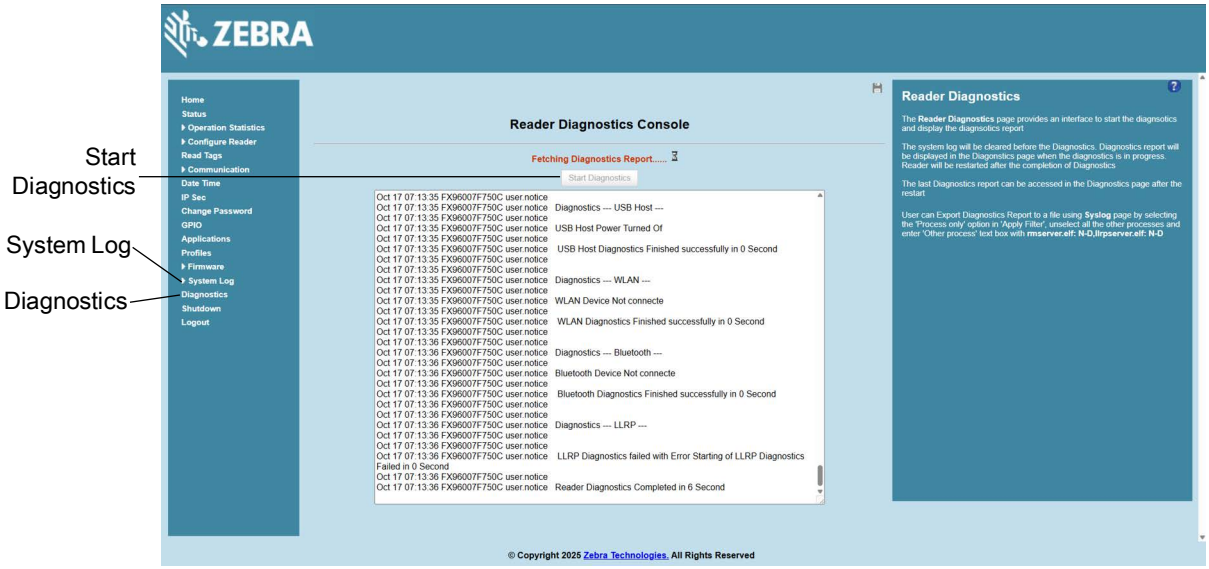
Select **Set Properties** to apply the changes. The **Operation Successful** window displays a **Saving. Please wait...** message with a progress symbol until the commit completes.

When the commit completes, a gray floppy disk icon displays indicating that the commit completed successfully. See Commit/Discard Functionality Changes on page 106 for more information.

Reader Diagnostics

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

Figure 74 Reader Diagnostics Window



Select **Start Diagnostics** to clear the system log and display the diagnostics report. The reader reboots when the diagnostics completes. Return to the **Diagnostics** window to view the diagnostics report.

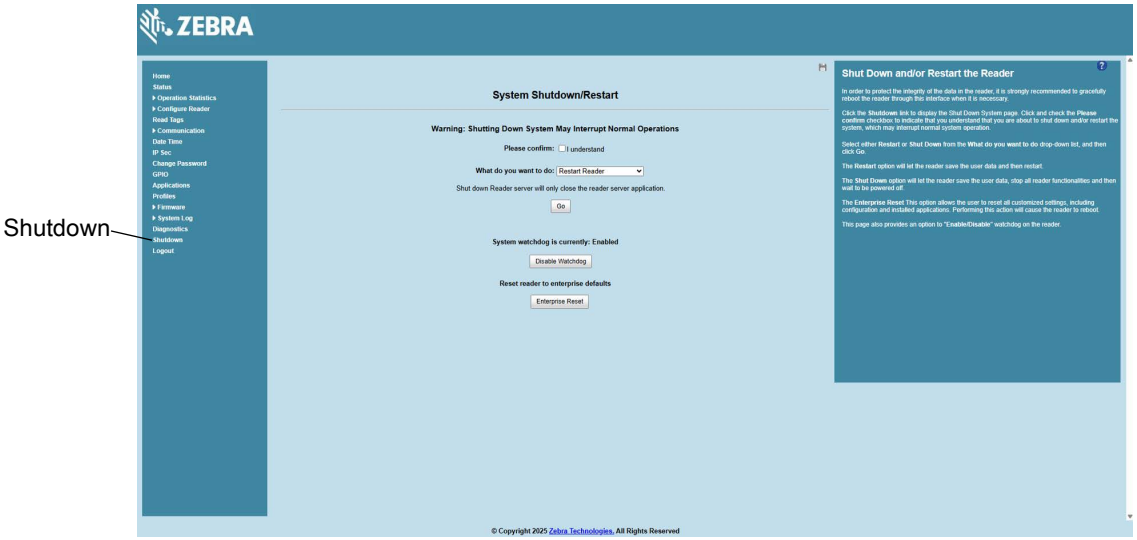
To export the diagnostics report to a file:

1. Select **System Log** (see Figure 74).
2. On the **System Log** window (see System Log on page 111):
   a. Select **Process Selection only** in the **Apply Filter** drop-down menu.
   b. De-select all other processes.
   c. In the **Other Process** text box enter:
   rmserver.elf: N-D,llrpserver.elf: N-D.

Shutdown

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

Figure 75 System Shutdown/Restart Window



To shut down or restart the reader:

1. Select the **Shutdown** from the selection menu 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 **Enterprise Reset** option clears all the customized user settings including the configuration and the installed application in the reader. The reader reboots after the Enterprise reset is complete.

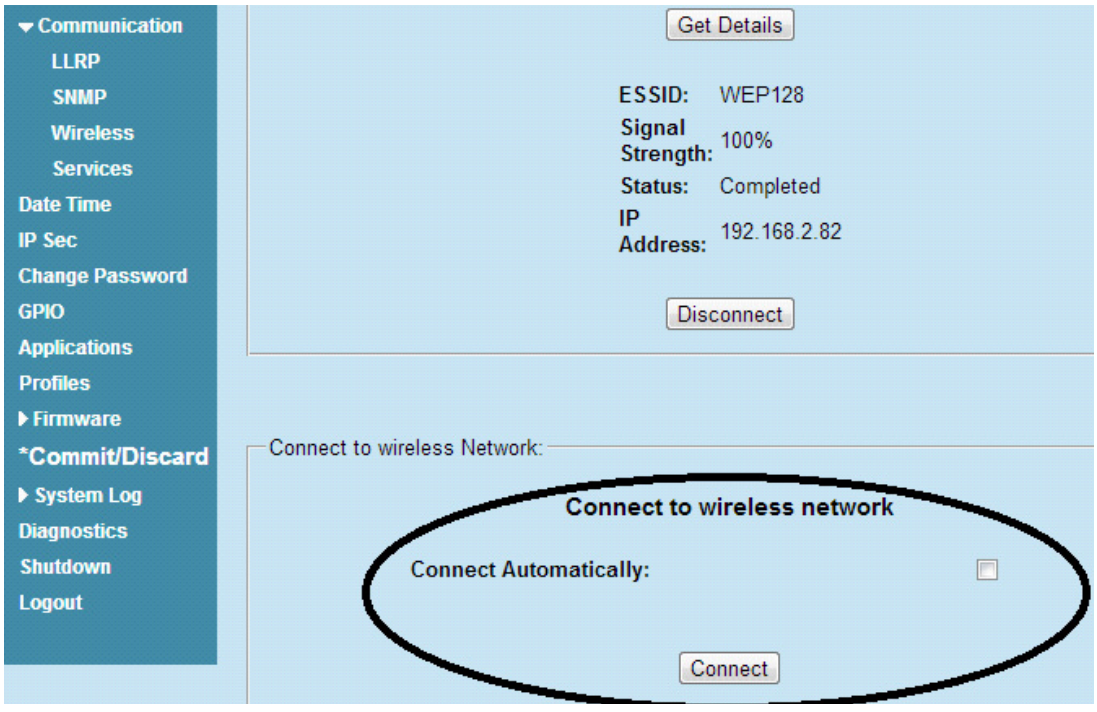
Configure and Connect via Wi-Fi and Bluetooth

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 linux.die.net/man/5/wpa_supplicant.conf for the most commonly used parameters and 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 76 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 linux.die.net/man/5/wpa_supplicant.conf for further examples.

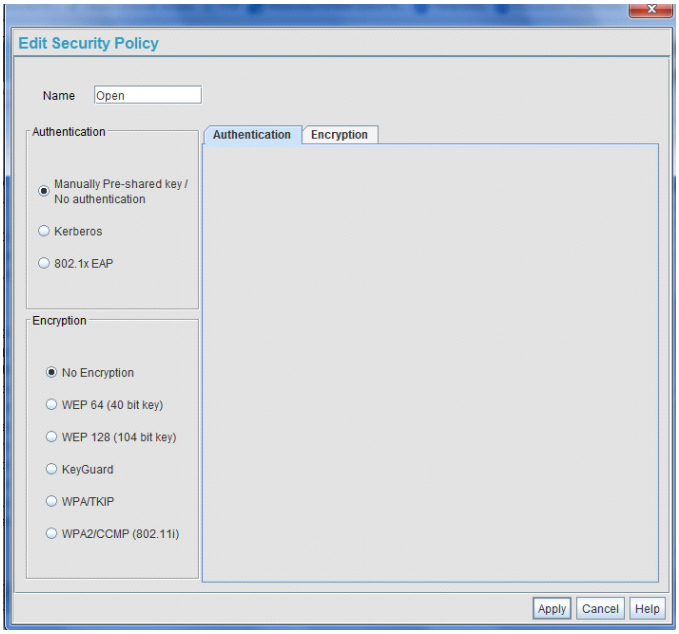
Preferred Configurations for Access Points

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 77 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**.

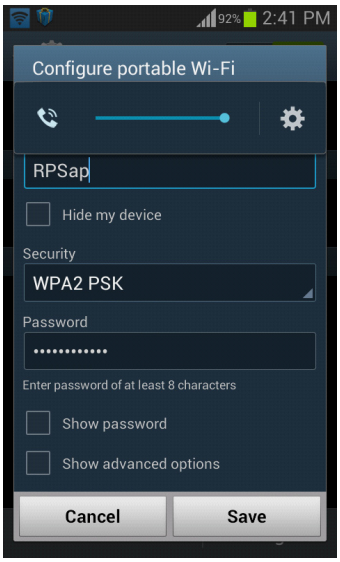
Figure 78 Open Network Configuration for Android Device

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 79 WPA2 PSK Configuration for Android Device

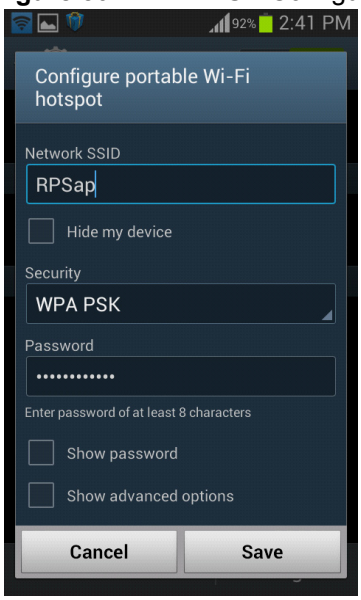


WPA PSK

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 80 WPA PSK Configuration for Android Device

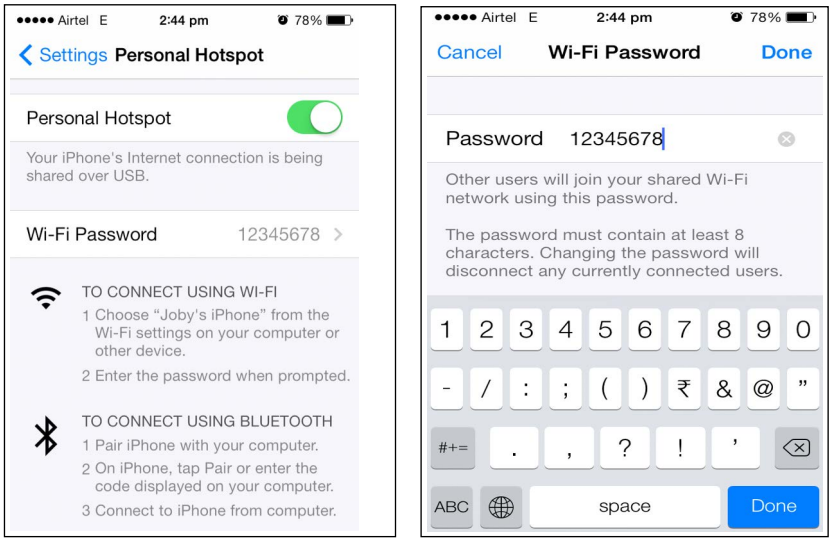


Internet Connection Configuration for iPhone

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 81 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 85 for a list of supported Wi-Fi dongles.

Figure 82 FX7500 USB Host Port Location for Dongle

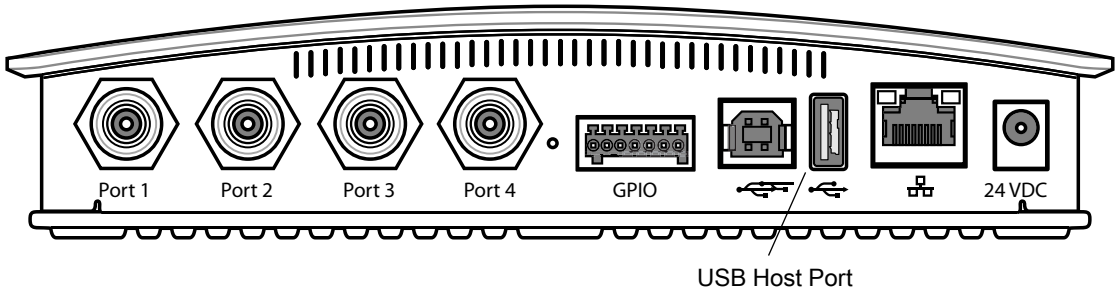
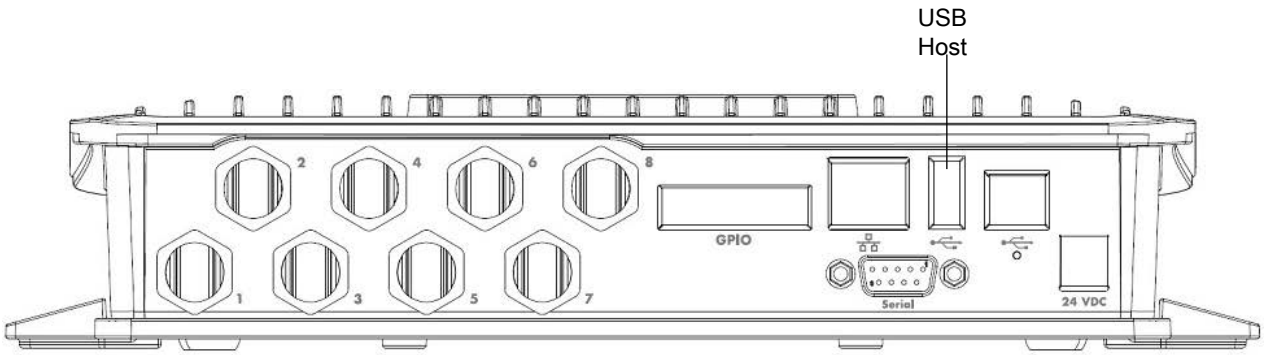
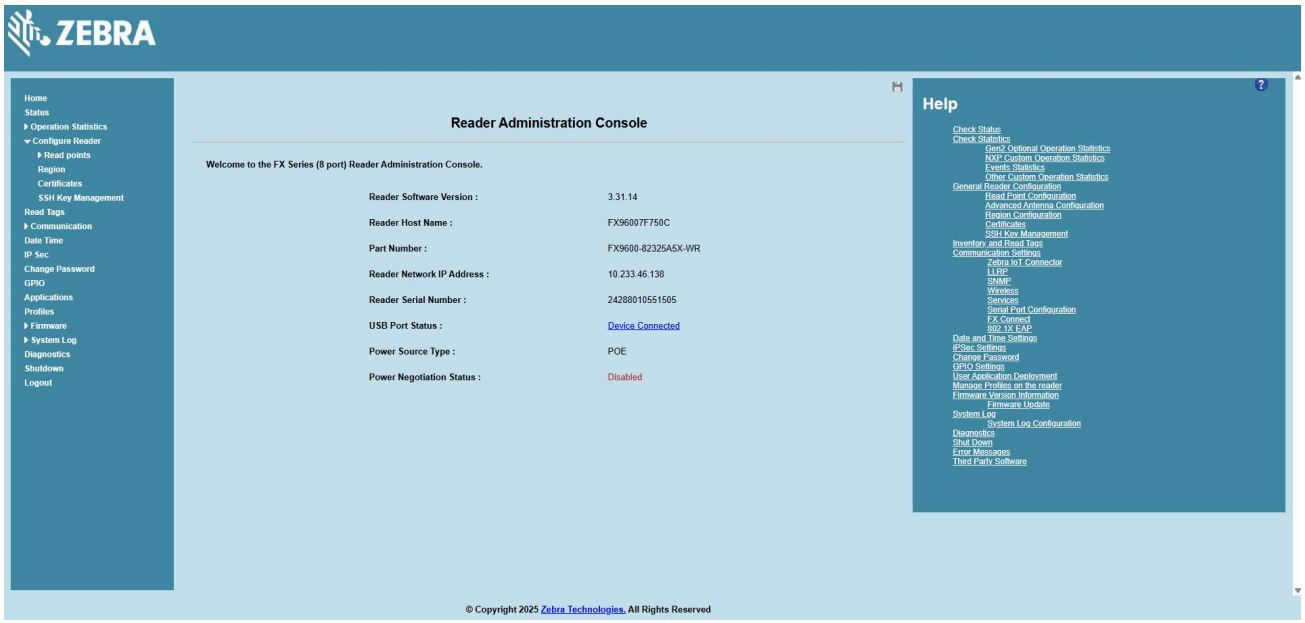


Figure 83 FX9600 USB Host Port Location for Dongle



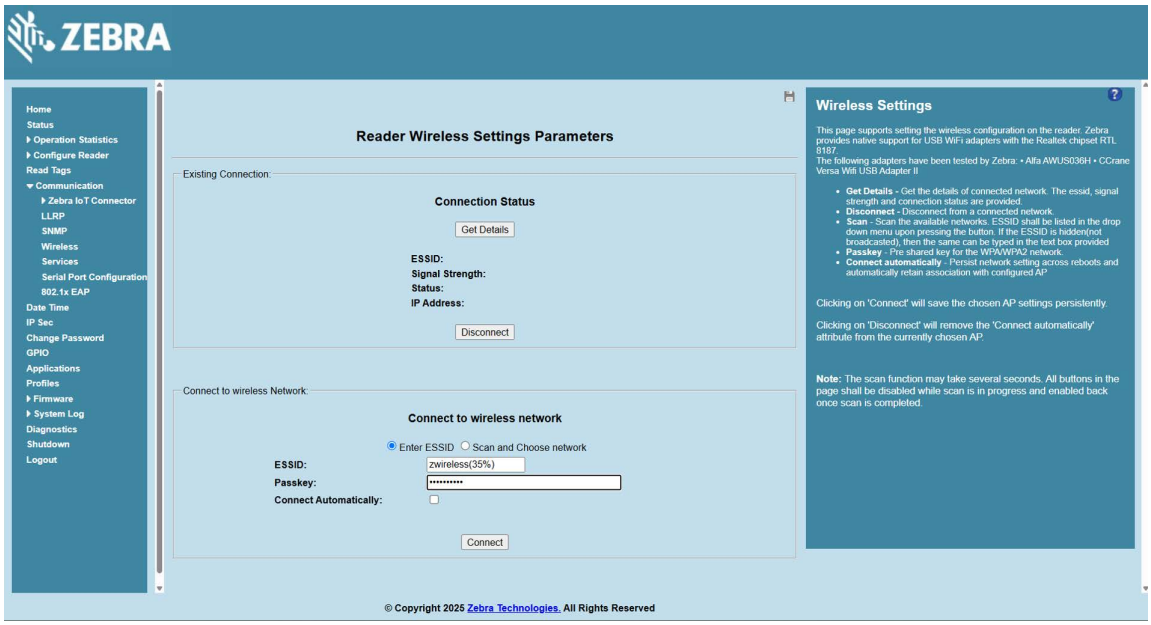
2. To confirm that the Wi-Fi dongle is detected properly, log in to the reader Administrator Console. On the Home page ensure the **USB Port Status** displays **Device Connected**. Hover the mouse pointer over this link to display the Wi-Fi dongle information shown in Figure 84.

Figure 84 Wi-Fi Dongle Connected



3. Select **Communication > Wireless**.

Figure 85 Wireless Settings

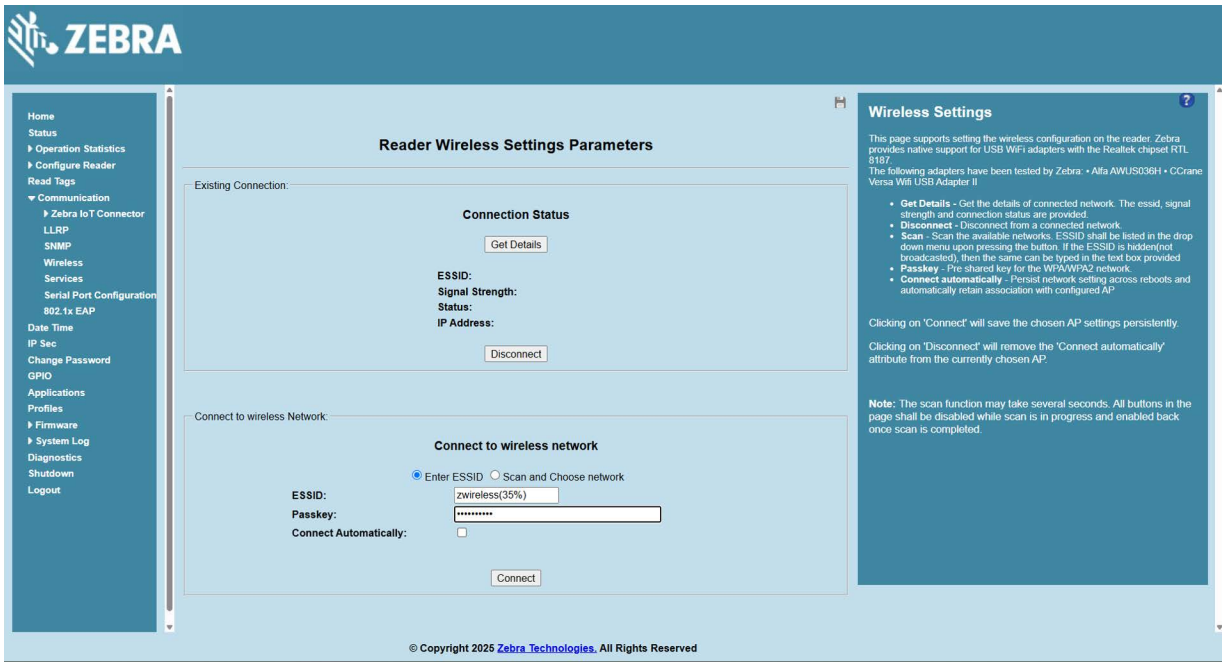


The Wi-Fi dongle can connect to the wireless network in one of two ways:

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

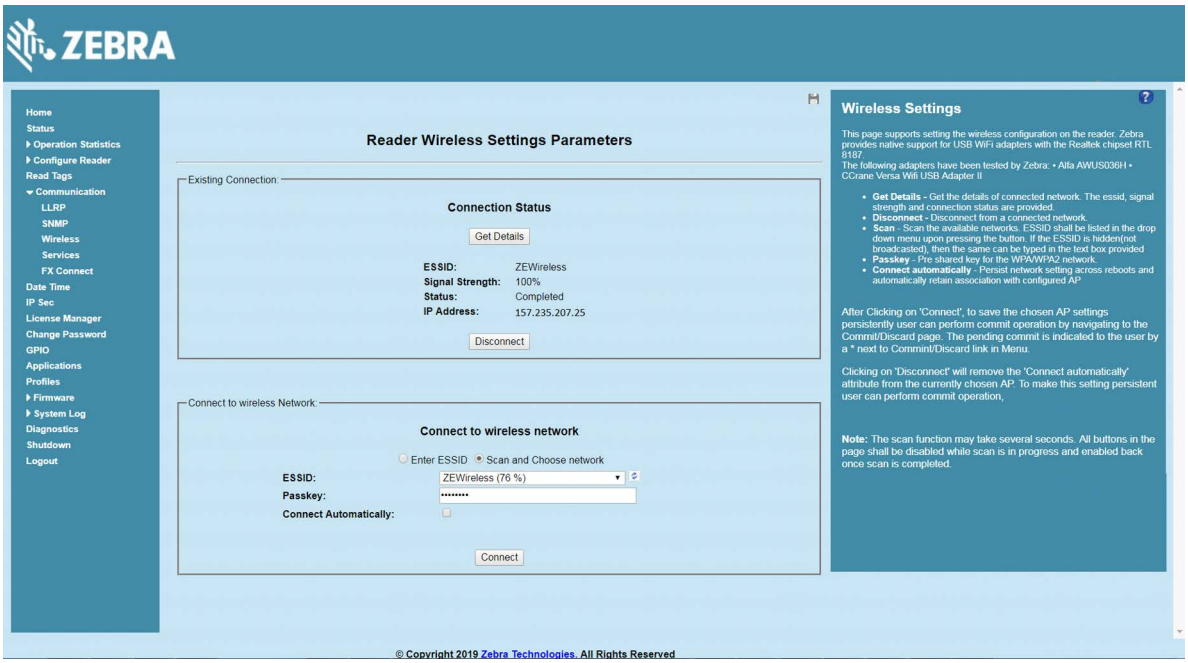
4. Once the APs are scanned, enter the appropriate passkey and enable **Connect Automatically** (if required to connect to the AP automatically if the connection is lost).

Figure 86 Entering Connect Information



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

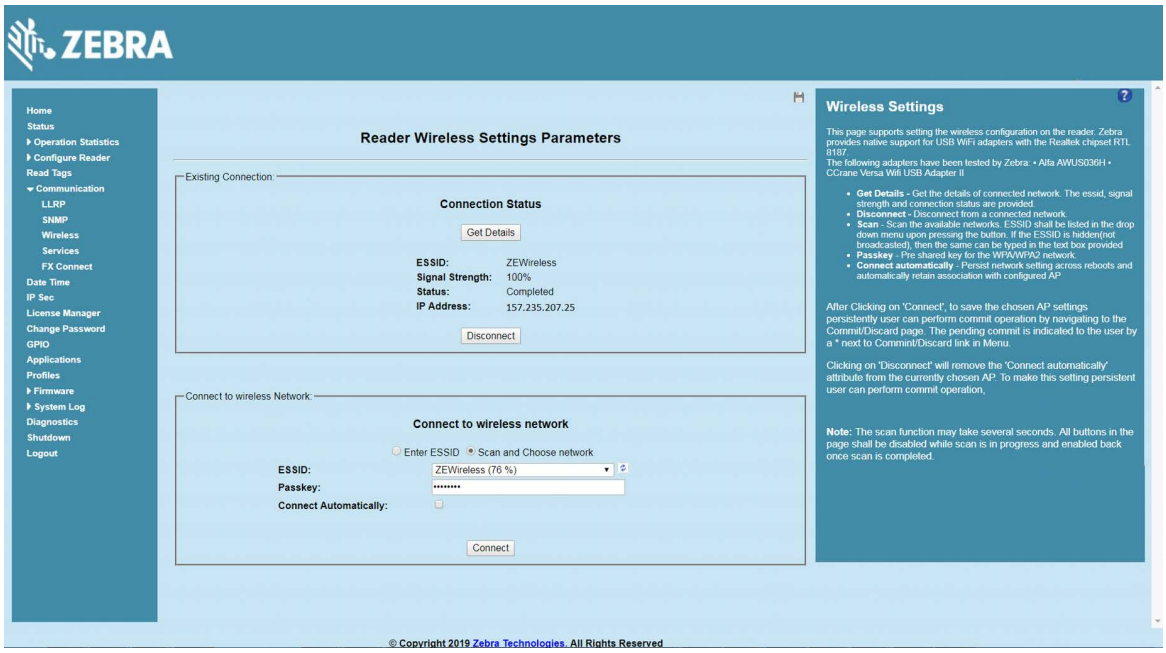
Figure 87 Assigned IP Address



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

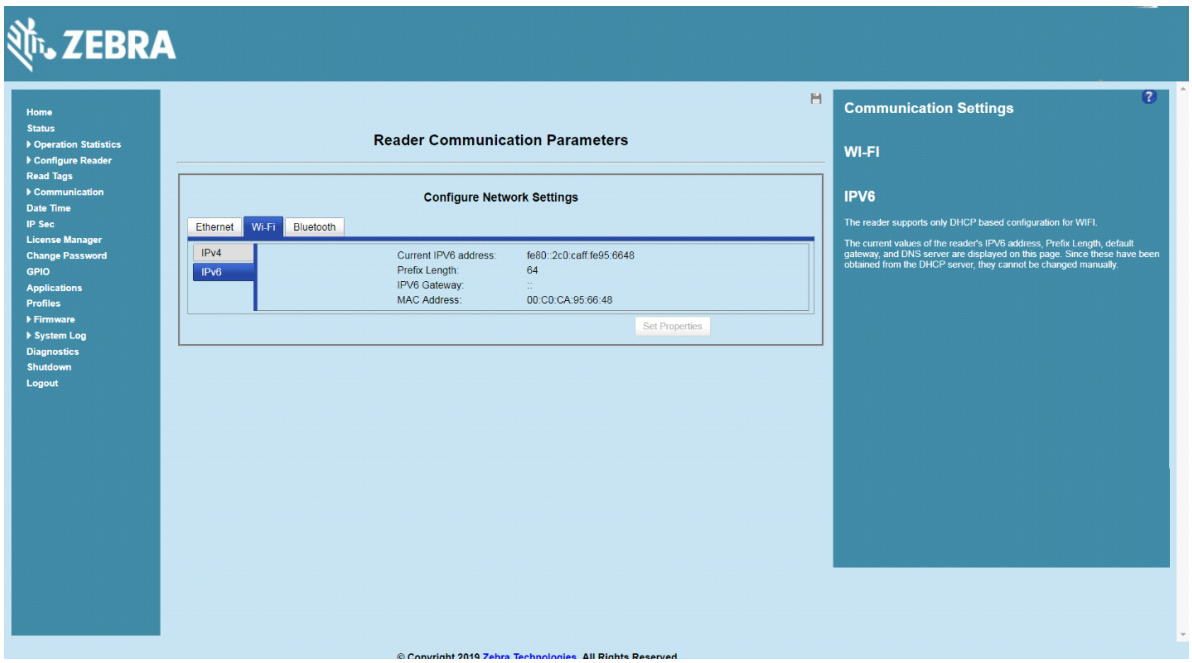
For wireless IP address details, select **Communication > Wi-Fi** tab.

Figure 88 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 89 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:

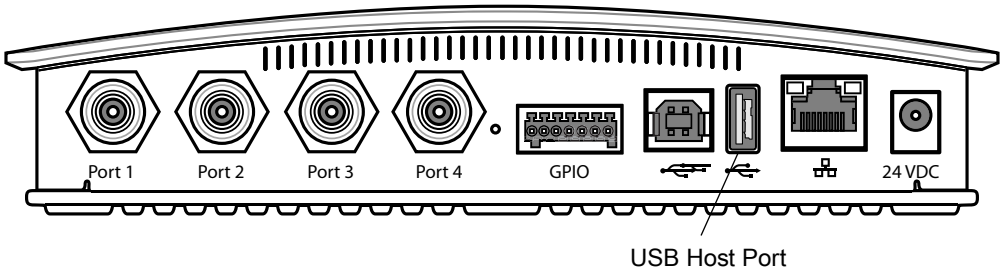
1. Plug the supported Bluetooth dongle into the USB host port on the FX Reader.

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

Table 9 Supported Bluetooth Dongles

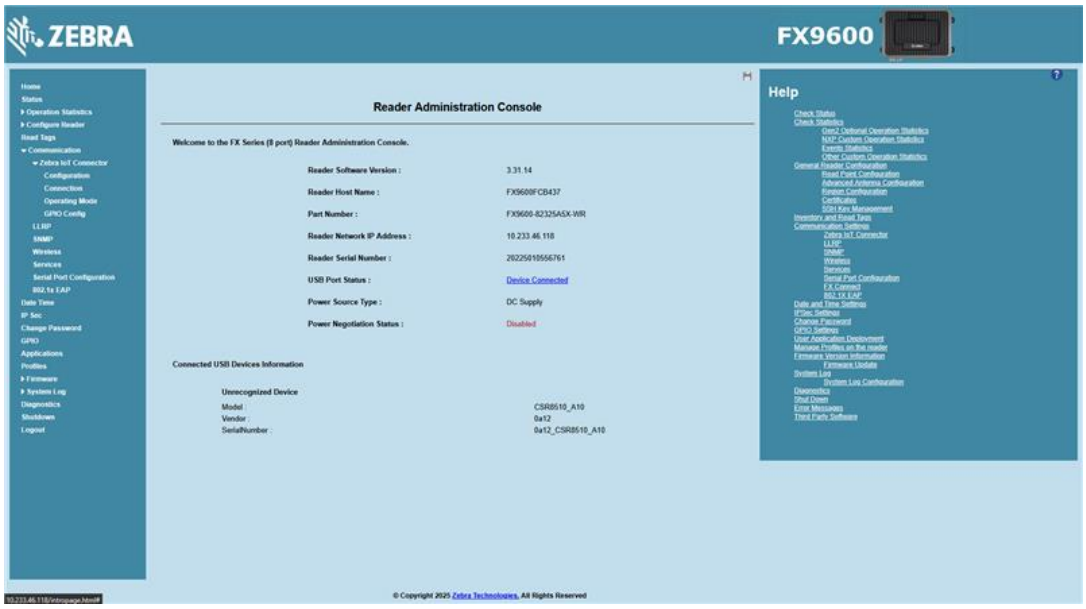
Dongle Model	Zebra FX7500	Zebra FX9600
Bluetooth CSR 4.0 dongle Qualcomm / Atheros CSR8510	Yes	Yes
Bluetooth 3.0+HS Ralink RT5370L	Yes	Yes
Asus Mini Bluetooth Dongle USB-BT211	Yes	Yes
MediaLink Bluetooth Dongle MUA-BA3	Yes	Yes
Broadcom BCM20702A0	Yes	Yes

Figure 90 USB Host Port Location for Dongle



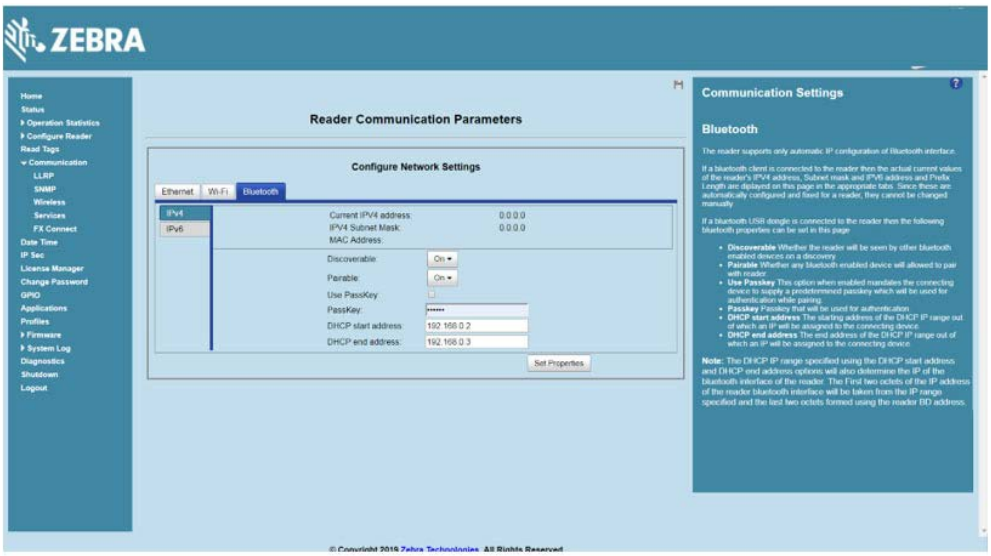
2. To confirm that the Bluetooth dongle is detected properly, log in to the reader Administrator Console. On the **Home** page ensure the **USB Port Status** displays **Device Connected**. Hover the mouse pointer over this link to display the Bluetooth dongle information.

Figure 91 Bluetooth Dongle Connected Select **Communication > Bluetooth**.



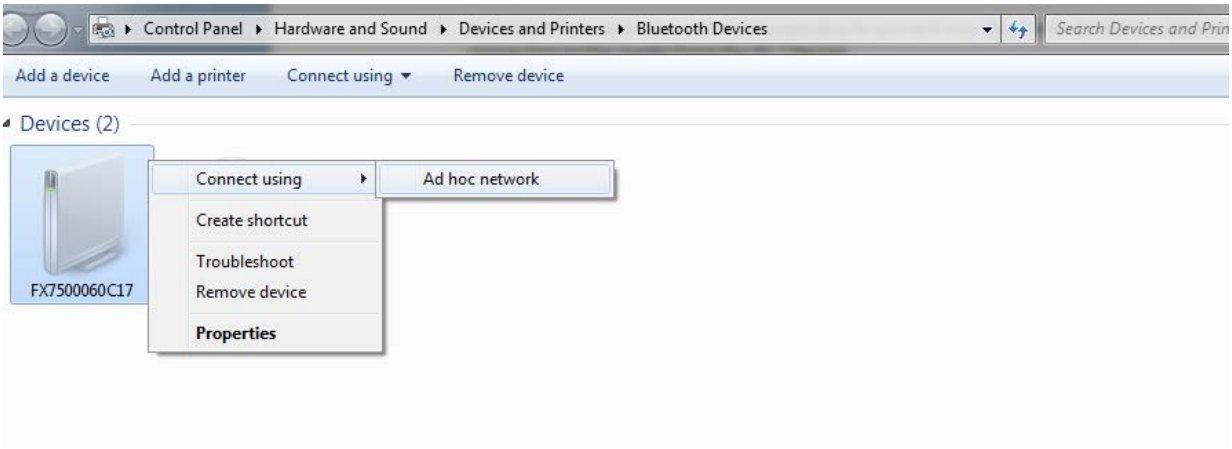
3. Change the **Discoverable** and **Pairable** properties to **On**.

Figure 92 Changing Discoverable and Pairable Properties



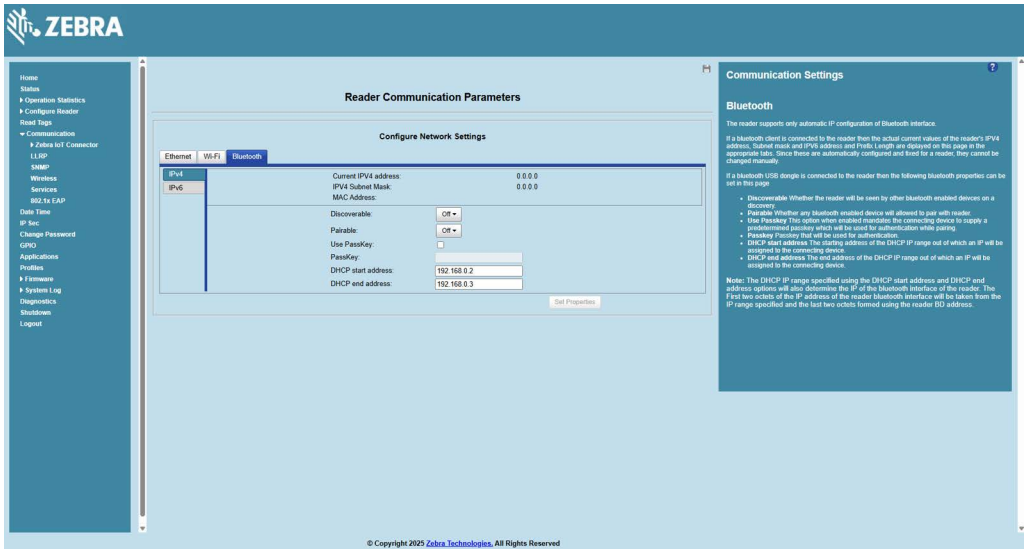
4. Optionally select **Use Passkey** and enter a passkey to validate the Bluetooth connection. The default passkey for the FX7500 and FX9600 is **0000**.
5. Discover the reader from a Bluetooth-enabled device (such as a laptop). Use the host name to identify the reader among the discovered devices (for 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 93 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 94 Communication Bluetooth Tab



Open the web page or sample application to connect to the Bluetooth IP (192.168.67.21 in Figure 94) 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 are 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.

Firmware Upgrade

Introduction

This chapter provides the reader firmware update information using the web-based **Administrator Console**. The following methods are available to update the firmware of the FX Series Readers:

- Using a USB drive. See Using a USB Drive (Recommended) on page 132.
- File-based update that allows uploading the firmware files from the PC (or a network location) to the reader and running the update. See File-Based Update on page 134.
- FTP, FTPS, or SCP server-based update. See FTP/SCP-Based Update on page 136.

Use this procedure to update the following software components:

- uboot
- OS
- Reader Server Application (includes the 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)
  - uImage_ *X.X.X.X* (OS, *X.X.X.X* is a filename variable)
  - rootfs_ *X.X.X.X*.jffs2 (Root FileSystem, *X.X.X.X* is a filename variable)
  - platform_ *X.X.X.X*.tar.gz (Platform partition, *X.X.X.X* is a filename variable).

Refer to the release notes to determine which files 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 displays red.

Two-step Firmware Update

NOTE: After the reader firmware is upgraded or downgraded from or to any other versions that are earlier than 3.0.35, some UI pages do not work properly due to cache. Refresh the browser to update the browser web page after update or downgrade.

Due to the increase of firmware footprint in some circumstances, a 2-step update is necessary.

Depending on the update method, to upgrade the firmware from version 2.6.7 or earlier to newer:

1. Upgrade to version 2.7.19.
2. After the version 2.7.19 is successfully installed, upgrade again to the required version.

For example, if the reader current firmware version is 1.2.11 or 2.6.7. To upgrade to 3.0.35, first upgrade to 2.7.19, and then upgrade to 3.0.35.

Depending on the update method, to downgrade the firmware from version 3.0.35 or newer to older:

1. Downgrade to version 3.0.35.
2. After the version 3.0.35 is successfully installed, downgrade again to the required version.

For example, if the reader current firmware version is 3.1.12. To downgrade to 2.6.7, first downgrade to 3.0.35, and then downgrade to 2.6.7.

Table 10 details the 2-step and 1-step upgrade or downgrade requirements that corresponds to the firmware installation methods for the FX7500 and FX9600.

Table 10 Firmware Update Support

Reader	Update/Downgrade		File-Based	FTP-Based	With USB
FX7500	Upgrade	2.6.7 or earlier to 3.x.x	2-step upgrade	1-step	1-step
		2.7.19 to 3.x.x	1-step	1-step	1-step
	Downgrade	3.x.x to 2.7.19 or earlier	2-step downgrade	2-step downgrade	2-step downgrade
		3.x.x to 3.x.x	1-step	1-step	1-step
FX9600	Upgrade	2.6.7 or earlier to 3.x.x	2-step upgrade	1-step	1-step
		2.7.19 to 3.x.x	1-step	1-step	1-step
	Downgrade	3.x.x to 2.7.19 or earlier	2-step downgrade	2-step downgrade	2-step downgrade
		3.x.x to 3.x.x	1-step	1-step	1-step

File-Based Update: The reader is updated with the web interface by using the file-based update. This method is also applicable to 123RFID application when the file-based option is used.

FTP-Based Update: The reader is updated with the web interface by using FTP or FPTS update. This method is also applicable to 123RFID application when the FTP-based option is used.

USB-Based Update: The reader is updated with an USB thumb drive.

1-step: The upgrade/downgrade is supported as usual.

2-step upgrade: Applicable to the file-based method, to upgrade to version 2.7.19 first and then upgrade to the latest 3.x.x version.

2-step downgrade: Applicable to the file-based method, to downgrade to version 3.0.35 first and then to 2.7.19 or the earlier version.

3.x.x: Any firmware version 3 followed by any major or minor number.

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.

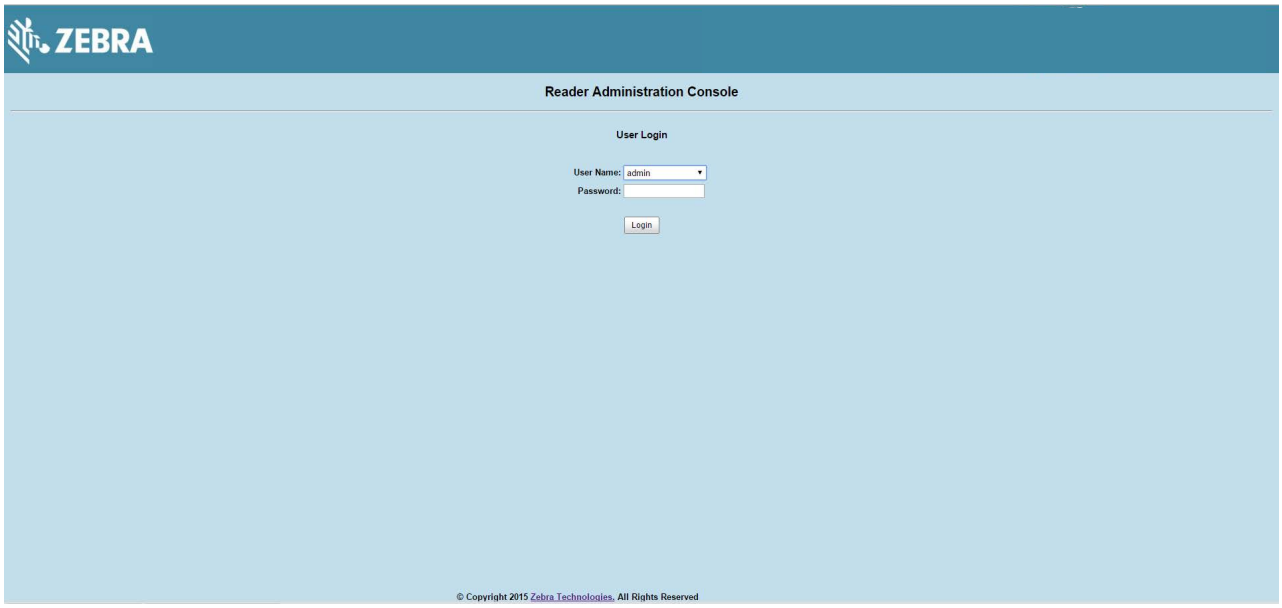
Updating FX Series Reader Software

Verifying Firmware Version

To check the FX7500 and FX9600 reader current firmware version:

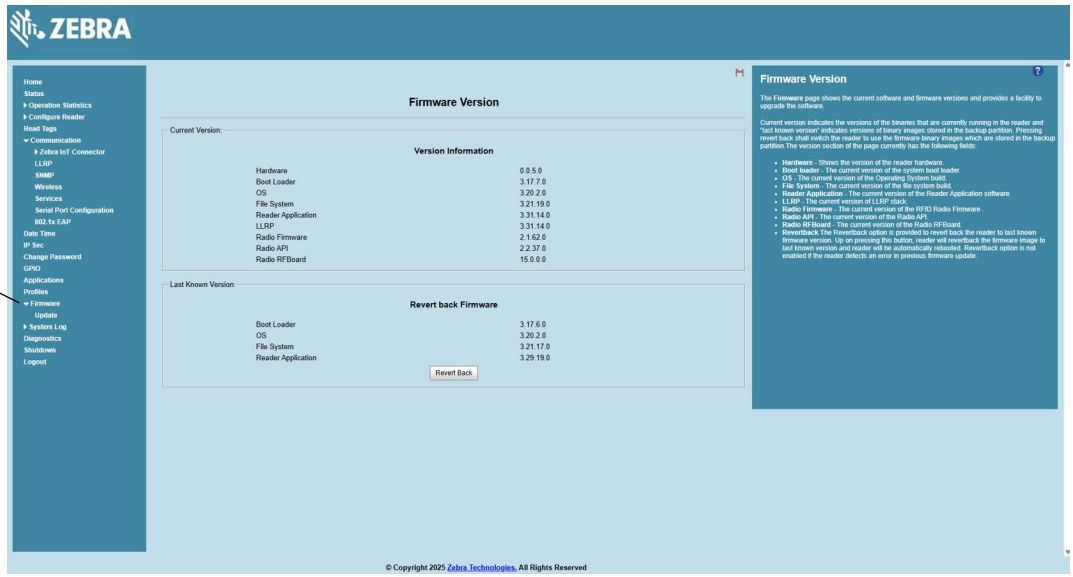
1. In the **User Login** window, select **admin** in the **User Name** drop-down menus and enter **change** in the **Password** field.

Figure 95 User Login Window



2. Select **Firmware** from the selection menu to verify if the current version of reader software is outdated (for example, 1.1.66).

Figure 96 Firmware Version Window



Updating Methods

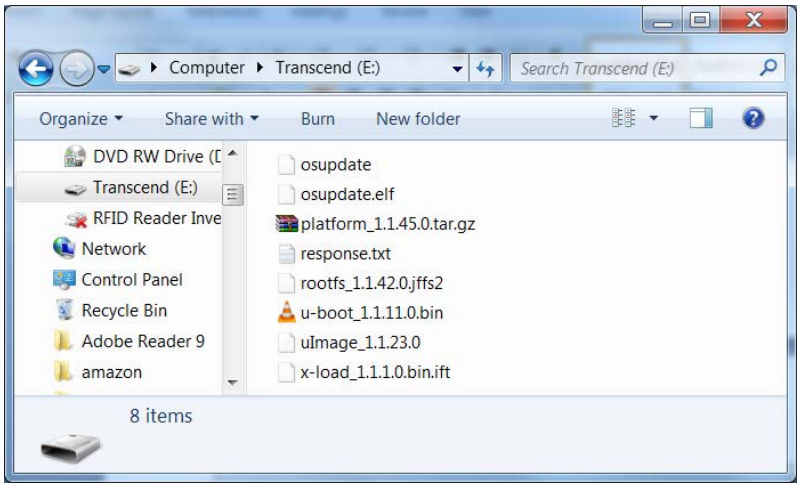
Download the reader update files from zebra.com/support, then use one of three methods listed below to update the reader software to a later version, such as 1.1.45.0 or higher:

- Using a USB Drive (Recommended)
- File-Based Update on page 134
- FTP/SCP-Based Update on page 136.

Using a USB Drive (Recommended)

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

Figure 97 USB Drive Root Folder



2. Insert the USB drive into the USB host port of the RFID reader (see Figure 98 and Figure 99).

Figure 98 FX7500 USB Host Port Window

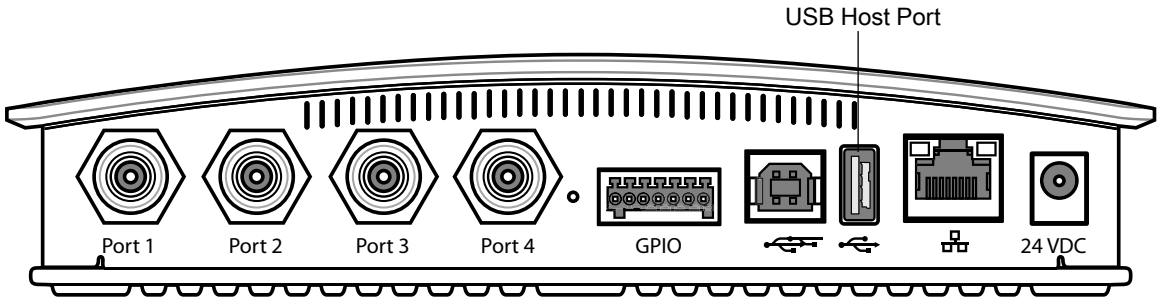
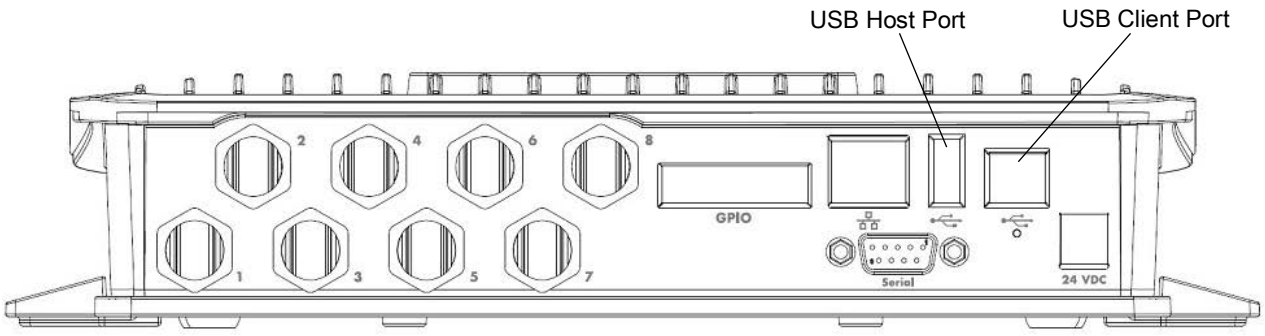


Figure 99 FX9600 USB Host Port Window



The reader starts the update process in 5 - 7 seconds, and indicates the 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 100 FX7500 Reader LEDs

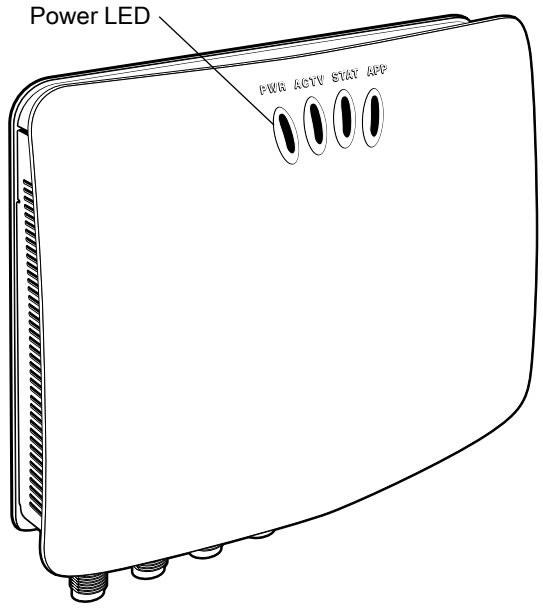
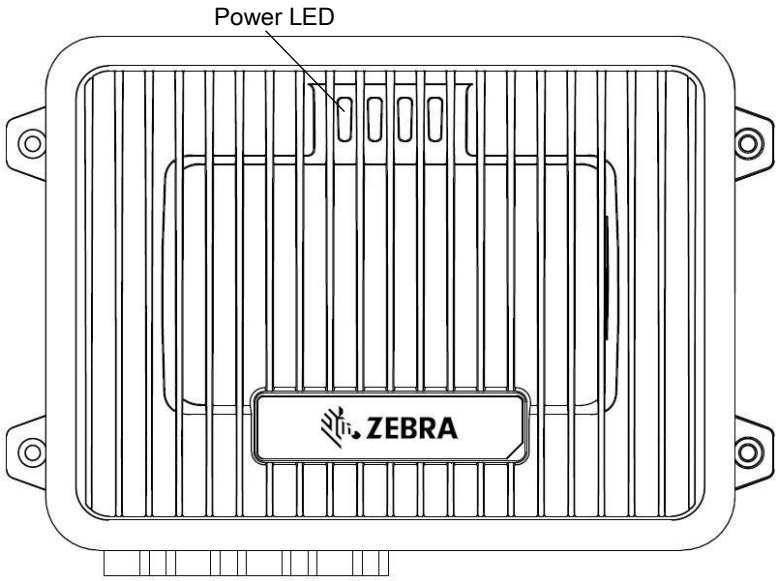


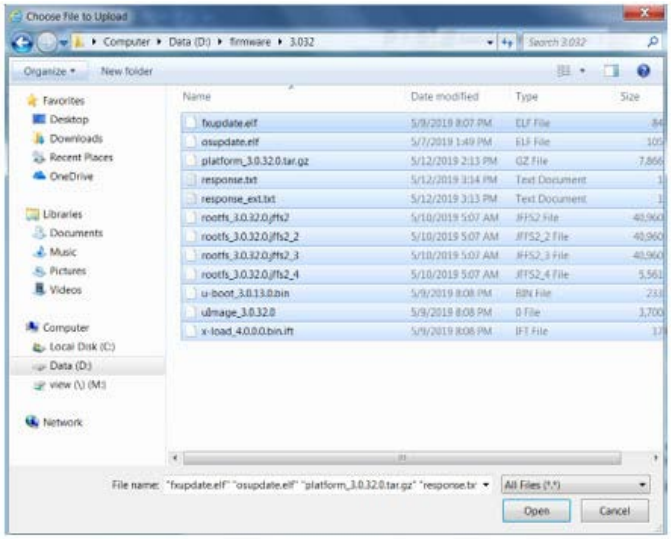
Figure 101 FX9600 Reader LEDs



File-Based Update

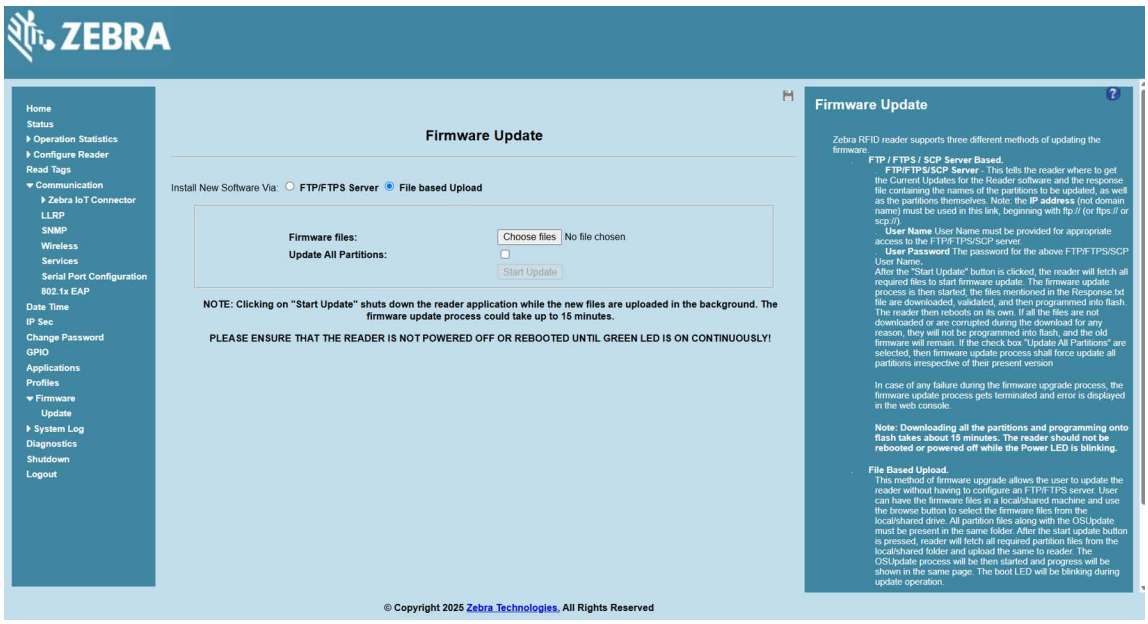
1. Copy all reader update files into any folder on a host computer.

Figure 102 Host Computer Folder



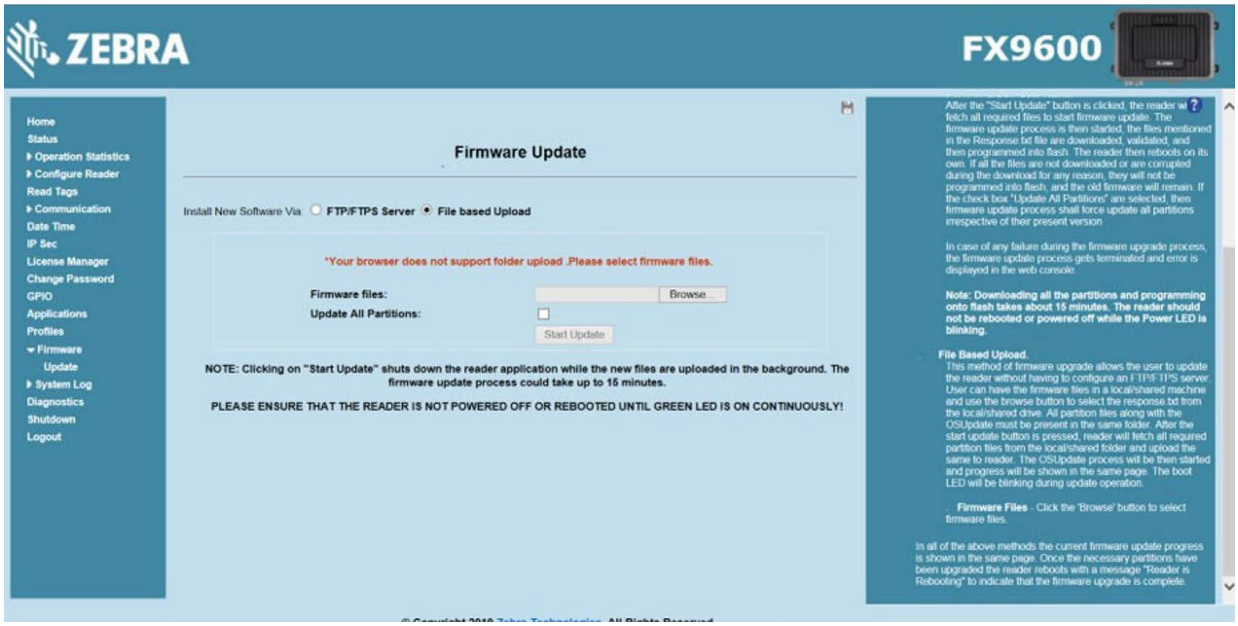
2. Log into the reader and navigate to the **Firmware Update** page.

Figure 103 Firmware Update Window



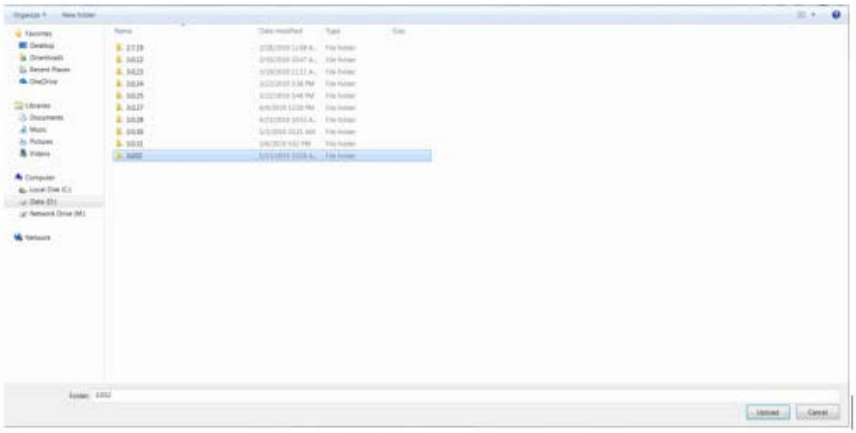
3. Select **File based Upload** (see Figure 104).

Figure 104 Firmware Update Window



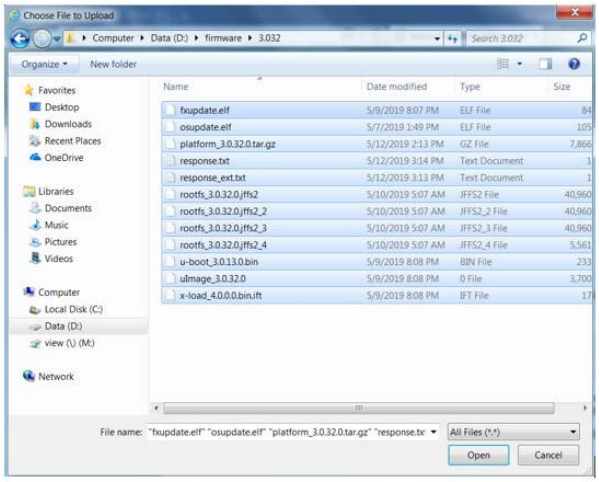
4. Select **Browse** and navigate to the folder or files that contains the firmware update files.

Figure 105 Browsing Update Folders



5. Select all the files (see Figure 106).

Figure 106 Browsing Update Files



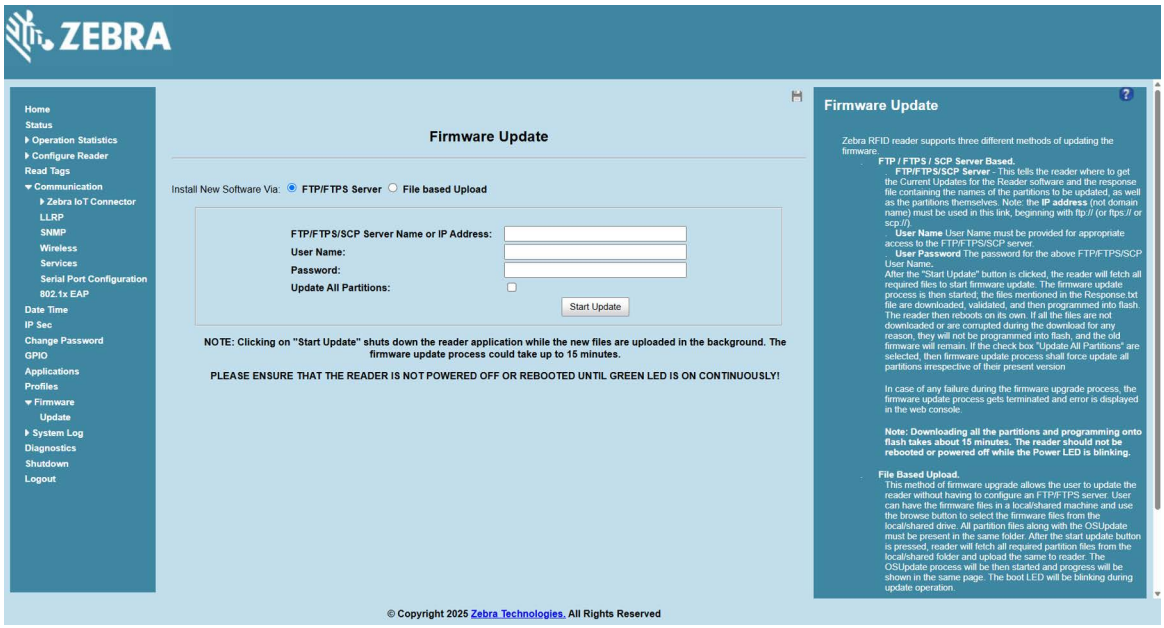
6. Select **Start Update**. The reader starts the update process and displays the update status as follows:
   - The reader continuously blinks the power LED red.
   - The reader blinks all four LEDs orange, one time.
   - The reader power LED remains steady orange.
   - The reader power LED remains solid green to indicate that the update is complete.
7. When the update completes, the reader reboots and returns to the login screen.

FTP/SCP-Based Update

Copy all the update files into an appropriate FTP/SCP location.

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

Figure 107 Firmware Update Window



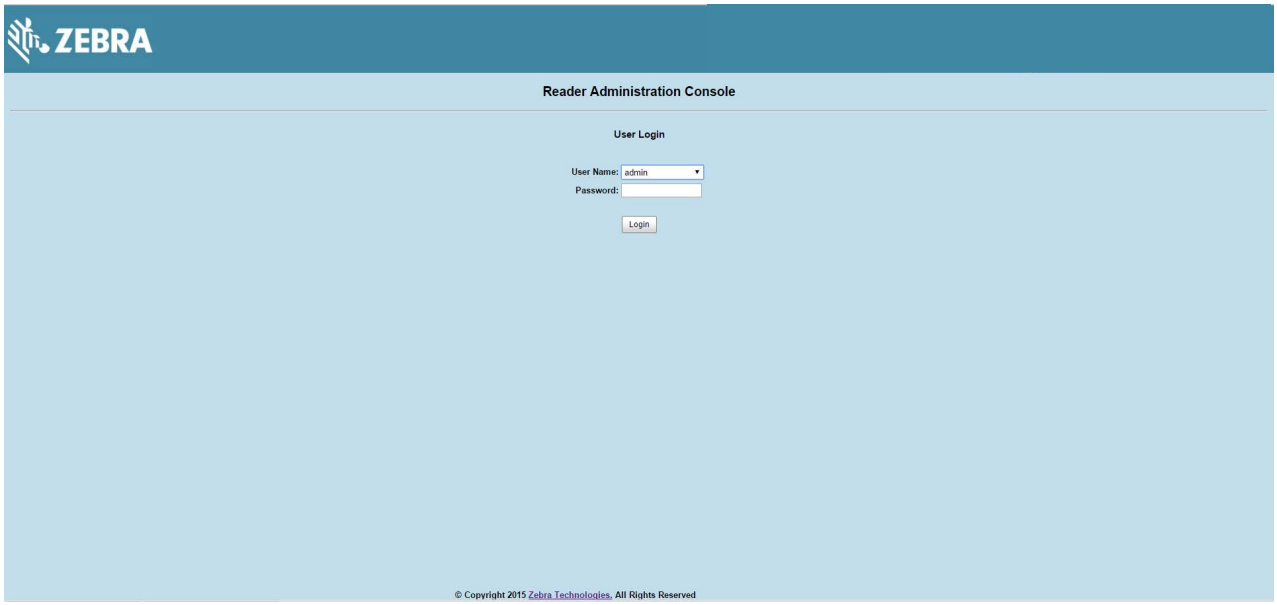
2. Select **FTP/FTPS/SCP Server**.
3. Enter the FTP/FTPS/SCP location where the files are located.
4. Enter the **User Name** and **Password** for the FTP/FTPS/SCP server login.
5. For the SCP-based firmware update, SSH key-based authentication can be used. In this case, a password is not required, provided the reader's public SSH key is already added to the authorized_keys file on the SCP server that provides the files. For more information on how to import SSH keys, refer to the SSH Key Management documentation.
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 4 LEDs orange once.
   - The reader Power LED remains steady orange.
   - The reader Power LED settles to a steady green to indicate that the update is complete.
7. When the update completes, the reader reboots and returns to the FX login screen.

Verifying Firmware Version

To verify if the firmware update is successful:

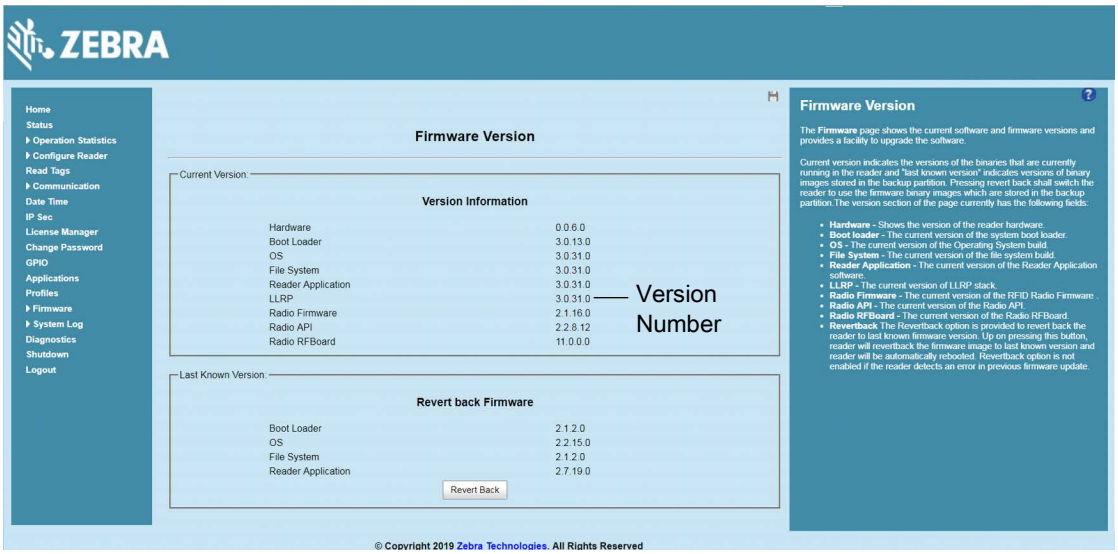
1. In the **User Login** window, select **admin** in the **User Name** drop-down menus and enter **change** in the **Password** field.

Figure 108 User Login Window



2. Select **Firmware** from the selection menu to verify if the current reader software displays a newer version number, which indicates the update is successful.

Figure 109 Firmware Version Window



EtherNet/IP

Introduction

This chapter provides the overview of EtherNet/IP for the FX9600 RFID Reader.

EtherNet/IP

EtherNet/IP (IP = Industrial Protocol) is an industrial network protocol that adapts the Common Industrial Protocol (CIP) to standard Ethernet. EtherNet/IP uses both of the most widely deployed collections of Ethernet standards - the Internet Protocol suite and IEEE 802.3 - to define the features and functions for its transport, network, data link and physical layers. EtherNet/IP performs at level session and above (level 5, 6 and 7) of the OSI model. CIP uses its object-oriented design to provide EtherNet/IP with the services and device profiles needed for real-time control applications and to promote consistent implementation of automation functions across a diverse ecosystem of products (go to en.wikipedia.org/wiki/EtherNet/IP for more details).

Zebra FX9600 RFID Reader supports EtherNet/IP for the industrial automation purposes, through which PLCs can connect with the reader and perform RFID operations.

The EtherNet/IP for the FX9600 RFID Reader is packaged with the reader firmware image and provided as an installable application package. Users can start and stop the EtherNet/IP application in service page (see Figure 55 and Figure 56 on page 94). The EtherNet/IP application enables the EtherNet/IP protocol adapter and uses standard EtherNet/IP port 2222 and 44818 to communicate with readers via PLC.

Using EtherNet/IP

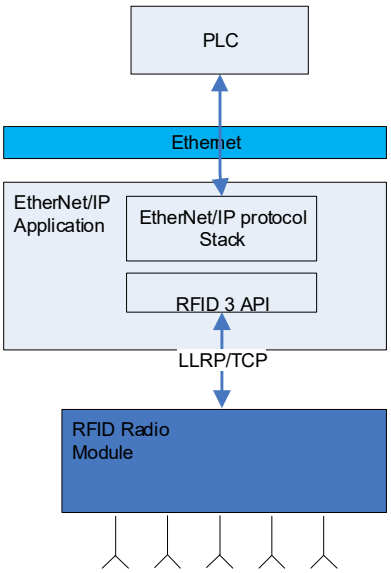
The Ethernet/IP is enabled through the installable application as mentioned above. Users can start or stop the application from the web console as per the requirement. See Applications on page 101 for more details.

The EtherNet/IP application consists of two parts:

- EtherNet/IP protocol stack: Communicates with other EtherNet/IP devices
- RFID3 API: Communicated with LLRP for RFID operations.

The basic architecture of EtherNet/IP is explained in Figure 110 on page 140.

Figure 110 EtherNet/IP Application Block Diagram



Supporting RFID Operations Through EtherNet/IP

The EtherNet/IP in the FX9600 RFID Reader supports both implicit and explicit operations. Below is the list of implicit and explicit operations which can be performed through EtherNet/IP.

Implicit Operations:

These are the synchronous operations to perform certain RFID operation. Each implicit/synchronous operation has its corresponding reply which is executed per connection with configured RPI.

- **Inventory Operation**: Through this, user can perform inventory operation and get TAG data as reply of the operation.
- **Access Operation**: Through this, user can perform Access operation on the TAGs and read memory bank data which is received as reply packets.

Explicit Operations:

These are the asynchronous operation which can be executed as per the requirement. Explicit operations are implemented to configure the reader with RFID parameters according to the end-user use case. Below are the supported explicit operations which can be used to get and set the RFID configuration parameters from/to readers.

- **Reader Capabilities**: This operation reads the reader capabilities.
- **Profile List**: This operation is to get count and the name of the profiles installed in reader and also to change the active profile through the EtherNet/IP interface itself. Reader configuration profiles can be customized and activated via the reader web interface. This is useful when a EtherNet/IP data model does not support a use case. In such case, it is possible to set the reader configuration via the reader profile instead. Besides, once a custom profile is loaded in the reader via reader web interface, the custom profile can be chosen via EtherNet/IP.

NOTE: After changing active profile in a reader using this explicit operation, reset the reader for EtherNet/IP to perform operations specified in the custom profile.

- **Antenna Configuration**: The RFID antenna configuration can be modified using this explicit message command. Parameters such as Sel, Session, Target, RF Mode, Tari, TAG population and Antenna Power can also be configured.

- **Pre-Filter Configuration**: This explicit message is used to Add/Delete pre-filter for consecutive RFID operation. Pre-filter has parameters such as Antenna ID, Memory Bank, Target, Action, Tag Pattern etc. which is used to perform the RFID operation on specific group of TAGs.
- **Post-Filter/Access-Filter Configuration**: Post-filter is used to apply filtering on the tags received from RFID radio module at API level. Access filter is used to apply filtering for access operation. This configuration is used as the post-filter for inventory operation and as the Access filter for access operation. Post/Access filter can be configured with parameters such as two sets of Tag Pattern for a specific memory bank, match pattern criteria, and RSSI range filtering.
- **Trigger Configuration**: This explicit operation is to configure triggers and report criteria for a RFID operation. Through this command, parameters such as start/stop triggers, event reporting, and periodic reporting can be configured.
- **GPIO Configuration**: FX9600 RFID reader has external GPI and GPOs which can be configured using this explicit message. GPI can be enabled/disabled and GPO values can be read via EtherNet/IP interface with this configuration.
- **Event Report**: Users get the event information which is generated during the RFID operation through this explicit message.The event can be form the GPI event, antenna event, temperature event or reader exception event.

EtherNet/IP Package Content:

Detailed information for the EtherNet/IP data model supported by the FX9600 RFID reader, Sample Application and other components are available at Zebra Support Central. The package includes:

- The EtherNet/IP application for FX9600 as a Debian package. The EtherNet/IP stack installed by the Debian package is already available in the reader out of the box. Zebra provides updates on the support site.
- Zebra FX9600 AOP for Studio 5000.
- EtherNet/IP Sample project for Studio 5000.
- The Sample Application user guide.
- Detailed Data Model document.
- Exported RUNGs and Data types from sample project to use with the older version of Studio 5000.

NOTE: Our sample application project is created with Studio 5000 v32 and to work with CompactLogix 5069-L306ER PLC.

- For PROFITNET configuration and setup, go to the user guide at zebra.com/content/dam/support-dam/en/documentation/unrestricted/guide/software/zebra-rfid-profinet-ug-en.pdf.
- For MODBUS configuration and setup, go to the user guide at zebra.com/content/dam/support-dam/en/documentation/unrestricted/guide/software/zebra-rfid-modbus-tcp-ug-en.pdf.

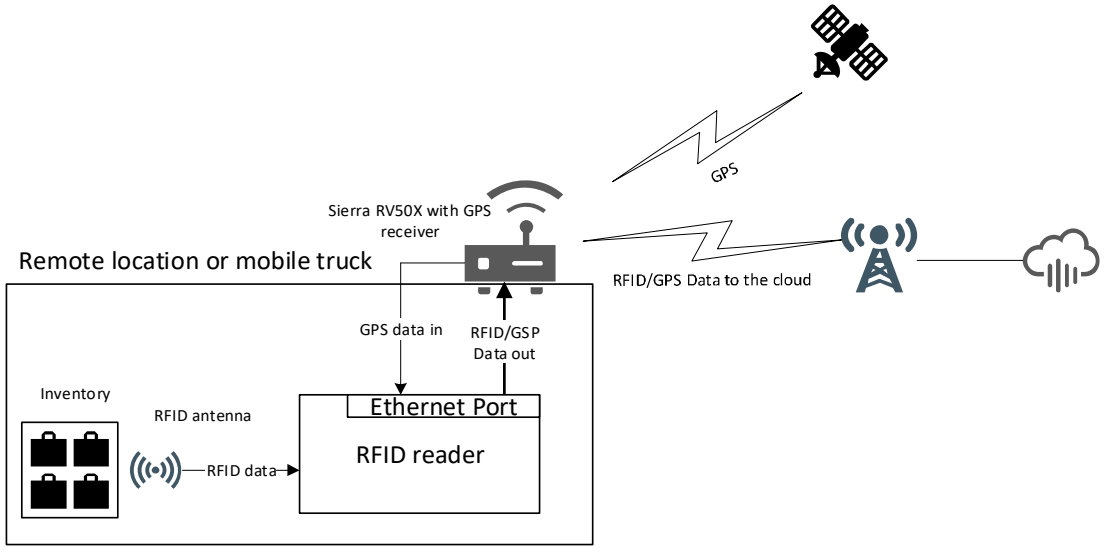
Cellular Connectivity with Sierra Modem

Introduction

This chapter describes the configuration of Sierra Modem RV50X to provide the cellular connectivity for Zebra FX9600 RFID Reader.

Cellular Connectivity with Sierra Modem

Figure 111 Cellular Connectivity with Sierra Modem



Zebra FX9600 RFID Reader is enabled with cellular connectivity through the Sierra Modem RV50X. The data from the reader is sent to the cloud via the Sierra Modem which has the Global coverage 3G/4G LTE (Cat 6). The modem requires a GNSS compatible antenna connected to the RV50X. This has been tested with the antenna AIRLINK® ANTENNA: 3-IN-1 SHARKFIN. Zebra FX9600 RFID Reader along with RV50X is enabled to provide the GPS coordinates.

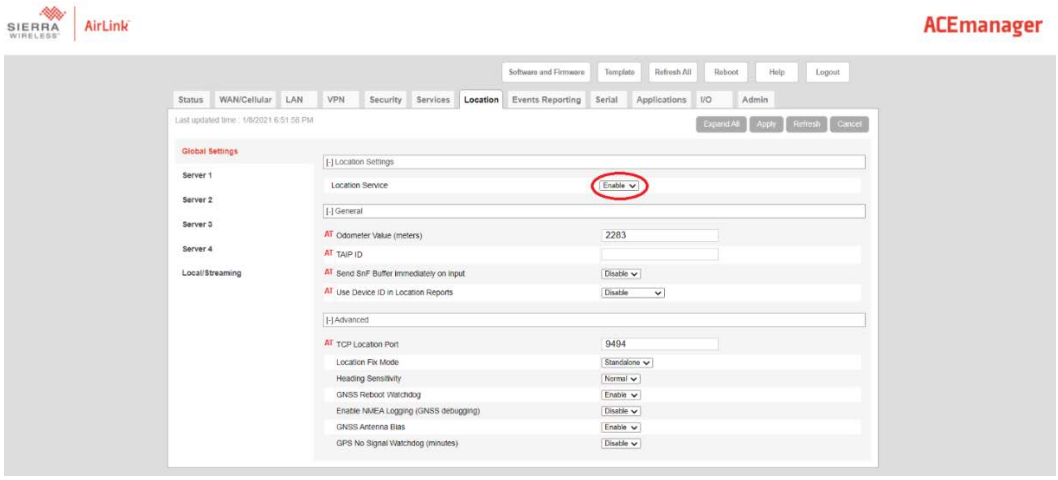
This feature enables the following asset tracking features:

- Remote locations (for example, Refinery plant)
- Delivery/Trucking Industries.

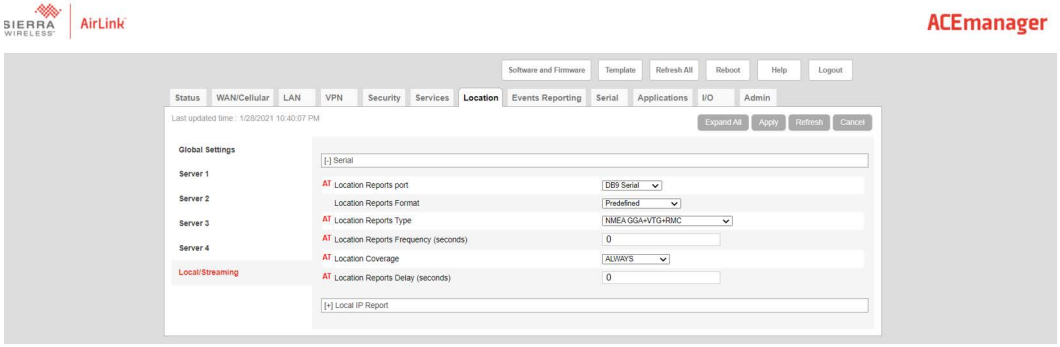
Steps to be followed for receiving GPS coordinates.

Configure RV50 for sending GPS coordinates:

1. Access the Sierra Modem.
   a. Connect the Modem and PC back-to-back with network cable. For more details to configure the RV50X follow the link scribd.com/document/448523280/4117313-AirLink-RV50-Series-Hardware-User-Guide-r5-pdf
   b. Factory reset the modem by pressing the reset button for 7 to 10 seconds until the power LED blinks red. (Sequence is blinking red, fast blinking green, then while fast blinking red release the reset button)
   c. Access http://192.168.13.31:9191/ in the PC with username "user" and Password as 12345 (should be changed after login)
2. GPS data in Serial Port.
   a. Open the modem web page, Go to **Location** and **Enable** the **Location Service** (default is disabled) and **Apply**. **Local/Streaming** settings on GPS **Location** setting Page



   b. In **Local/streaming**, Set **Location Reports Port** as **DB9 Serial.** Then **Apply** and **Reboot** the modem.



   c. Connect Serial cable between modem and PC.
   d. Open tera term with the COM available, with baudrate **115200**.
   e. Place the Sierra modem dolphin wing antenna facing open space.

f. To get the GPS coordinates through LLRP and API3, enable GPS in ROReportSpec as follows:

<moto:MotoTagReportContentSelector>

<moto:EnableGPS>true</moto:EnableGPS>

</moto:MotoTagReportContentSelector>

Example of GSP meta data reported in LLRP:

<moto:MotoTagGPS>

<moto:longitude>776816</moto:longitude>

<moto:latitude>129245</moto:latitude>

<moto:altitude>9140000</moto:altitude>

</moto:MotoTagGPS>

g. Use the following code snippet below is for retrieving GPS data using .net API.

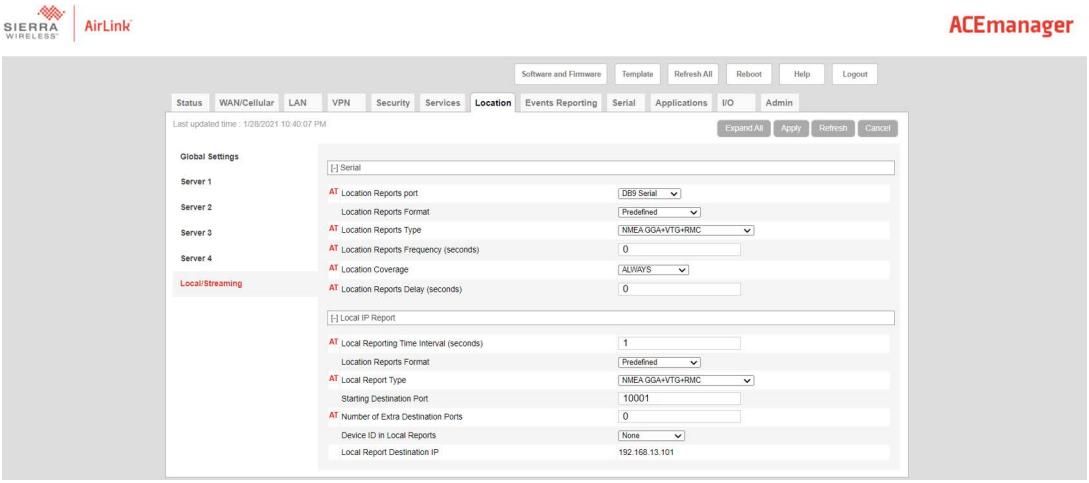
```
using System;
using Symbol.RFID3;
using System.Threading;


namespace GPSdata
{
    class Program
    {
        static RFIDReader reader = new RFIDReader("X.X.X.X", 5084, 0);
        static void Main(string[] args)
        {

            // Establish connection to the reader
            reader.Connect();
           Console.WriteLine("Press any key to start inventory... and press again any
key to stop");
            Console.ReadLine();
            // Register for Read Notification
            reader.Events.ReadNotify += Events_ReadNotify;
            reader.Events.AttachTagDataWithReadEvent = true;

            //This is optional by default all tag fields will be enabled
            TagStorageSettings tagStorageSettings =
reader.Config.GetTagStorageSettings();
            tagStorageSettings.TagFields = TAG_FIELD.GPS_COORDINATES |
TAG_FIELD.PEAK_RSSI | TAG_FIELD.TAG_SEEN_COUNT | TAG_FIELD.CRC;

            reader.Config.SetTagStorageSettings(tagStorageSettings);
            reader.Actions.PurgeTags();
            reader.Actions.Inventory.Perform();
            Thread.Sleep(3000);
            reader.Actions.Inventory.Stop();
            reader.Disconnect();
```

```
                    Console.ReadLine();
                    System.Environment.Exit(0);


                }


            private static void Events_StatusNotify(object sender, Events.StatusEventArgs
e)
            {

            }

             private static void Events_ReadNotify(object sender, Events.ReadEventArgs e)
             {
                 // fetch tags from the Dll by specifying the number of expected tags
                 TagData[] myTags = reader.Actions.GetReadTags(100);

                 if (myTags != null)
                 {
                     for (int nIndex = 0; nIndex < myTags.Length; nIndex++)
                     {
                         Console.WriteLine("TagID/EPC : " + myTags[nIndex].TagID + " Lat:
" + myTags[nIndex].GPSLocation.Latitude + " Long: " +
myTags[nIndex].GPSLocation.Longitude + " Alt: " + myTags[nIndex].GPSLocation.Altitude
);
                     }
                 }
             }


        }
}
```

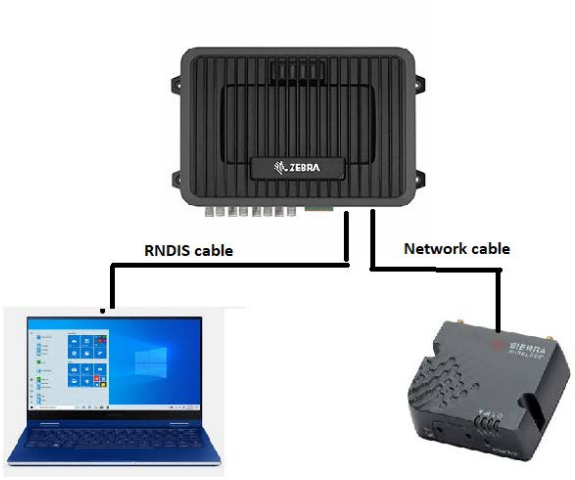
Sierra Modem and reader can be connected in two different ways.

Connection Via RNDIS

1. In **Location** Tab under **Local/Streaming** link expand **Local IP Report. Local Reporting Time Interval** (seconds) should be set to non-zero value(as zero is disable).
2. Set **Local Report Type** as **NMEA GGA+VTG+RMC**.
3. Set **Starting Destination Port** to 10001.
4. Then **Apply** and **Reboot** the Modem.

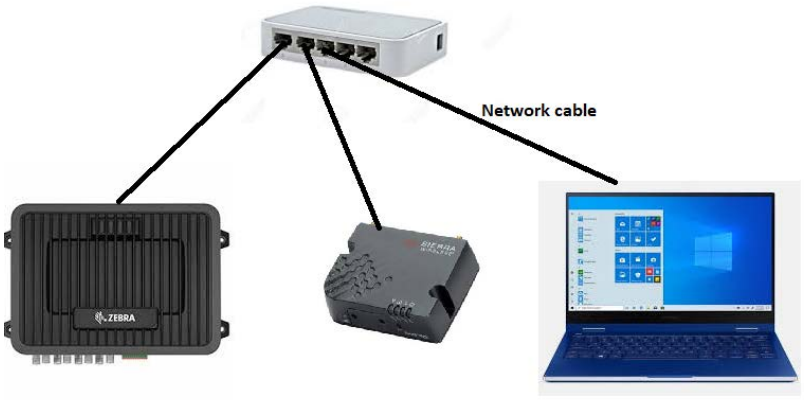


5. The reader and Sierra modem are connected via network cable. Reader and PC are connected via RNDIS cable. Perform inventory with GPS data enabled, Coordinates will be reported.

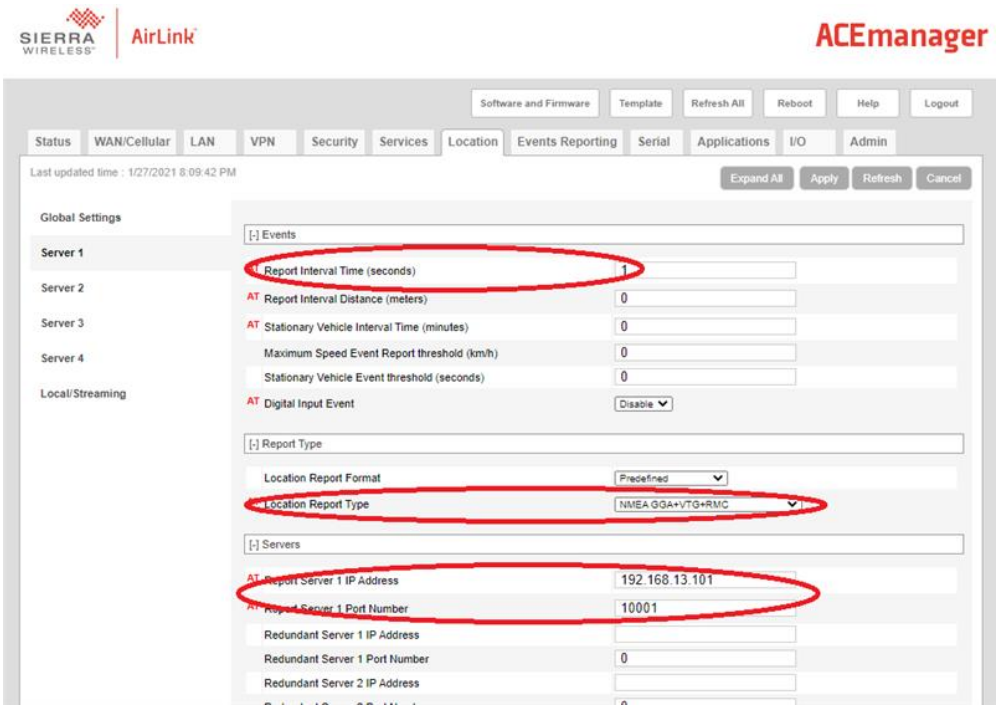


Connection via network hub:

1. Connect Modem, Reader and PC to a network hub or unmanaged switch.

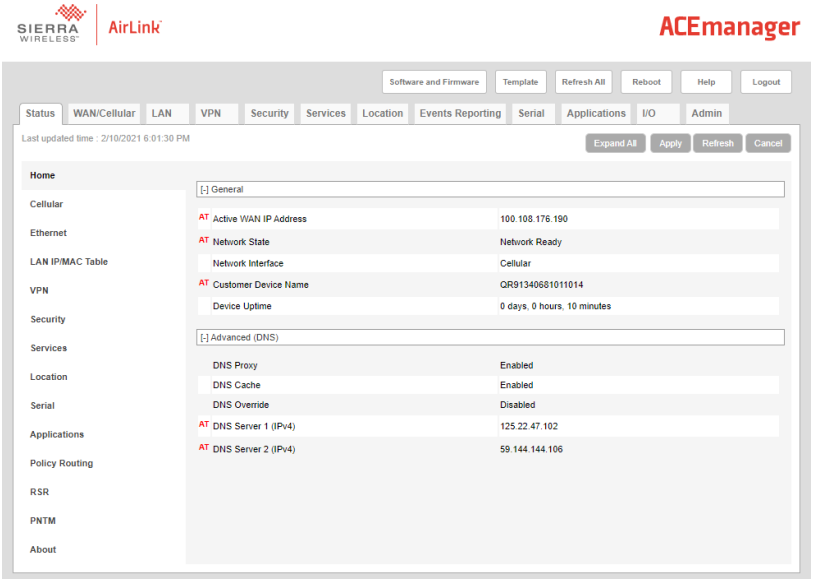


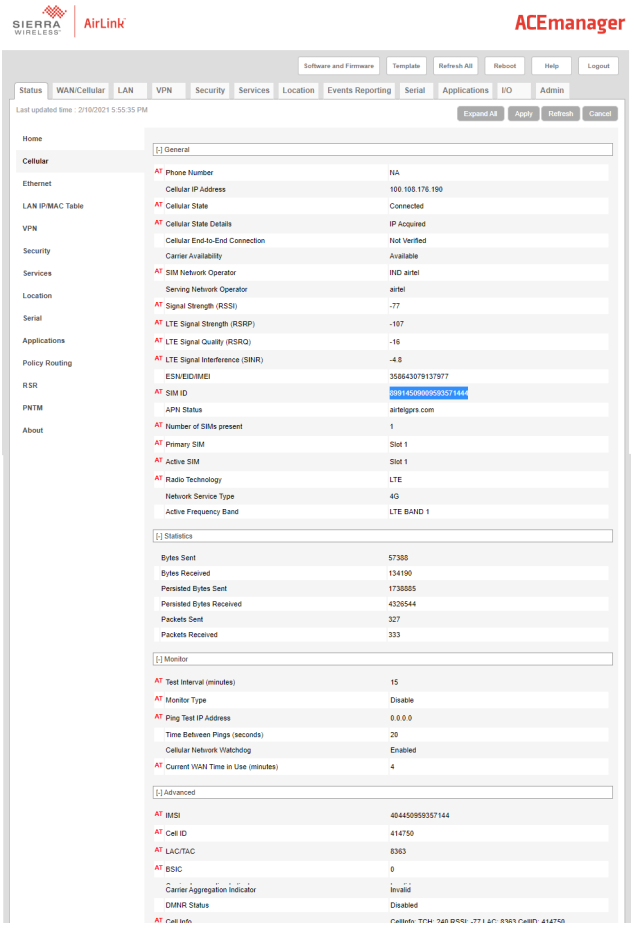
2. In **Local Streaming** Tab **Local Reporting Time Interval** (seconds) should be set to non-zero value.as zero is disable under **Local IP Report**
3. Set **Local Report Type** as **NMEA GGA+VTG+RMC**.
4. Set **Starting Destination Port** to 10001.
5. Then go to **Server1** and set **Report Interval time as 1** under Events.
6. Set **Location Report Type** as **NMEA GGA+VTG+RMC** under Report Type.
7. Set **Report Server 1 IP Address** as **<reader IP>** and **Report Server 1 Port Number** as **10001**.
8. Then **Apply** and **Reboot** the Modem.
9. While rebooting the modem disconnect the modem from the network by removing the network cable from the modem. After the modem comes up connect the network cable to the modem. By doing this the default ip address in local reporting will be set to 192.168.13.100 which will be the ip of the reader. After then connect the reader to the network hub , finally connect the PC to the network hub
10. Once the modem comes up perform the inventory with GPS data enabled, Coordinates will be reported.



Steps to be followed to send reader data to cloud using Sierra Modem.

SIM card should be added in the Modem for cellular connectivity. Once the Sim card is added the Status and WAS/Cellular tab looks like below.




SIERRA WIRELESS
AirLink
ACEmanager
Software and Firmware
Template
Refresh All
Reboot
Help
Logout
Status
WAN/Cellular
LAN
VPN
Security
Services
Location
Events Reporting
Serial
Applications
I/O
Admin
Last updated time : 2/10/2021 5:55:35 PM
Expand All
Apply
Refresh
Cancel
Home
Cellular
Ethernet
LAN IP/MAC Table
VPN
Security
Services
Location
Serial
Applications
Policy Routing
RSR
PNTM
About
[-] General
Phone Number
NA
Cellular IP Address
100.100.176.190
Cellular State
Connected
Cellular State Details
IP Acquired
Cellular End-to-End Connection
Not Verified
Carrier Availability
Available
SIM Network Operator
IND airtel
Serving Network Operator
airtel
Signal Strength (RSSI)
-77
LTE Signal Strength (RSRP)
-107
LTE Signal Quality (RSRQ)
-16
LTE Signal Interference (SINR)
-4.8
ESN/EID/IMEI
358643079137977
SIM ID
8991450999959357144
APN Status
airtelgprs.com
Number of SIMs present
1
Primary SIM
Slot 1
Active SIM
Slot 1
Radio Technology
LTE
Network Service Type
4G
Active Frequency Band
LTE BAND 1
[-] Statistics
Bytes Sent
57388
Bytes Received
134190
Persisted Bytes Sent
1738885
Persisted Bytes Received
4326544
Packets Sent
327
Packets Received
333
[-] Monitor
Test Interval (minutes)
15
Monitor Type
Disable
Ping Test IP Address
0.0.0.0
Time Between Pings (seconds)
20
Cellular Network Watchdog
Enabled
Current WAN Time in Use (minutes)
4
[-] Advanced
IMSI
404450959357144
Cell ID
414750
LAC/TAC
8363
BSIC
0
Carrier Aggregation Indicator
Invalid
DMNR Status
Disabled

SOTI MOBI Client

Introduction

This chapter provides information on SOTI Mobicontrol and includes references to the appropriate guides.

SOTI MOBI Client

SOTI Mobicontrol is an enterprise mobile management solution to help users in managing and monitoring enterprise devices.
Lists of supported APIs are as follows:

- Zebra Configuration:
  - API setup
  - Agent specific to Zebra
  - Run time password change to access API
  - Fix for HTTPS communication.
- Application life cycle management:
  - Install application through packages.
  - Uninstall applications.
  - **Installed Applications** information panel.
  - Identify whether an application is set to as **auto start** (as a custom application property in the information panel).
- Actions:
  - Soft Reset
  - Firmware update.
- Remote Maintenance:
  - Remote Zebra Web Console access
  - Remote terminal access
  - File Transfer
  - Alerts and actions
  - Out of Contact payload.

- Implemented custom data through Zebra APIs:
  - CPU Utilization
  - Up time
  - Connectivity type
  - Time Zone
  - Capture LLRP Server IP in client Mode
  - Reader name
  - Reader Serial number
  - Location
  - Radio Firmware Version
  - Flash Available
  - Ram Total
  - Ram Used
  - Ram Available
  - Ram Info.
- Implemented custom data through Zebra APIs:
  - LLRP Server IP
  - Ambient Temperature High Alarm Count
  - Ambient Temperature Critical Alarm Count
  - PA Temperature High Alarm Count
  - PA Temperature Critical Alarm Count
  - Forward Power High Alarm Count
  - Forward Power Low Alarm Count
  - Reverse Power High Alarm Count
  - Echo Threshold Alarm Count
  - Database Warning Count
  - Database Error Count
  - PIO Information Count
  - Reader IP Address
  - Device Info
  - Client IP Address.

For the SOTI MOBI CONTROL help, go to soti.net/mc/help/v15.0/en/setup/setupindex.html.

By accessing the device info or properties and displaying it on Web console, users can generate alert and perform an action based on these device properties. For more details, go to: discussions.soti.net/kb/configuring-custom-data-on-zebra-fx7500-9600-1/.

For the firmware upgrade, go to: discussions.soti.net/kb/upgrading-zebra-fx7500-9600-firmware-from-mobicontrol.

To have more information on Remote Control (Web Console and Terminal access), go to: discussions.soti.net/kb/take-remote-control-of-your-linux-devices.

To have more information on Enrollment Utility for Zebra device to enroll in MobiControl, go to: discussions.soti.net/kb/enrol-multiple-zebra-rfid-devices-using-zebra-rfid-enrolment-utility-1.

For troubleshooting, go to: discussions.soti.net/kb/not-able-to-access-device-apis-exposed-by-zebra-fx7500-9600-via-custom-data/?postbadges=true.

Gen2 V2 Enhancement

Introduction

This chapter describes the Gen2V2 commands supported by the FX Series RFID Reader.

Gen2 V2 Enhancement

The LLRP and RFID3 APIs extensions add four new access commands to support the GS1 Gen2 V2 standard features. For more details on the following list of commands, go to: gs1.org/standards/epc-rfid/uhf-air-interface-protocol.

- Authenticate:
  - The Gen2 V2 standard command supports a variety of cryptographic suites.
  - The end user application can perform tag authentication.
- ReadBuffer:
  - The Gen2 V2 standard command reads response data of Authentication command.
- Untracable:
  - The Gen2 V2 standard command hides a whole or partial tag memory bank for security and/or reading efficiency.
  - The Tag operation range can be reduced for security.
- Crypto:
  - NXP custom extension uses ISO/IEC 29167-10 (AES-128) Crypto Suite.
  - Contact NXP to get document **286910 How to use UCODE AES**.

Above commands are tested with tags that have the following tag identifiers (TIDs)

- E2C06892200042021F0B3C21 (NXP DNA tag)
- E2C06F922000000200105CB3 (NXP AES tag)

Contact Zebra for a sample application.

Reader Configuration via USB Thumb Drive

Introduction

This chapter provides the steps to transfer a reader configuration to another reader via a USB thumb drive.

Configuring Reader with USB Thumb Drive

A USB thumb drive can be used to transfer the reader configuration from a reader to another reader. More specifically, swapping a reader is now very simple if a physical access to the reader is possible. This process assumes reader is functional via the USB host port. At a high level, the use case and the work flow is as follows:

- The use case is when a reader replacement is required and a new reader is available to replace it.
- Copy the configuration from the reader to be replaced by using a USB flash drive.
- Reset the new reader and effectively assume the role of the replaced reader.

To enable this work flow, you must have a USB flash drive. The details are as follows:

1. Create a special XML control file in a USB flash drive:
   a. Format the USB thumb drive using FAT.
   b. Create a USBCommand directory in root.
   c. Create a XML file with the file name USBCommand.xml.
   d. Copy the following XML excerpt to the USB drive. The file directory is **/USBCommand/USBCommand.xml**

```
<FX_USB_COMMAND>
    <command name="configuration_one_to_one">
        <Input>reader_to_usb</input>
        <state></state>
        <output></output>
    </command>
</FX_USB_COMMAND>
```

IMPORTANT: The used XML control file in the USB thumb drive cannot be used for a second new reader. Users must always create a new XML control file following Step 1 and save it in the USB flash drive to transfer a reader configuration to each new reader.

2. The old reader retrieves (the reader APP LED blinks yellow) the XML control file when USB flash drive is inserted.
3. The old reader copies its configuration file AdvReaderConfig.xml to the USB flash driver. It is safe to disconnect drive when yellow LED turns off.
4. The new reader parses the control file then loads the older reader configuration (the reader APP LED blinks green for 10 seconds).
5. After the APP green LED turns off, restart the reader manually. It is safe to keep the USB flash drive connected while the reader resets.
6. If there is an update issue, the APP LED blinks red for 10 seconds. Logs are written to the USB flash drive. The USB flash drive can be removed after the red APP LED stops blinking.

GPS and Triggers for Trucking and Delivery

Introduction

This chapter explains the GPS feature and three new added triggers for trucking and delivery.

GPS and New Triggers for Trucking and Delivery Use Cases

The reader must have a cellular connectivity for the RFID data and GPS data to be sent to the cloud (see Cellular Connectivity with Sierra Modem on page 142).

With the cellular connectivity, the readers send the RFID data and GPS data to the cloud at the instant they are created. In addition, the GPS data are updated only when vehicle moves. This prevents transmission of redundant GPS data when vehicle is not moving and the RFID operations are enabled.

Deliver Driver Use Case

1. A delivery driver carrying baked goods in a van stops at 5 bakeries each morning to deliver fresh product.
2. The van is loaded up in the morning at a central warehouse. When the van door is open, the reader mounted on the van is triggered by a GPI trigger to track the products that are going through each dock door and onto the van.
3. The driver leaves the warehouse. The GPS data are captured as part of the tag meta data.
4. The GPS data are captured every x seconds/minutes when the reader takes an inventory.
5. When the driver stops at the first bakery to deliver product, the driver opens the door and the reader performs another inventory (the GPI is triggered). The GPS data are captured.
6. The driver finishes delivery and continues to the next bakery. The inventory is taken and GPS data are captured.
7. Steps 4 to 6 are repeated for the next deliveries.

Government or Military Use Case

1. A convoy carrying top-secret tagged assets leaves the remote facility.
2. When truck door is opened, the GPI triggers the reader to start capturing data. The GPS data are captured.
3. After y km of travel distance, the reader takes inventory to ensure assets are still with the convoy. The GPS data are also captured.

Trucking Company Use Case

1. The tractor-trailer is loaded with product at a central warehouse.
2. The reader mounted at the warehouse dock door tracks the products that are loaded in the truck.

3. The reader mounted in the truck starts an inventory cycle at a specific time of day (no date can be specified).
4. The truck completes delivery route. The GPS readings are taken at regular time intervals and when the truck returns to the warehouse at 4PM.

There are 2 new start triggers and 1 stop trigger:

- Time lapse start trigger:
  - Specific time of day (for example, 8:00am EST)
  - Certain period (second unit, for example 10 seconds).
- GPS distance start trigger:
  - Inventory starts after x km of moving.
- Time lapse stop trigger:
  - Specific total duration (for example, 14400 seconds (4 hours to 2:00PM))
  - Certain periodic duration (second unit, for example 5 seconds).

The new triggers works with some existing triggers. For example, a GPI trigger (old trigger) can work with the new time lapse stop trigger. The matrix of supported triggers is shown in Table 11.

Table 11 Supported Trigger and Combinations Matrix

		Stop Trigger					
		No Stop Trigger defined or configured	Duration[1]	Tag Observation with Timeout[2]	Attempt with Timeout[3]	GPI[4]	Time lapse Stop Trigger[5]
Start Trigger	Immediate[6]						Not supported
	GPI[7]		*			Supported	Supported
	Periodic[8]						Not Supported
	Time lapse Start Trigger[9]	Supported	*	*	*	Supported	Supported
	Distance[10]	Supported	*	*	*	Supported	Supported

1. (LLRP) ROSpecStopTrigger.DurationTriggerValue; (RFID3 API) STOP_TRIGGER.value.duration
2. (LLRP) AISpecStopTrigger.TagObservationTrigger.NumberOfTags; (RFID3 API) STOP_TRIGGER.value.tagObservation
3. (LLRP) AISpecStopTrigger.TagObservationTrigger.NumberOfAttempts; (RFID3 API) STOP_TRIGGER.value.numAttempts
4. (LLRP) AISpecStopTrigger.GPITriggerValue; (RFID3 API) STOP_TRIGGER.value.gpi
5. (LLRP) ZebraROSpecStopTrigger.ZebraTimelapseStop; (RFID3 API) STOP_TRIGGER.value.timelapse
6. (LLRP) ROSpecStartTrigger.ROSpecStartTriggerType.Immediate; (RFID3 API) START_TRIGGER.type.START_TRIGGER_TYPE_IMMEDIATE
7. (LLRP) ROSpecStartTrigger.GPITriggerValue; (RFID3 API) START_TRIGGER.value.gpi
8. (LLRP) ROSpecStartTrigger.PeriodicTriggerValue; (RFID3 API) START_TRIGGER.value.periodic
9. (LLRP) ZebraROSpecStartTrigger.ZebraTimelapseStart; (RFID3 API) START_TRIGGER.value.timelapse
10. (LLRP) ZebraROSpecStartTrigger.ZebraDistance; (RFID3 API) START_TRIGGER.value.distance

* Trigger combinations that are currently not supported.

Specific Examples Of Trigger Configuration

Single trigger pair: Timelapse Start/Timelapse Stop

Configuration:

Start trigger [Time of Day: “08:24:00”, Period: 10 seconds]

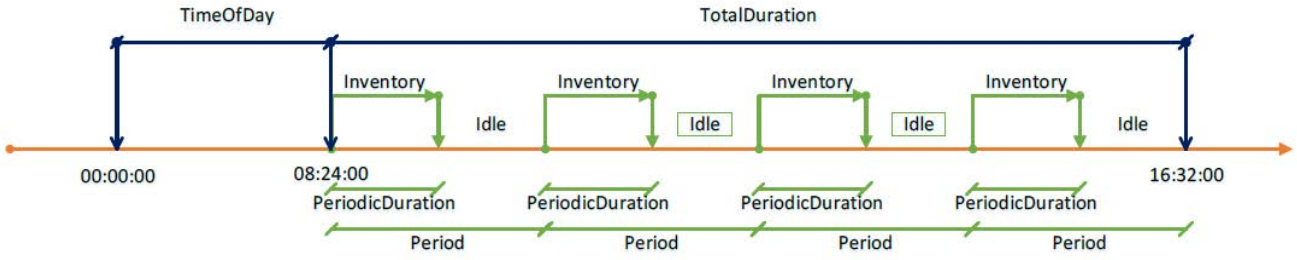
Stop trigger [TotalDuration: 14880 seconds (4 hours 8 minutes, on “16:32:00”), PeriodicDuration: 5 seconds]

Expected:

If time is lesser than “08:24:00”, OR greater than “16:32:00”, there is no inventory.

If time is greater than “08:24:00”, AND lesser than “16:32:00”, the reader does inventory 5 seconds per 10 seconds.

Figure 112 Single Trigger Pair: Timelapse Start/Timelapse Stop



Single trigger pair: Timelapse Start/Timelapse Stop (TotalDuration = 0)

Configuration:

Start trigger [Time of Day: “08:24:00”, Period: 10 seconds]

Stop trigger [TotalDuration: 0 second, PeriodicDuration: 5 seconds]

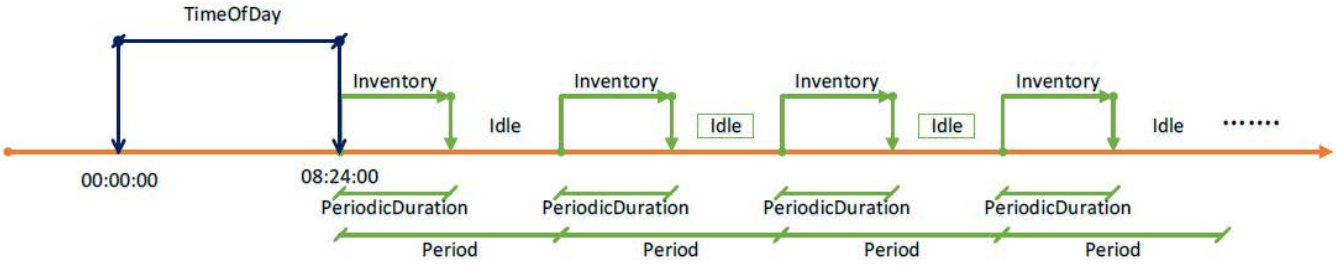
Expected:

If time is lesser than “08:24:00”, there is no inventory.

If time is greater than “08:24:00”, reader does inventory 5 seconds per 10 seconds without termination.

Since TotalDuration is zero, inventory cycles repeat periodically and indefinitely.

Figure 113 Single Trigger Pair: Timelapse Start/Timelapse Stop (TotalDuration = 0)



Single trigger pair: Timelapse Start/Timelapse Stop (Period = 0, PeriodicDuration = 0)

Configuration:

Start trigger [Time of Day: “08:24:00”, Period: 0 seconds]

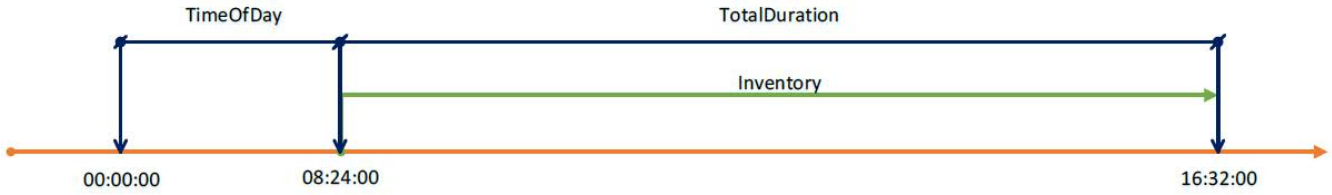
Stop trigger [TotalDuration: 14880 seconds (4 hours 8 minutes, on “16:32:00”), PeriodicDuration: 0 second]

Expected:

If time is lesser than “08:24:00”, OR greater than “16:32:00”, there is no inventory.

If time is greater than “08:24:00”, AND lesser than “16:32:00”, reader does inventory constantly.

Figure 114 Single Trigger Pair: Timelapse Start/Timelapse Stop (Period = 0, PeriodicDuration = 0)



Single trigger pair: Timelapse Start/Timelapse Stop (Period = 0, TotalDuration = 0, PeriodicDuration = 0)

Configuration:

Start trigger [Time of Day: “08:24:00”, Period: 0 seconds]

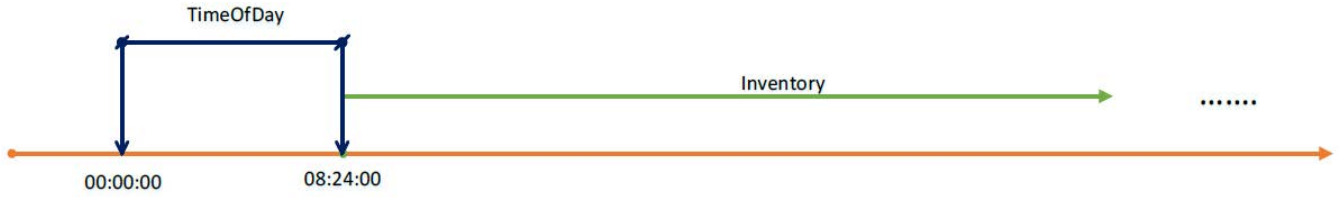
Stop trigger [TotalDuration: 0 second, PeriodicDuration: 0 second]

Expected:

If time is lesser than “08:24:00”, there is no inventory.

If time is greater than “08:24:00”, reader does inventory constantly without termination.

Figure 115 Single Trigger Pair: Timelapse Start/Timelapse Stop (Period = 0, TotalDuration = 0, PeriodicDuration = 0)



Single trigger pair: Displacement Start/Timelapse Stop

Configuration:

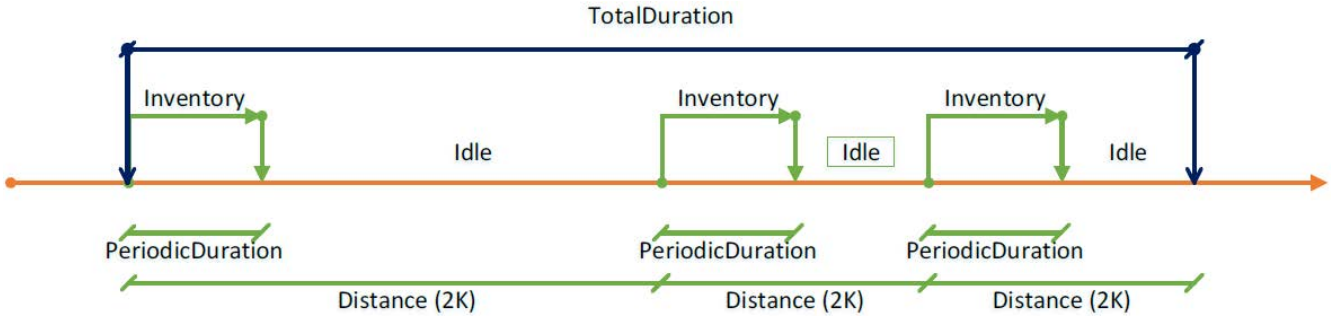
Start trigger (Distance: value 2 km)

Stop trigger [TotalDuration: 14880 seconds (4 hours 8 minutes), PeriodicDuration: 5 seconds]

Expected:

When reader moves 2 km, will do inventory 5 seconds till duration over 14880 seconds (count 4 hours 8 minutes from trigger's creation). In below graph th horizontal line represents time. Truck displacement of 2K in time varies.

Figure 116 Single Trigger Pair: Displacement Start/Timelapse Stop



Single trigger pair of Distance/Timelapse (TotalDuration = 0)

Configuration:

Start trigger (Distance: value 2 km)

Stop trigger [TotalDuration: 0 seconds (4 hours 8 minutes), PeriodicDuration: 5 seconds]

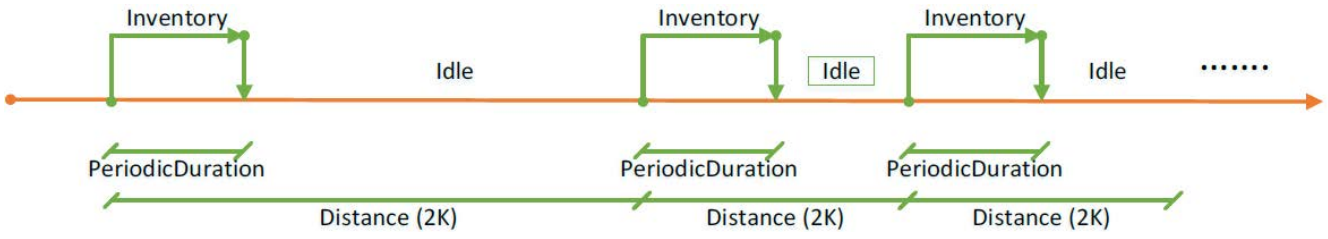
Expected:

When reader moves 2 km, will do inventory 5 seconds

Since TotalDuration is zero, inventory cycles repeat periodically indefinitely.

In below graph the horizontal line represents time. Truck displacement of 2K in time varies.

Figure 117 Single Trigger Pair of Distance/Timelapse (TotalDuration = 0)



Two trigger pair: GPI Start/GPI Stop; Timelapse Start/No Stop

The GPI trigger has higher priority, and it can preempt Timelapse trigger.

Priority is determined by the order of the trigger configuration. The first trigger gets higher priority.

Configuration:

First trigger pair (high priority)

Start trigger (GPI1: low value)

Stop trigger (GPI1: high value)

Second trigger pair (low priority)

Start trigger [Time of Day: “08:24:00”, Period: 0 seconds]

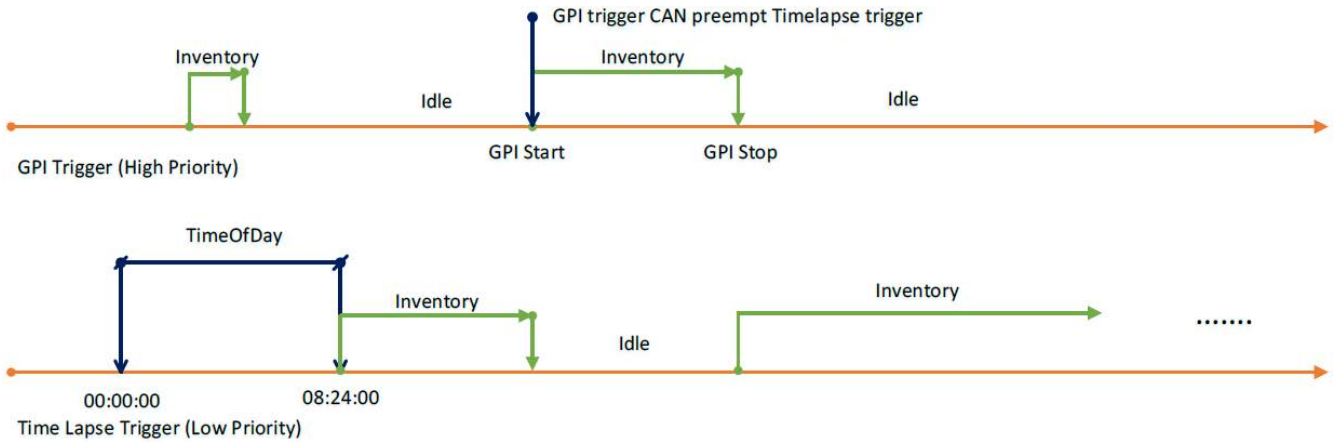
Stop trigger [TotalDuration: 0 second, PeriodicDuration: 0 second]

Expected:

After 8:24AM, reader begins inventory due to second trigger.

The high priority GPI trigger can preempt the low priority timelapse trigger.

Figure 118 Two Trigger Pair: GPI Start/GPI Stop; Timelapse Start/No Stop



Two trigger pair: Timelapse Start; GPI Start/GPI Stop

The GPI of second trigger has lower priority, and it can't preempt Timelapse (first).

Configuration:

First trigger pair (high priority)

Start trigger [Time of Day: "08:24:00", Period: 0 seconds]

Stop trigger [TotalDuration: 0 second, PeriodicDuration: 0 second]

Second trigger pair (low priority)

Start trigger (GPI1: low value)

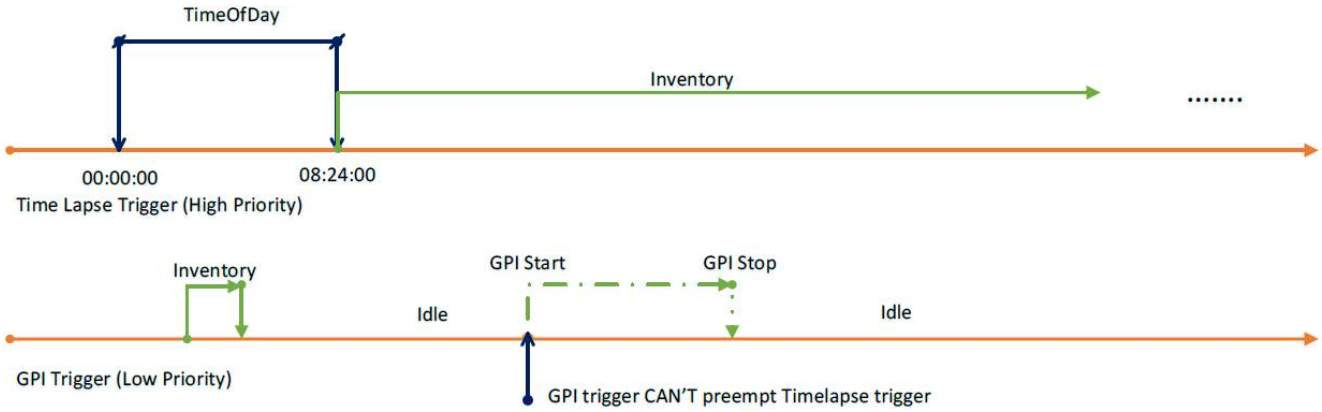
Stop trigger (GPI1: high value)

Expected:

After 8:24AM, reader begins inventory due to the first trigger.

The low priority GPI trigger can't preempt the high priority timelapse trigger.

Figure 119 Two Trigger Pair: Timelapse Start; GPI Start/GPI Stop



Moving and Stationary Tags

Introduction

This chapter recommends the settings in LLRP and RFID3 APIs to read the moving and stationary tags.

Moving vs Stationary

Some use cases require the readers to monitor moving and stationary tags in a read zone which are defined by strategically installed antennas. This feature does not report tag direction but provides information if new tags come in or leave the monitored zone.

An application can also query tags that are detected as not moving by the reader.

If the tag direction through a transition point is required, users can consider the transition readers offered by the SmartLens solution.

The result accuracy is very sensitive with the number of stationary tags in FOV, the moving tag is not big factor in algorithm. Tag stationary moderated timeout could be adjusted according to the number of stationary tags within range from 5 to 10 seconds. Timeout could be 5 seconds if 10 stationary tags, On the contrary, 500 stationary tags can set timeout to 10 seconds.

This feature can be enabled and leveraged via LLRP and RFID3 APIs.
This feature works reliably if the read zone does not have tags that are hard to read.

To get the stationary tags (which are present in the reader FOV for a defined time) the configuration required is as follows.

Let us assume if we have first set of 10 tags which are not moving and are stationary in the reader FOV. And, there is a second set of 10 tags that enter and exit the reader FOV.

First, we need to enable the feature by
`tInfo.TagEventReportInfo.setReportTagMovingEvent(TAG_MOVING_EVENT_REPORT.ENABLE);`

We need to set the ***setTagStationaryModeratedTimeoutMilliseconds*** parameter to 10 secs

setReportNewTagEvent, ***setReportTagInvisibleEvent***, ***setReportTagBackToVisibilityEvent*** to MODERATED and their respective timeouts to 3000ms

Perform inventory for more than 30 secs and then call `reader.Actions.getStationaryTags();`. This will only report the tags which have stayed in the reader FOV for more than 10secs(*setTagStationaryModeratedTimeoutMilliseconds*) and will not report the tags which came in reader FOV and left with in 10secs(*setTagStationaryModeratedTimeoutMilliseconds*). MOVING_TAG event will be generated for second set of 10 tags.

If the tag has stayed for 10secs(*setTagStationaryModeratedTimeoutMilliseconds*) in reader FOV and then moved out of Reader FOV within 30secs of inventory, even then the tags are reported as stationary as it stayed in Reader FOV for 10secs(*setTagStationaryModeratedTimeoutMilliseconds*)

So depending on the value set in *setTagStationaryModeratedTimeoutMilliseconds* we need to set the duration of inventory to get best results.

Recommendation:

1. Few moving tags / few stationary tags

   If the number of both stationary tags and moving tags are less (< 10), it is recommended to set the new tag event moderated timeout **(LLRP: NewTagEventModeratedTimeout; RFID3: newTagEventModeratedTimeoutMilliseconds)** value to 3 seconds. The stray tag moderate timeout **(LLRP: StrayTagModeratedTimeout; RFID3: tagStationaryModeratedTimeoutMilliseconds)** could be set to 5 secconds.
2. Few moving tags / many stationary tags

   If the number of stationary tags is large (> 500) and the number moving tags through the read zone is less (< 10), it is recommended to set the new tag event moderated timeout **(LLRP: NewTagEventModeratedTimeout; RFID3: newTagEventModeratedTimeoutMilliseconds)** value to 3 seconds. The stray tag moderate timeout **(LLRP: StrayTagModeratedTimeout; RFID3: tagStationaryModeratedTimeoutMilliseconds)** should be set to larger value > 10 secs. So that the reader will read all the 500 tags within 10 seconds(for the reader to identify it is stationary)
3. Many moving tags / few stationary tags

   If the number of stationary tags is less (<10) and the number moving tags through the read zone is large (>500), it is recommended to set the new tag event moderated timeout **(LLRP: NewTagEventModeratedTimeout; RFID3: newTagEventModeratedTimeoutMilliseconds)** value to 3 seconds. The stray tag moderate timeout **(LLRP: StrayTagModeratedTimeout; RFID3: tagStationaryModeratedTimeoutMilliseconds)** could be set to value 6 secconds.

LLRP Configuration

This feature can be configured in the **MovingStationaryTagReport** parameter. This parameter has two fields to be configured. The **ReportMovingTag** field can enable/disable moving tag reporting event. The **StrayTagModeratedTimeout** field sets timeout in milliseconds for the change of tag from moving state to stationary state. The timeout value needs optimization as described earlier. The **MovingStationaryTagReport** parameter is a custom parameter of **ROReportSpec**.

```
<customParameterDefinition name="MovingStationaryTagReport"

   <fieldtype="u8" name="ReportMovingTag "enumeration="TagEventSelectorReportMovingTag"/>

   <fieldtype="u16" name="StrayTagModeratedTimeout"/>

   <allowedIntype="ROReportSpec" repeat="0-1"/>

</customParameterDefinition>


<customEnumerationDefinition    name="TagEventSelectorReportMovingTag">

   <entry    value="0"       name="Disable"/>

   <entry    value="1"       name="Enable"/>

</customEnumerationDefinition>
```

The new tag moderated timeout parameter also plays an important role as described earlier.

For this feature, the following moderated timeout settings affect the result.

It is recommended to set the tag invisible moderated timeout to 3 seconds.

It is recommended to set the tag visibility change moderated timeout to 1 second.

```
<customParameterDefinition      name="MotoTagEventSelector">
   <field       type="u8"       name="ReportNewTagEvent"
                        enumeration="MotoTagEventSelectorReportNewTagEvent"/>
   <field       type="u16"      name="NewTagEventModeratedTimeout"/>
   <field       type="u8"       name="ReportTagInvisibleEvent"
                        enumeration="MotoTagEventSelectorReportTagInvisibleEvent"/>
   <field       type="u16"      name="TagInvisibleEventModeratedTimeout"/>
   <field       type="u8"       name="ReportTagVisibilityChangeEvent"
                        enumeration="MotoTagEventSelectorReportTagVisibilityChangeEvent"/>
   <field       type="u16"      name="TagVisibilityChangeEventModeratedTimeout"/>
   <allowedIn    type="ROReportSpec" repeat="0-1"/>
</customParameterDefinition>
```

LLRP Report

The **MotoTagEventTypeEnum** enumeration adds 2 new entries **Tag_Moving** and **Tag_Stationary** to extend the event type in tag event report. If **TagEventSelectorReportMovingTag** is enabled, the Tag Moving event is used to report tags whenever the **New Tag Visible**, **Tag Not Visible**, and **Tag Visibility Changed** events take place. Stationary tags can be obtained by sending the **GET_REPORT** command to the reader. The moving/stationary event is in **TagReportData** > **MotoTagEventList** > **MotoTagEventEntry** > **EventType** > **Tag_Moving**.

```
<parameterDefinition name="TagReportData">
   <choice    repeat="1"   type="EPCParameter"/>
   <parameter repeat="0-1" type="ROSpecID"/>
   <parameter repeat="0-1" type="SpecIndex"/>
.....
   <parameter repeat="0-1" type="MotoTagEventList"/>
</parameterDefinition>

<customParameterDefinition      name="MotoTagEventList">
   <parameter repeat="0-N" type="MotoTagEventEntry"/>
</customParameterDefinition>
```

```
<customParameterDefinition      name="MotoTagEventEntry">
   <field       type="u8"       name="EventType"
                                enumeration="MotoTagEventTypeEnum"/>
   <field       type="u64"      name="Microseconds" format="Datetime"/>
</customParameterDefinition>


<customEnumerationDefinition    name="MotoTagEventTypeEnum"
                                namespace="moto">
   <entry     value="0"        name="Unknown"/>
   <entry     value="1"        name="New_Tag_Visible"/>
   <entry     value="2"        name="Tag_Not_Visible"/>
   <entry     value="3"        name="Tag_Visibility_Changed"/>
   <entry     value="4"        name="Tag_Moving"/>
   <entry     value="5"        name="Tag_Stationary"/>
</customEnumerationDefinition>
```

RFID3 API Configuration

The structure **TAG_EVENT_REPORT_INFO** adds 2 new member variables. **reportTagMovingEvent** can enable/disable this feature. **tagStationaryModeratedTimeoutMilliseconds** is a timeout setting in milliseconds for moderating tag stationary status transition. The timeout value needs optimization as described earlier.

```
typedef enum _TAG_MOVING_EVENT_REPORT
{
TAG_MOVING_EVENT_DISABLE = 0,/**< Disable moving event reporting. */
TAG_MOVING_EVENT_ENABLE  = 1,/**< Enable moving event reporting. */
}TAG_MOVING_EVENT_REPORT;
```

The new tag moderated timeout parameter also plays a role as described earlier.

For this feature, the following moderated timeouts setting affects the result.

It is recommended to set the tag invisible moderated timeout to 3 seconds.

It is recommended to set the tag visibility change moderated timeout to 1 second.

typedef struct _TAG_EVENT_REPORT_INFO

{

TAG_EVENT_REPORT_TRIGGER reportNewTagEvent;/**< Report criteria when a new Tag is visible.*/

UINT16 newTagEventModeratedTimeoutMilliseconds;/**< Timeout in milliseconds for moderating new tag event reporting. Use this only when reportNewTagEvent is set to MODERATED.*/

TAG_EVENT_REPORT_TRIGGER reportTagInvisibleEvent;/**< Report criteria when a Tag is invisible.*/

UINT16 tagInvisibleEventModeratedTimeoutMilliseconds;/**< Timeout in milliseconds for moderating tag invisible event reporting. Use this only when reportTagInvisibleEvent is set to MODERATED.*/

TAG_EVENT_REPORT_TRIGGER reportTagBackToVisibilityEvent;/**< Report criteria when a Tag is back to visibility.*/

UINT16 tagBackToVisibilityModeratedTimeoutMilliseconds;/**< Timeout in milliseconds for moderating tag back to visibility event reporting. Use this only when reportTagBackToVisibilityEvent is set to MODERATED.*/

TAG_MOVING_EVENT_REPORT reportTagMovingEvent;/**< Report criteria when a Tag is in moving.*/

UINT16 tagStationaryModeratedTimeoutMilliseconds;**< Timeout in milliseconds for moderating tag stationary status transition. Use this only when reportTagMovingEvent is enabled.*/

}TAG_EVENT_REPORT_INFO, *LPTAG_EVENT_REPORT_INFO;

RFID3 API Report:

The **TAG_EVENT** adds 2 new event type **TAG_MOVING** and **TAG_STATIONARY**. If this feature is enabled by **reportTagMovingEvent**, the moving event can be generated and send to application from reader. The stationary event needs **RFID_GetReadTag()** function to do polling. The moving/stationary event is in **TAG_DATA > TAG_EVENT > TAG_MOVING.**

typedef struct _TAG_DATA

{

UINT8* pTagID; /**< Tag ID, for C1G2 this field refers EPC Data.*/

UINT32tagIDLength; /**< Tag ID Length (Number of Bytes).*/

.....

TAG_EVENTtagEvent;

.....

} TAG_DATA, *LPTAG_DATA;

typedef enum _TAG_EVENT

{

UNKNOWN_STATE = 0, /**< This implies that the Tag is a result of autonomous mode operation and but the state of the tag is not known.*/

NEW_TAG_VISIBLE = 1, , /**< This implies that the Tag is a result of autonomous mode operation and the tag is visible for the first time.*/

TAG_NOT_VISIBLE = 2, This implies that the Tag is a result of autonomous mode operation and the tag is not visible.*/

TAG_BACK_TO_VISIBILITY = 3, , /**< This implies that the Tag is a result of autonomous mode operation and the tag is back to visibility.*/

TAG_MOVING = 4, /**< This implies that the Tag is moving generated by moving/stationary check */

TAG_STATIONARY = 5, /**< This implies that the Tag is stationary generated by moving/stationary check */

NONE = 6

}TAG_EVENT;

Compliance and Implications of EU RED for the FX7500 and FX9600

Introduction

This chapter provides detailed information on the definition of BS EN 18031-1 and the EU Radio Equipment Directive (RED). It also addresses the compliance and implications for the FX7500 and FX9600.

About BS EN 18031-1 & The EU Radio Equipment Directive (RED)

BS EN 18031-1 is a technical standard that provides a detailed cybersecurity checklist for any "internetconnected radio equipment" sold in the EU.

It was created to enforce the EU's Radio Equipment Directive (RED), which made cybersecurity a mandatory legal requirement for these devices. The standard translates the broad legal goal of "not harming the network" into specific, testable engineering requirements.

For manufacturers, complying with this standard provides a **"presumption of conformity"**. It means their product is legally presumed to meet the cybersecurity obligations of the RED, which is essential for placing the CE mark on the product and selling it in the EU market.

Applicability of BS EN 18031-1 for the FX7500 and FX9600

The FX7500 and FX9600 are subject to this standard. It is designed to be network-connected via its Ethernet port, placing it directly in the scope of the RED cybersecurity regulation. Compliance is a mandatory requirement for market access.

Security is Based on "Environmental Controls"

The key to the FX7500 and FX9600 compliance strategy is that it is an enterprise device, not a standalone consumer product. Its security model relies heavily on its intended operational environment. The standard is designed to accommodate this through its "except for" clauses.

How Compliance is Justified

Access Control (ACM) & Authentication (AUM)

To view/modify any sensitive security parameters listed below, the user needs to enter a valid authorization password.

- Web Console
- Shell access

- IOTC APIs
- IOTC configuration
- Certificate configuration Management

Secure Communication (SCM)

This is applicable because the Ethernet network interface allows access to the API and network services on the device. The FX7500 and FX9600 **PASSES** by implementing strong, authenticated encryption protocols such as **802.1x for Ethernet.**

Best Practice Cryptography (CRY)

This is applicable. The FX7500 and FX9600 **PASSES** by demonstrating that its encryption methods used are the "best practice".

The standard provides the mandatory rulebook, and Zebra justifies the FX7500 and FX9600 compliance by demonstrating how it meets those rules—either directly on the device or through the mandatory security of the host computer and the operating environment.

Applicability of BS EN 18031-1

Currently, the changes related to BS EN 18031-1 are applicable only to European Union countries that adhere to the BS EN 18031-1 standards. For a comprehensive list of these countries, see Annexure 1.

Default Authorization Password & Update

Users will need to authenticate to the device to perform any configuration, such as setting the region, performing inventory, scanning operations, and more. The user will be forced to change the default admin password on their first login as described in the previous chapters..

It is now required to set the rfidadm password in order to enable the SSH shell.

Guest User, which is a read-only user, must also have a password set.

LLRP Settings

LLRP is configured to secure mode by default out of the box. As a result, port 5085 can be used to connect to LLRP.

SSH Settings

SSH is disabled by default. Setting the rfidadm password is mandatory for enabling the SSH service.

SNMP Settings

SNMP is disabled by default. It can be enabled in the **Communication > Services** page.

Annexure 1

The following is the list of European Union countries where BS EN 18031-1 standards are applicable.

SL NO	EU RED Country List	WR SKU with 900M Support	E8 SKU Support	Remarks
1	Austria	Yes	Yes	
2	Belgium	Yes	Yes	
3	Bulgaria	Yes	Yes	
4	Croatia	Yes	Yes	
5	Cyprus	Yes	Yes	
6	Czech Republic	Yes	Yes	
7	Denmark	Yes	Yes	
8	Estonia	Yes	Yes	
9	Finland	Yes	Yes	
10	France	Yes	Yes	
11	Germany	No	Yes	
12	Greece	No	Yes	
13	Hungary	Yes	Yes	
14	Iceland	Yes	Yes	
15	Ireland	Yes	Yes	
16	Italy	No	Yes	
17	Latavia	No	Yes	
18	Liechtenstein	Yes	Yes	
19	Lithuania	Yes	Yes	
20	Luxembourg	No	Yes	
21	Malta	No	Yes	
22	Netherlands	No	Yes	
23	Norway	Yes	Yes	
24	Poland	No	Yes	
25	Portugal	Yes	Yes	
26	Romania	Yes	Yes	
27	Slovakia	Yes	Yes	
28	Slovenia	Yes	Yes	
29	Spain	Yes	Yes	

SL NO	EU RED Country List	WR SKU with 900M Support	E8 SKU Support	Remarks
30	Sweden	Yes	Yes	
31	Switzerland	Yes	Yes	
32	Turkeye	No	Yes	
33	Albania	No	Yes	
34	Andorra	No	Yes	
35	Bosnia Herzegovina	No	Yes	
36	French Guiana	No	Yes	
37	Georgia	No	Yes	
38	Guadeloupe	No	Yes	
39	Macedonia	No	Yes	
40	Martinque	No	No	Not supported by RFD40
41	Monaco	No	Yes	
42	Montenegro	No	Yes	
43	Reunion Isl.	No	No	Not supported by RFD40
44	San Mariano	No	No	Not supported by RFD40
45	Sao Tome and Principe	No	No	Not supported by RFD40
46	St Pierre & Miqueion	No	No	Not supported by RFD40
47	Vatican City	No	No	Not supported by RFD40

Troubleshooting

Troubleshooting

Table 12 provides FX Series troubleshooting information.

Contact the distributor or call the local support if problems persists. See page 16 for contact information.

Table 12 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 37.
Reader is not reading tags.	The tag is out of its read range.	Move the tag into read range. See Read Tags on page 79.
	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 37 to view the IP address, or use the host name to connect to the reader.

Table 12 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 16*.
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 16*.
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 12 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
User name is not correct.	The user name does not match the current user registry (illegal characters, too long, too short, unknown, or duplicate).	Accurately retype the user name.
	User forgot the user ID. Web console supports the following users: - **Admin** (default password is **change**) - **Guest** (no password required) - **rfidadm** - supported over SSH, 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 42.
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 16.*
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 42.
The name, serial number, or IP address entered already exists in the system.	The name, serial number, or IP address entered was already used.	Enter a unique value for the new name, serial number, or IP address.
Another administrator is currently logged in. Try again later.	The system does not allow more than one administrator to log in at a time.	Wait until the other administrator logs out (or times out) before logging in or override the current session with the new one.
Backup configuration file does not exist.	The system cannot revert to a backup configuration unless a backup file exists.	Commit the new configuration to create a backup file.

Table 12 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
Failed to confirm the new password.	The system requires entering the password identically two times.	Accurately retype the password twice.
Network configuration change(s) have not been saved.	The user requested log out prior to 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 16*.
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 16*
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 16*.
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 16*.

Table 12 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 16*.
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 16*.
The action must be confirmed.	The user must confirm the requested action before it is executed.	Select the confirmation option when issuing this request.
Invalid network adapter when navigating to the Bluetooth configuration page.	The Bluetooth dongle is not plugged in or not supported.	Plug in a supported Bluetooth dongle and refresh the browser.
Wireless scan error.	Wireless dongle is not plugged in or not supported.	Plug in a supported wireless dongle and repeat the wireless scan.
Unable to connect to the wireless network.	Access point is off or unreachable.	Turn on the access point and make sure it is accessible.
	Encryption type is not supported in the access point.	Use one of the following supported encryption types: WEP128, WPA/WPA2 and Open.
	The wireless page displays **Adapter not found**.	Connect the wireless adapter to the reader.
Wireless connection is complete, but no IP address.	No DHCP server is running in the network.	Add a DHCP server to the network.
OS update in progress.	Firmware update on the reader is ongoing. The current operation is not permitted.	Wait for the firmware update to complete and then retry the operation.
Cannot change password.	Cannot change password for guest.	Guest does not need a password to log in to the Administrator Console.

Table 12 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
The following reader web console pages do not load correctly: • Advanced Antenna Configuration • ReadTags • Services • Serial Port Communication • License Manager • User Application • Profiles • File based firmware upload • Syslog Export	Port 8001 is not accessible.	Allow port 8001 to be accessible across the networks. These web pages all use port 8001 to communicate to the reader and without this port the pages cannot function.
Serial Port Push Data: Unable to get TAG data over the serial port in Push Data mode.	The Serial Port configuration between the host and target is not matched.	The configuration on the receiving end should be same as in the Serial Port Configuration window.
	Serial cable is not connected when inventory started and the serial port buffer full.	Serial cable must be attached to the reader and host machine when inventory started. Stop and start the inventory again after connecting the serial cable.

System Log Error Code Descriptions

Table 13 System Log Error Code Descriptions

Code	Error Code Message
0	Success.
1	One of the input parameters is bad.
2	Provided buffer is not big enough to hold the data.
3	Callout failed but did not set error information.
4	Data corruption found.
5	Provided data exceeds maximum size allowed.
6	The size of provided data is incorrect.
7	Information for the date is invalid.
9	Requested feature has expired.
10	Requested feature's host ID does not match system host ID.
11	Requested feature is not found.

Table 13 System Log Error Code Descriptions (Continued)

Code	Error Code Message
12	Start date for the requested feature is in the future.
13	Feature is issued by a different vendor.
14	Feature with the requested version is not found.
15	Type of the host ID is currently unsupported.
16	Version of identity is not supported.
17	Item already exists in the collection.
18	Provided item is not found in the collection.
19	Item's value has a different type than expected.
20	Provided index is out of bounds.
21	Key already exists in the collection.
22	Provided key is not found in the collection.
26	The allowed time to process response has expired.
27	Response does not match system host ID.
28	Server is not able to process request correctly.
29	Response is out of order with previous responses.
30	Signature did not pass validation.
31	Inconsistent signature type used.
32	This trial is already loaded.
33	Trial duration has expired.
34	Trial ID is invalid.
35	Storage anchor break found.
36	Storage binding break found.
37	Trusted storage is corrupted.
38	Trusted storage contains inconsistent data.
39	This version of trusted storage is not supported.
40	Storage implementation class provided is not complete.
41	Vendor keys have expired.
42	Vendor keys are invalid.
43	Vendor keys do not support this platform.
44	Identity data has changed; unable to decrypt trusted storage or anchor data.
45	Clock wind back is detected.

Table 13 System Log Error Code Descriptions (Continued)

Code	Error Code Message
46	Clock wind back is disabled; unable to test if wind back has happened.
47	Data version is not supported.
48	Insufficient count for the requested feature.
49	Object cannot be modified because it is being used by another object.
50	Version string is invalid.
51	A signature signed with a revision of key which is not present in identity data.
52	Requested feature's server host ID does not match system host ID.
53	No server data found in TS. The Client probably never receives a capability response.
54	Regular update from the server is not needed as renew interval is set to 0 by the server.
55	Feature is node locked and cannot be served by the server.
56	Feature is a duplicate on the server and cannot be served.
57	Input type mismatch.
58	Failed to get a response from any of the servers.
59	New servers sent by the configuration server are not responding.
60	Required data is missing from capability response.
61	Capability response is not available - sync from the back office is not completed.
62	Identity is of different type than expected.
63	System machine type does not match expected machine type.
64	Requested unique identifier is not found.
65	Callout error is set using an inappropriate error code.
66	Callout error is set using an inappropriate unit identifier.
67	Tolerance specifier version is not supported.
68	A non-client tolerance specifier is specified by the client.
69	A badly formed tolerance specifier is encountered.
70	A tolerance specifier is rejected as not valid for this client.
71	An unsupported tolerance specifier type is specified.
72	A bad tolerance specifier ratio is specified.
73	Information message can hold either existing or usage-based features, but not both.
74	Trusted storage host ID does not match system host ID.
75	Response UUID does not match system UUID.
76	Trusted storage does not exist.

Table 13 System Log Error Code Descriptions (Continued)

Code	Error Code Message
77	The UUID in a message can originate from the back office or can be explicitly set, but not both.
78	Character set is invalid.
80	Requested publisher data is not set.
81	Checksum segment length mismatch.
82	Short code scheme is not supported.
83	CRC validation of short code failed.
84	Request host ID does not match host ID recorded by server.
85	Checksum validation failed.
86	The host ID in an info message can originate from trusted storage or can be explicitly set, but not both.
88	Unsupported certificate keyword.
89	Unknown certificate keyword.
90	Vendor dictionary can be requested as a whole, or by key; but not both.
91	Flag to include vendor dictionary is not set.
92	The specified capability request option conflicts with an option previously set.
93	Feature count exceeds the maximum supported value.
94	Features with an overdraft count are not supported on the client.
95	Features with an overdraft count are not supported on the server.
99	Metered features with the same name must have identical metered attributes.
100	Undo interval for the acquired feature has expired.
101	Metered functionality is not enabled.
103	Capability response type is invalid for operation.
107	Capability response contains a different server instance than the capability request.
108	Trusted storage already contains data from one of the capability response server host IDs stored in a different instance location.
109	The specified information message option conflicts with an option previously set.
111	Feature from a preview response cannot be acquired.
112	Server received a request of unknown type.
113	Required data is missing from capability request.
114	Vendor name in capability request does not match server vendor name.
115	No server records are found for the device.
117	Required data is missing from information message.

Table 13 System Log Error Code Descriptions (Continued)

Code	Error Code Message
118	Request type is invalid for operation.
119	Vendor name in information message does not match server vendor name.
120	Server is not a designated backup server.
121	Server maintenance interval is not set.
122	Server maintenance interval is not started.
123	Server maintenance interval has passed.
124	Backup server is performing active fail-over support.
125	Information message is out of order with previous messages.
126	No detailed usage info.
127	Host ID that enabled server is not connected.
128	No reservations are found for the device.
129	Device is not served any features and does not have any reservations.
130	Required data is missing from the sync related message.
131	Vendor name in sync related message does not match server vendor name.
132	Identity name in sync related message does not match server identity name.
133	Target id in the sync related message is invalid.
134	Source id in the sync related message is invalid.
135	Time units mismatch in the sync related messages.
136	Desired feature is not available and cannot be served by the server.
137	Device is dropped from the server.
140	Sync time mismatch in the sync related messages.
141	Host ID in information message is invalid.
142	Host ID in capability request message is invalid.
143	Virtual clients are not supported.
144	Unexpected information message type received.
145	Usage based information message support is not enabled.
146	Collection of the sync data offline is not supported.
147	Offline sync to FNO cannot be performed due to other sync in progress.
148	The message UUID does not match the device record UUID.
149	Unable to parse malformed or incorrect XML version.
150	Error in converting Julian date.

Table 13 System Log Error Code Descriptions (Continued)

Code	Error Code Message
151	An unsupported request operation is specified.
152	One-time activations are not supported.
153	Trusted storage cannot be reset with unsynchronized distribution data present.
154	Served buffer features cannot be returned early.
155	Client cannot switch from use of served buffer to trusted storage and vice versa.
156	Overage detected on server. Update from back office could not be processed because the outstanding license count is greater than the updated count.
158	Request has invalid content.
159	Invalid desired-feature count specified.
160	Server is currently running in environment tolerance interval.
161	Server environment tolerance interval has expired.

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, SFPT, SCP, SSH, HTTP, 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)

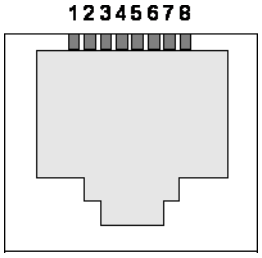
Item	Description
Transmit Power Output FX7500 FX9600	 10dBm to +31.5dBm (PoE+, 12V ~ 48V External DC, Universal 24 VDC Power Supply; +10dBm to +30.0dBm (PoE) 0dBm to +33.0dBm (PoE+, 12V ~ 24V External DC, Universal 24 VDC Power Supply; +0dBm to +31.5dBm (PoE)
Max Receive Sensitivity FX7500 FX9600	 -82dBm -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: 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 120 Ethernet Connections



USB Client Connector

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

Figure 121 USB Client Connector

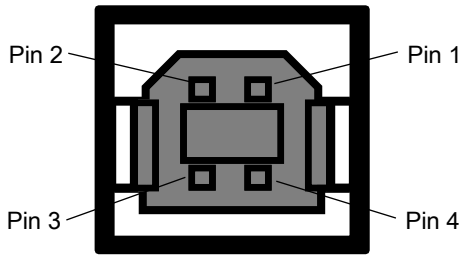


Table 15 USB Client Port Connector Pinout

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 122 USB Host Connector (J22)

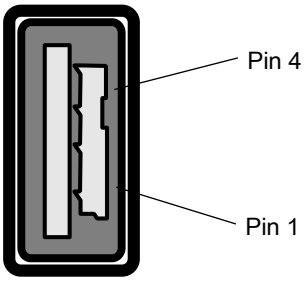


Table 16 USB Host Port Connector (J22) Pinout

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 123 FX7500 RFID Reader GPIO Connection

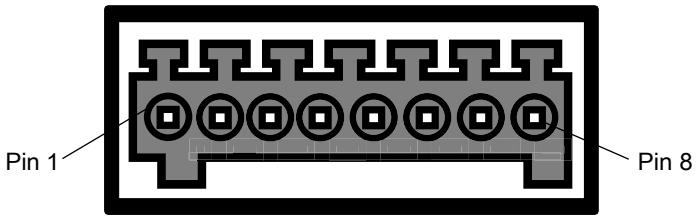


Table 17 FX7500 GPIO Pinouts

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 124 FX9600 RFID Reader GPIO Connection

Table 18 FX9600 GPIO Pinouts

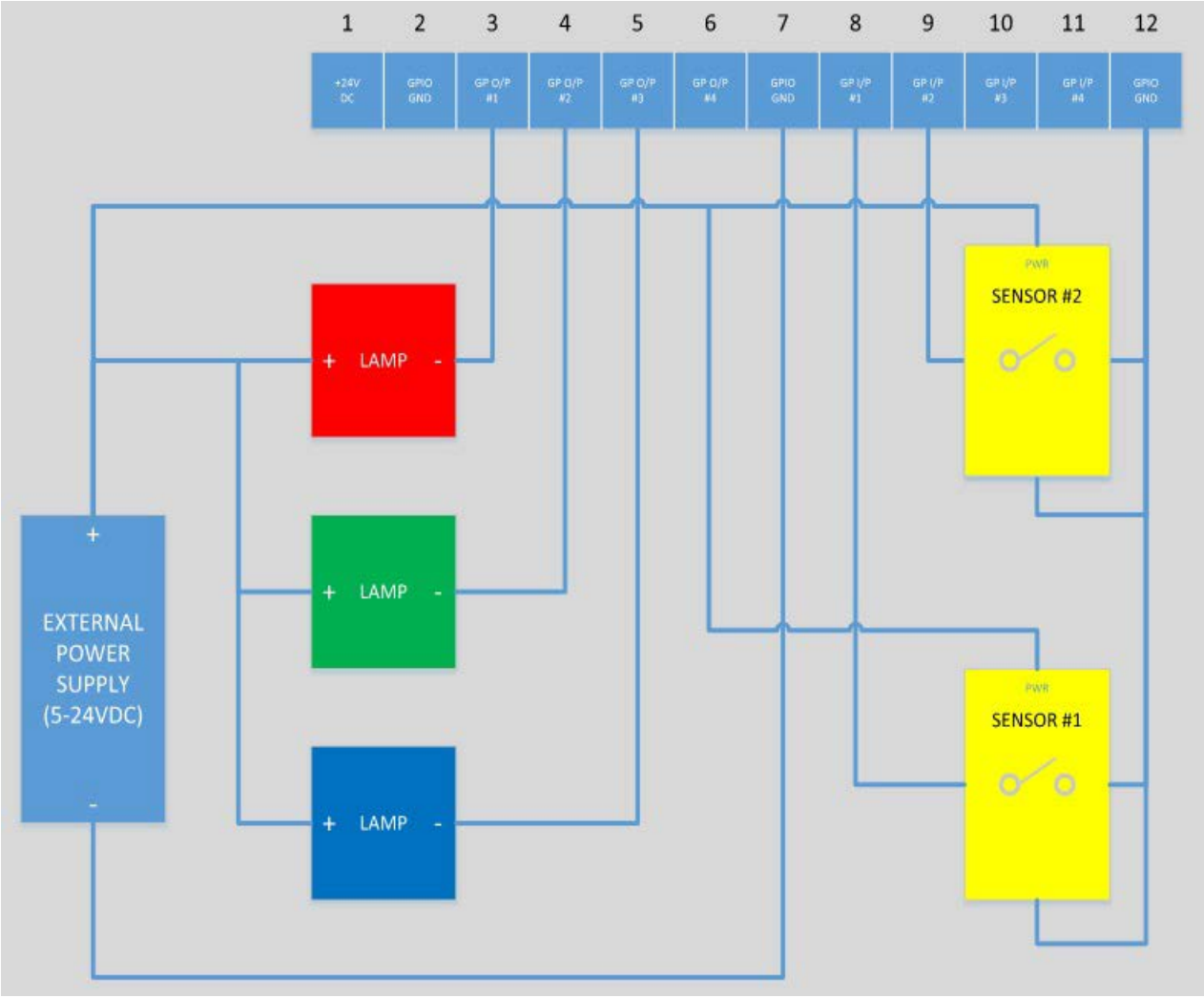
Pin #	Pin Name	Direction	Description
1	+24V DC Power	O	Supplies +24VDC At up to 1 Amp
2	GND	-	Ground connection
3	GP output #1	O	Signal for GP output #1
4	GP output #2	O	Signal for GP output #2
5	GP output #3	O	Signal for GP output #3

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

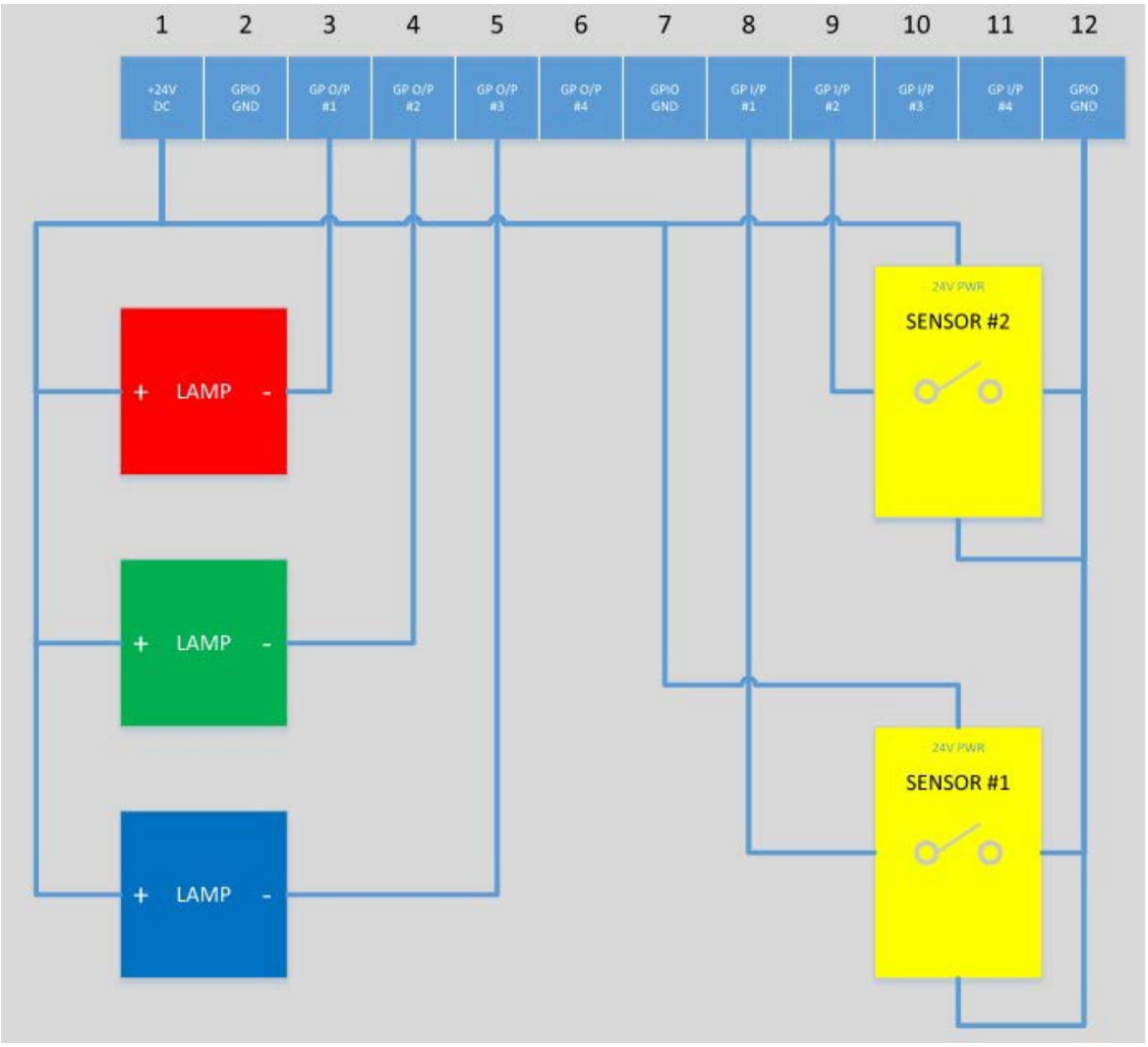
The Figure 125 provides an example of a typical GPIO setup with the power derived from an external power supply.

Figure 125 FX9600 GPIO Setup Example with Power Derived from External Power Supply



The Figure 126 provides an example of a typical GPIO setup with the power derived from GPIO 24V Pin.

Figure 126 FX9600 GPIO Setup Example with Power Derived from GPIO 24V Pin



Static IP Configuration

Introduction

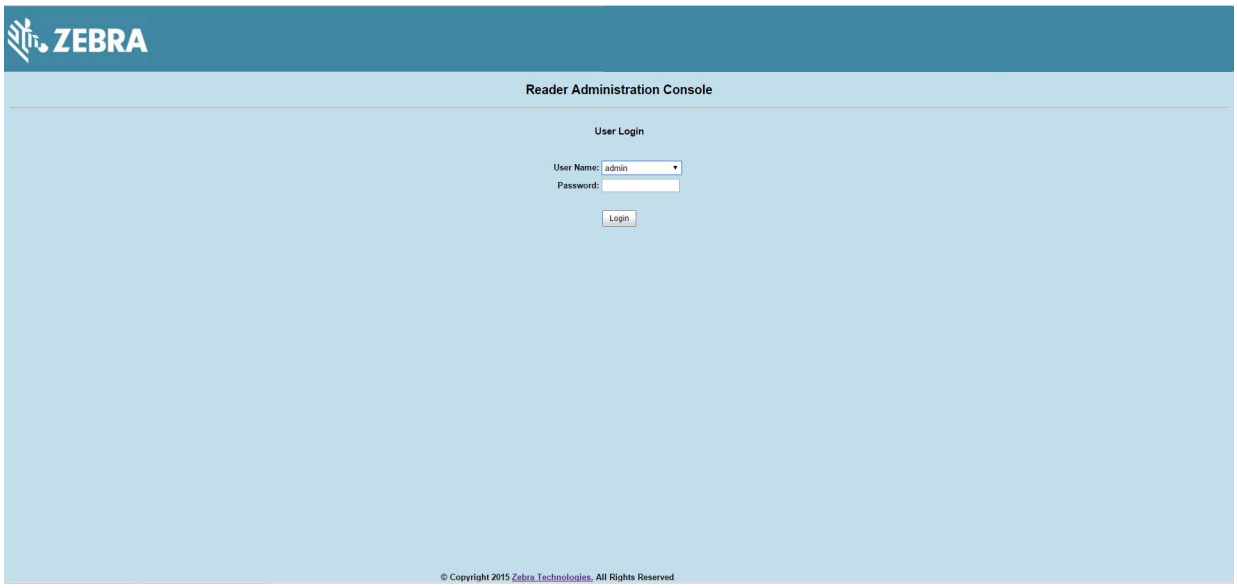
This chapter describes three methods to set the static IP address on the FX7500 and FX9600 RFID Readers.

Reader IP Address or Host Name is Known

To set the Static IP on the Web Console when you know the reader IP address or host name:

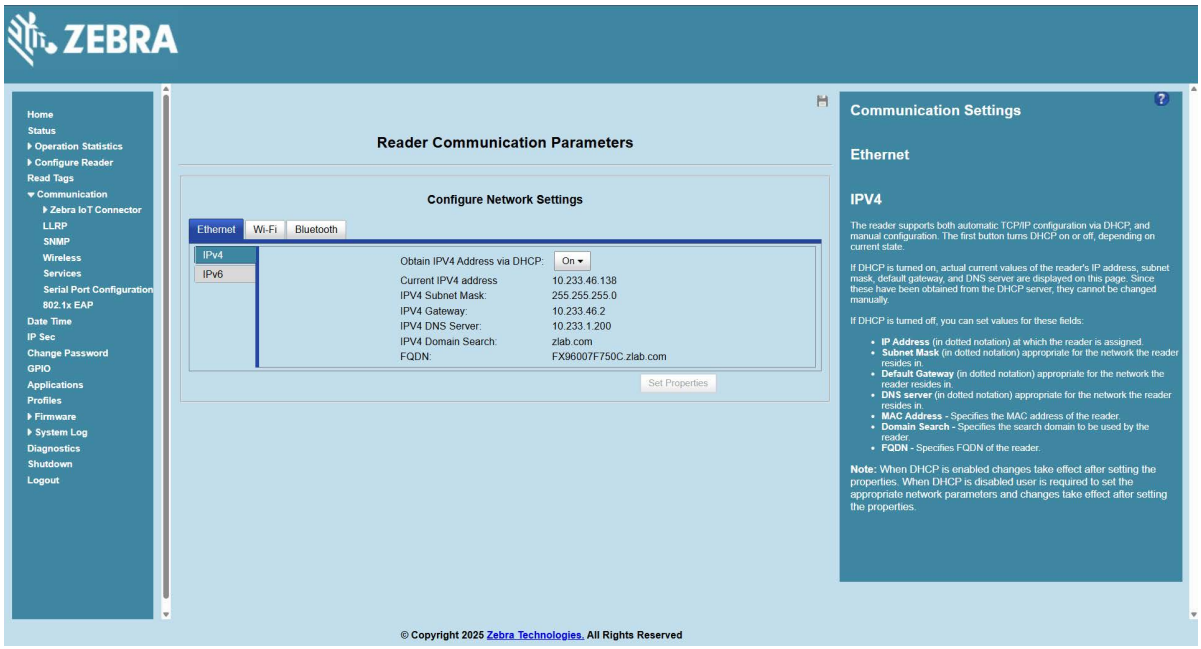
1. Browse the device using the host name, for example: FX7500CD3B1E.
2. Log in to the device.

Figure 127 Reader Administration Console Login Window



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

Figure 128 Reader Communication Parameters Window



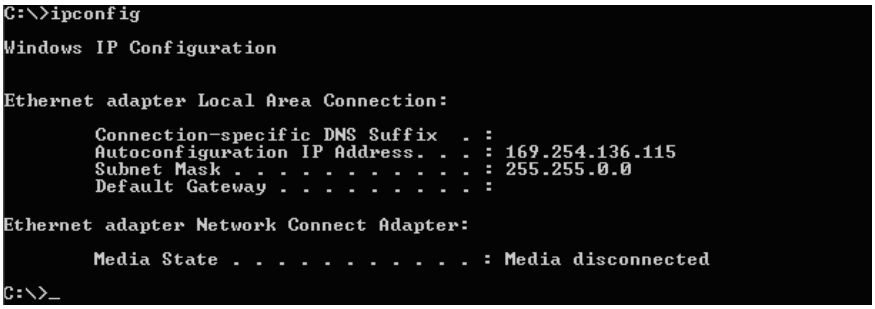
5. Select **Set Properties**. You can set a static IP that doesn't belong to this DHCP network.
6. The window displays a **Saving. Please wait...** message with a progress symbol until the commit completes.
7. When the commit completes, a gray floppy disk icon displays indicating that the commit completes 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)

To set the Static IP on the Web Console when you do not have the reader IP address:

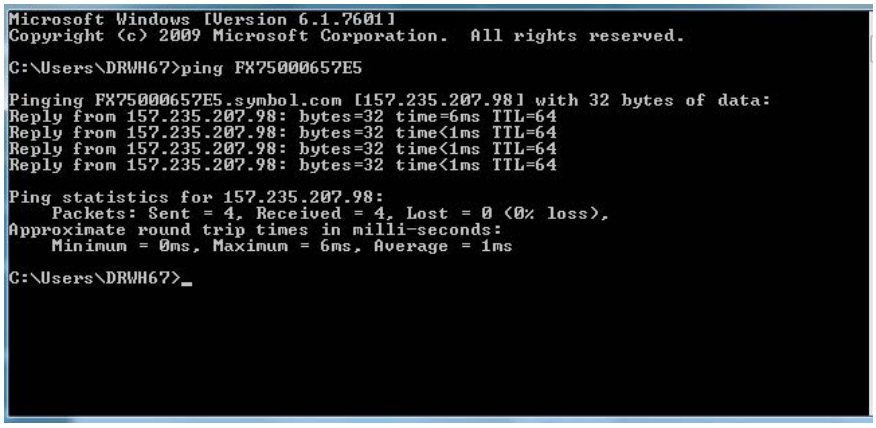
1. Connect the device and a PC running Windows XP to the same network that doesn't have a DHCP server, or connect the device directly to the PC.
2. Ensure both the device and PC Ethernet jack use at least one LED to indicate network connection detect.
3. If the PC uses an assigned static IP, update it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

Figure 129 Obtain IP Address



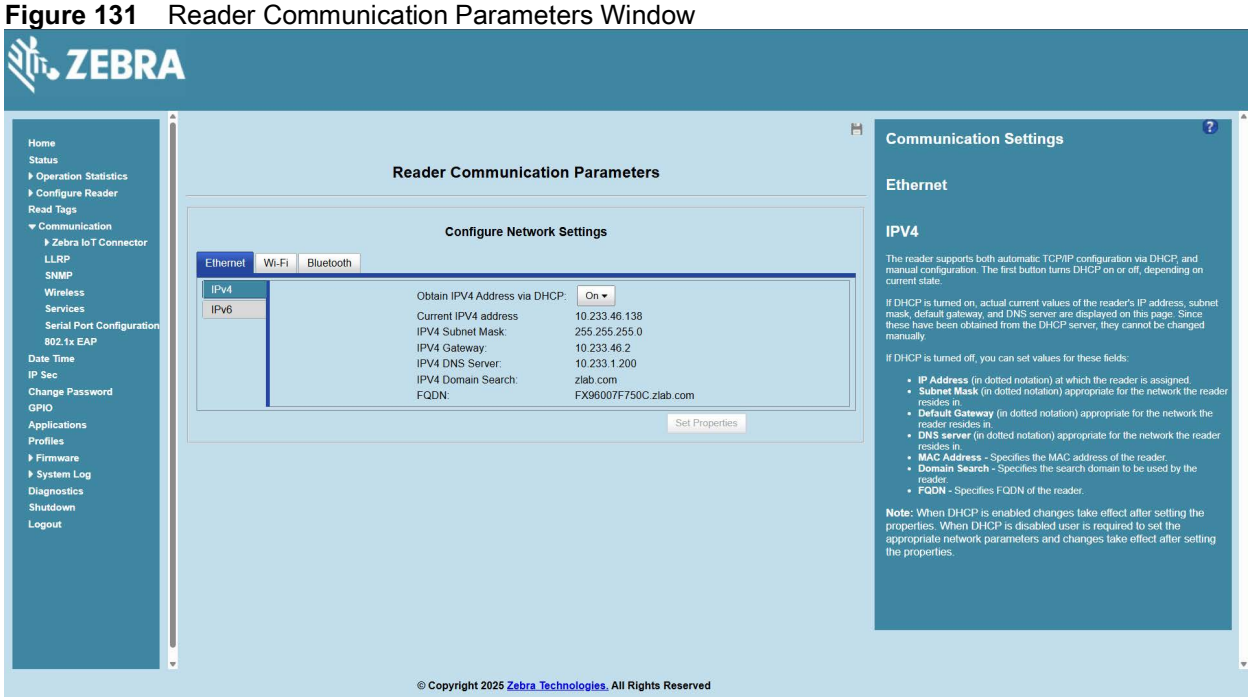
4. When possible, ping the host name of the device.

Figure 130 Ping the Host Name



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 131 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 section lists the supported air link configurations. The air link configuration is available through the LLRP and RFID3 API interfaces.

Radio Modes

The supported modes are exposed as a list of individual **UHFC1G2RfModeTableEntry** parameters in the 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 Conform-ance
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

*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.

Empty bracket [ ] indicates that this RF mode is not supported in FX7500; A number in the bracket indicates the RF Mode for the FX7500; No bracket indicates RF mode supported by both FX9600 and FX7500.

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 Conform-ance
11	64/3	160000	2	PR_ASK	1500	12500	18800	2100	Dense	false
12	64/3	160000	2	PR_ASK	2000	12500	18800	2100	Dense	false
13	64/3	60000	4	PR_ASK	1500	25000	25000	0	Dense	false
14	64/3	60000	4	PR_ASK	1500	12500	23000	2100	Dense	false
15	64/3	60000	4	PR_ASK	2000	25000	25000	0	Dense	false
16	64/3	60000	4	PR_ASK	2000	12500	23000	2100	Dense	false
17	64/3	64000	4	PR_ASK	1500	25000	25000	0	Dense	false
18	64/3	64000	4	PR_ASK	1500	12500	23000	2100	Dense	false
19	64/3	64000	4	PR_ASK	2000	25000	25000	0	Dense	false
20	64/3	64000	4	PR_ASK	2000	12500	23000	2100	Dense	false
21	64/3	80000	4	PR_ASK	1500	12500	18800	2100	Dense	false
22	64/3	80000	4	PR_ASK	2000	12500	18800	2100	Dense	false
*23	64/3	variable	variable	PR_ASK	variable	6250	25000	variable	variable	false
24	64/3	320000	1	PR_ASK	1500	12500	18800	2100	Dense	false
25	64/3	320000	1	PR_ASK	2000	12500	18800	2100	Dense	false
26	64/3	30000	8	PR_ASK	1500	25000	25000	0	Dense	false
27	64/3	30000	8	PR_ASK	1500	12500	23000	2100	Dense	false
28	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
29	64/3	30000	8	PR_ASK	2000	12500	23000	2100	Dense	false
30	64/3	32000	8	PR_ASK	1500	25000	25000	0	Dense	false
31	64/3	32000	8	PR_ASK	1500	12500	23000	2100	Dense	false
32	64/3	32000	8	PR_ASK	2000	25000	25000	0	Dense	false
33	64/3	32000	8	PR_ASK	2000	12500	23000	2100	Dense	false
34	64/3	40000	8	PR_ASK	1500	12500	18800	2100	Dense	false
35	64/3	40000	8	PR_ASK	2000	12500	18800	2100	Dense	false
36 [ ]	64/3	120000	4	PR_ASK	1500	10400	10400	0	Dense	false

*RF Mode 23 is the automac air link profile which is also the default.

**Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.

Empty bracket [ ] indicates that this RF mode is not supported in FX7500; A number in the bracket indicates the RF Mode for the FX7500; No bracket indicates RF mode supported by both FX9600 and FX7500.

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 Conform-ance
37 [36]	64/3	120000	4	PR_ASK	2000	10400	10400	0	Dense	false
38 [ ]	64/3	160000	4	PR_ASK	1500	6250	10400	4150	Dense	false
[37]	64/3	160000	4	PR_ASK	2000	6250	6250	0	Dense	false
39 [38]	64/3	668	1	PR_ASK	668	668	668	0	Dense	false

*RF Mode 23 is the automac air link profile which is also the default.

**Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.

Empty bracket [ ] indicates that this RF mode is not supported in FX7500; A number in the bracket indicates the RF Mode for the FX7500; No bracket indicates RF mode supported by both FX9600 and FX7500.

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 Indica-tor**	EPC HAG T&C Conform-ance
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

*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 Indica-tor**	EPC HAG T&C Conform-ance
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	30000	8	PR_ASK	1500	25000	25000	0	Dense	false
23	64/3	30000	8	PR_ASK	1500	12500	23000	2100	Dense	false
24	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
25	64/3	30000	8	PR_ASK	2000	12500	23000	2100	Dense	false
26	64/3	32000	8	PR_ASK	1500	25000	25000	0	Dense	false
27	64/3	32000	8	PR_ASK	1500	12500	23000	2100	Dense	false
28	64/3	32000	8	PR_ASK	2000	25000	25000	0	Dense	false
29	64/3	32000	8	PR_ASK	2000	12500	23000	2100	Dense	false
30	64/3	40000	8	PR_ASK	1500	12500	18800	2100	Dense	false
31	64/3	40000	8	PR_ASK	2000	12500	18800	2100	Dense	false
32	64/3	668	1	PR_ASK	668	668	668	0	Dense	false
33	64/3	32000	1	PR_ASK	1500	12500	18800	2100	Dense	false
34	64/3	32000	1	PR_ASK	2000	12500	18800	2100	Dense	false
35	64/3	12000	4	PR_ASK	1500	10400	10400	0	Dense	false
36	64/3	12000	4	PR_ASK	2000	10400	10400	0	Dense	false
37	64/3	32000	2	PR_ASK	1500	10400	10400	0	Dense	false
38	64/3	16000	4	PR_ASK	1500	10400	10400	0	Dense	false

*RF Mode 21 is the automac air link profile which is also the default.

**Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.

Table 21 Radio Modes for Japan 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 Conform-ance
1 [1]	64/3	120000	2	PR_ASK	2000	25000	25000	0	Dense	false
2	64/3	120000	2	PR_ASK	2000	12500	23000	2100	Dense	false
3 [2]	64/3	128000	2	PR_ASK	2000	25000	25000	0	Dense	false
4	64/3	128000	2	PR_ASK	2000	12500	23000	2100	Dense	false
5	64/3	160000	2	PR_ASK	2000	12500	18800	2100	Dense	false
6 [3]	64/3	60000	4	PR_ASK	2000	25000	25000	0	Dense	false
7	64/3	60000	4	PR_ASK	2000	12500	23000	2100	Dense	false
8 [4]	64/3	64000	4	PR_ASK	2000	25000	25000	0	Dense	false
9	64/3	64000	4	PR_ASK	2000	12500	23000	2100	Dense	false
10	64/3	80000	4	PR_ASK	2000	12500	18800	2100	Dense	false
11	64/3	320000	1	PR_ASK	2000	12500	18800	2100	Dense	false
12 [5]	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
13	64/3	30000	8	PR_ASK	2000	12500	23000	2100	Dense	false
14 [6]	64/3	32000	8	PR_ASK	2000	25000	25000	0	Dense	false
15	64/3	32000	8	PR_ASK	2000	12500	23000	2100	Dense	false
16	64/3	40000	8	PR_ASK	2000	12500	18800	2100	Dense	false

**Spectral mask indicator may vary for certain Tari values. Detailed information is available upon request.

Empty bracket [ ] indicates that this RF mode is not supported in FX7500; A number in the bracket indicates the RF Mode for the FX7500; No bracket indicates RF mode supported by both FX9600 and FX7500.

Copying Files To and From the Reader

Introduction

The FX7500 and FX9600 RFID readers support the SCP protocols for copying files.

SCP

The following examples illustrate SCP use:

scp SourceFileName rfidadm@MyReaderIP:/apps

scp rfidadm@MyReaderIP:/apps/SourceFileName userid@MyLinuxMachineIP:/MyFolderName

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 the 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 is 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 Dense Reader Mode (DRM) 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.

Security Recommendations

Introduction

This chapter covers general security guidelines to undertake while using the FX Series RFID readers.

Enable Strong Password for User Authentication

The reader enforces secure HTTP connections and changes the default password on the first login. It is recommended that a strong password be used for 'admin' account. The password must meet the following criteria:

- Should contain a minimum of 8 and a maximum of 32characters.
- English uppercase characters (A through Z).
- English lowercase characters (a through z).
- Base 10 digits (0 through 9).
- Non-alphabetic characters (for example, !, $, #, %).
- Should not use previously used five passwords.

The 'rfidadm' account on the reader has an empty password by default. It is highly recommended that a strong password be set for this account before deployment of readers.

Reader does not enforce password rotation. But rotation of all passwords is recommended by reader administrator on a periodic basis, e.g. once in 30 days.

User Login and Password

There are three user roles: admin, guest, and rfidadm. It is highly recommended to set passwords for all users.

1. The guest user cannot log in until a password is set by the admin.
2. By default, SSH is disabled. To enable SSH, the rfidadm user must have a password set with a minimum length of 16 and a maximum of 32 characters.
3. All passwords must meet the strong password criteria specified in “Enable Strong Password for User Authentication.”

Configure Required Reader Services in Secure Mode

Network services on the reader have secure mode options, which may not be enabled by default. It is highly recommended that all required services be enabled with secure mode. For example, choose HTTPs for web server instead of HTTP over unencrypted FTP etc.

If any service is not required, for example, ssh shell access to the reader, it may be turned off. Refer Network Services Settings section for details on reader services and configurations.

Update Default Self-Signed Certificate

Readers by default initialize with self-signed certificates. It is highly recommended that the reader self-signed certificate be updated with a trusted CA assigned certificate. Refer Certificate Configuration section for details.

Secure IoT Connector Interface

It is highly recommended endpoints to which reader connection for IoT use case by secured with trusted certificates and mutual TLS authentication be enabled for such connections.

Refer to the Certificate Configuration section in this reader integration guide for details on importing reader certificates and trusted CA certificates to the reader.

Note that reader allows two ways to import trusted CA certificates in X509 format to the reader:

- The CA certificate can be bundled with the PKCS#12 format .pfx file that includes the reader's private key.
- CA certificates can be imported to the reader's trusted certificate store using addCAcert RM command. See addCAcert, deleteCAcert and listCAcerts command documentation in FX Series Reader Interface Control Guide.

Refer to the certificate configuration section in Zebra IoT connector documentation zebradevs.github.io/rfid-ziotc-docs for details on how certificates can be set on the reader for endpoint connection security.

An alternate, but less preferred option for securing IoT interface is to use 'Basic Authentication' that requires username and password for endpoint connection authentication. Refer 'Device Setup' section in the Zebra IoT connector documentation for details.

Enable TLS Security for LLRP

For data protection over LLRP mode, reader supports secure LLRP connections. It is recommended secure LLRP be used to authorize and encrypt client to reader LLRP channel. TCP port 5085 is used for this purpose. Certificate based authentication is used and it requires the reader be updated with trusted CA assigned server certificates. Refer to the Certificate Configuration and Configure LLRP Settings sections for more information.

Monitor Reader Certificate Expiry and Update Certificates Before Expiry

Refer to the Certificate Configuration section for different types of reader certificates and how these certificates can be updated.

Certificates have an expiration date. It is highly recommended that administrators keep track of expiration date for certificates issued to the reader and update the certificates before they expire. If certificates expire, the connection attempt to remote endpoints can fail. Refer to the 'viewCurrentCertificateDetails' RM command that can be used to programmatically check for current installed certificate details including its expiry.

Update Custom Trusted CA Certificates to Reader Trusted Certificate Store

Reader has a trusted CA certificate store that may be updated with custom CA certificates. Such CA certificates can be used by the reader to trust remote endpoints before connecting to those endpoints, provided those endpoints are issued certificates by same CA.

Reader currently supports only RM commands for managing such CA certificates. Refer to the addCAcert, deleteCAcert, and listCAcerts RM command documentation in the FX Series Reader Interface Control Guide for details.

Enable FIP 140-2 Mode

FX series readers support reader services in secure mode to use only FIPS 140-2 compliant algorithms. Refer to the FIPS Support section in this integrator guide for details on how to configure FIPS 140-2 mode. Note that as of 3.20.x release, FIPS 140-2 mode is supported for HTTPS and LLRP services. FIPS 140-2 mode is not supported for IoT connector interfaces.

Enable Port-Based Network Access Control

Reader supports 802.1x EAP over ethernet. If deployment supports 802.1x EAP, it is highly recommended to enable it. Refer to the 802.1x EAP Configuration section for details.

Disable Serial Port

On FX9600 and ATR7000 the external serial port and serial-to-USB port respectively are recommended to be turned off if applications or deployment do not require access to the serial port. Refer to the FX9600 Serial Port Configuration section for details on port usage and how it can be set to disabled mode.

Index

Numerics

A

B

C

R

S

T

U

V

W

Z