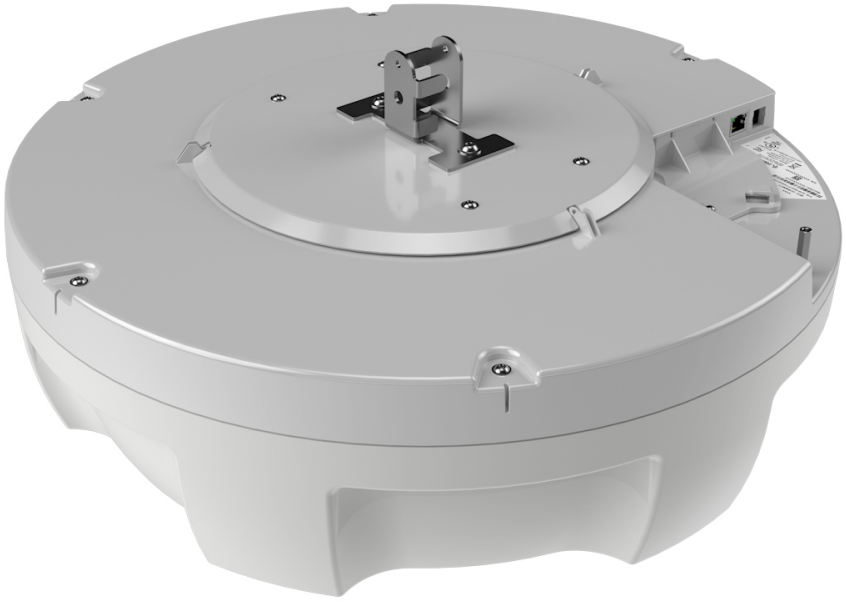
ATR7000

Advanced Array RFID Reader



Integration Guide

ZEBRA

MN-003191-05EN

Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2025 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/informationpolicy
COPYRIGHTS: zebra.com/copyright
PATENTS: ip.zebra.com
WARRANTY: zebra.com/warranty
END USER LICENSE AGREEMENT: zebra.com/eula

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 guide are listed below:

Change	Date	Description
-05 Rev A	12/2025	New sections: - Compliance and Implications of EU RED for the ATR7000 section. Updates: - Revised Reader Administration Console First-Time/Start-Up procedures - Updates to User Login and Password in Security Recommendations. - Administrator Console updates including: - Screenshots - Content relating to IPv4, IPv6, LLRP settings, SNMP settings, Network Services settings, ATR7000 User Accounts - New topics including 802.1x EAP Configuration, 802.1 EAP Configuration/ Testing with FreeRADIUS, Cisco Switch Configuration, and FX Reader 802.1 EAP Authentication - Removed sections: Reading Tags through Administrator Console, Commit/ Discard (and related content), FTP
-04 Rev A	11/2024	Updates: - Added SSH Key Management in the Administrator Console section. - Added SCP-based update in the Firmware Upgrade section. - Added Security Recommendations.
-03 Rev A	3/2020	Updates: - Note about points to follow when powering the ATR7000 in the Ethernet: Power through PoE+ (802.3at) section. - PowerSession - Select Reader and Read Tags screens in the Reading Tags section. -Reader Parameters Window screen to show the current reader default setting, and the Power Negotiation bullet point in the Reader Parameters section.
-02 Rev A	4/2019	Updates: - Reserved Polarization added to Beam Configuration Table
-01 Rev A	9/2018	Initial Release

Table of Contents

Copyright 2
Terms of Use 2
Proprietary Statement 2
Product Improvements 2
Liability Disclaimer 2
Limitation of Liability 2
Revision History 3

About This Guide
Introduction 6
Chapter Descriptions 6
Notational Conventions 7
Related Documents 7
Service Information 7

Quick Start
Introduction 9
Quick Start Demonstration 9
Step 1, Setup 9
Step 2, Connecting to the Reader 10
Step 3, First Time / Start-Up Login 11
Step 4, Set Region 14
Step 5, Read Tags 16

Getting Started
Introduction 17
Features 17
ATR7000 Parts 18
ATR7000 Side Panel 18
ATR7000 Side Panel Components 19
ATR7000 LED 20

Installation and Communication
Introduction 22

Unpacking the Reader 22
Installing the ATR7000 in an Open Ceiling 23
Required Equipment 23
Additional Equipment (Not Included, Dependent on Installation Requirements) 23
Tools Required 23
Installation Options 23
Installing Directly on the Truss 24
Installing Using a Strut Channel Clamped to the Bottom of the Truss 25
Installing Using a Strut Channel and Threaded Rods Clamped to the Top of the Truss 26
Mounting the ATR7000 27
VESA Mounting 29
Communications and Power Connections 30
Ethernet Connection 30
Ethernet: Power through AC Outlet 30
Ethernet: Power through PoE+ (802.3at) 31
USB Connection 31
GPIO Interface Connection 31
LED Sequences 33
System Start-up/Boot LED Sequence 33
Reset to Factory Defaults LED Sequence 33
LED Sequence for Software Update Status 33

ATR Beam Configuration
Introduction 34
Reference Coordinate System for ATR7000 34
ATR Beam Configuration 37

Administrator Console
Introduction 38
Profiles 39
Resetting the Reader 39
Auto Discovery 39
Connecting to the Reader 40
Obtaining the IP Address via Command Prompt 40
Connecting via Host Name 41
Connecting via IP Address 41
Using Zero-Configuration Networking when DHCP Server is Not Available 42
Administrator Console Login 42
First Time / Start-Up Login 42
Logging In with Default User ID and Password 42
Setting the Region 43
Administrator Console Option Selections 45
Status 46
Reader Statistics 47
Reader Gen2 Optional Operation Statistics 48
NXP Custom Command Operation Statistics 49
Event Statistics 50
NTP Statistics 51
Configure Reader 52

Reader Parameters 52
Configure Region 53
Certificates 54
Certificate Configuration 54
Creating a Custom Certificate 56
Script Usage 66
SSH Key Management 66
Generating a New SSH Key Pair 66
Importing SSH Keys 66
Adding SSH Key to a Remote Server 67
Read Tags 68
Communication Settings 69
Configure Network Settings with Ethernet 69
IPV4 69
IPV6 70
Configure LLRP Settings 70
SNMP Settings 72
Network Services Settings 73
802.1x EAP Configuration 74
802.1x EAP Configuration/Testing with FreeRADIUS 75
RADIUS Server (FreeRADIUS) Configuration 75
Cisco Switch (Cisco C1000-24FP-4G-L) Configuration 76
FX Reader 802.1 EAP authentication testing with RADIUS server (FreeRADIUS) 77
System Time Management 79
IPV6 IP Sec 80
Change Password 81
ATR7000 User Accounts 81
Managing User Login and Logout 82
GPIO 82
Reader Profiles 84
FIPS Support 85
Firmware Version/Update 85
System Log 87
Configure System Log 88
Reader Diagnostics 89
Shutdown 89

Application Development

Introduction 91
Reference Guides 91

Compliance and Implications of EU RED for the ATR7000

Introduction 92
About BS EN 18031-1 & The EU Radio Equipment Directive (RED) 92
Applicability of BS EN 18031-1 for the ATR7000 92
Security is Based on "Environmental Controls" 92
How Compliance is Justified 92
Applicability of BS EN 18031-1 93
Default Authorization Password & Update 93

LLRP Settings 93
SSH Settings 93
SNMP Settings 93
Annexure 1 94

Troubleshooting
Troubleshooting 96

Firmware Upgrade
Introduction 101
Prerequisites 101
Failsafe Update 102
Update Phases 102
Updating ATR7000 Reader Software 103
Verifying Firmware Version 103
Updating Methods 104
File-Based Update 104
FTP/SCP-Based Update 105
Verifying Firmware Version 106

Technical Specifications
Technical Specifications 108
Cable Pinouts 110
10/100bT Ethernet / PoE Connector 110
USB Debug Connector 110
USB Host Connector 111
GPIO Port Connections 111

Static IP Configuration
Introduction 114
Reader IP Address or Host Name is Known 114
Reader IP is Not Known (DHCP Network Not Available) 116

RF Air Link Configuration
Introduction 118
Radio Modes 118

Copying Files To and From the Reader
Introduction 120
SCP 120

Data Protection
Introduction 121

Security Recommendations
Introduction 122
Enable Strong Password for User Authentication 122
User Login and Password 122
Configure Required Reader Services in Secure Mode 123
Update Default Self-Signed Certificate 123
Secure IoT Connector Interface 123
Enable TLS Security for LLRP 123
Monitor Reader Certificate Expiry and Update Certificates Before Expiry 123
Update Custom Trusted CA Certificates to Reader Trusted Certificate Store 124
Enable FIP 140-2 Mode 124
Enable Port-Based Network Access Control 124
Disable Serial Port 124

About This Guide

Introduction

This Integration Guide provides information about installing, configuring, and using the ATR7000 Advanced Array RFID Reader and is intended for use by professional installers and system integrators. The ATR7000 reader is part of Zebra's FX series fixed reader platform and provides real time, seamless tag processing for EPC Class1 Gen2 compliant tags.

The ATR7000 reader fulfills the RFID fixed reader infrastructure component of Zebra's Advanced Asset Tracking Solution (ZAATS) to provide continuous identification, location, and tracking of tagged items.



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 ATR7000 RFID fixed reader features, parts, and LED indications.
- Installation and Communication provides information on installing and setting up the ATR7000 reader.
- ATR Beam Configuration provides information so the user can control the beams in a pre-determined way and includes reference coordinate system information for ATR7000, beam configuration, and information about reading tags.
- Administrator Console describes how to connect to the reader and how to use the web-based Administrator Console to configure and manage the ATR7000 reader.
- Application Development provides information on developing applications for the ATR7000, and includes references to the appropriate guides.
- Firmware Upgrade provides reader firmware upgrade information on using the web-based Administrator Console and an FTP or FTPS server running a host computer.
- Troubleshooting describes ATR7000 reader troubleshooting procedures.
- Technical Specifications includes the technical specifications for the reader.
- Static IP Configuration describes three methods of setting the static IP address on an ATR7000 RFID reader.

- RF Air Link Configuration describes how to select air link configuration from a set of available air link profiles.
- Copying Files To and From the Reader describes the SCP, FTP, and FTPS protocols for copying files.
- Data Protection describes how the ATR7000 protects RFID data in transition.

Notational Conventions

The following conventions are used in this document:

- “RFID reader”, “RFID fixed reader”, or “reader” refers to the Zebra ATR7000 RFID reader.
- Bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Related Documents

The following documents provide more information about the reader.

- ATR7000 Advanced Array RFID Reader Quick Reference Guide (p/n MN-003193-xx).
- RFID Demo Applications User Guide (p/n 72E-160038-xx). Provides instructions for using sample applications such as PowerSession.
- RFID Reader Software Interface Control Guide (p/n 72E-131718-xx). Describes Low Level Reader Protocol (LLRP) and Reader Management (RM) extensions for the reader.
- FX Series Embedded SDK Installation Guide. Provides instructions for installing the embedded SDK for C and Java.
- FX Series Embedded SDK Sample Application Guide. Explains how to use the embedded sample application with an integrated development environment.
- FX Series Embedded SDK Programmers Guide. Provides instructions for creating embedded applications.
- RFID3 API
- EPCglobal Low Level Reader Protocol (LLRP) Standard

For the latest version of these guides and software, go to www.zebra.com/support.

Service Information

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

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

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

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

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

Quick Start

Introduction

This chapter provides a Quick Start setup demonstration.

Quick Start Demonstration

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

- Step 1, Setup on page 9
- Step 2, Connecting to the Reader on page 10
- Step 3, First Time / Start-Up Login on page 11
- Step 4, Set Region on page 14
- Step 5, Read Tags on page 16

Step 1, Setup

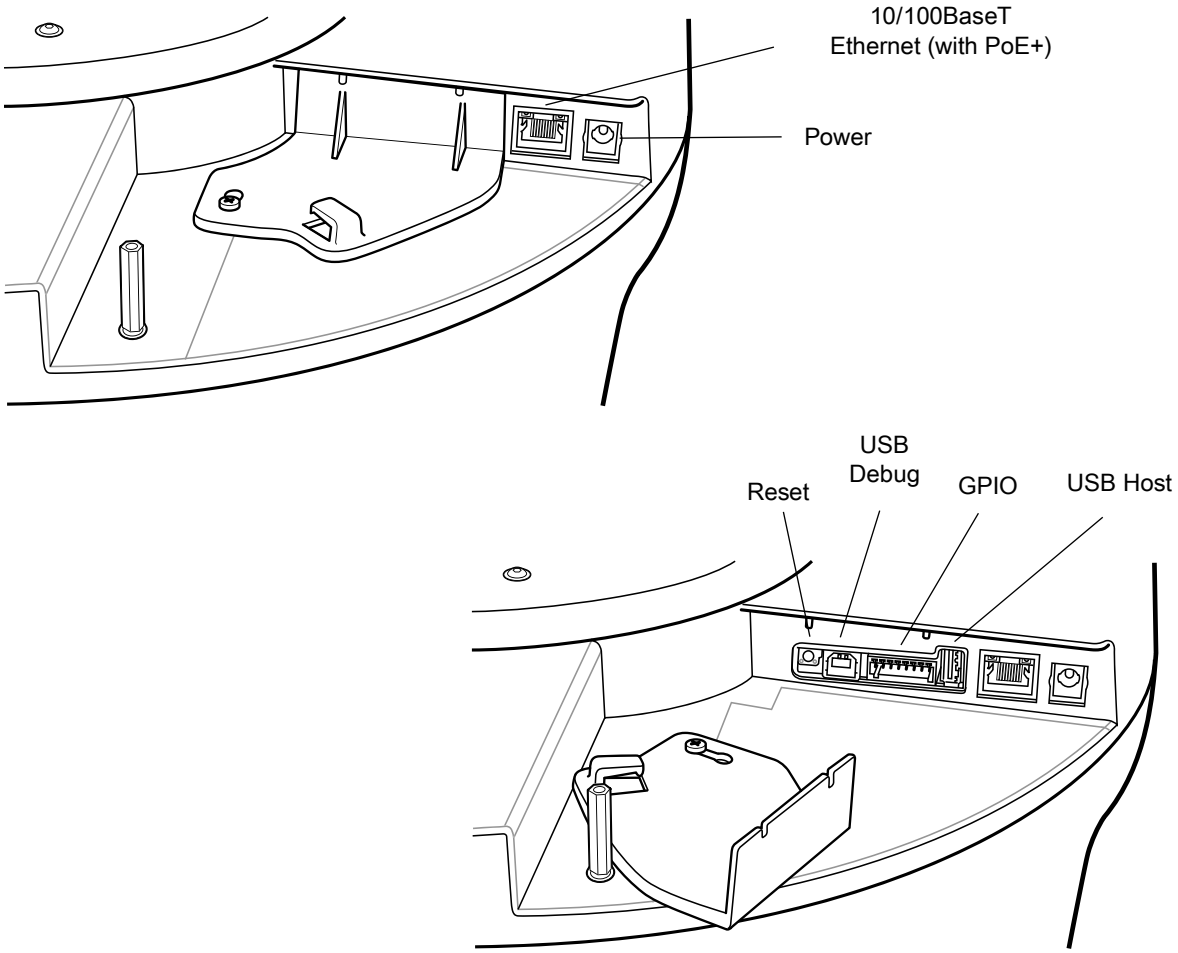
For information on complete component kits available from Zebra, see Technical Specifications.

1. Unpack the reader. See Unpacking the Reader on page 22.
2. Place the reader on a desktop.
3. Connect the Ethernet cable to the Ethernet port. See Figure 1.

NOTE: The factory default for the reader is DHCP enabled. 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.

4. 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+, plug the Ethernet cable into the PoE+ injector.
5. Wait for the green power LED to stay lit, boot up time is approximately 60 seconds. See System Start-up/Boot LED Sequence on page 33 for additional boot-up details.

Figure 1 ATR7000 RFID Fixed Reader Side Panel Connections



Step 2, Connecting to the Reader

To connect via host name:

1. Open a browser. The minimum browser recommendations are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54**.**
2. Enter the host name followed by the last three octets of the MAC, provided on a label on the reader, in the browser (For example, for an ATR7000 MAC address of 0023683BA63A, use the prefix ATR7000, followed by 3BA63A. Enter http://ATR70003BA63A in the browser address bar) and press **Enter**. The **User Login** window appears and the reader is ready.

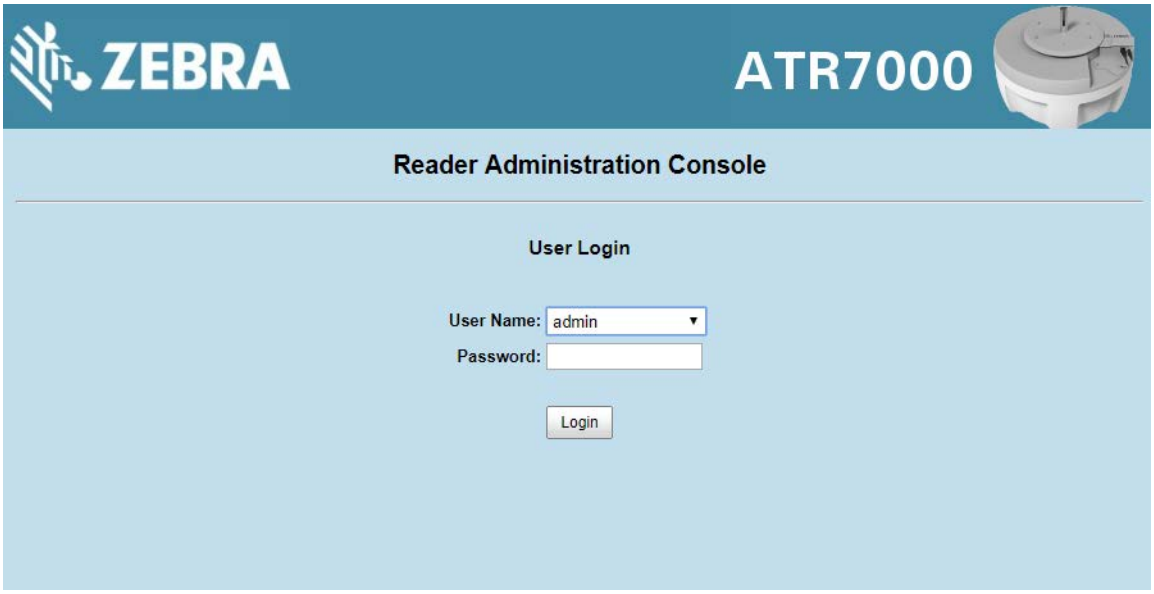
NOTE: Connect the reader to a network that supports host name registration and lookup to ensure the network can access the reader using the host name. For instance, some networks can register host names through DHCP. When first connecting to the reader, it is recommended to keep DHCP enabled in both the PC and in the reader, although it is not guaranteed that host name will work all the time. Use the host name printed on the reader label, or construct it using the reader MAC address on the bottom of the reader.

Step 3, First Time / Start-Up Login

When starting the reader for the first time:

1. In the **User Login** window, select **admin** from the **User Name** drop-down menu, and then type **change** into the **Password** field. Click **Login** to continue.

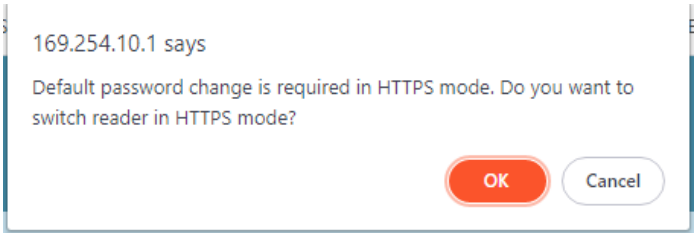
Figure 2 User Login Window



NOTE: If you forget the user ID and/or password, see Reset to Factory Defaults LED Sequence on page 33 to reset the reader to factory defaults, and then select **admin** for the user name and enter **change** in the password field to regain access.

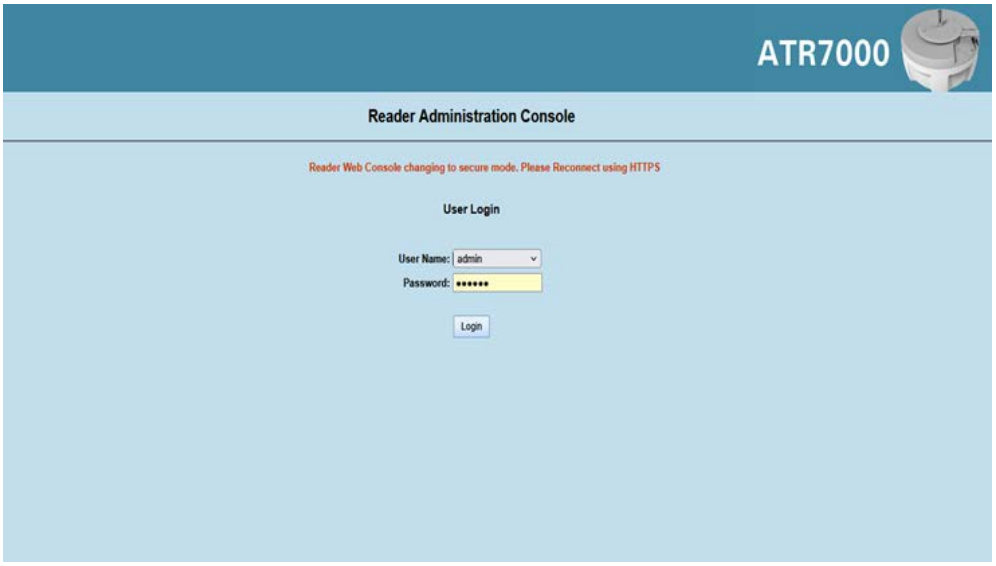
2. A dialog appears indicating the reader login is performed using the default password and the reader must switch to HTTPS mode to allow the users to change the password. Click **OK**.

Figure 3 Switch Reader to HTTPS Mode Prompt



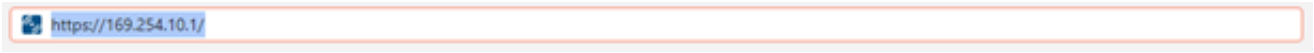
3. The reader switches to HTTPS mode and displays a message asking the user to log in again using HTTPS mode.

Figure 4 User Login Window Using HTTPS



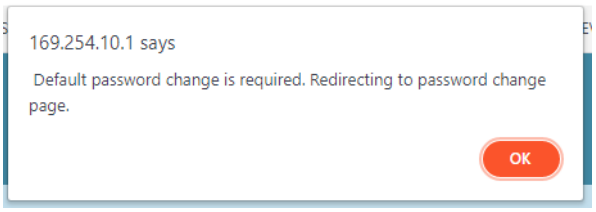
4. Change the URL in the browser address box to use HTTPS instead of HTTP, and press **Enter**. Since the reader starts up with a self-signed certificate, the browser might issue a warning about it not being able to verify the certificate. Accept any risks and continue.

Figure 5 Changing the Address Box URL



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

Figure 6 Redirecting to Password Change Prompt

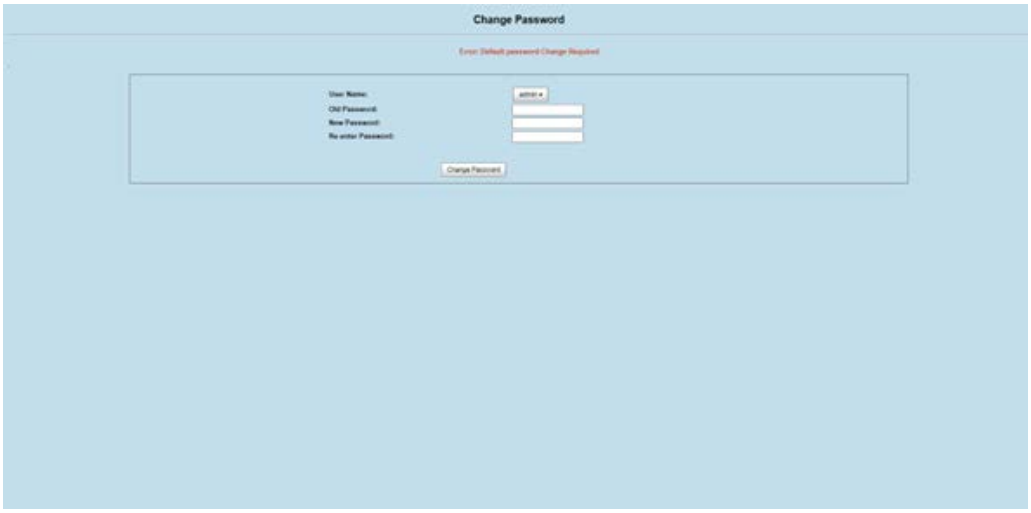


6. A Change Password page appears. Enter the Old Password as change and enter the New Password. Re-enter the new password to confirm.

   Enter your password that should satisfy the following criteria:

   - Should contain a minimum of 8 and a 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.

Figure 7 Default Password Change Required



NOTE: The Region Configuration window does not appear for US reader configurations. For these models, the Administrator Console main window appears. See Figure 28 on page 39.

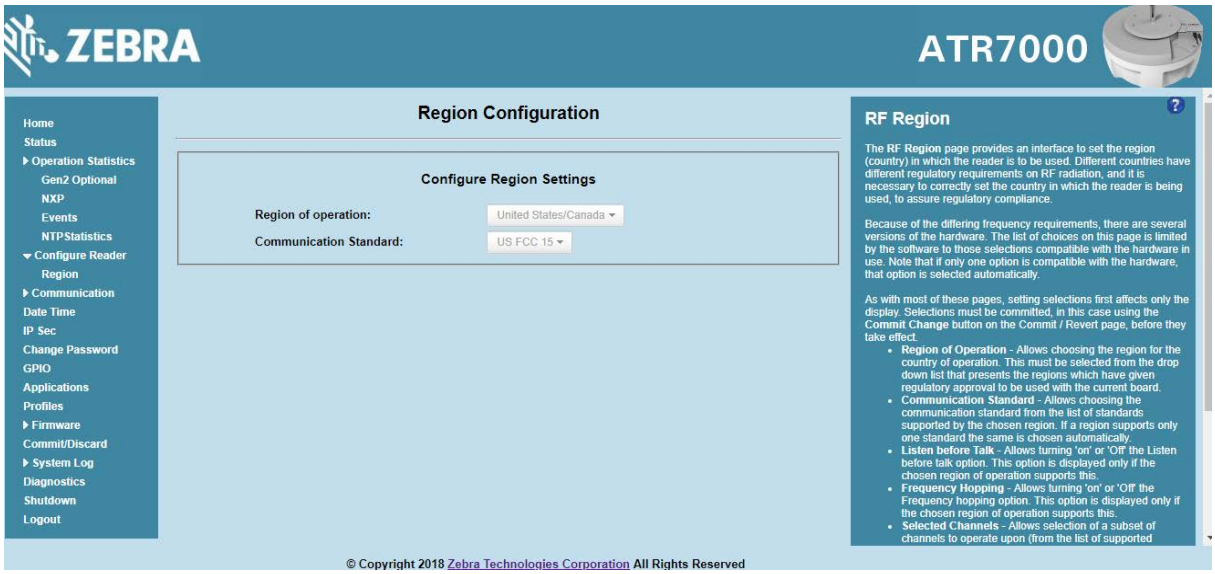
Step 4, Set Region

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

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

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

Figure 8 Selecting the Region



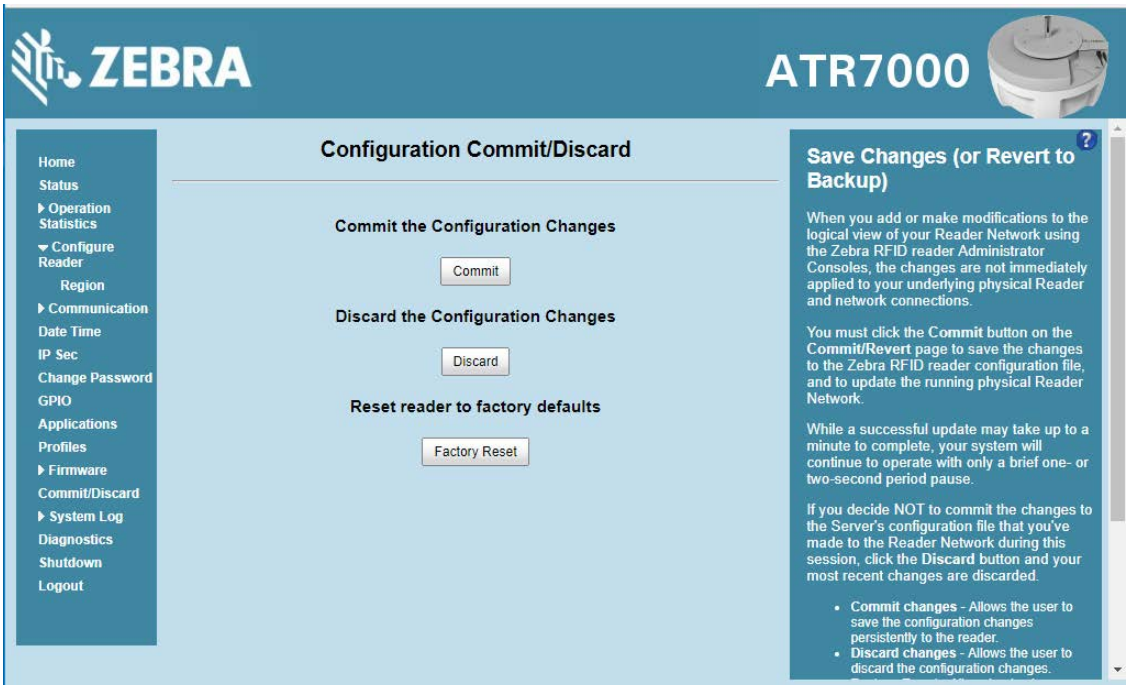
2. Select the **Communication Standard**, if applicable.
3. Select **Frequency Hopping**, if applicable.
4. Select the appropriate channel(s), if applicable.
5. Select the **I understand** check box.
6. Select **Set Properties** to complete the region selection. The **Operation Successful** window appears.

Figure 9 Region Configuration, Operation Successful Window



7. Select **Commit/Discard**.

Figure 10 Commit/Discard Window

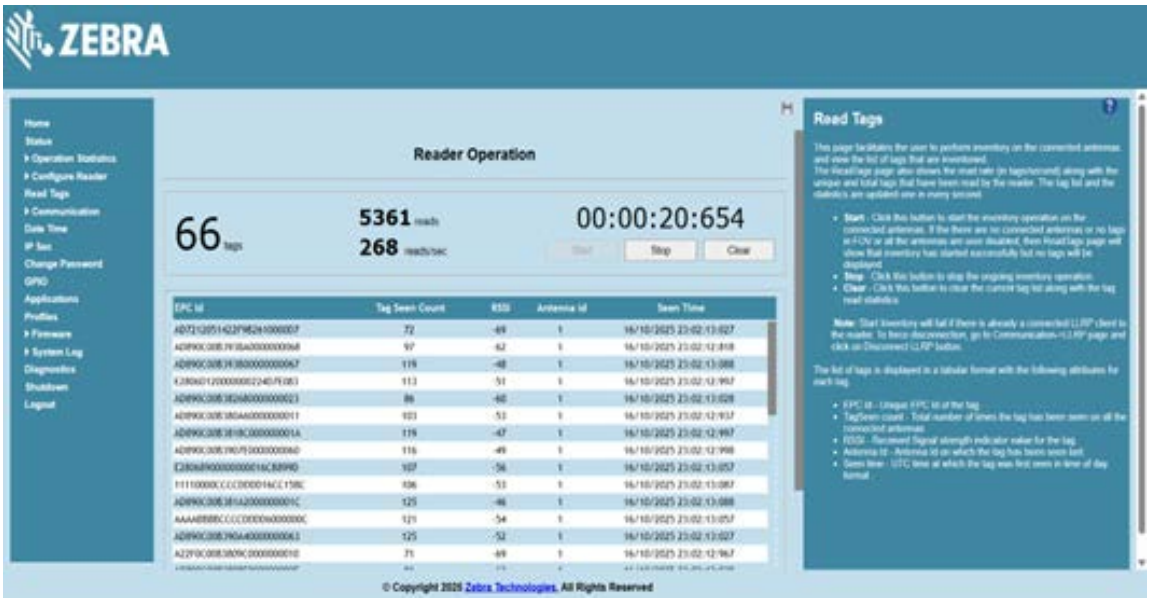


8. Click **Commit** to save the new region configuration and apply these changes to the reader configuration file, or click **Discard** to discard the region configuration changes. When the commit completes, the **Commit Successful** window appears.

Step 5, Read Tags

Select Read Tags on the navigation panel to the left to view the Reader Operation window.

Figure 11 Read Tags Window



- **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 ATR7000 RFID fixed reader features, parts, and LED indications.

Features

The ATR7000 RFID reader is based on Zebra's FX Series fixed reader platform and is 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 ATR7000 RFID reader provides a wide range of features that enable implementation of complete, high-performance, intelligent RFID solutions.

Table 1 ATR7000 RFID Reader Features

Feature	Zebra ATR7000
Air Protocol	ISO 18000-63 (EPC Class 1 Gen2 V2)
Operating System	Linux
Operating Temperature	-20° to +55° C
Antenna Elements	14 (internal)
Power Supply	+24V DC, POE+
API	RFID3
GPIO	2 Input, 3 Output
Maximum RF Output Power	+36 dBm EIRP
RX Sensitivity	-85 dBm
IP Sealing	IP51
Power-Over-Ethernet	802.3at
Embedded Applications	Yes
Wi-Fi/Bluetooth Dongle Support	Future

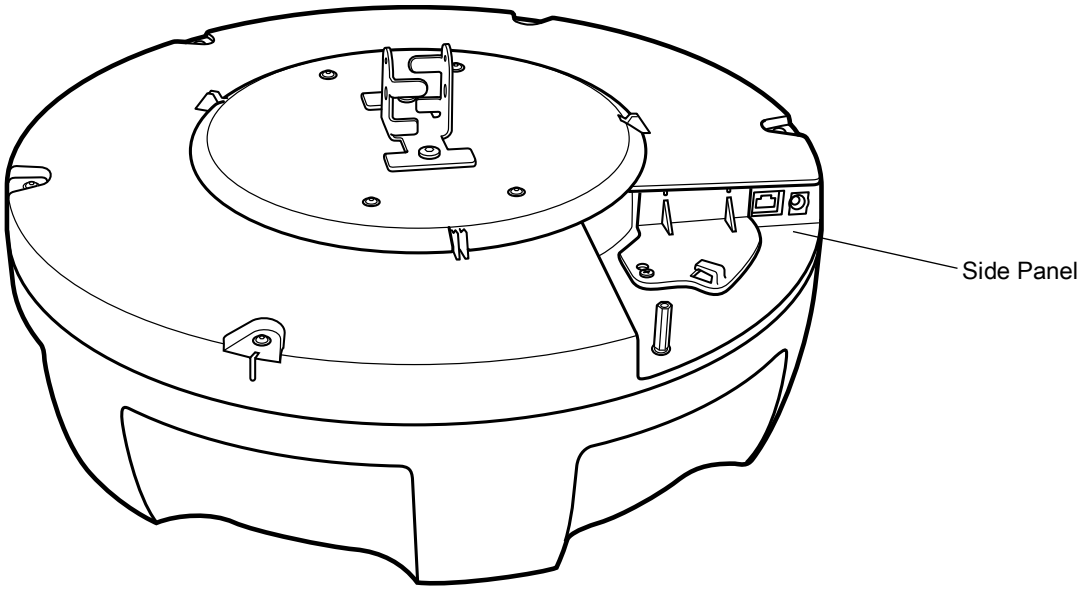
Table 1 ATR7000 RFID Reader Features

Feature	Zebra ATR7000
SDKs	
Embedded Applications: Host Based Applications:	C, Java C, Java, Net

ATR7000 Parts

ATR7000 Side Panel

Figure 12 ATR7000 RFID Reader



CAUTION: Use only parts provided with the ATR7000 RFID reader, or Zebra approved/recommended parts. Substituting other cables or parts can degrade system performance, damage the reader, and/or void the warranty.

ATR7000 Side Panel Components

Figure 13 ATR7000 RFID Reader Side Panel Connections

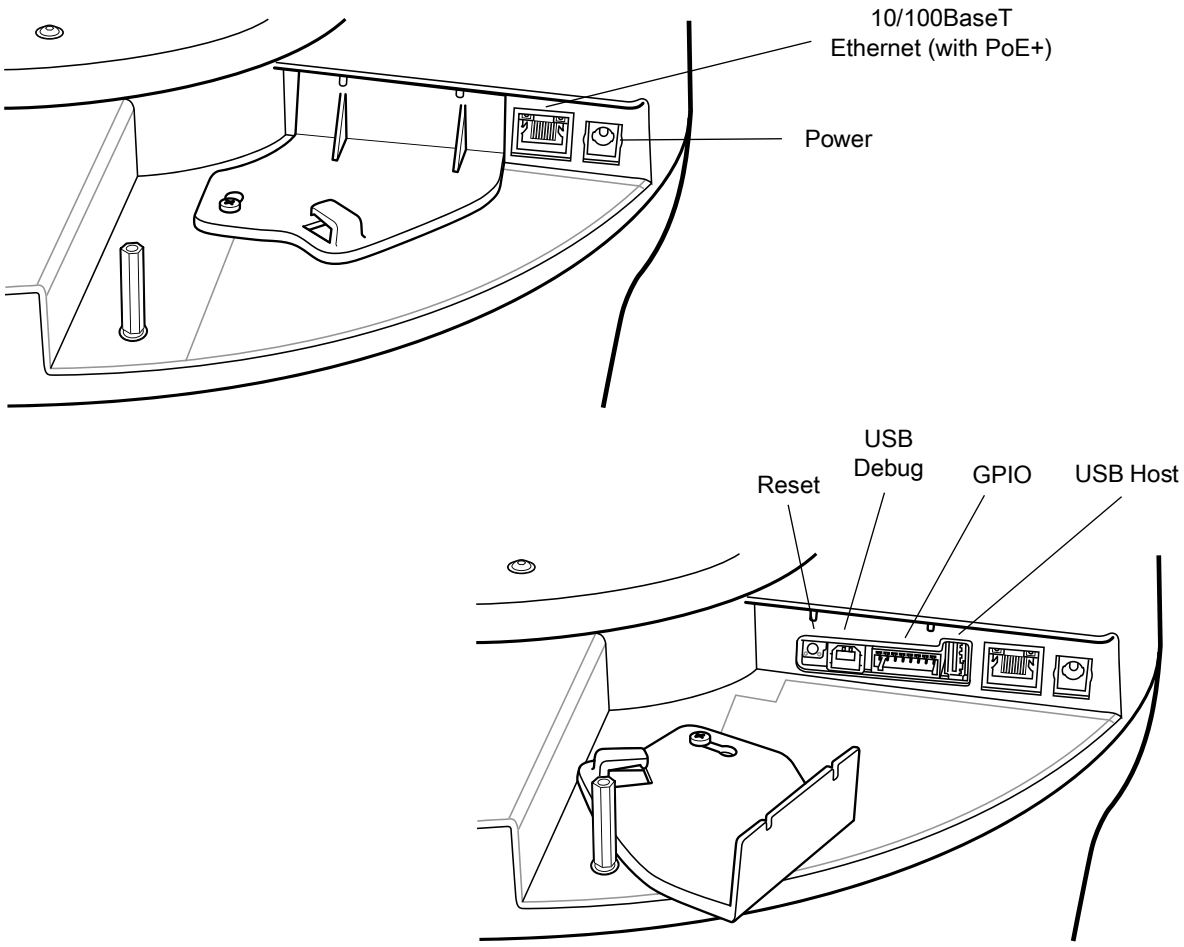


Table 2 Side Panel Descriptions

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 30 for connection information.
Power	DC connector connects to a Zebra approved, certified LPS rated power supply. Rated 24 VDC, 3.25 A min., 55 deg. C.
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 31 for more information.
USB Debug	USB debug port is for log purposes and only for use by technicians.
USB Host	The USB host port is reserved for future use.

ATR7000 LED

The reader LED indicates reader status as described in Table 3. For the LED boot up sequence see System Start-up/Boot LED Sequence on page 33.

Figure 14 ATR7000 RFID Reader LED

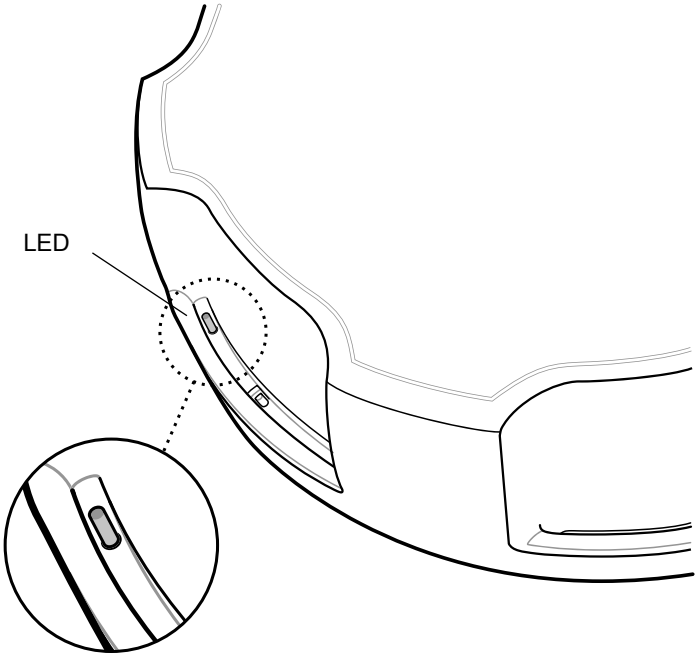


Table 3 ATR7000 LED Indications

Color/Status	Description	Transition Time
Off	Reader is powered off	
Solid Red, then Solid Amber	Power applied to reader and reader booting	Transition from Off to Solid Red happens in around a second. Transition from Solid Red to Amber happens in a second, then remains in Amber state for around 40 seconds.
Slow Blinking Green	Sub-components and application initializing	Reader typically remains in this state for 10 seconds, but can be up to 70 seconds if sub-components need software update, which usually happens on first bootup of the reader after deployment or first bootup as part of a reader software upgrade.
Solid Green	Applications up and ready for operation	
Fast Blinking Green	Continuous reading (inventory) of tags	
Fast Blinking Green with Intermittent Amber/Red	Reader operations on tags with intermittent errors	

Color/Status	Description	Transition Time
Solid Amber	Ethernet cable not connected	State changes to solid green if Ethernet link is restored
Repeated Blinking Red Followed By Blinking Green	Antenna port is faulty	
Solid Red	Hard Error	

Installation and Communication

Introduction

CAUTION: The ATR7000 RFID reader must be professionally installed.

This chapter includes the following ATR7000 RFID reader installation and communication procedures:

- Unpacking the Reader on page 22
- Installing the ATR7000 in an Open Ceiling on page 23
  - Installation Options on page 23
  - Mounting the ATR7000 on page 27
- Communications and Power Connections on page 30
  - Ethernet Connection on page 30
  - USB Connection on page 31
  - GPIO Interface Connection on page 31
- System Start-up/Boot LED Sequence on page 33

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.

Installing the ATR7000 in an Open Ceiling

WARNING: Do not install the ATR7000 in an Environmental Air Handling Space (EAHS).

Depending on the site truss configuration, the ATR7000 can be mounted directly to the truss, or to a strut channel secured to the trusses.

Required Equipment

- ATR7000 reader
- Telescoping pole mounting kit (multiple length ranges available).

NOTE: Mounting pole must be UL certified model rated to support 12 lb min. load.

Additional Equipment (Not Included, Dependent on Installation Requirements)

- SK5500-SR0 adapter kit, includes VESA bracket, nest, hand mount, and mounting screws

Tools Required

- Level
- Laser length measuring device
- Lift platform
- Set of wrenches and screw drivers
- Beam clamps (varied based on I-beam types)
- Miscellaneous: gloves, ties, extra hardware as needed.

Installation Options

The ATR7000 reader is designed to be installed overhead at a typical height (off the floor) between 12’ and 18’. Select one of the following three options for mounting the ATR7000 that best suits the installation environment:

- Installing Directly on the Truss on page 24
- Installing Using a Strut Channel Clamped to the Bottom of the Truss on page 25
- Installing Using a Strut Channel and Threaded Rods Clamped to the Top of the Truss on page 26

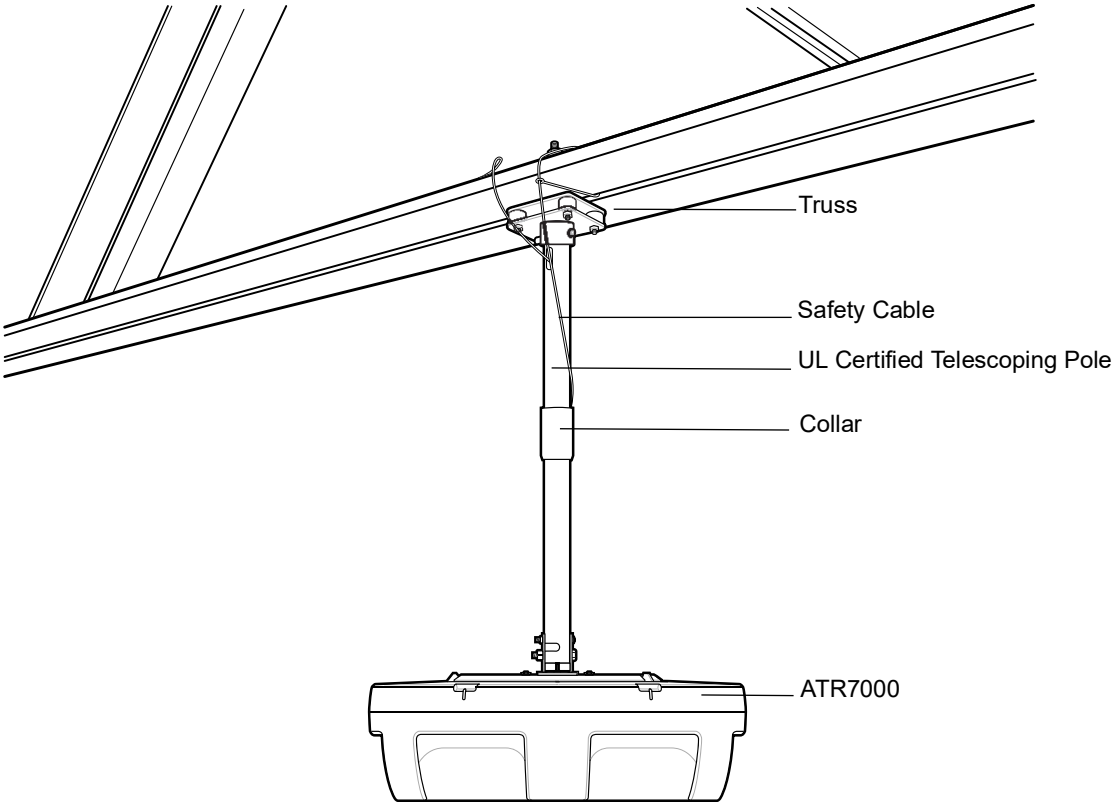
After selecting the installation configuration, proceed to Mounting the ATR7000 on page 27.

Installing Directly on the Truss

For locations with high ceilings where the bottom of the trusses are at least 14 ft from the floor, ATR7000 devices can be mounted directly to the truss using UL certified mounting pole (not included).

NOTE: Refer to the site survey report for the proper mounting height of each ATR7000. In general, this is 12 ft from the bottom of the device to the floor.

Figure 15 Installing the ATR7000 Directly on the Truss

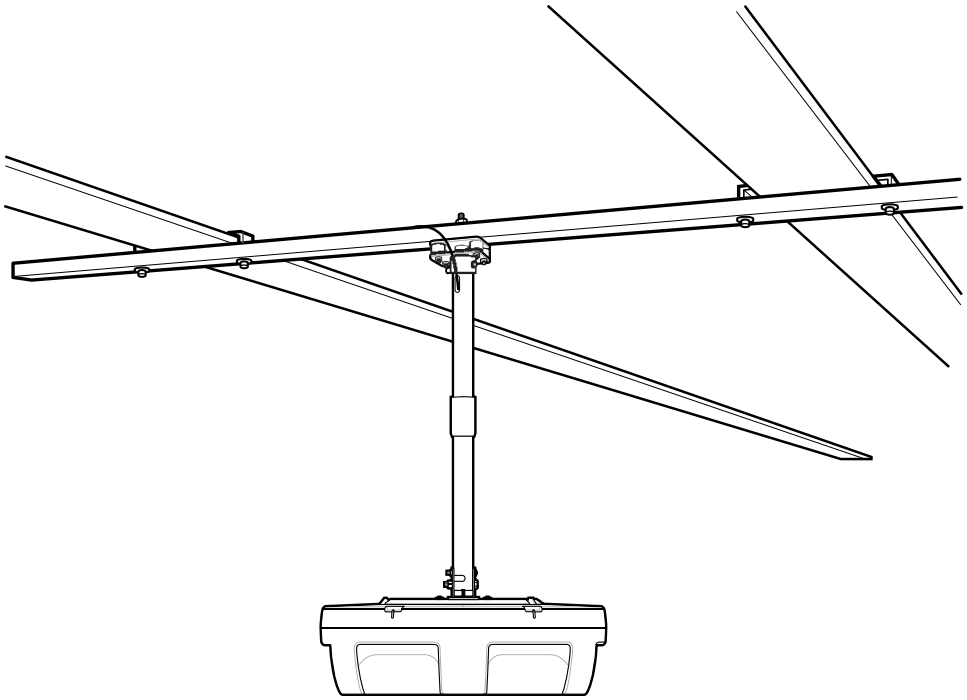


Installing Using a Strut Channel Clamped to the Bottom of the Truss

For locations with high ceilings where the bottom of the trusses are at least 15' 3" from the floor and where the ATR7000 cannot be located directly under a truss, add a strut channel to the lower section of two trusses and mount the ATR7000 on the strut channel.

NOTE: Refer to the site survey report for the proper mounting height of each. In general, this is 12‘ from the bottom of the device to the floor.

Figure 16 Installing the ATR7000 Using a Strut Channel



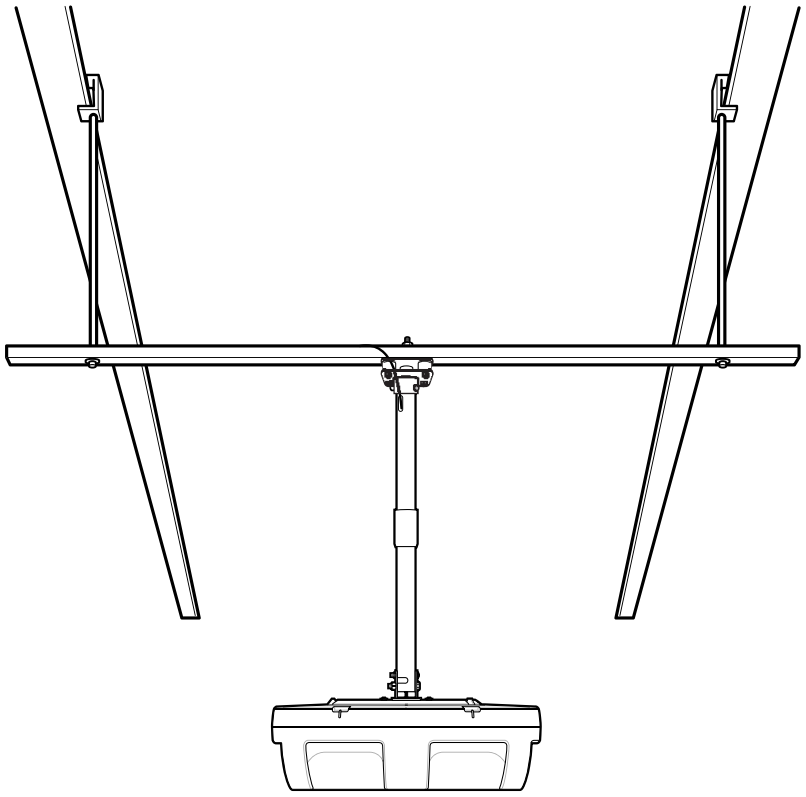
Secure the strut channel to two trusses using beam clamps appropriate for the installation. Refer to the instructions provided with the beam clamp used.

Installing Using a Strut Channel and Threaded Rods Clamped to the Top of the Truss

For an alternative configuration using a strut channel, mount the strut channel to the top of the truss using threaded rods and beam clamps, and mount the ATR7000 on the strut channel.

NOTE: Refer to the site survey report for the proper mounting height of each. In general, this is 12 ft from the bottom of the device to the floor.

Figure 17 Installing the ATR7000 to the Top of the Truss

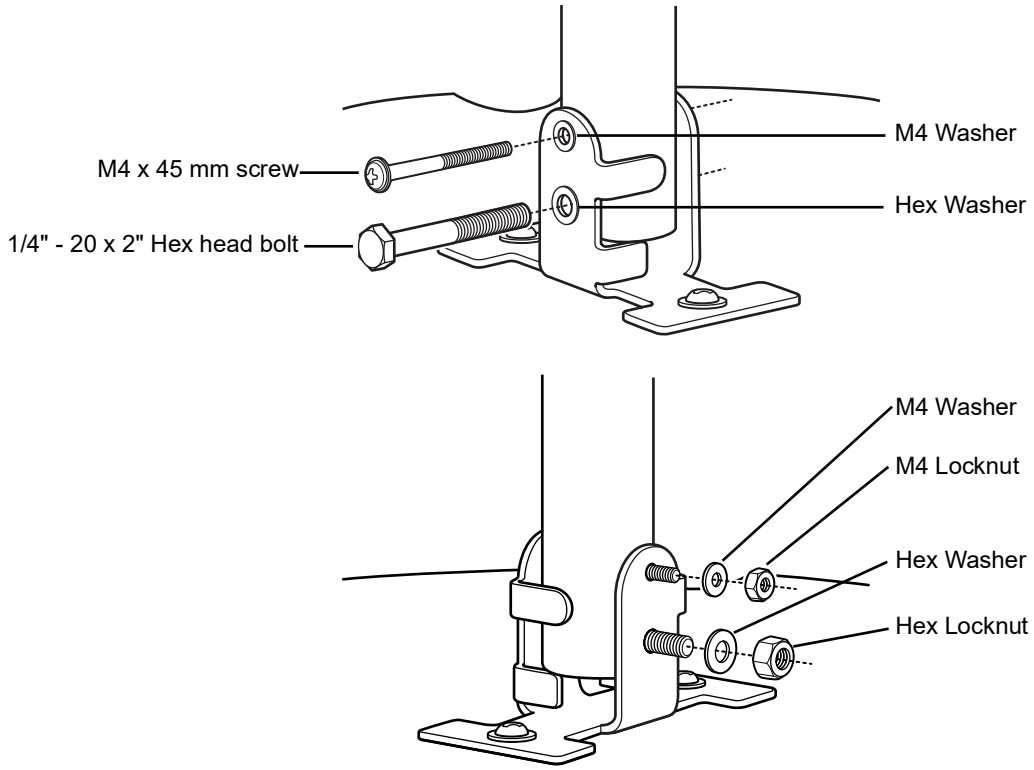


Mounting the ATR7000

1. Turn the center collar on the telescoping pole to expose the lower portion of the pole, and then turn the collar back to tighten it.
2. Attach the ATR7000 unit to the lower portion of the pole using the fasteners shown in Figure 18.

NOTE: Only use mounting hardware included with certified mounting pole.

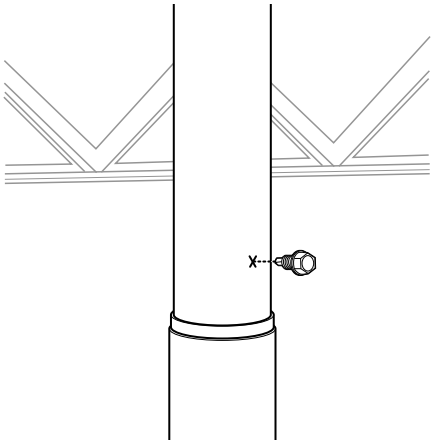
Figure 18 Attaching the ATR7000 unit to the Telescoping Pole



3. Attach the telescoping pole to the truss or strut channel according to manufacturer recommendations.
4. Adjust the length of the telescoping pole to accommodate the ATR7000 height per the site survey report.
5. Level the telescoping pole to accommodate the angle of the truss, if necessary.
6. Drive the self-tapping screw (included with pole hardware) into the pole approximately 1/2" above the collar, locking the pole. Remove any cables from the pole before fastening this screw.

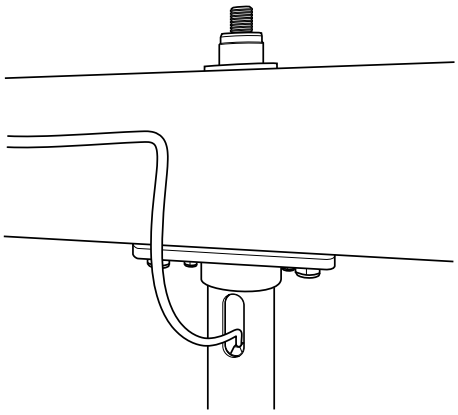
NOTE: Pole adjustment instructions are included for reference only. Always follow the mounting and adjustment instructions provided with the certified mounting pole.

Figure 19 Driving the Self-Tapping Screw Into the Pole



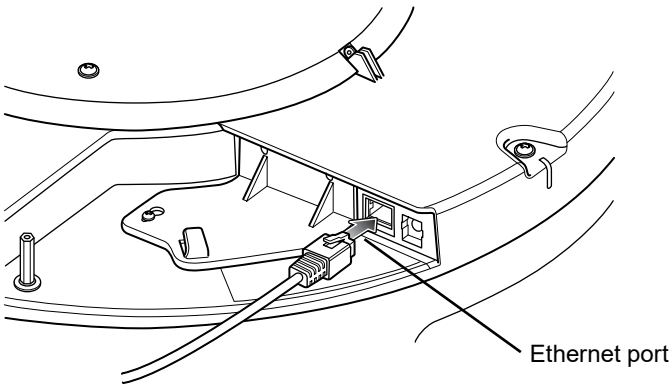
7. Connect the Cat5e/6 UTP Ethernet cable installed as part of the network infrastructure.
   a. Route the network cable into the hole at the top of the pole and out through the bottom of the pole.

Figure 20 Running the Cable Through the Management Hole



   b. Terminate the cable after routing it through the pole.
   c. Connect the cable to the Ethernet port on the ATR7000.

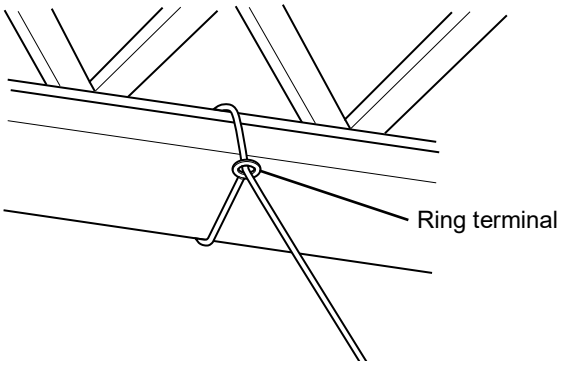
Figure 21 Connecting the Cable to the ATR7000 PoE+ Port



8. Install the safety cable.

   a. Loop the ring terminal end of the safety cable around a truss, and pass the other end of the cable through the ring terminal to securely fasten the cable to the truss.

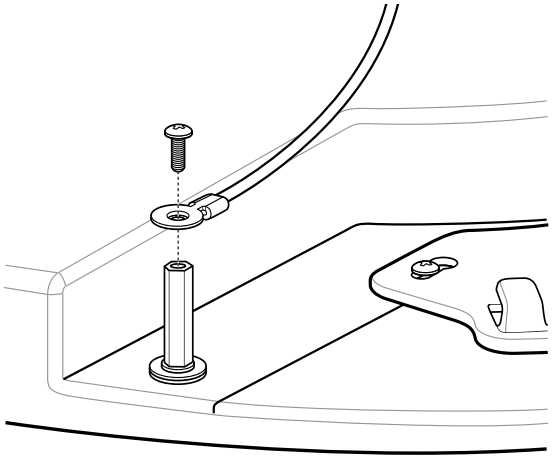
Figure 22 Securing the Safety Cable to the Truss



   b. Run the safety cable into the hole at the top of the pole and out through the bottom of the pole.

   c. Secure the eyelet with the M4x10 mm screw.

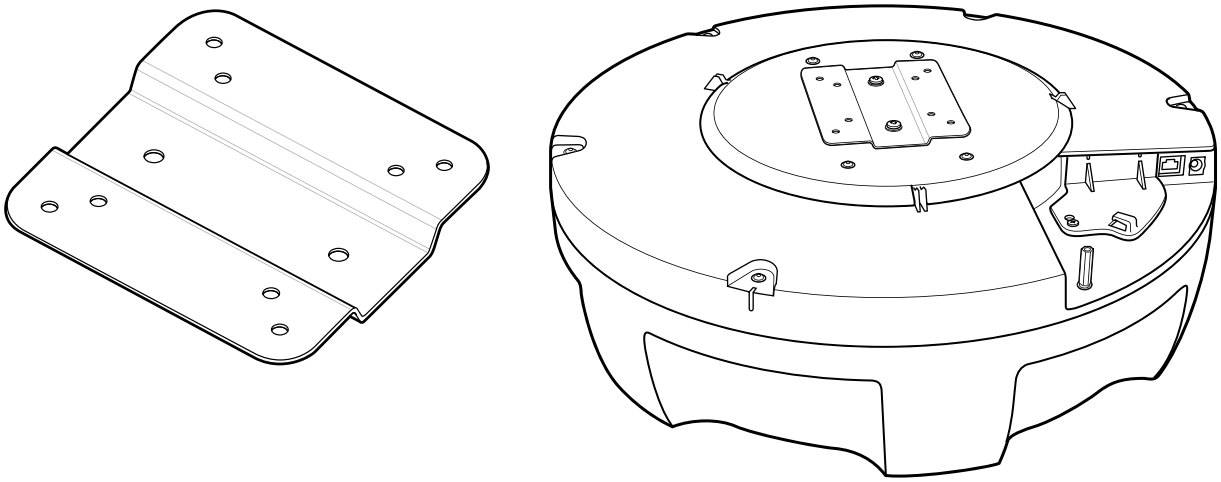
Figure 23 Securing the Safety Cable to the ATR7000



VESA Mounting

The VESA mount is an accessory to enable the ATR7000 installation using VESA-75 or VESA-100 standard patterns. The ATR7000 may optionally be mounted via four VESA holes on 100 mm x 100 mm and 75 mm x 75 mm patterns using M4 screws, that have been provided with the VESA support you are mounting to. Make sure VESA support is rated to support a 12 lb min. load. Mount the VESA Mount Adapter to the ATR7000 using the two mounting screws provided with the ATR7000.

Figure 24 VESA Mount Adapter



Communications and Power Connections

Use a standard Ethernet connection or PoE + Ethernet to connect the ATR7000 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 ATR7000 RFID reader using either the reader Zebra AC power supply, or by POE+ through the Ethernet cable.

Ethernet: Power through AC Outlet

The ATR7000 RFID reader communicates to the host through a 10/100Base-T Ethernet cable and receives power through a Zebra AC power supply.

1. Route the Ethernet cable.
2. Route the power cable.
3. Terminate the Ethernet cable.
4. Connect the Ethernet cable to the LAN port on the ATR7000 reader (see Figure 13 on page 19).
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 ATR7000 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 33.
9. On a networked computer, open an Internet browser and connect to the reader. See Connecting to the Reader on page 40.
10. Log in to the **Administrator Console**. See Administrator Console Login on page 42.

CAUTION: If the AC power supply is used, use caution to ensure that it is securely located and/or fastened to prevent falling from the overhead installation.

Ethernet: Power through PoE+ (802.3at)

The PoE installation option allows the ATR7000 RFID reader to communicate and receive power on the same 10/100Base-T Ethernet cable.

1. Insert the PoE Ethernet connector on the RJ45 Ethernet cable into the reader 10/100BaseT Ethernet port. See Figure 13 on page 19.
2. Connect the other end of the cable to an Ethernet network with PoE+ capability.
3. Verify that the reader booted properly and is operational. See System Start-up/Boot LED Sequence on page 33.
4. On a networked computer, open an Internet browser and connect to the reader. See Connecting to the Reader on page 40.
5. Log in to the **Administrator Console**. See Administrator Console Login on page 42.



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



NOTE: Ensure to follow these points when powering the ATR7000:

- When powering the ATR7000 over Ethernet, any PoE+ (802.3at) compliant Power Source Equipment such as a switch, midspan, or PoE+ injector may be used to power the ATR7000, provided the power source supply is at least 22.9 W at the ATR7000 port.
- When powering the ATR7000 from a PoE+ (802.3at) switch that supports LLDP Power Negotiation, ensure that LLDP is enabled in the switch configuration, and Power Negotiation is enabled (default setting) in the ATR7000 reader configuration. See Configure Reader on page 52.
- The ATR7000 can be powered from a PoE+ switch that does not support LLDP or has LLDP power negotiation disabled in its configuration, provided such a switch is capable of supplying at least 22.9 W through its device port. In such a case, disable the Power Negotiation configuration in the ATR7000 reader configuration. See Configure Reader on page 52.
- In the switch configuration when a maximum power cap is specified, ensure that at least 22.9 W of power is supplied at the reader port. Power loss due to the cabling used must be accounted, to ensure that the power supply configuration is set correctly.

USB Connection

The USB debug port is used by service technicians as a debug console.

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 10 on page 111 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

1. During system start-up:The reader LED turns off and turns on red for a second when power is applied to the reader.
2. The reader LED turns amber.
3. After approximately 60 seconds, the reader LED turns green to indicate successful RFID application initialization.
4. When the sequence completes, the green reader LED remains on.

LED Sequence to Indicate Network Status After BootingAfter the RFID application initializes:

1. The reader LED turns green for 5 seconds to indicate success (following the sequence from System Start-up/Boot LED Sequence).
2. The reader checks the Ethernet address and indicates the status using the reader LED:
   - If the reader has a DHCP address, the reader LED blinks green for 3 seconds.
   - If the reader has static IP address, the reader LED blinks amber 3 seconds.
   - If the reader has an IP address from zero-configuration networking algorithm, the reader LED blinks red for 3 seconds.
   - If the reader doesn't have valid IP, the reader 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 reader LED stops blinking.
3. The reader 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. Reader LED turns on RED when you press and hold the reset button.
2. Reader LED blinks amber.
3. Reader 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

The reader LED activity reflects the software update progress as follows:

1. The reader LED blinks red during software update.
2. After reset, the reader LED is solid amber until the update completes.
3. The reader LED blinks green until all components are fully initialized with the updated software.
4. The reader LED turns solid green when the reader is fully initialized and ready for operations

ATR Beam Configuration

Introduction

The most notable difference between an ATR7000 and a standard fixed reader is that in a fixed reader, an antenna is associated with a physical port (i.e. antenna connector, cable, and antenna). For the ATR7000, with its integral beam steered antenna array, an antenna is “virtual” in the sense that an antenna is defined as a beam with a specific polarization steered in a specific direction.

This chapter provides information so the user can control the beams in a pre-determined way and includes the following:

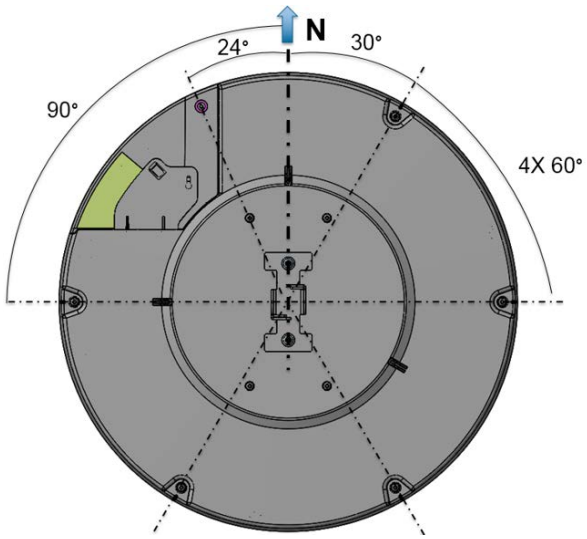
- Reference Coordinate System for ATR7000
- ATR7000 Beam Configuration
- Reading Tags

Reference Coordinate System for ATR7000

The directional orientation of the ATR7000 in the field (after installation) is important for ensuring that a user can precisely control the beam steering direction, and therefore, the coverage area of a reader. As the ATR7000 steers its beam, the beam direction is defined in terms of an azimuth and an elevation. In a multi-reader RTLS deployment the orientation of each reader is critical for the location analytics to properly “triangulate” and determine a tags precise location.

To define a reference coordinate system for beam direction (pointing angle), the ATR7000 has established a “True-North” direction, defined as 0º azimuth, and a “boresight” direction, defined as 0º elevation (the beam pointing directly at the ground when an ATR7000 is mounted overhead parallel to the ground).

Figure 25 True North Orientation - Location of Notches

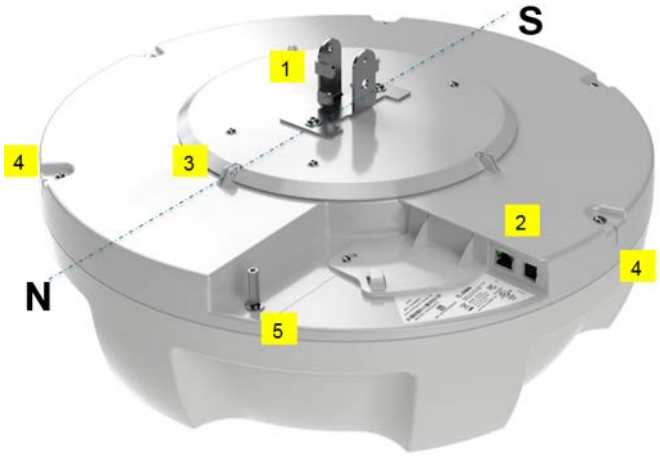


In both cases of either a standalone ATR7000 or an ATR7000-based RTLS deployment, the term “True-North” is not synonymous with magnetic north (i.e. North on a compass); nor is it synonymous with the direction towards the north pole. “True-North” for an ATR7000 is defined in the context of a local facility coordinate system where the facility origin is defined as x=0, y=0, z=0, and True-North is defined as the direction of the positive y axis (0 º azimuth). Similarly in this context, 0 º elevation is defined as the direction of the negative z axis.

During installation, it is typical that a reader is installed directly overhead with the bottom of the antenna radome parallel to the floor for additional installation information, please refer to Figure 15 and Figure 16. The boresight direction (the beam pointed directly at the floor) is defined as 0 º elevation and the horizon is at an elevation equal to 90 º .

There are several features built into the ATR7000 which can be referenced for orientation during installation (visible from the top) and post installation (visible from the ground). As shown in Figure 26, there are 5 notches in the ATR7000. The True-North orientation of an ATR7000 reader in relation to the notches is shown (top view) in Figure 25. Note the safety cable mount is 24° counter-clockwise from True-North.”

Figure 26 Orientation Features 1, 2, 3 Visible from the Top

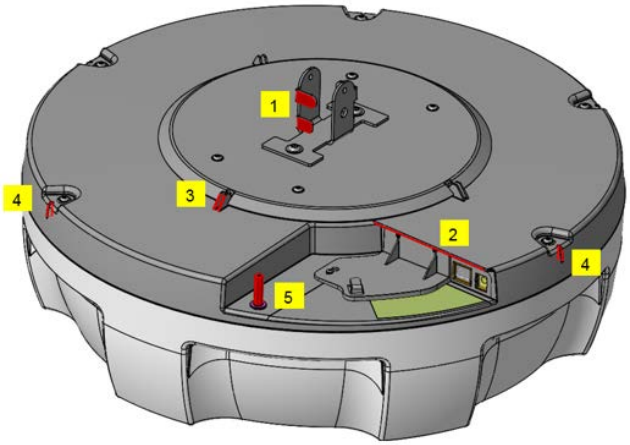


1- Tabs on Pole Mounting Bracket

2- I/O ports – overhang/protective edge

3- One of the three Top Plate Locating Ribs

Figure 27 Orientation Features 4, 5 Visible from Floor



4- Five notches (~2 mm wide) by the Top Cover mounting screws

5- Safety cable mounting standoff

Even In applications that use a standalone ATR7000, it is important to align the reader to the True-North direction. Alternately, a compensation to azimuth should be factored in to account for the difference. In an ATR7000-based RTLS deployment, beam direction is under the control of software. As long as the actual installation orientation is known (and recorded), the software will compensate for any deviation, however, the deviation to True-North must be recorded accurately.

ATR Beam Configuration

The ATR7000 has defined 291 beams, 97 directions with three distinct polarizations for more precise control over RF coverage.

The table below shows a complete list of all beam scanning options available using Zebra's standard APIs or PowerSession. In general, the best performance is obtained using Left Hand Circular Polarization (LHCP). Additional polarization options are provided for optimizing for certain tag types and/or for certain use cases.

Table 4 ATR7000 Beam Configuration

ATR7000 Beam Configuration																								
"Reserved"																								
Azimuth	0	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225	240	255	270	265	300	315	330	345
Elevation																								
60	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
45	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
30	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
15	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
0	97																							
Theta Polarization																								
Azimuth	0	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225	240	255	270	265	300	315	330	345
Elevation																								
60	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124
45	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148
30	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172
15	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196
0	197																							
Phi Polarization																								
Azimuth	0	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225	240	255	270	265	300	315	330	345
Elevation																								
60	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224
45	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248
30	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272
15	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296
0	297																							
Left Hand Circular Polarization (LHCP)																								
Azimuth	0	15	30	45	60	75	90	105	120	135	150	165	180	195	210	225	240	255	270	265	300	315	330	345
Elevation																								
60	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324
45	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348
30	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372
15	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396
0	397																							

Administrator Console

Introduction

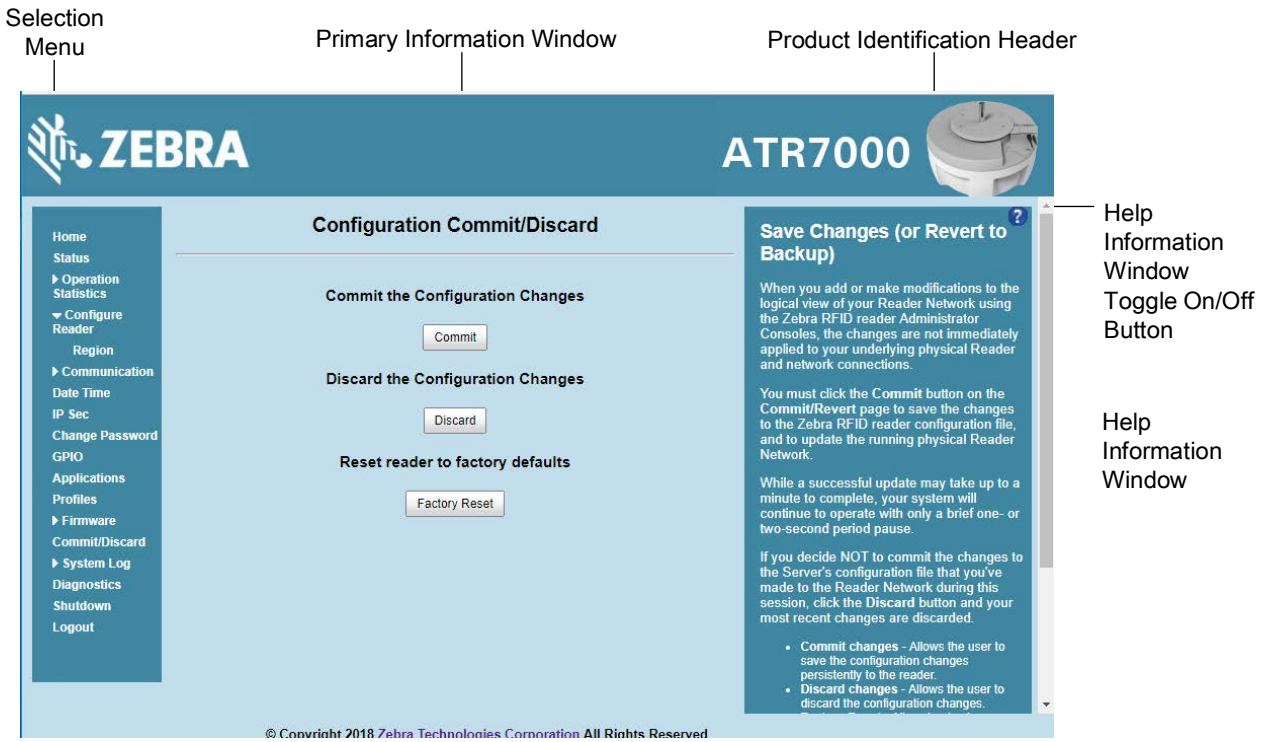
This chapter describes the ATR7000 web-based **Reader Administrator Console** functions and procedures. Access the **Administrator Console** using a web browser from a host computer, and use this to manage and configure the readers. The **Administrator Console** main window and support windows have four areas, each containing unique information about the reader.



NOTE: The screens and windows in this chapter may slightly differ from actual screens and windows.

- **Selection Menu** - selects the function for the primary information window.
- **Primary Information Window** - provides the primary function information.
- **Product Identification Header** - identifies the product.
- **Help Information Window**:
  - provides detailed information to support the primary information window.
  - includes a scroll bar to scroll through information.
  - includes a toggle button to turn on/off the help information window.

Figure 28 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 84.

Resetting the Reader

To reset the reader, press and hold the reset button for not more than 2 seconds. See Figure 13 on page 19 for the reset button location. The reader reboots but retains the user ID and password. See System Start-up/Boot LED Sequence on page 33.

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

Auto Discovery

The ATR7000 reader can automatically belong to a network. The reader implements WS-Discovery conforming to RFID Reader Management Profile (RDMP) specification in ISO 24791-3. RDMP is based on an extension for Device Profile for Web Services (DPWS). The discovery mechanism is limited to subnets and does not work across subnets. The PowerSession 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 7/10 computers by clicking on the **Network** icon in a file browser.

Connecting to the Reader

To use the Administrator Console to manage the reader, first power up the reader and connect it to an accessible network. A solid green state of the reader LED indicates that the reader is ready. If the reader LED is not lit, reset the reader. See Resetting the Reader on page 39.

Connect to the reader in one of two ways:

- Connecting via Host Name on page 41.

or

- Connecting via IP Address on page 41. (To obtain the IP address, see Obtaining the IP Address via Command Prompt on page 40)

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

- Using DHCP on the network.

or

- Using Zero-Configuration Networking when DHCP Server is Not Available on page 42.

or

- Statically assigning an IP. See Static IP Configuration on page 114.

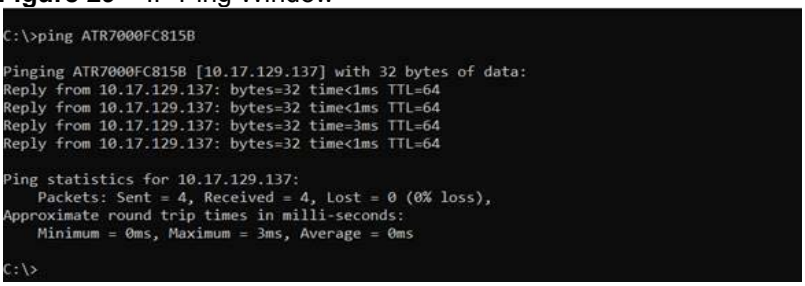
Any method of assigning the IP supports connection using host name or IP address. Alternatively, connect the reader directly to a local computer using zero-configuration networking. See Using Zero-Configuration Networking when DHCP Server is Not Available on page 42.

NOTE: When using zero-configuration networking, the ATR7000 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

To obtain the reader IP address without logging into the reader, open a command window and ping the reader host name.

Figure 29 IP Ping Window



Connecting via 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.

To connect to the reader using the host name:

1. Open a browser. Recommended browsers are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54.
2. Enter the host name provided on the reader label in the browser (for example, http://ATR7000cd3b0d) and press **Enter**. The **Console Login** window appears and the reader is ready.
3. Proceed to Administrator Console Login on page 42 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 ATR7000, followed by the last three MAC address octets. For example, for a MAC address of 00:15:70:CD:3B:0D, use the prefix ATR7000, followed by the last three MAC address octets (CD, 3B, and 0D), for the host name ATR7000CD3B0D. Type http://ATR7000CD3B0D in the browser address bar to access the reader.

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

Connecting via IP Address

To use the IP address to connect to the reader:

1. Open a browser. The minimum browser recommends are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox v54**.**
2. Enter the IP address in the browser (e.g., http://157.235.88.99) and press **Enter**. The **Console Login** window appears and the reader is ready.
3. Proceed to Administrator Console Login on page 42 to login to the reader.

Using Zero-Configuration Networking when DHCP Server is Not Available

If a DHCP server is not available, the ATR7000 readers can use zero-configuration networking to automatically provide a unique network IP address. The reader can then use TCP/IP to communicate with other computers also using a zero-configuration networking-generated IP address.

NOTE: When using zero-configuration networking, the ATR7000 reader cannot communicate with computers on different subnets, or that do not use automatic private IP addressing. Automatic private IP addressing is enabled by default.

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

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

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

Administrator Console Login

NOTE: The recommended browsers are IE11 (disabling Compatibility View is recommended), Chrome v58, and FireFox 54. These browsers were tested and validated to work properly. Other browsers may or may not work properly.

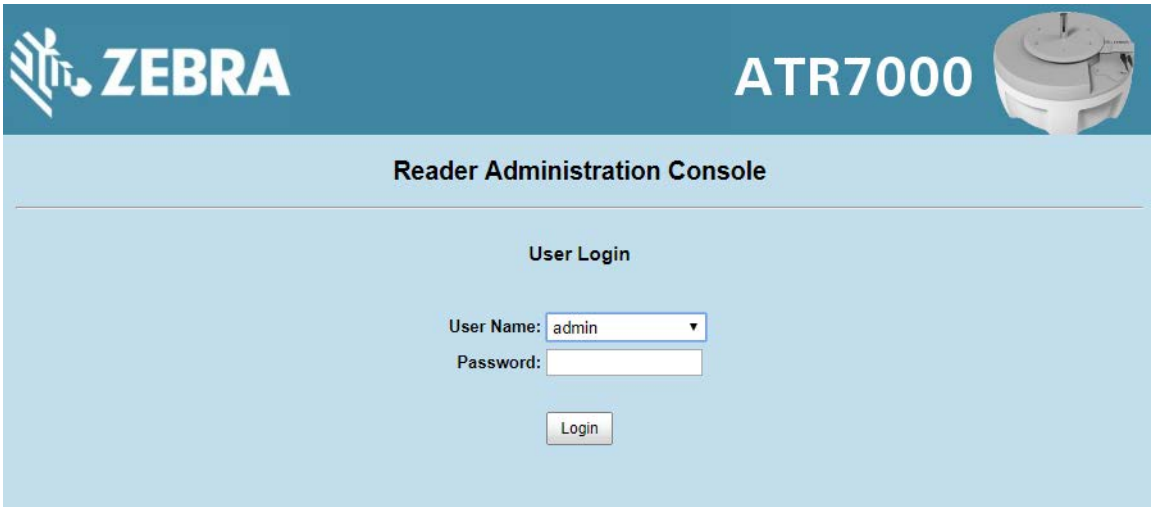
First Time / Start-Up Login

When starting the reader for the first time, set the region of reader operation. Setting the reader to a different region is illegal.

Logging In with Default User ID and Password

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

Figure 30 User Login Window



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

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

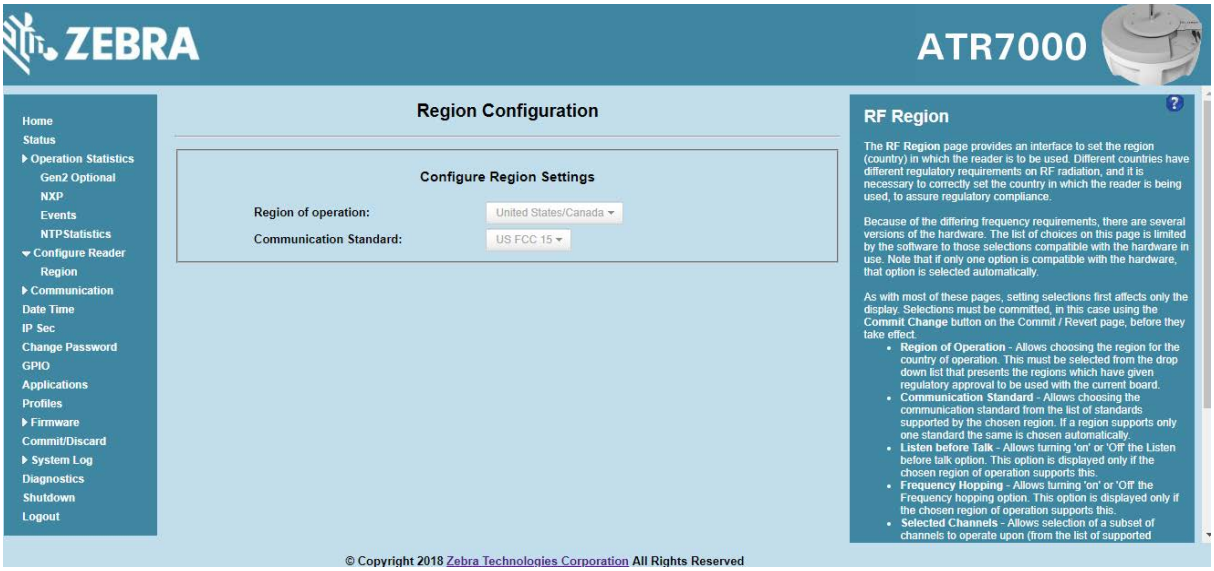
Setting the Region

The ATR7000 currently supports only United States and Canada regions. For global reader configurations (supported in future), set the region of operation.

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. Setting the unit to a different region is illegal.

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

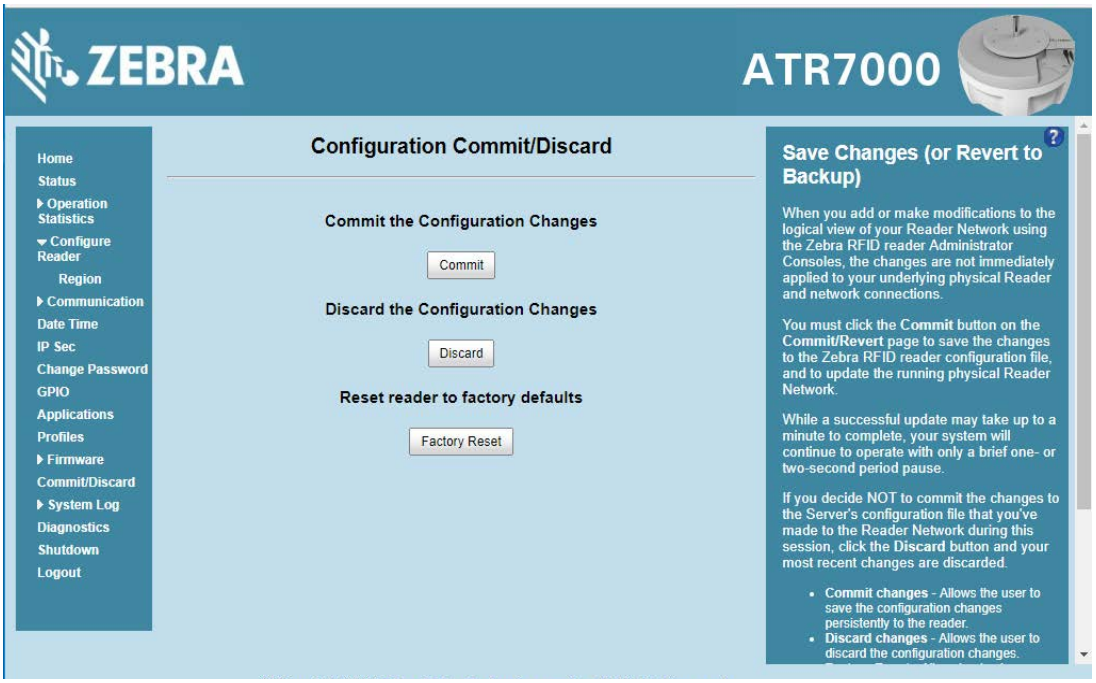
Figure 31 Region Configuration Window



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

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

Figure 32 Commit/Discard Window



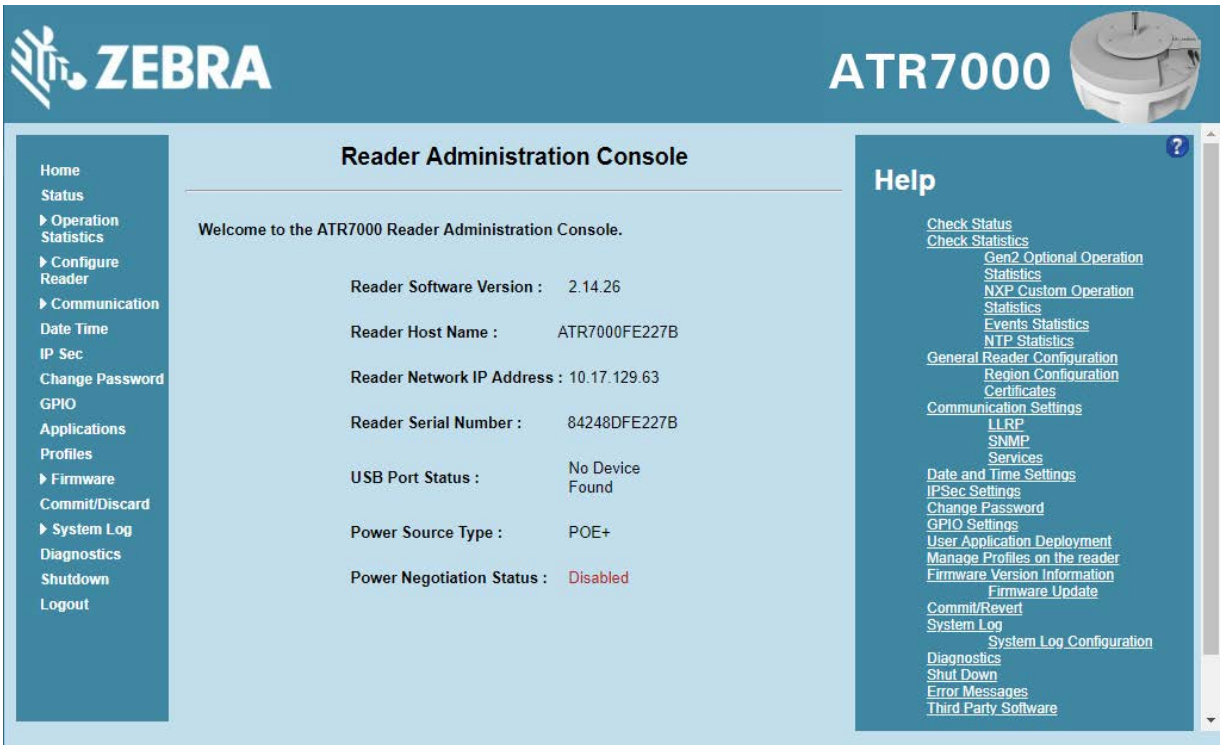
8. Click **Commit** to apply the changes to the reader configuration file, or **Discard** to discard the new region configuration changes.

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

Reader Administrator Console

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

Figure 33 Reader Administrator Console Main Window



Administrator Console Option Selections

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

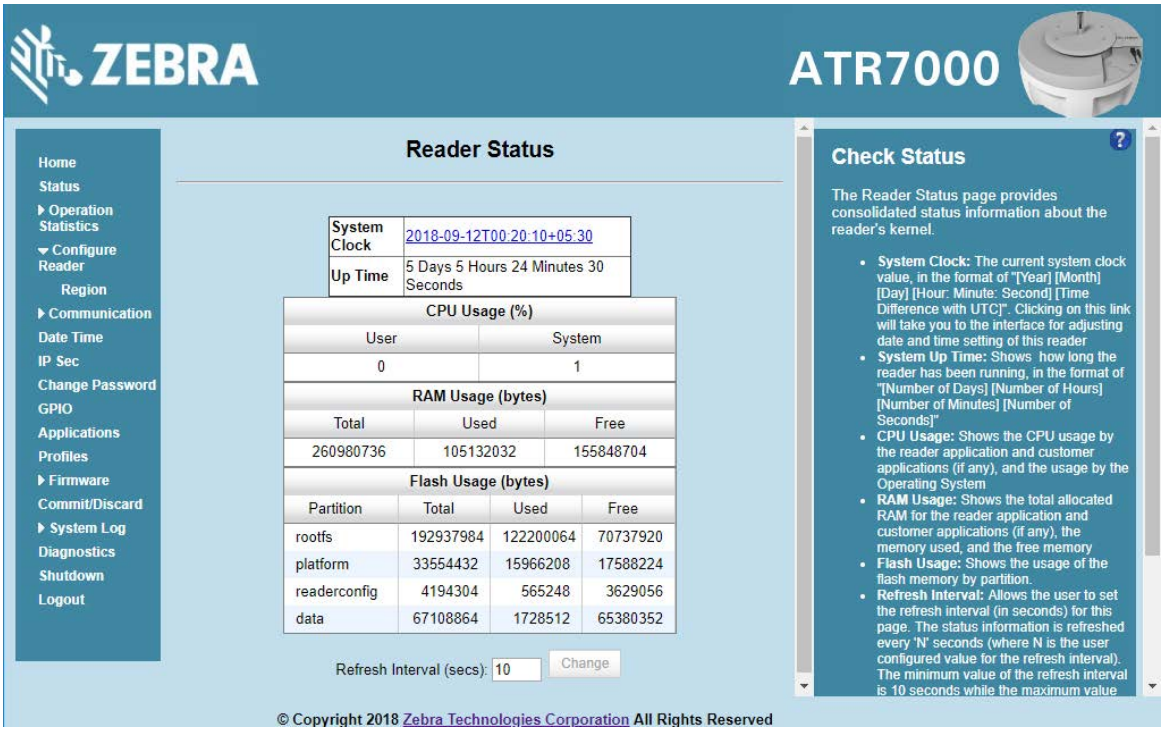
- **Status** - see Status on page 46
- **Operation Statistics** - see Reader Statistics on page 47
  - **Gen2 Optional** - see Reader Gen2 Optional Operation Statistics on page 48
  - **NXP** - see NXP Custom Command Operation Statistics on page 49
  - **Events** - see Event Statistics on page 50
  - **NTP Statistics** - see NXP Custom Command Operation Statistics on page 49
- **Configure Reader** - see Configure Reader on page 52
  - **Region** - see Configure Region on page 53
  - **Certificates** - see Certificates on page 54
- **Read Tags** - see Communication Settings on page 69
- **Communication** - see Communication Settings on page 69
  - **LLRP** - see Configure LLRP Settings on page 70
  - **SNMP** - see SNMP Settings on page 72
  - **Services** - see Network Services Settings on page 73
- **Date/Time** - see System Time Management on page 79
- **IP Sec** - see IPV6 IP Sec on page 80
- **Change Password** - see Change Password on page 81
- **GPIO** - see GPIO on page 82

- **Applications** - see Applications on page 83
- **Profiles** - see Reader Profiles on page 84
- **Firmware** - see Firmware Version/Update on page 85
  - **Update** - see Select **Revert Back to revert the firmware to last known version. The reader automatically reboots. This option is not enabled if the reader detects an error in the previous firmware update. Firmware Update on page 86**
- **Commit/Discard** - see For instructions on updating the firmware, see Firmware Upgrade. on page 86
- **System Log** - see System Log on page 87
  - **Configure** - see Configure System Log on page 88
- **Diagnostics** - see Reader Diagnostics on page 89
- **Shutdown** - see Shutdown on page 89
- **Logout** - click **Logout** to immediately log out of the **Administrator Console.**

Status

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

Figure 34 Reader Status Window



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

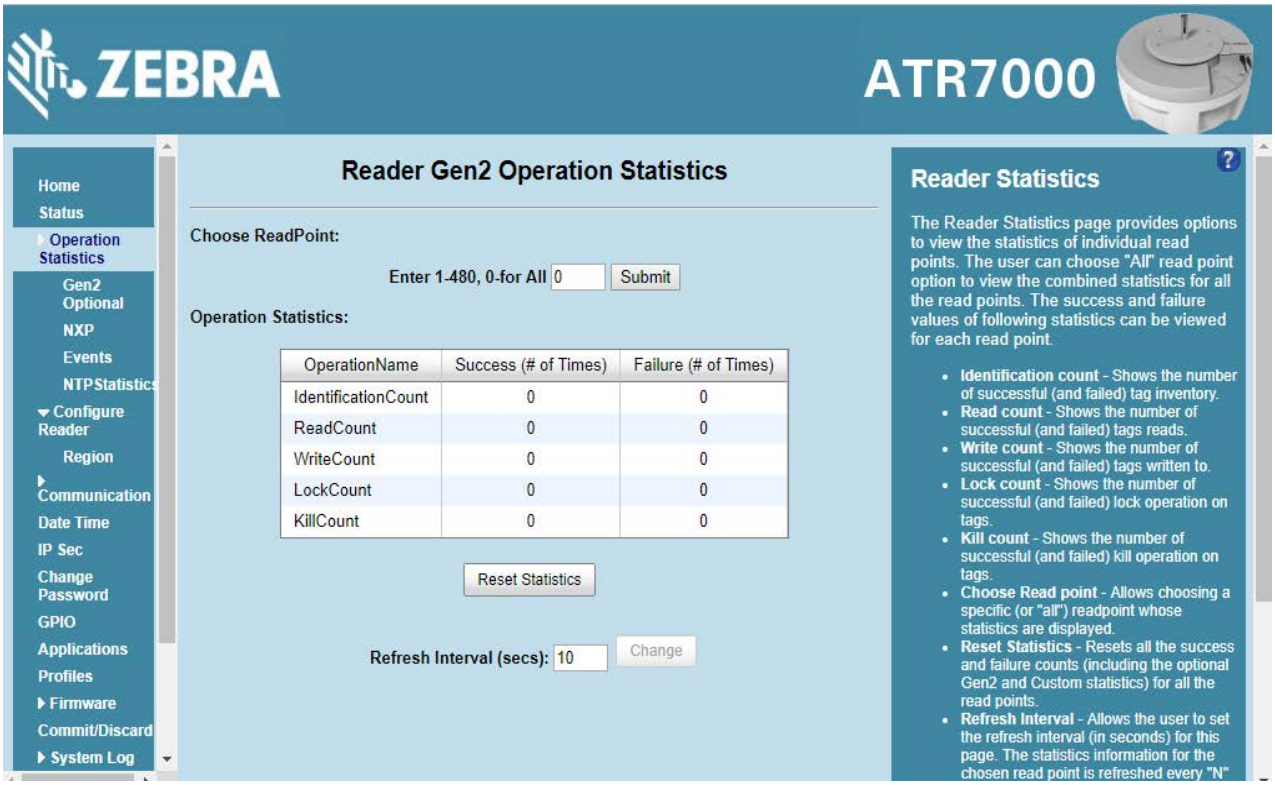
- **System Clock:** The current system clock value, in the format of [Year] [Month] [Day] [Hour: Minute: Second] [Time Difference with UTC]. Click the link to adjust the reader date and time settings.
- **Up Time** - Displays how long the reader has been running, in the format [Number of Days] [Number of Hours] [Number of Minutes] [Number of Seconds].

- **CPU Usage:** Displays the CPU usage for the system and reader applications, including customer applications.
- **RAM Usage:** Displays the total allocated RAM for the reader application and customer applications (if any), the memory used, and the free memory.
- **Flash Usage:** Displays the flash memory usage by partition.
- **Refresh Interval** - Sets the refresh interval (in seconds) for the window. The status information refreshes every **N** seconds (where **N** is the user configured value for the refresh interval). The minimum refresh interval value is 10 seconds; the maximum allowed is 86,400 seconds.

Reader Statistics

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

Figure 35 Reader Operation Statistics Window



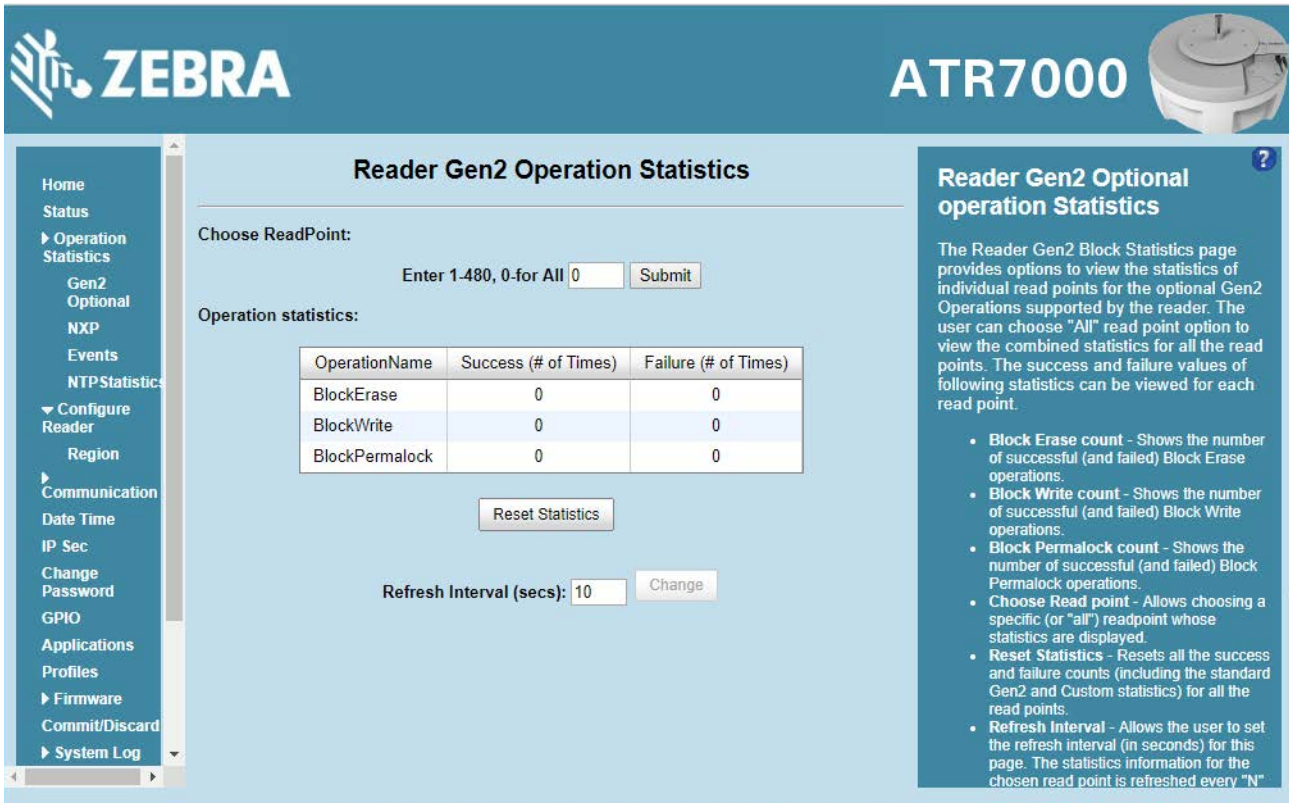
- **Choose ReadPoint** - Select a specific read point or select **All** from the drop-down list to display the statistics.
- **IdentificationCount** - Displays the number of successful (and failed) tag inventories.
- **ReadCount** - Displays the number of successful (and failed) tag reads.
- **WriteCount**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

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

Reader Gen2 Optional Operation Statistics

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

Figure 36 Reader Gen2 Operation Statistics Window

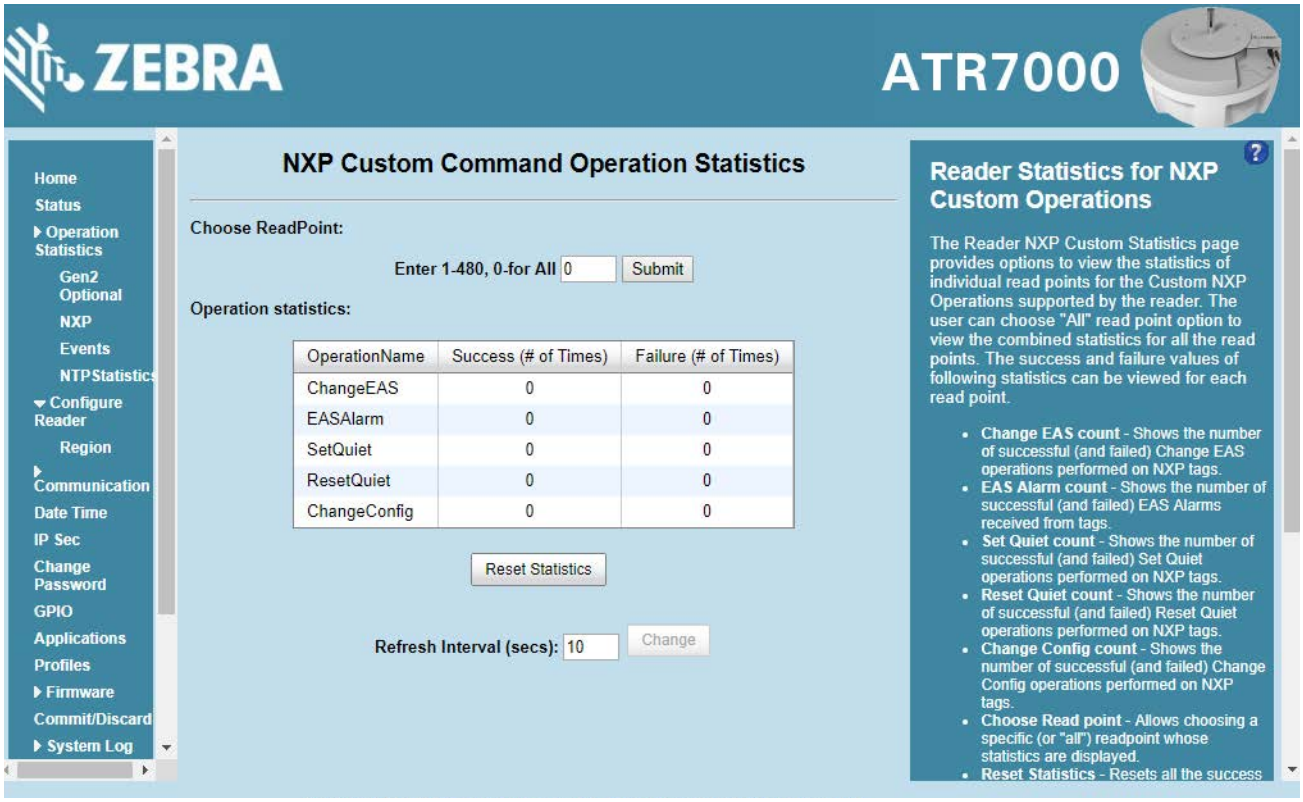


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **BlockErase** - Displays the number of successful (and failed) block erase operations.
- **BlockWrite** - Displays the number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

NXP Custom Command Operation Statistics

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

Figure 37 NXP Custom Command Operation Statistics Window

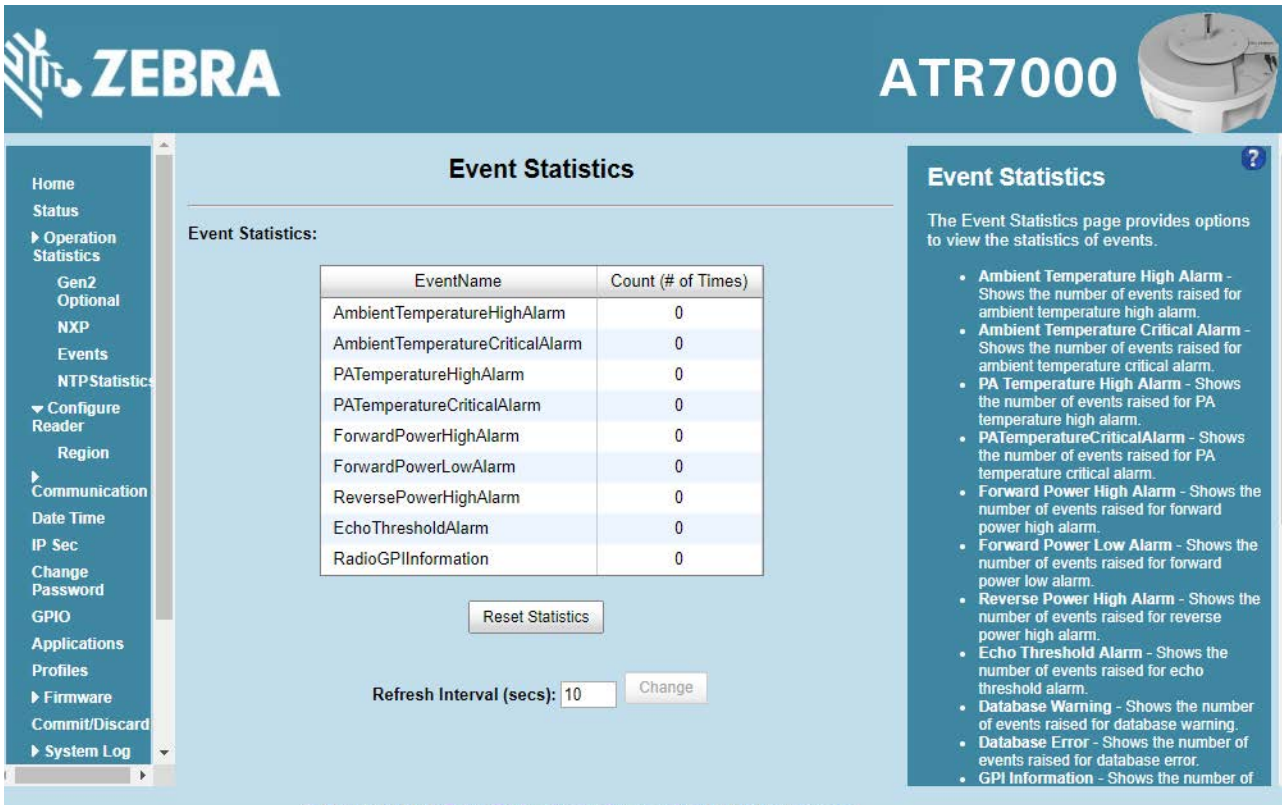


- **Choose ReadPoint** - Select a specific read point from the drop-down list to display the statistics, or select **All** to view the combined statistics for all read points.
- **ChangeEAS** - Displays the number of successful (and failed) change EAS operations performed on NXP tags.
- **EASAlarm**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

Event Statistics

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

Figure 38 Event Statistics Window

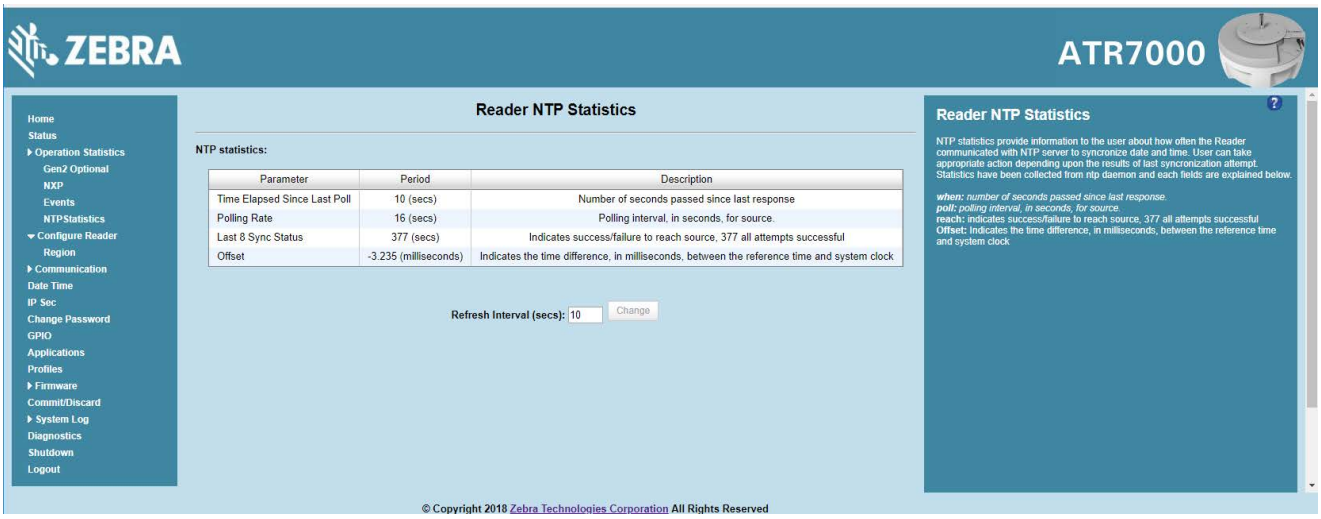


- **AmbientTemperatureHighAlarm** - Displays the number of events raised for ambient temperature high alarm.
- **AmbientTemperatureCriticalAlarm** - Displays the number of events raised for ambient temperature critical alarm.
- **PATemperatureHighAlarm** - Displays the number of events raised for PA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

NTP Statistics

NTP statistics provide information to the user about how often the reader communicated with the NTP server to synchronize date and time. User can take appropriate action depending upon the results of the last synchronization attempt. Statistics have been collected from NTP daemon and each field are explained below.

Figure 39 NTP Statistics Window



Statistics have been collected from NTP daemon, each field is explained below.

- **When:** Number of seconds elapsed since last response.
- **Poll:** Polling interval, in seconds, for source.
- **Reach:** Indicates success/failure to reach source. A reading of 377 shows that all attempts were successful.
- **Offset:** Indicates the time difference, in milliseconds, between the reference time and system clock.

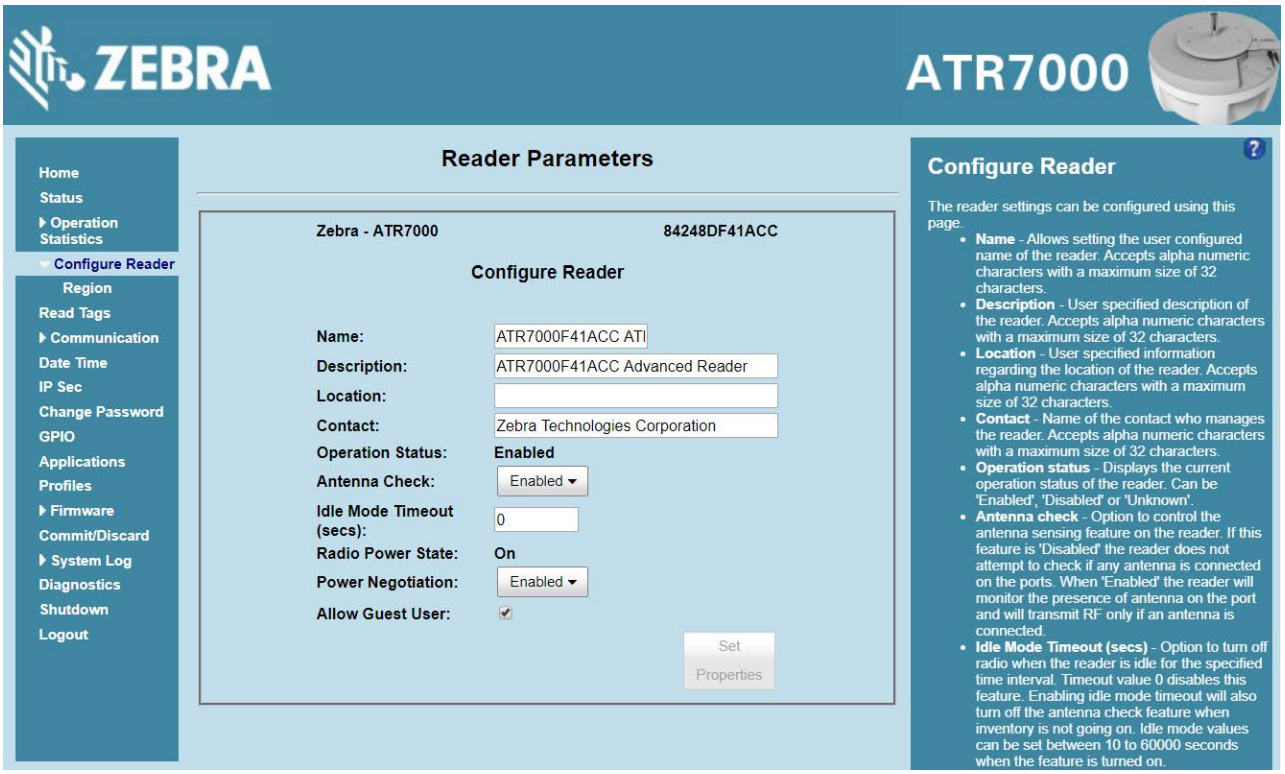
Configure Reader

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

Reader Parameters

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

Figure 40 Reader Parameters Window



- **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** - When enabled, the reader checks for any port fault and send event to the host indicating the faulty port. When disabled, no error is sent back for faulty port status.
- **Idle Mode Timeout (secs)** - Turns off the radio when the reader is idle for the specified time interval. A value of **0** disables this feature. Enabling this also turns off the antenna check feature when idle mode is entered after time out.
- **Radio Power State** - Displays the current state (**On** or **Off**) of the radio. The radio can be turned off if the **Idle Mode Timeout** is set to a non-zero value and the radio is not performing RF operations for a time period greater than the time specified by this timeout. The radio turns on automatically when RF operation starts.

- **Power Negotiation** - The ATR7000 requires at least 22.9 W to function properly. When the reader is Powered over Ethernet, PoE+ switches typically offers only PoE power levels to powered devices unless the device negotiates required power using LLDP protocol. When the Power Negotiation option is set as enabled, and committed, the ATR7000 readers negotiate PoE+ power level for its operation with the switch. Status of power negotiation is displayed in the Home page of the Administrative Console.

These settings only affect the display. Use For instructions on updating the firmware, see Firmware Upgrade. on page 86 to save the changes.

Configure Region

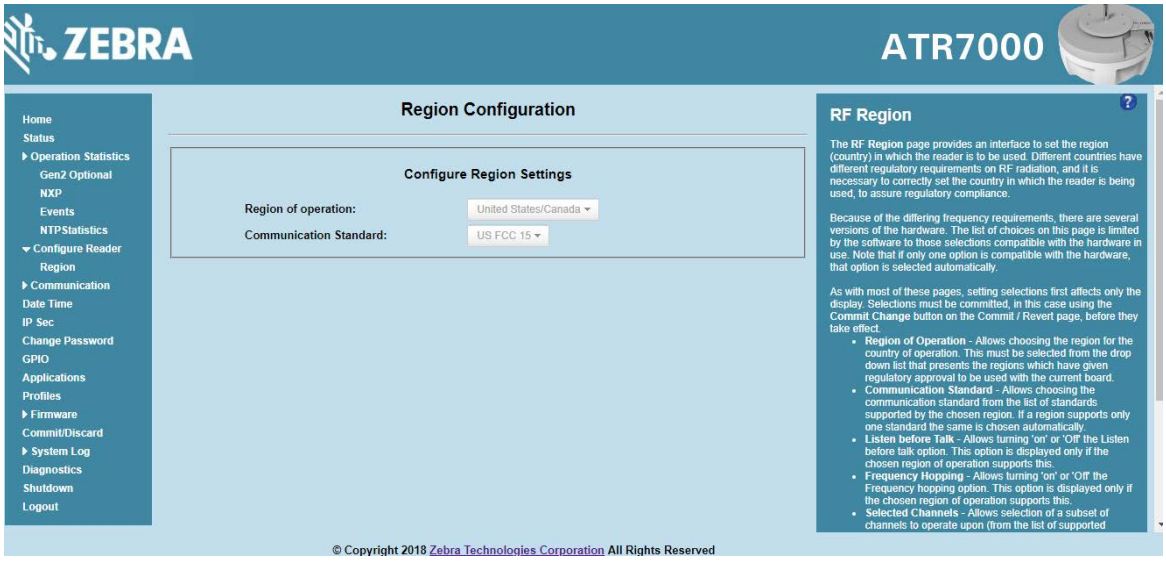
The ATR7000 currently supports United States, Canada, and other regions in 900 MHz RFID band. For global reader configurations, set the region of operation. **Setting the unit to a different region is illegal**.

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 41 Region Configuration Window



- **Region of Operation** - Select the region for the country of operation from the drop-down list. This list includes regions which have regulatory approval to use with the current board.
- **Communication Standard** - Select the communication standard from the list of standards that the chosen region supports. If a region supports only one standard, it is automatically selected.
- **Frequency Hopping** - Check to select frequency hopping. This option appears only if the chosen region of operation supports this.
- **Selected Channels** - Select a subset of channels on which to operate (from the list of supported channels). This option appears only if the chosen region of operation supports this.

- **Please confirm** - Check the **I understand** check box to confirm your understanding that the choices are in compliance with local regulatory requirements.
- **Set Properties** - Click to apply the changes. Select For instructions on updating the firmware, see Firmware Upgrade. on page 86 to save the changes to the reader.

Certificates

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

- Web **Administrator Console** service (HTTPS). See Network Services Settings on page 73.
- File Transfer Service (FTPS - explicit SSL/TLS over FTP). See Network Services Settings on page 73.
- 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 70.

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

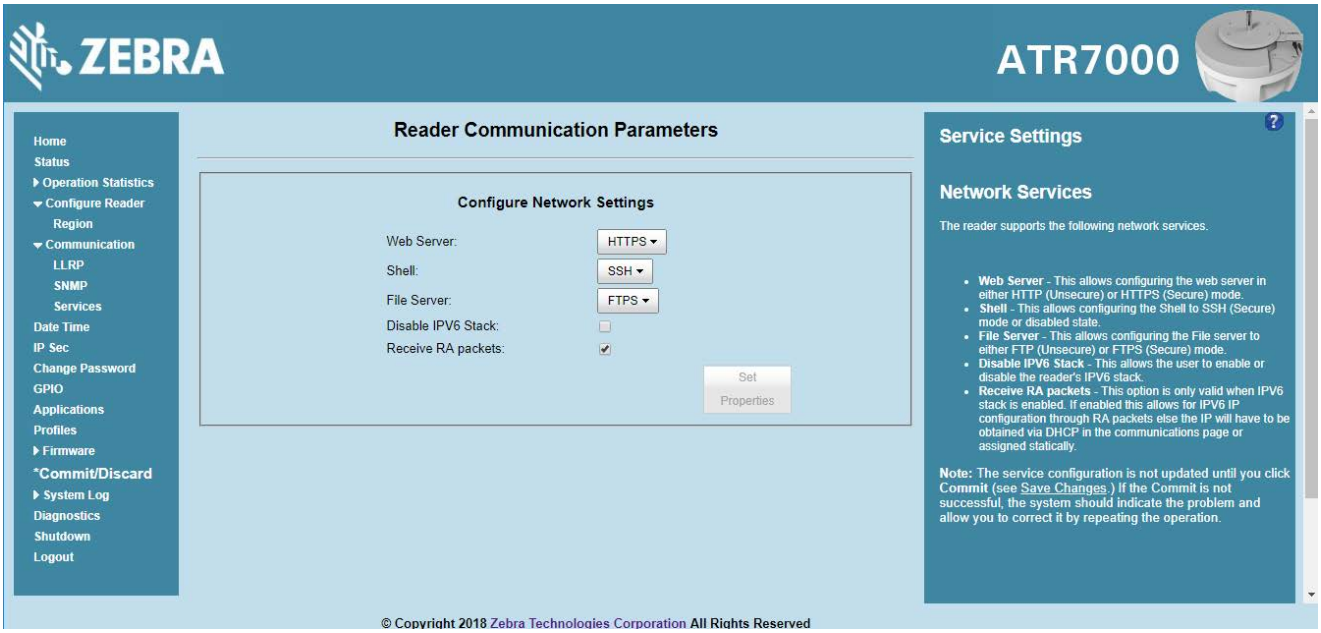
NOTE: The **Validate Peer** option in Secure LLRP Service configuration enables authentication of reader and/or clients using digital certificates. You must import a custom certificate (instead of the default self-signed certificate) to the reader to enable this option. See Configure LLRP Settings on page 70 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

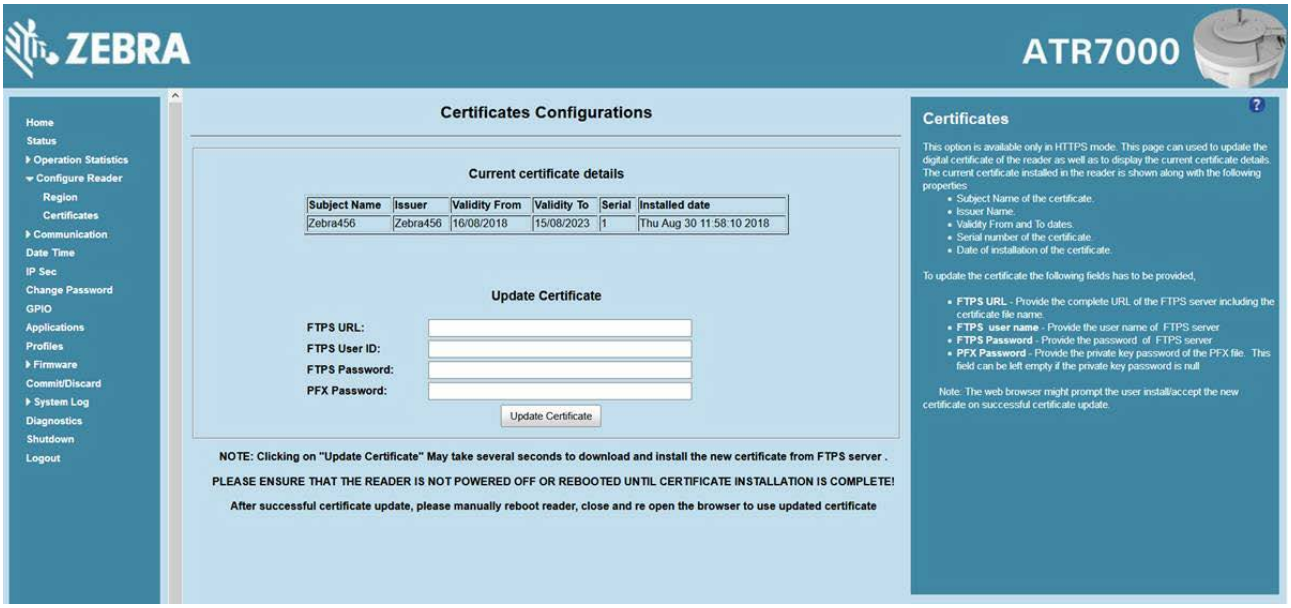
The **Certificate Configuration** page is available under the **Configure Reader** menu when the **Administrator Console** is in HTTPS mode only. To enable HTTPS mode, select **Communication > Services**, and on the **Reader Communication Parameters** page select **HTTPS** from the **Web Server** drop-down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

Figure 42 Setting HTTPS Mode



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

Figure 43 Certificate Configuration Window



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

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

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

- LLRP by default does not authenticate the client or reader. Security extensions to the standard allow client or reader authentication using digital certificates. The entities involved validate digital certificates by confirming the certificates were issued from a trusted source. Therefore a custom certificate is required to authenticate the client or reader. See the **Validate Peer** option in Configure LLRP Settings on page 70.
- 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 73. 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.

ATR7000 readers do not allow automatic certificate request and updating. The reader certificate must be issued externally and imported to the reader.

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

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

NOTE: The ATR7000 supports only a single digital certificate. If a custom certificate is installed, the issuer of the certificate is trusted by the reader, so any client attempting to connect to the reader over secure LLRP mode is trusted if the certificate issued to the client is from the same issuer.

NOTE: The ATR7000 supports 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

ATR7000 readers require that custom certificates are created externally and imported to the reader using a secure FTP, as described previously. The certificate and key used by the reader must be in PKCS#12 format (a single .pfx file), while the certificate and keys used by clients interfacing to the LLRP service on the reader must be in PEM format. If you obtain a certificate in a different format it must be converted to the appropriate format using a tools such as OpenSSL (www.openssl.org).

Digital certificates are typically requested and issued from a certification authority hosted internally in an enterprise environment or by a trusted third party certification authority. The process of requesting and creating certificates varies between platforms. For example, a Windows Server environment typically uses Microsoft Certification Server to process certificate requests and issue certificates. Unix-based systems typically use OpenSSL. This guide can not document all options. The following example illustrates one method of creating custom certificates.

Custom Certificate Creation Example

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

Create the following text files in a suitable folder on the host machine:

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

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

Edit configuration options to accommodate the deployment environment.

caconfig.cnf

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


#
#
# Default policy to use when generating server certificates.  The following
# fields must be defined in the server certificate.
#
```

```
[ local_ca_policy ]
commonName              = supplied
stateOrProvinceName     = supplied
countryName             = supplied
emailAddress            = supplied
organizationName        = supplied
organizationalUnitName  = supplied

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

```
[ root_ca_extensions ]
basicConstraints       = CA:true

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

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

[ ssl_client_server ]
basicConstraints       = CA:FALSE
nsCertType             = server, client
keyUsage               = digitalSignature, keyEncipherment
extendedKeyUsage       = serverAuth, clientAuth, nsSGC, msSGC
nsComment              = "SSL/TLS Certificate"
```

samplereader.cnf

```
#
# samplehost.cnf - customized for a reader. Edit last 4 octets after ATR7000 to suit hostname of reader to which certificate is issued
#


[ req ]
prompt                = no
distinguished_name    = ATR7000123456.ds


[ ATR70000657E5.ds ]
commonName            = ATR7000123456
stateOrProvinceName   = IL
countryName           = US
emailAddress          = root@ATR7000123456
organizationName      = Company Name
organizationalUnitName  = Department Name
```

samplehost.cnf

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


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


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

InitRootCA.sh

```
#Initialize from current directory

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

#export OPENSSL_FIPS=1

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

#Make sure CA key password is unique and secret

export CA_KEY_PASSWORD=CA-abcd12345

#Cleanup Certificate Store folder

rm -rf $WORKSPACE_DIR/CA-Certs

#Change directory to CA-Certs and create folders for certificate and key storage in myCA

mkdir -p $WORKSPACE_DIR/CA-Certs

cd $WORKSPACE_DIR/CA-Certs

mkdir -p myCA/signedcerts

mkdir -p myCA/private

cd myCA

#Initialize serial number

echo '01' > serial  && touch index.txt

#Create CA private key and certificate

export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf

echo 'Creating CA key and certificate....'

openssl req -x509 -newkey rsa:2048 -out cacert.pem -outform PEM -days 1825 -passout pass:$CA_KEY_PASSWORD

openssl x509 -in cacert.pem -out cacert.crt

echo 'Test Certificate Authority Initialized. CA certificate saved in cacert.crt. Install it to trusted CA certificate store'
```

CreateReaderCert.sh

```
#Initialize from current directory

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

#export OPENSSL_FIPS=1

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

#Make sure passwords are unique and secret

export CA_KEY_PASSWORD=CA-abcd12345

export GENERATED_CERT_KEY_PASSWORD=abcd12345

cd $WORKSPACE_DIR/CA-Certs/myCA

#Create sample reader key and certificate

export OPENSSL_CONF=$WORKSPACE_DIR/samplereader.cnf

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

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

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

echo 'CA Signing reader certificate....'

export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf

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

rm -f tempreq.pem

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

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

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

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

CreateClientCert.sh

```
#Initialize from current directory

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

#export OPENSSL_FIPS=1

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

#Make sure passwords are unique and secret

export CA_KEY_PASSWORD=CA-abcd12345

export GENERATED_CERT_KEY_PASSWORD=abcd12345

cd $WORKSPACE_DIR/CA-Certs/myCA

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

#Create sample client key and certificate

export OPENSSL_CONF=$WORKSPACE_DIR/samplehost.cnf

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

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

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

echo 'CA Signing client certificate....'

export OPENSSL_CONF=$WORKSPACE_DIR/caconfig.cnf

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

rm -f tempreq.pem

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

Script Usage

The following section illustrates how to use the previous scripts 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 without password authentication. SSH keys enable secure, passwordless login to remote servers.

Generating a New SSH Key Pair

Before importing SSH keys into the reader, you need to generate them. This step creates 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).



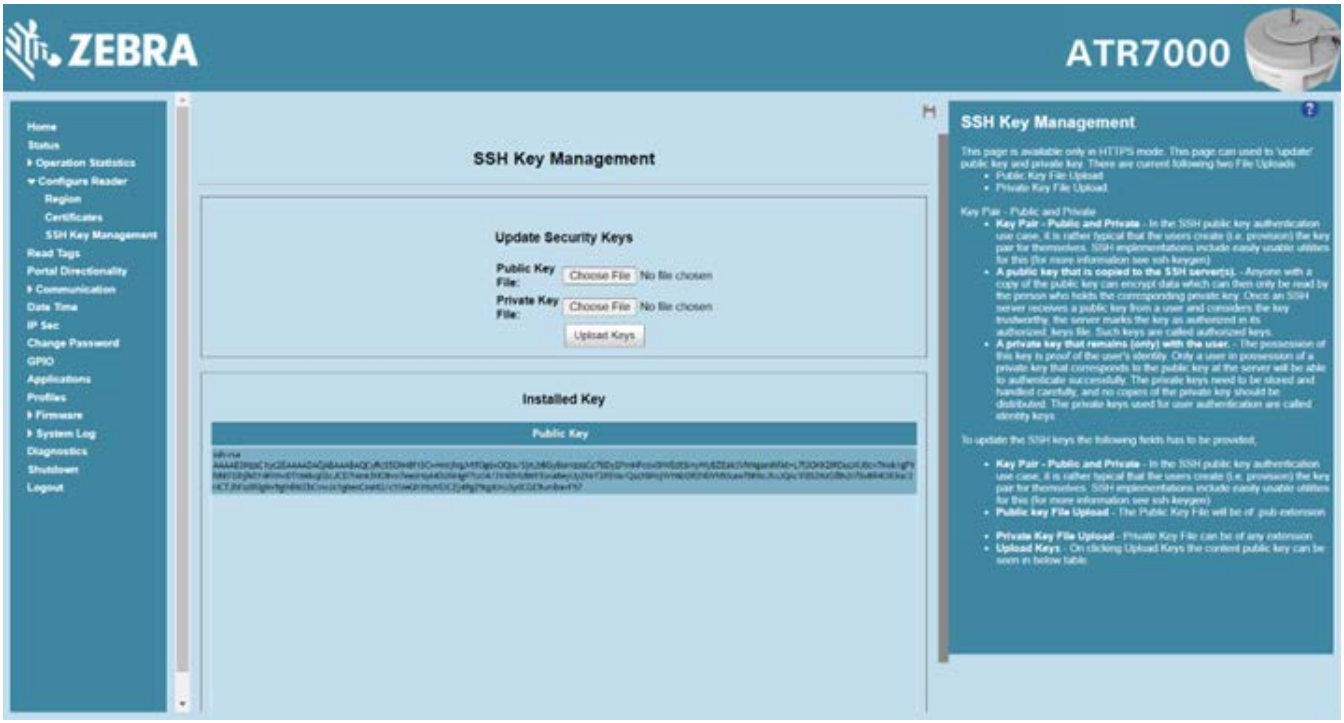
NOTE: FX readers currently support 2048- and 4096-bit RSA SSH keys only.

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).

Once 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**.



NOTE: The current public key is displayed under the **Installed Key** section.

Import both the public and private keys into the reader by selecting **Public Key File** and **Private Key File** and navigating to the appropriate location on your local machine.

When selected, click **Upload Keys** to upload the files to the reader and replace the existing keys.

NOTE: The reader can possess only a single active public SSH key.

The new public key will now be displayed under the **Installed Key** section.

Adding SSH Key to a Remote Server

Adding the SSH key tells the remote server to allow 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. When logged in, append your public key to the server's ~/.ssh/authorized_keys file:
   echo "your_public_key_here" >> ~/.ssh/authorized_keys

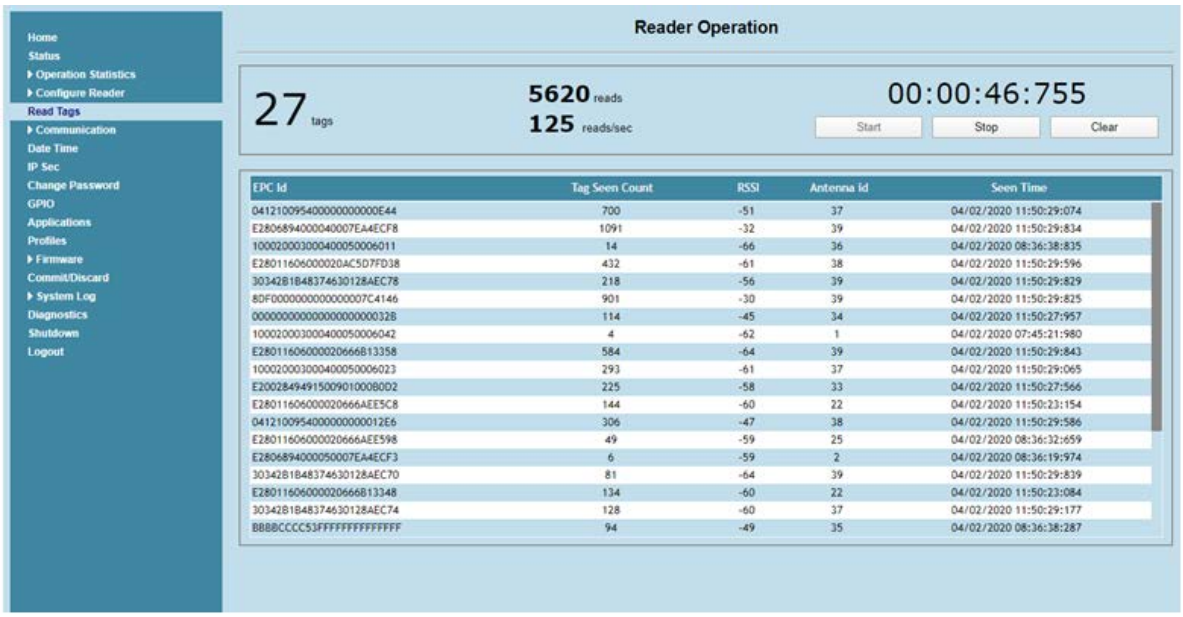
NOTE: The public key begins with “ssh-rsa. Ensure the entire file content is copied.

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 perform an inventory of tags in the field of view of the reader.

Figure 44 Reader Operation



Inventory operation on all tags in the field of view is initiated by clicking the Start button. Inventory is performed on all virtual antennas of the ATR7000. Statistics on total unique tags read, total number of inventory responses, and read rate is displayed.

For each inventoried tag, its EPC ID, number of times the tag was seen, peak RSSI of tag's response, virtual antenna on which tag was observed, and the last seen timestamp are displayed in a table.

The Inventory operation is continuous and may be stopped by clicking the Stop button.

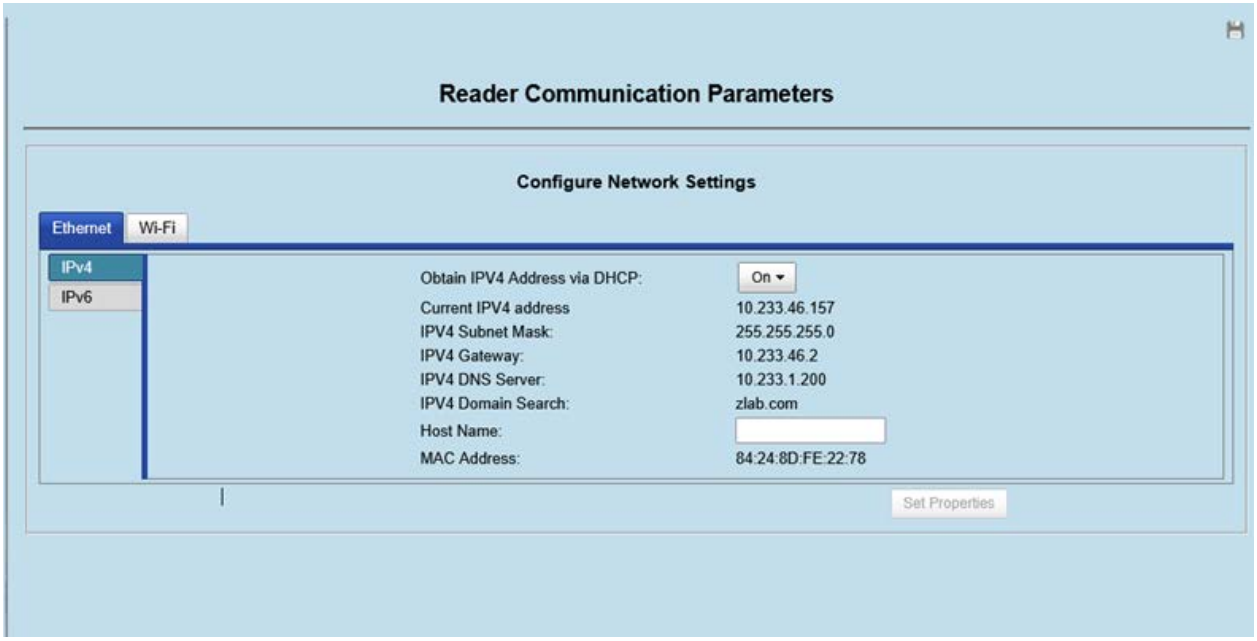
Current inventory statistics are cleared by clicking the Clear button.

Communication Settings

Select **Communication** to view the **Configure Network Settings** window.

Configure Network Settings with Ethernet

Figure 45 Configure Network Settings - Ethernet



IPV4

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

- **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

NOTE: Also enable automatic configuration for IPV6 through RA packets configuration. To enable or disable RA packet configuration go to the Services window.

- **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.

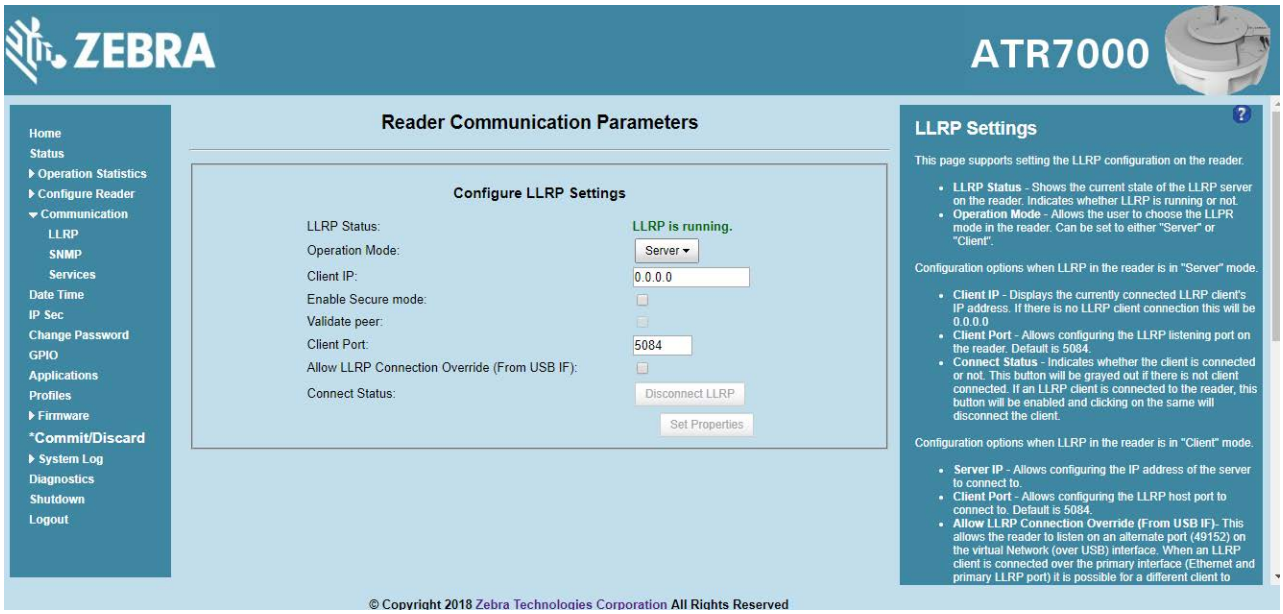
NOTE: You must select Set Properties to update the network configuration. If saving changes is not successful, the system indicates the problem and allows correcting it by repeating the operation. DHCP and IP address updates do apply until the reader is rebooted.

NOTE: Also enable automatic configuration for IPV6 through RA packets configuration. To enable or disable RA packet configuration, go to the Services window.

Configure LLRP Settings

Select **LLRP** to view and set the LLRP settings. By default, LLRP activates in server mode with secure connection enabled, where LLRP clients can connect to the reader using the port number specified in the **Client** port field. The reader can also be configured 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 46 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; click this button to disconnect the client.

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

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

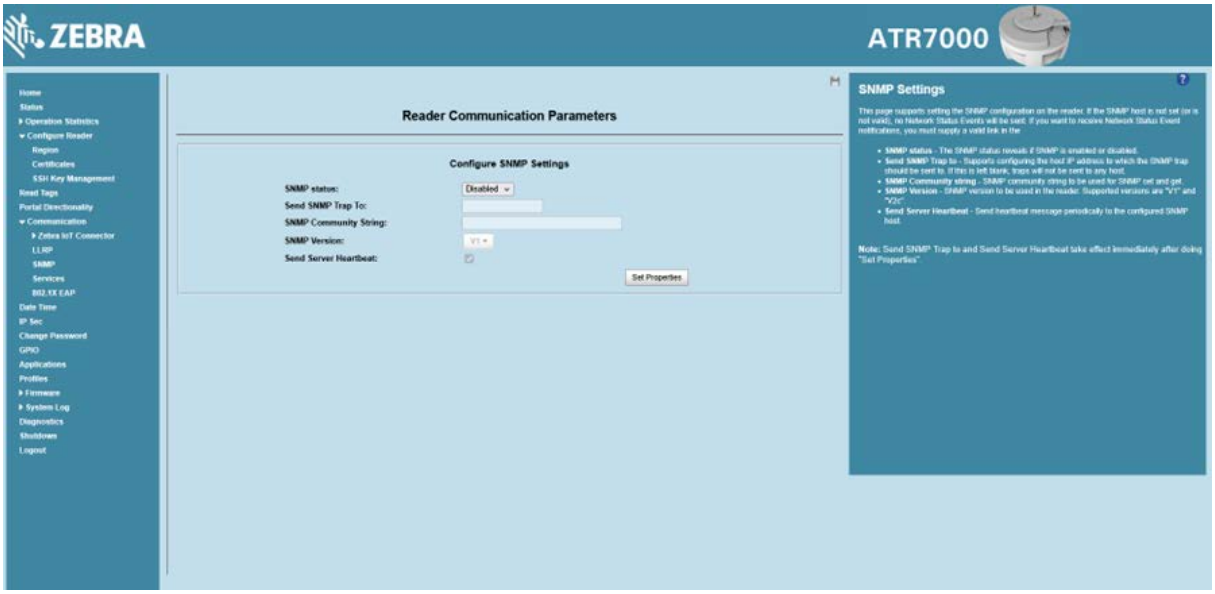
LLRP configuration options when the reader is in **Secure** mode:

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

SNMP Settings

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

Figure 47 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.

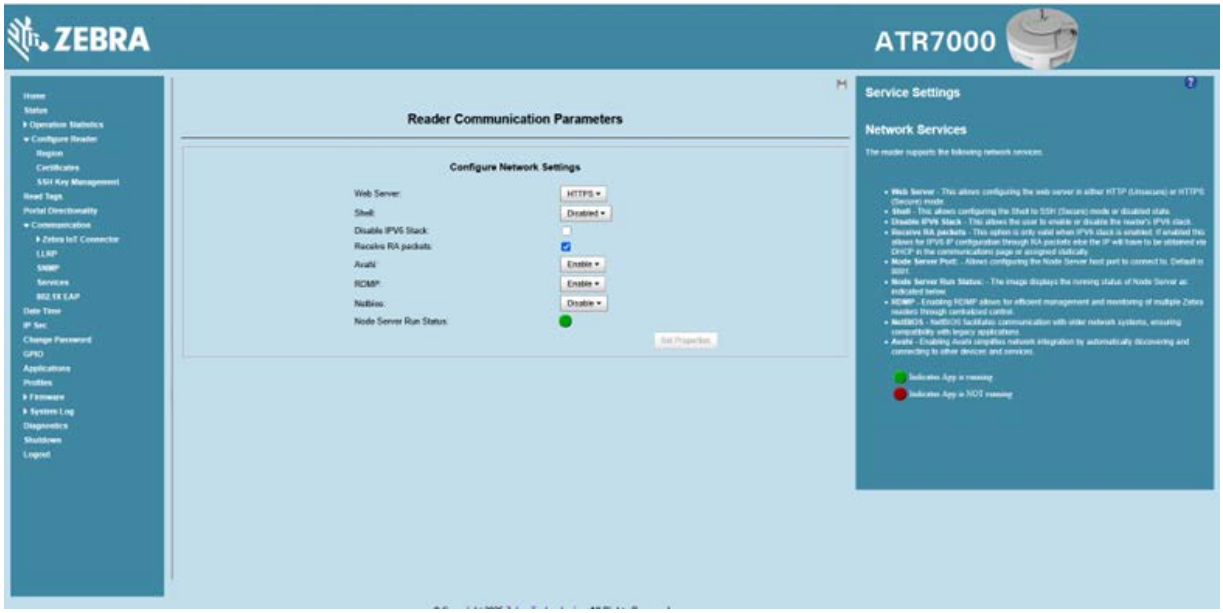
NOTE: **Send SNMP Trap To** and **Send Server Heartbeat** take effect immediately after clicking **Set Properties**. However, perform a **Commit** to persist the changes. The modified **SNMP Community String** and **SNMP Version** are not affected until the reader reboots.

- **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.

Network Services Settings

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

Figure 48 Configure Network Service Settings Window



The reader supports the following network services.

- **Web Server** - Configures the web server in either HTTP (unsecure) or HTTPS (secure) mode.
- **Shell** - Sets the shell to SSH (secure) mode or a disabled state. By default, SSH is disabled.
  - **Enable SSH by setting the rfidadm password from the change password page**. Setting the rfidadm password should satisfy the following criteria:
    - Should contain a minimum of 16 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.

802.1x EAP Configuration

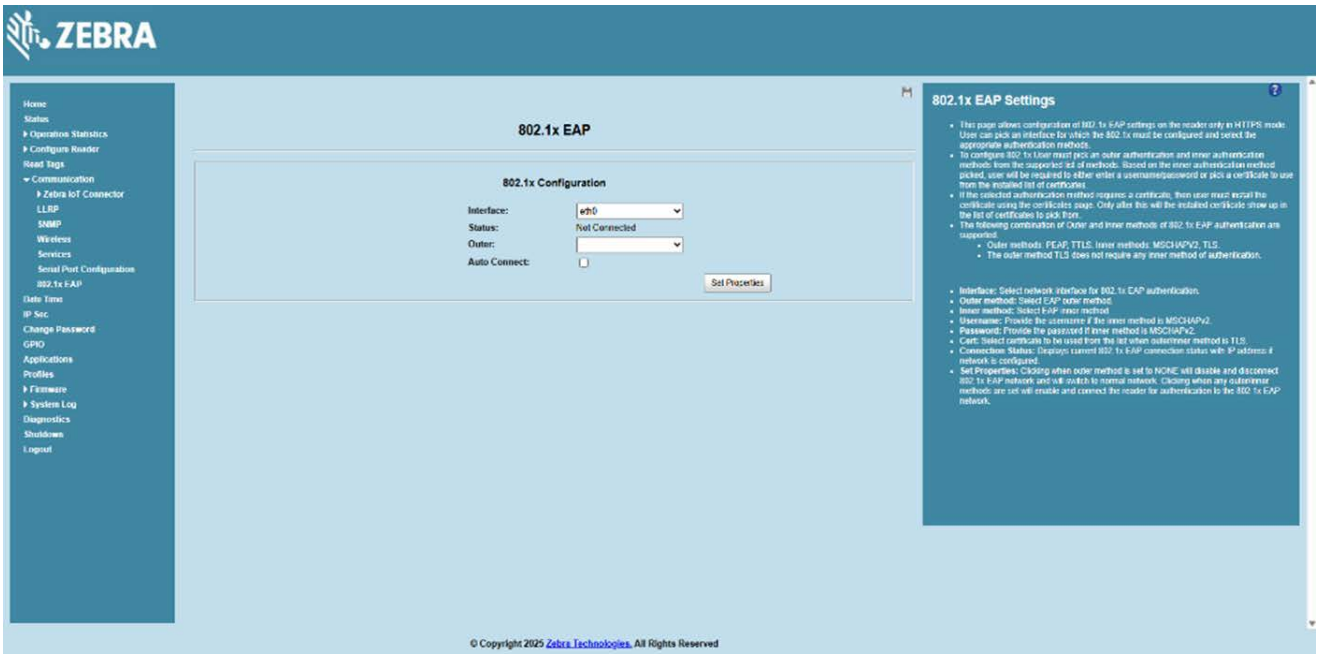
Select **802.1x EAP** to view the 802.1x EAP configuration.

NOTE: The ATR7000 supports 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.

Table 5 802.1x EAP Authentication Methods

Outer Method	Inner Method
PEAP	TLS, MSCHAPV2
TTLS	TLS, MSCHAPV2
TLS	N/A

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.

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 74.

2. Update the IP address and secret password of the Cisco switch at file '/etc/freeradius/3.0/clients.conf' under the section 'client localhost' as seen in the following:

   ```
   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 the 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 PFF 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 the update certificate. See Certificate Configuration on page 54.

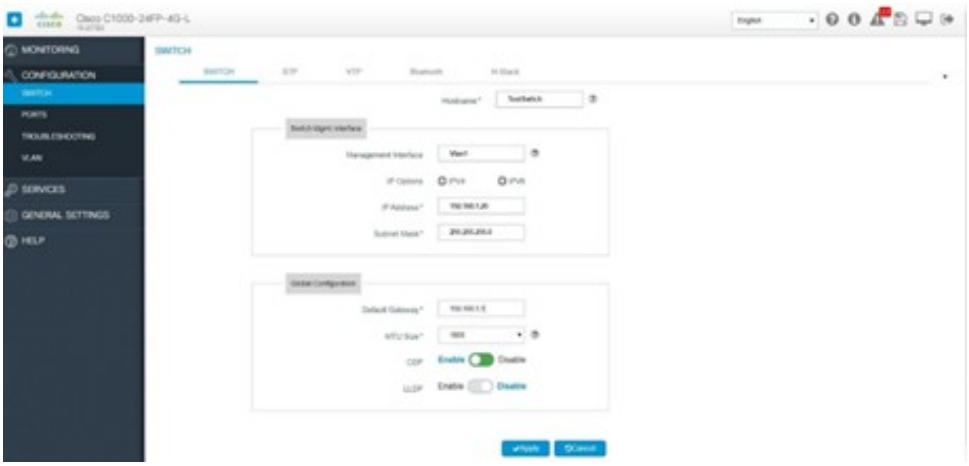
5. Start FreeRADIUS server.

$ sudo freeradius -X

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

The following figure shows configuring the switch with IP address details under the menu: **Configuration > Switch > Switch.**

Figure 50 Switch Configuration with IPAddress



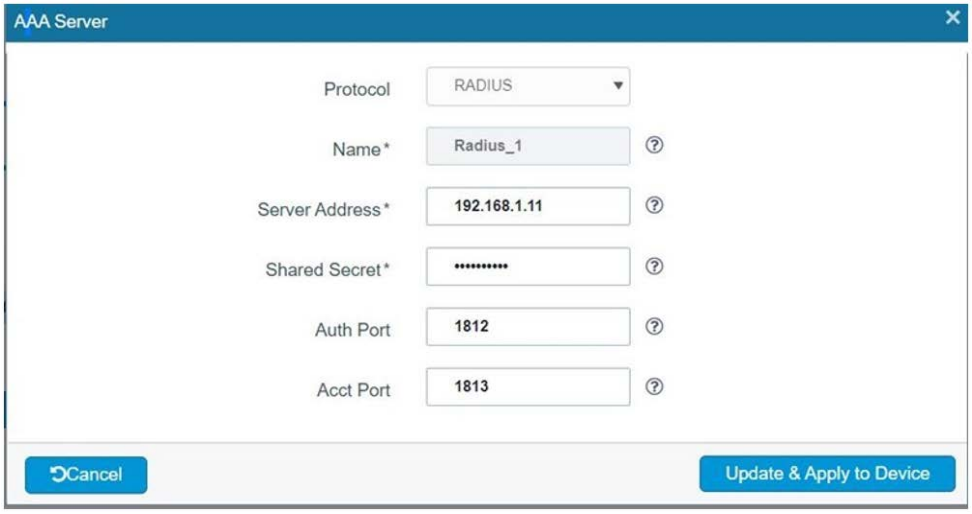
The following figure shows configuring Radius server details in switch under menu: **Services > Security > AAA Server > Server > +Add**.

Figure 51 Configuring Radius Server



NOTE: Add the IP address of FreeRADIUS to the Server Address field, and utesnng123 to the Shared Secret, while using the port details as seen in the following. Shared Secret is already mentioned in file '/etc/freeradius/3.0/clients.conf' under the section client localhost, while configuring FreeRADIUS at Ubuntu 11.00 x18_80 host.

Figure 52 AAA Server Settings



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 54 for more information.
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 74.

NOTE:

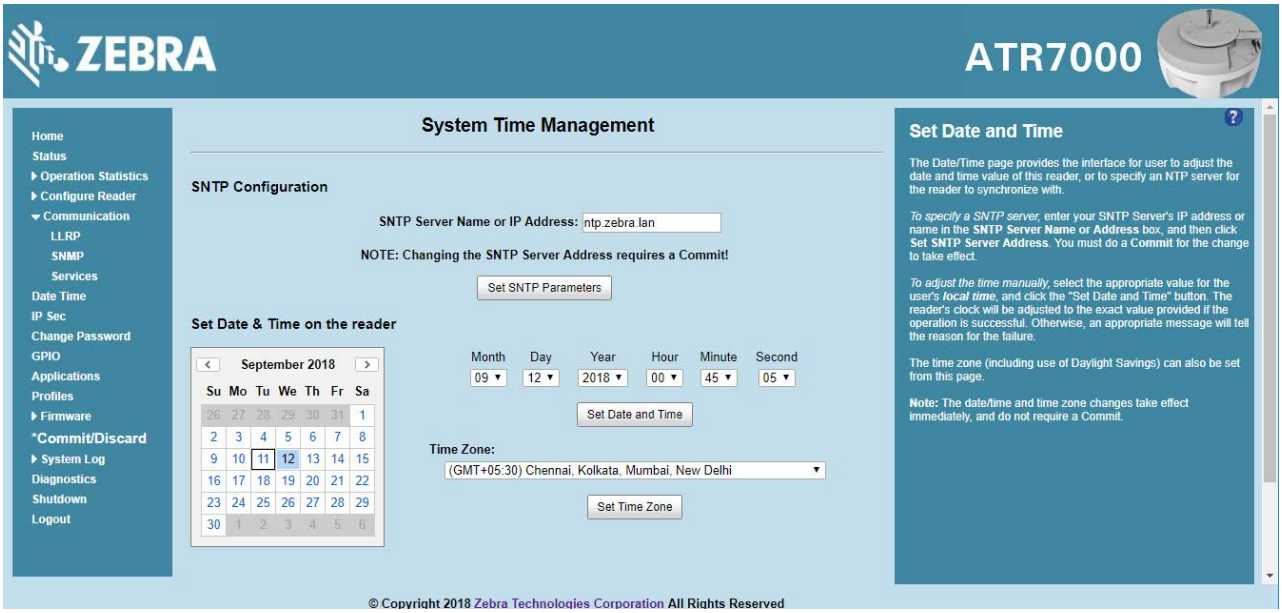
- Both the FX Reader and FreeRADIUS server must be synchronized for date and time, or certificate base 802.1x authentication like TLS for to work and on generating certificate at Ubuntu x86_64 host.
- Following 802.1x EAP outer/inner authentications are successful with FreeRADIUS server:
  1. PEAP/MACHAPv2
  2. TTLS/MSCHAPv2
  3. TLS
  4. TTLS/TLS

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.

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

Figure 53 System Time Management Window



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

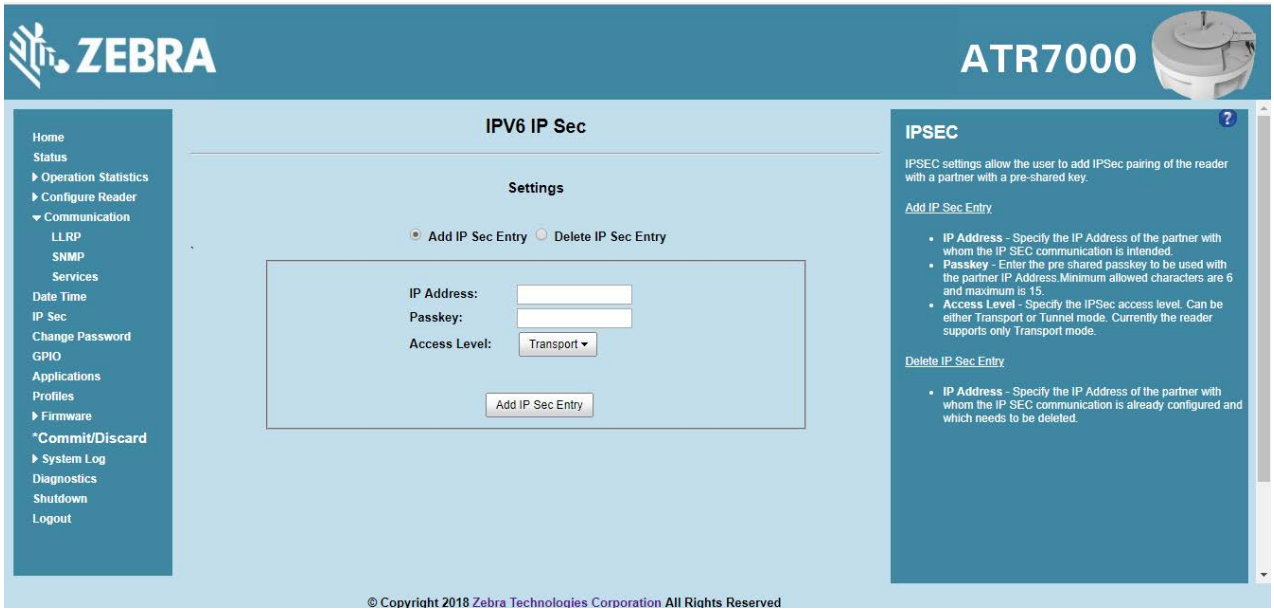
To adjust the time manually, select the appropriate value for the user's local time, and click the Set Date and Time button. This adjusts the reader's clock to the value provided if the operation is successful. Otherwise, an appropriate message indicates the reason for the failure.

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

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 54 IPV6 IP Sec Window



To add an IP Sec entry:

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

To delete an IP Sec entry:

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

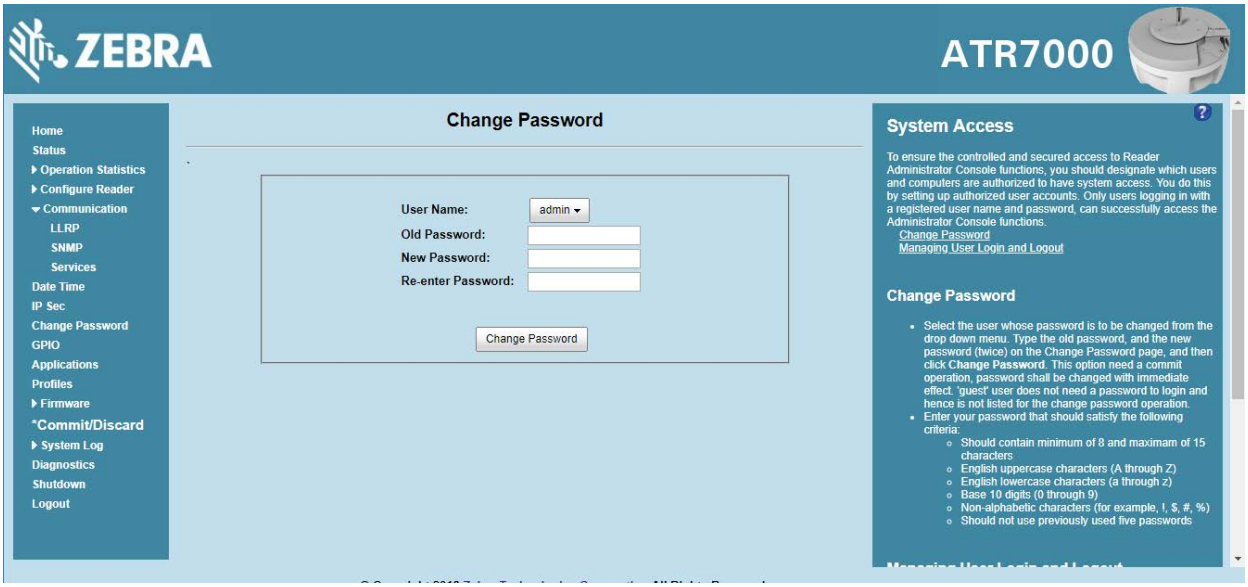
ATR7000 User Accounts

The ATR7000 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
  - Must include at least one digit [0,6,43,etc.]
  - Must include at least one special character [@,%,$,#]
  - Must include at least one uppercase letter [H,J,L,etc.]
  - Must include at least one lowercase letter [w,r,cs,etc.]
- **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 55 Change Password Window



To set a user password:

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

Managing User Login and Logout

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

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

GPIO

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

NOTE: The ATR7000 has two inputs and three outputs.

Figure 56 GPIO Control Window



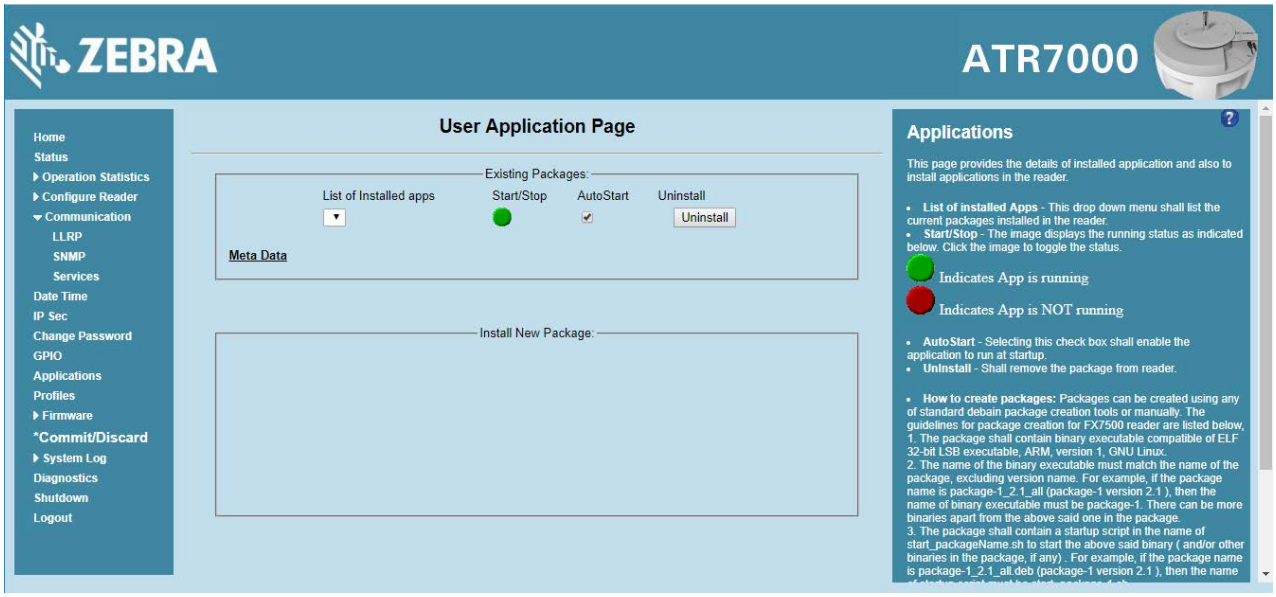
- **Settings** - Map the reader GPI and/or GPO with the host GPIO. Select **Host** for **GPIx** or **GPOx** where *x* = 0 or 1. An attempt to violate this condition changes the selection to either **Host GPIx** or **Host GPOx** automatically. The settings are disabled if a configuration is not supported.

- **Status** - To set a GPO pin high or low, click on the image next to the required pin number:
  - Green  indicates GPIO HIGH
  - Red  indicates GPIO LOW
  - Yellow  indicates GPIO unknown
- **GPI Debounce Time** - Enter a value of up to 1000 milliseconds to minimize spikes that can occur when a device connects to the GPIO port of the reader. The default is 50. Debounce time applies to all input pins, and pins must work independently of each other. Events and callback functions occur only after the debounce time expires, provided the pin state remains at the same level for the debounce time duration. GPIO debounce does not impact GPO and input operations when set to 0.
- **Set Properties** - Click this when all selections are made.

Applications

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

Figure 57 User Application Window



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

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

To create packages for the ATR7000 reader, use any of the standard Debian package creation tools, or create them manually. *The FXSeries 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 ATR7000 User Accounts on page 81 for information on **rfidadm** user privileges.

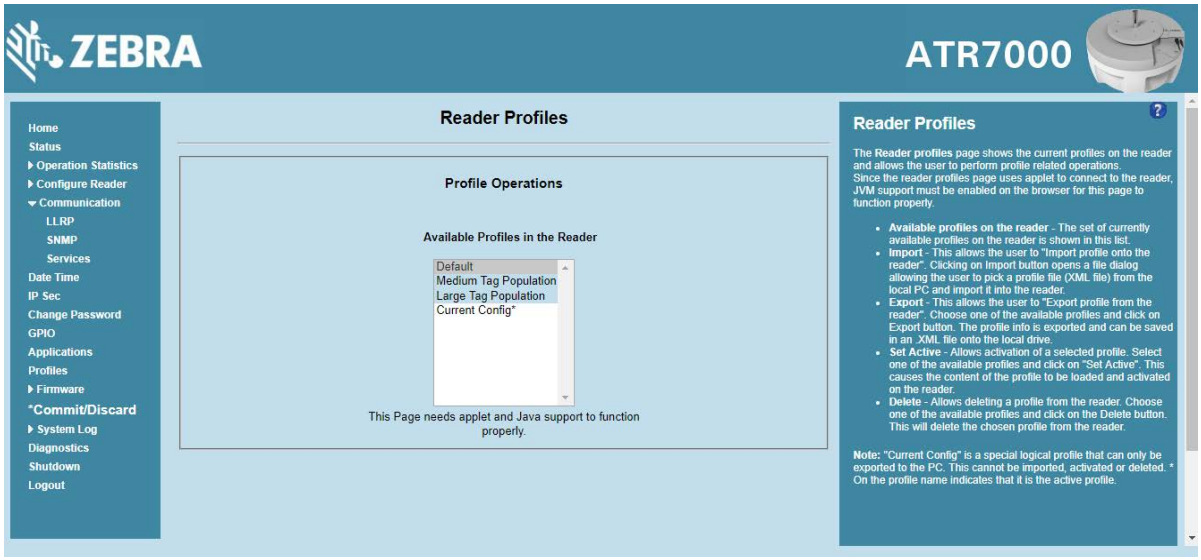
Reader Profiles

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

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

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

Figure 58 Reader Profiles Window



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.

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.

The **Reader Profiles** window functions are:

- **Available Profiles in the Reader** - Displays the available reader profiles.
- **Import** - Click to open a file dialog and pick a profile (XML file) from the local PC and import it into the reader.
- **Export** - Select an available profile and click **Export** to export profile information and save an XML file onto the local drive.
- **Set Active** - Activates a selected profile. Select an available profile and click **Set Active** to load the profile content in the reader.
- **Delete -** Select an available profile and click **Delete** to delete the 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 ATR7000 supports FIPS 140-2 Level 1 for the following interfaces.

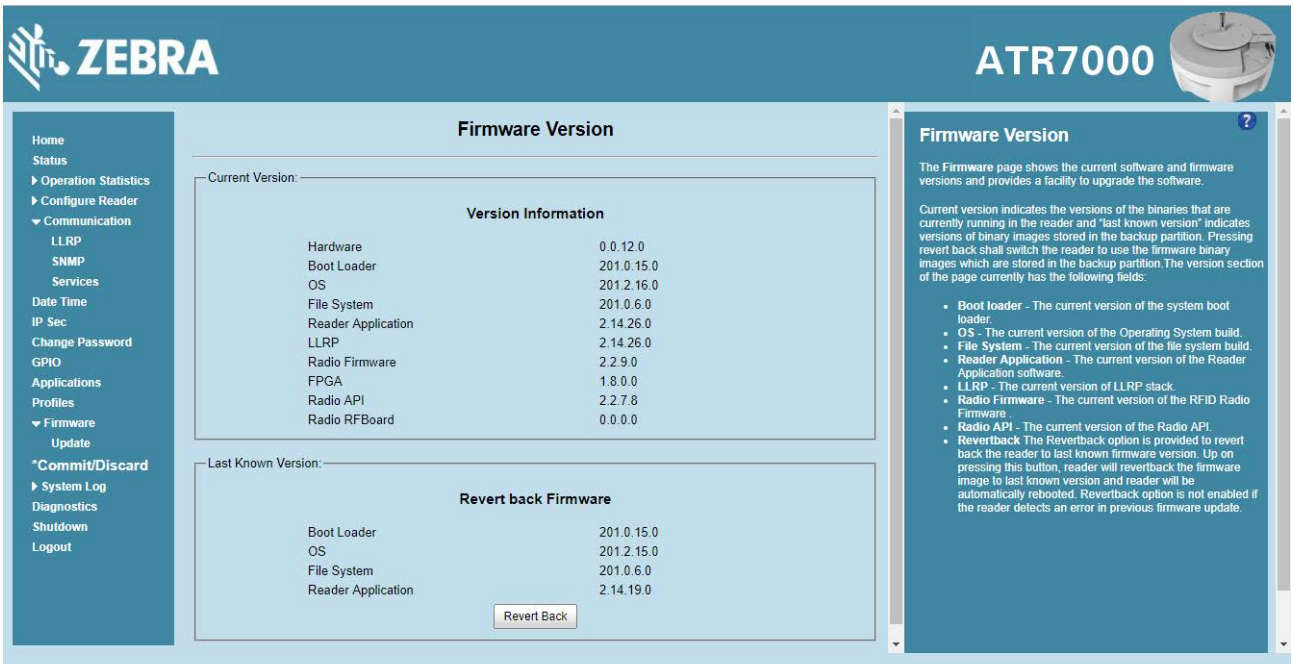
- HTTPS
- FTPS
- SSH
- LLRP Server
- IPSec

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

Firmware Version/Update

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

Figure 59 Firmware Version Window



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

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

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

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

NOTE: You must be logged in with Administrator privileges in order to access this window. See Change Password on page 81.

The reader supports two different methods of updating the firmware:

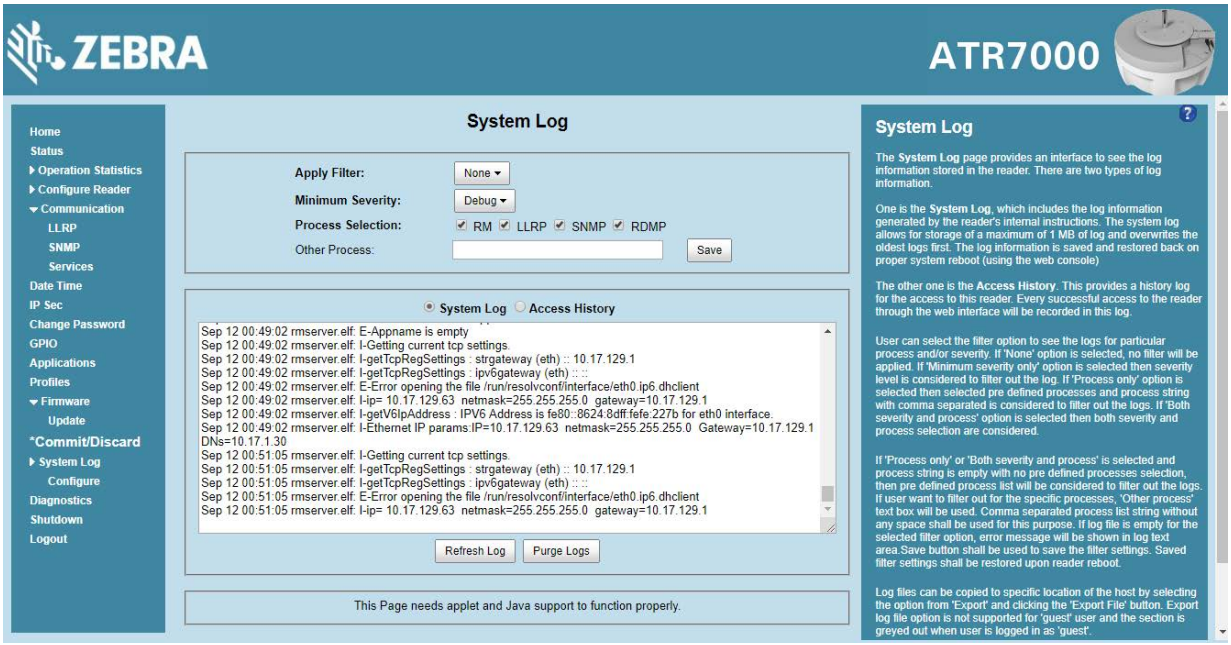
- File-based update that allows uploading the firmware files from the PC (or a network location) to the reader and running the update.
- FTP / FTPS / SCP server-based update.

For instructions on updating the firmware, see Firmware Upgrade.

System Log

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

Figure 60 System Log Window



This window offers the following options:

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

  If you select **Process Selection only** or **Minimum Severity & Process Selection** and the process string is empty with no pre-defined process selection, then the pre-defined process list filters the logs.

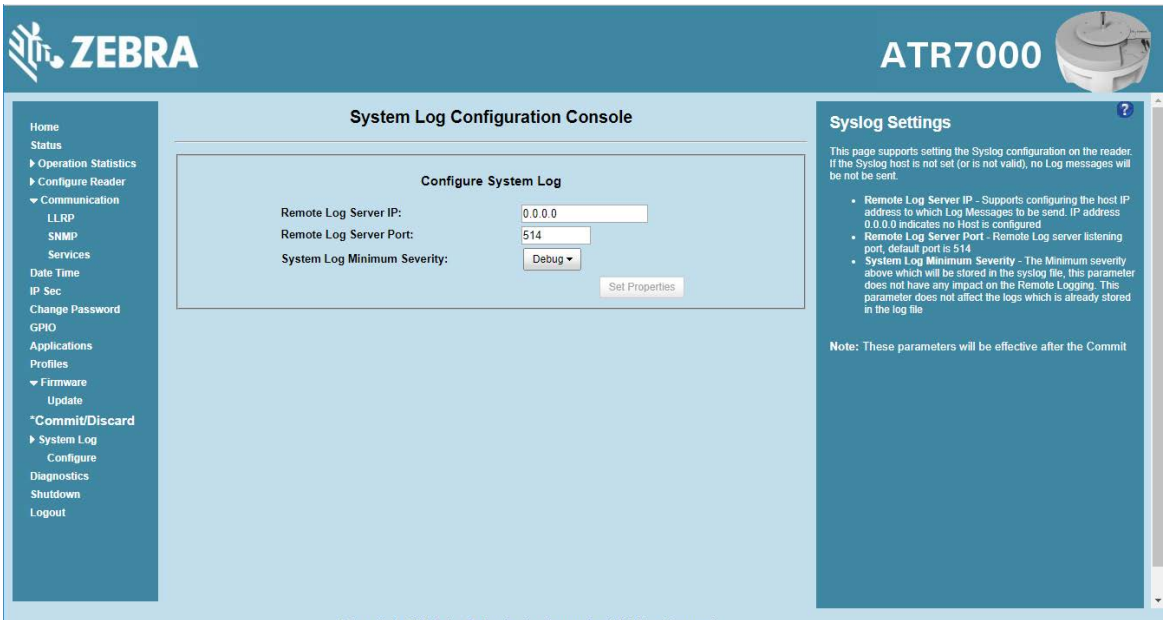
- **Minimum Severity** - Select the severity level on which to filter.
- **Process Selection** - Select the types of processes to filter upon.
- **Other process** - To filter for specific processes, enter the process in this text box using a comma-separated process list string with no spaces. If the log file is empty for the selected filter option, an error message appears in the log text area. Click **Save** to save the filter settings, which persist upon reader reboot.

- **Log area** - Select a radio button for one of the two types of log information offered:
  - **System Log** - Includes the log information generated by the reader internal instructions. This stores up to 1 MB of log information, and overwrites the oldest logs first. The log information is saved and restored on proper system reboot (via the Administrator Console).
  - **Access History** - Provides a history log for reader access, including every successful access to the reader through the Administrator Console.
- Select the **Refresh Log** to refresh the information in the log, or **Purge Logs** to clear the information.
- To copy the log file to a specific location on the host select an option from the **Export** drop-down. Enter the location in the **File Path** field, then select the Export File button.

Configure System Log

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

Figure 61 Configure System Log Window



This window offers the following options:

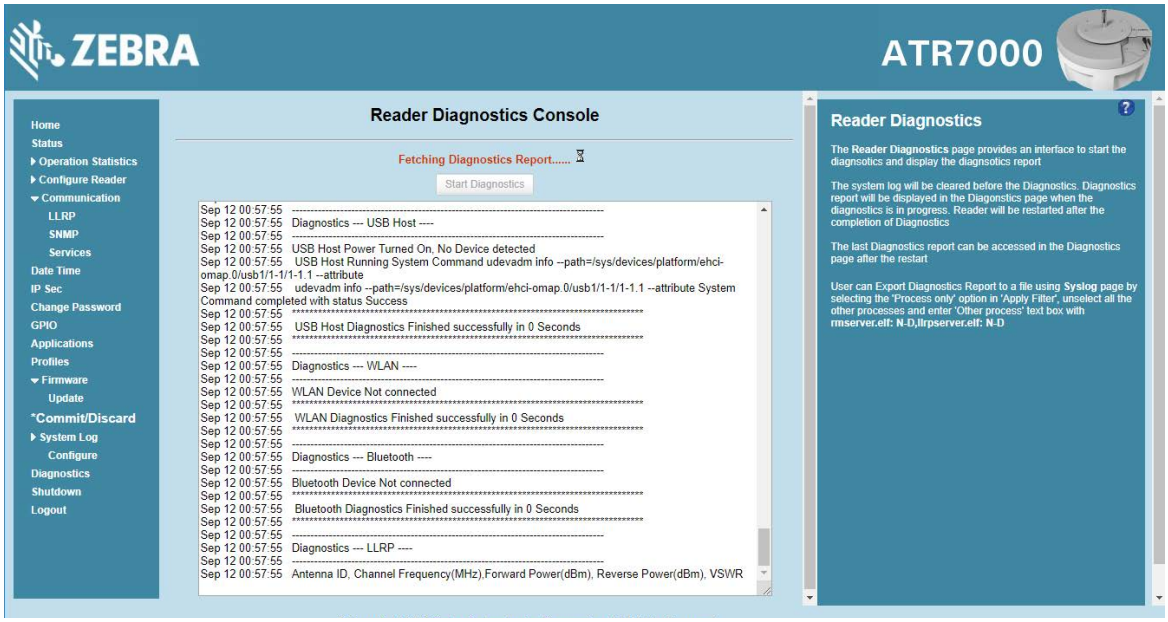
- **Remote Log Server IP** - Configures the host IP address to which log messages are sent. IP address 0.0.0.0 indicates that no host is configured.
- **Remote Log Server Port** - Remote log server listening port. The default port is 514.
- **System Log Minimum Severity** - The minimum severity above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

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

Reader Diagnostics

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

Figure 62 Reader Diagnostics Window



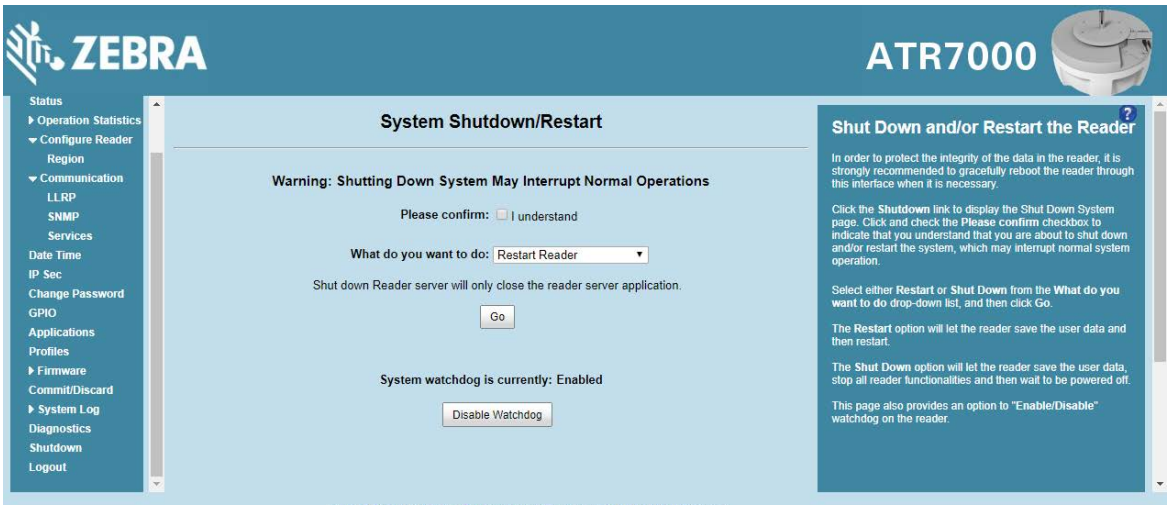
Selecting **Start Diagnostics** clears the system log and displays the diagnostics report. The reader reboots when the diagnostics completes. Return to the **Diagnostics window to view the** diagnostics report.

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

Shutdown

Reader settings in LLRP allow tags that have been read by reader, but not yet reported to the user to be saved on the reader. However, such tag data is lost if reader is powered off abruptly. To protect the integrity of the reader data, gracefully reboot the reader via the Administrator Console when necessary. This saves the tags list and restores it on the next reboot in a reportable state.

Figure 63 System Shutdown/Restart Window



To shut down or restart the reader:

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

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

Application Development

Introduction

The ATR7000 RFID reader can host embedded applications, so data can be parsed directly on the reader. Since data is processed in real time at the network edge, the amount of data transmitted to your backend servers is substantially reduced, increasing network bandwidth and improving network performance. Latencies are reduced, improving application performance. And the integration of data into a wide variety of middleware applications is simplified, reducing deployment time and cost. The ATR7000 also provides flexibility for host embedded applications on the reader or on a separate PC.

Reference Guides

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

- RFID Reader Software Interface Control Guide (p/n 72E-131718-xx)
- Programmer's Guide provided with the Zebra RFID SDK. This introductory guide describes how to perform various functions using the RFID3 API set.
- FX Series Embedded SDK Installation Guide provided with the Zebra RFID SDK.
- FX Series Embedded SDK Programmers Guide provides instructions on creating new embedded applications.
- See Related Documents on page 7 for more documentation regarding RFID API and application development.

Compliance and Implications of EU RED for the ATR7000

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 ATR7000.

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 ATR7000

The ATR7000 is 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 ATR7000 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 ATR7000 **PASSES** by implementing strong, authenticated encryption protocols such as **802.1x for Ethernet.**

Best Practice Cryptography (CRY)

This is applicable. The ATR7000 **PASSES** by demonstrating that its encryption methods used are the "best practice".

The standard provides the mandatory rulebook, and Zebra justifies the ATR7000 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

NOTE: If problems still occur, contact the distributor or call the local contact. See Service Information on page 7 for contact information.

Table 6 provides ATR7000 troubleshooting information.

Table 6 Troubleshooting

Problem/Error	Possible Causes	Possible Solutions
Reader LED remains solid red 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 30.
Reader is not reading tags.	The tag is out of its read range.	Move the tag into read range. See Communication Settings on page 69.
	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 30 to view the IP address, or use the host name to connect to the reader.

Table 6 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 7.
Invalid User Name and/or Password.	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 7.
Session has Timed-out.	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 6 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
User name is not correct.	The user name does not match the current user registry (illegal characters, too long, too short, unknown, or duplicate).	Accurately retype the user name.
	User forgot the user ID. Web console supports the following users: - **Admin** (default password is **change**) - **Guest** (no password required) - **rfidadm** - supported over SSH,FTP/FTPS, SCP, but not over **Administrator Console**.	Reset the reader to factory defaults and select **Admin** for user name and enter **change** in the password field to regain access. See Reset to Factory Defaults LED Sequence on page 33.
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 7.
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 33.
The name, serial number, or IP address entered already exists in the system.	The name, serial number, or IP address entered was already used.	Enter a unique value for the new name, serial number, or IP address.

Table 6 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
Another administrator is currently logged in. Try again later.	The system does not allow more than one administrator to log in at a time.	Wait until the other administrator logs out (or times out) before logging in or override the current session with the new one.
Backup configuration file does not exist.	The system cannot revert to a backup configuration unless a backup file exists.	Commit the new configuration to create a backup file.
Failed to confirm the new password.	The system requires entering the password identically two times.	Accurately retype the password twice.
Network configuration change(s) have not been saved.	The user requested log out prior to committing/ discarding the changes made during the session.	Select one of the **Commit/Discard** options.
New password is the same as the old one.	The system requires entering a new password (different from the existing password) during the **Change Password** operation.	Enter a password that is different from the existing password.
Old password is not correct.	The system requires entering the existing password during the **Change Password** operation.	Accurately retype the existing password.
Unspecified error occurred - code: ####	A specific error message is missing for the given status code.	Note the code number, and contact Zebra support. See Service Information on page 7.
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 7.
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.
Could not read complete post message.	The system stopped a POST operation before completion.	Retry the operation, and allow it to complete.

Table 6 Troubleshooting (Continued)

Problem/Error	Possible Causes	Possible Solutions
Unhandled reply type.	The system generated an unexpected value.	Contact Zebra support. See Service Information on page 7.
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 7.
Invalid Device Address.	The device address information (parent) is invalid, missing, or formatted inaccurately.	Contact Zebra support. See Service Information on page 7.
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 7.
The action must be confirmed.	The user must confirm the requested action before it is executed.	Select the confirmation option when issuing this request.
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.
Reader powers up but does not allow network connection for RF operations.	• Regulatory configuration may be incomplete. • Reader not powered from 25W power source. • Power negotiation over PoE was enabled but PoE+ power negotiation failed with the switch.	• Confirm region of operation is correctly configured in Administrative Console. • Check power supply rating if reader is power from a fixed power supply. • If powered from network switch, confirm switch is PoE+ capable and enabled with LLDP negotiation.

Firmware Upgrade

Introduction

This chapter provides reader firmware update information on using the web-based **Administrator Console**. The following methods are available to update the firmware on the ATR7000 reader.

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

Use this procedure to update the following software components:

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

Prerequisites

The following items are required to perform the update:

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

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

Failsafe Update

The ATR7000 reader provides 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 reader LED remains solid red.

Update Phases

The firmware update takes place in three phases:

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

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

```
;platform partition

-t5 -fplatform_1.1.15.0.tar.gz -s8004561 -u8130879
```



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

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

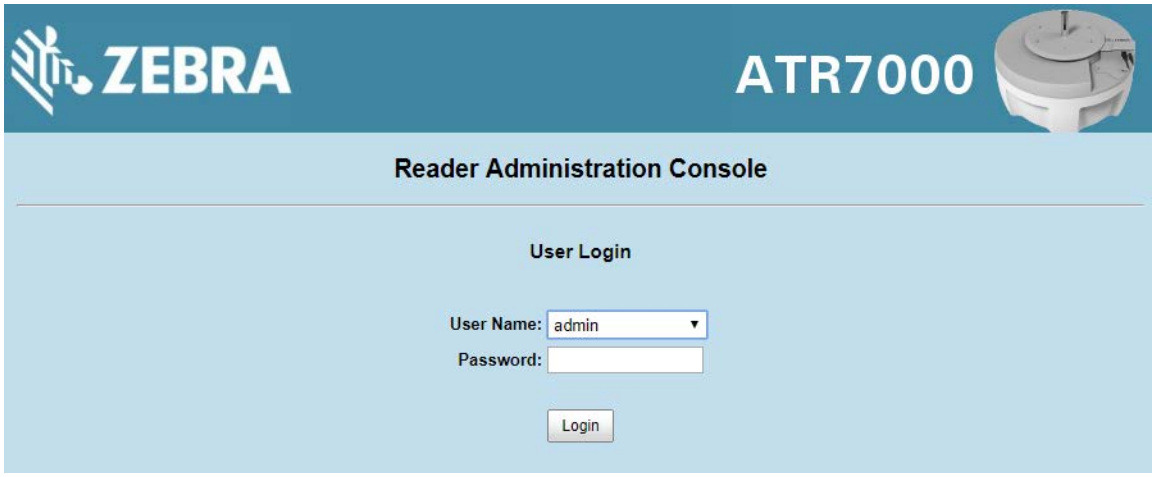
Updating ATR7000 Reader Software

Verifying Firmware Version

To verify that the ATR7000 reader firmware is outdated:

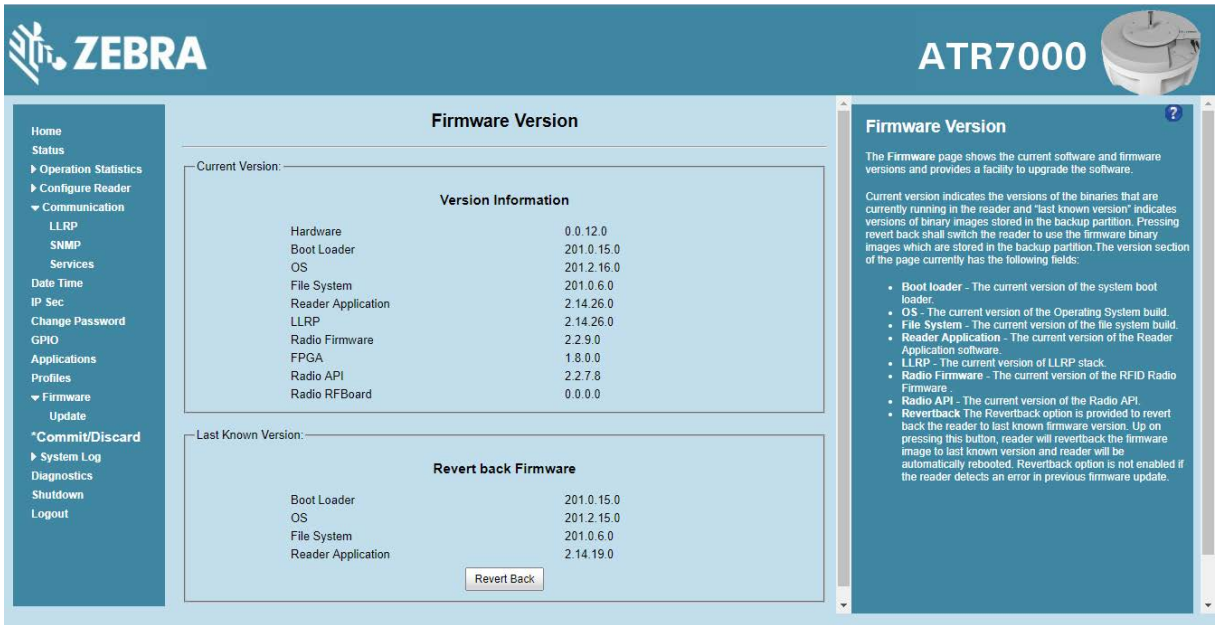
1. Log into the reader. In the **User Login** window, enter **admin** in the **User Name:** field and enter **change** in the **Password:** field.

Figure 64 User Login Window



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

Figure 65 Firmware Version Window



Updating Methods

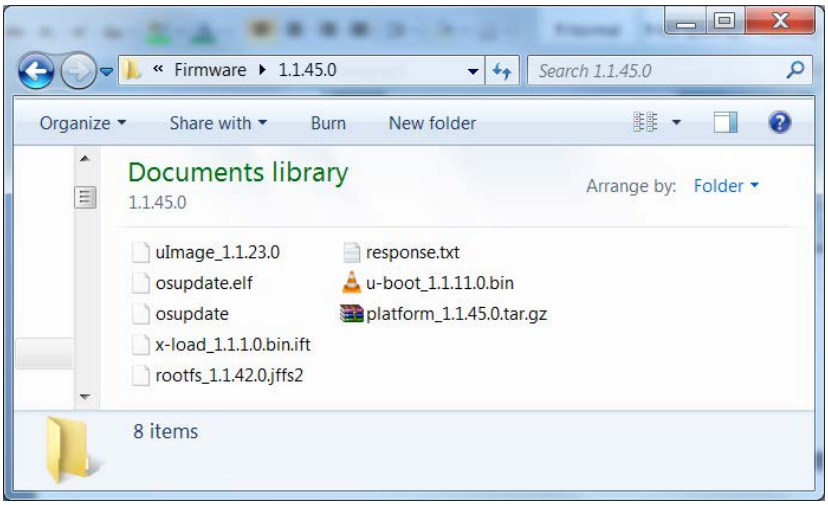
Download the reader update files from www.zebra.com/support, then use one of three methods to update the reader software to a later version, e.g., 1.1.45.0 or higher:

- File-Based Update on page 104
- FTP/SCP-Based Update on page 105 (Recommended)

File-Based Update

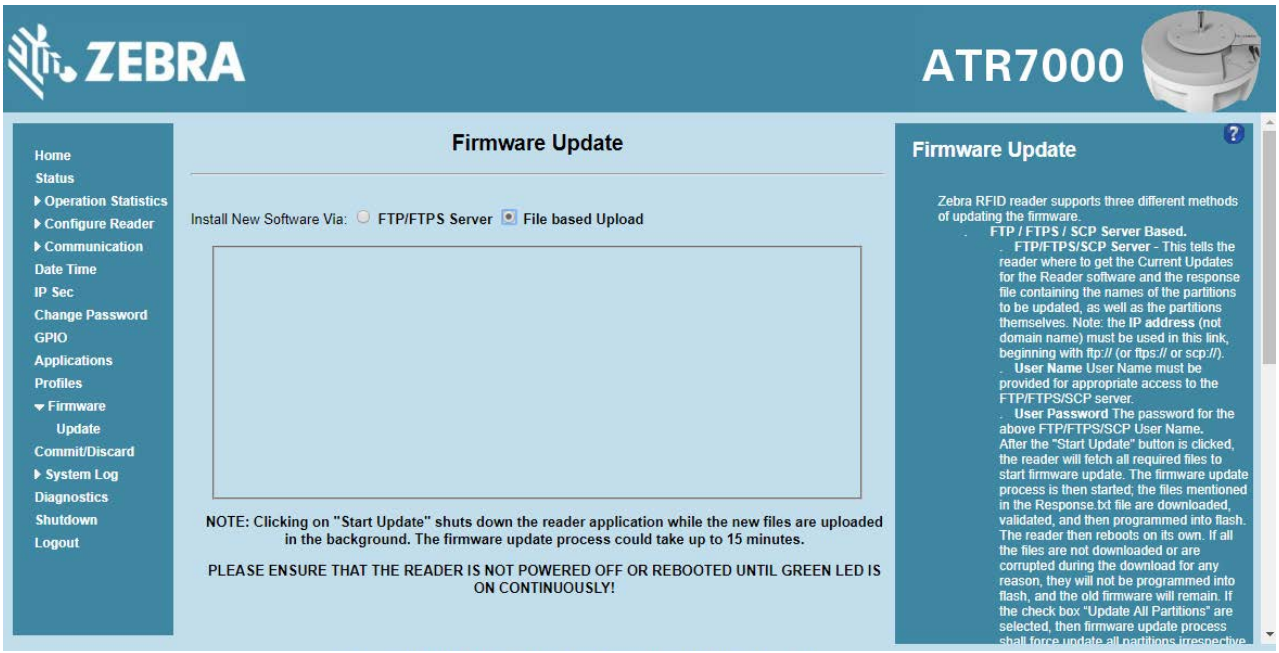
1. Copy all reader update files into any folder on a host computer.

Figure 66 Host Computer Folder



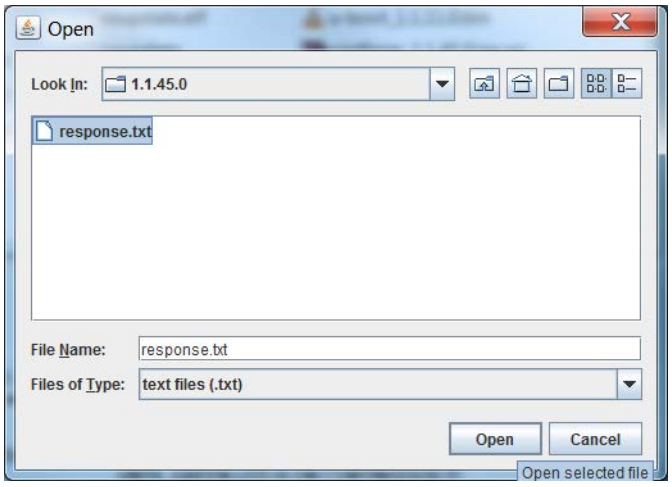
2. Log into the reader and navigate to the **Firmware Update** page.

Figure 67 Firmware Update Window



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

Figure 68 Browsing Update Files



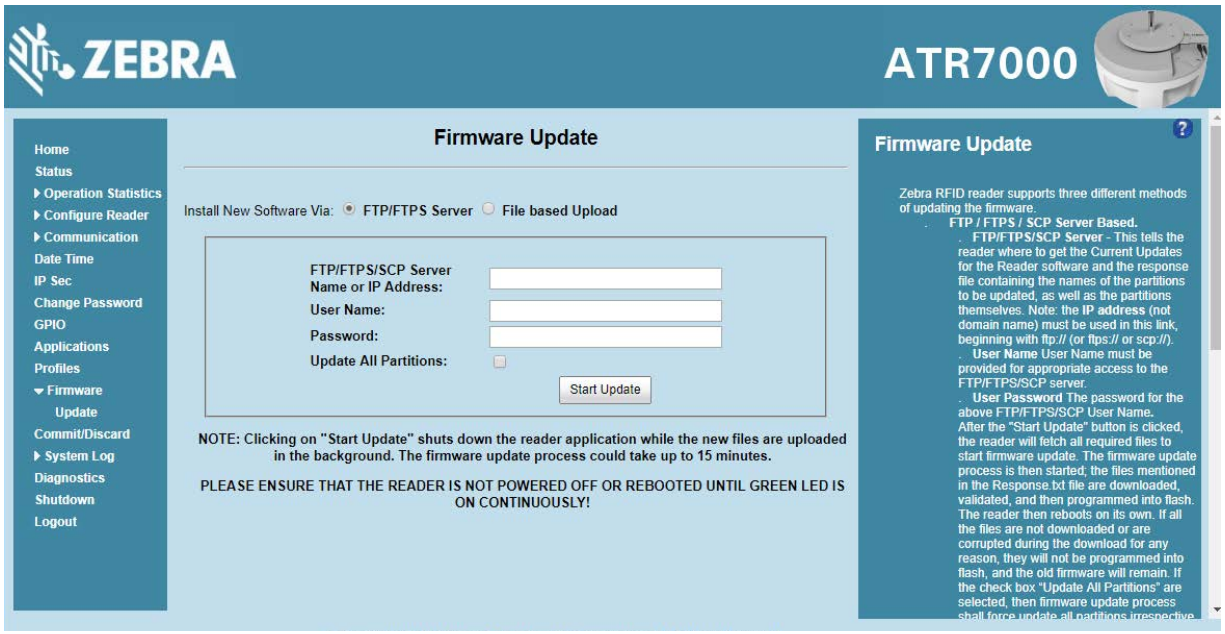
5. Select all files and click **Open**.
6. Click **Start Update**. The reader starts the update process and displays the update status as follows:
   - The reader continuously blinks the power/status LED red.
   - The reader power/status LED remains steady orange.
   - The reader power/status LED settles to a steady green to indicate that the update is complete.
7. When the update completes, the reader reboots and returns to the login screen.

FTP/SCP-Based Update

Copy all the update files into an appropriate FTP location.

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

Figure 69 Firmware Update Window



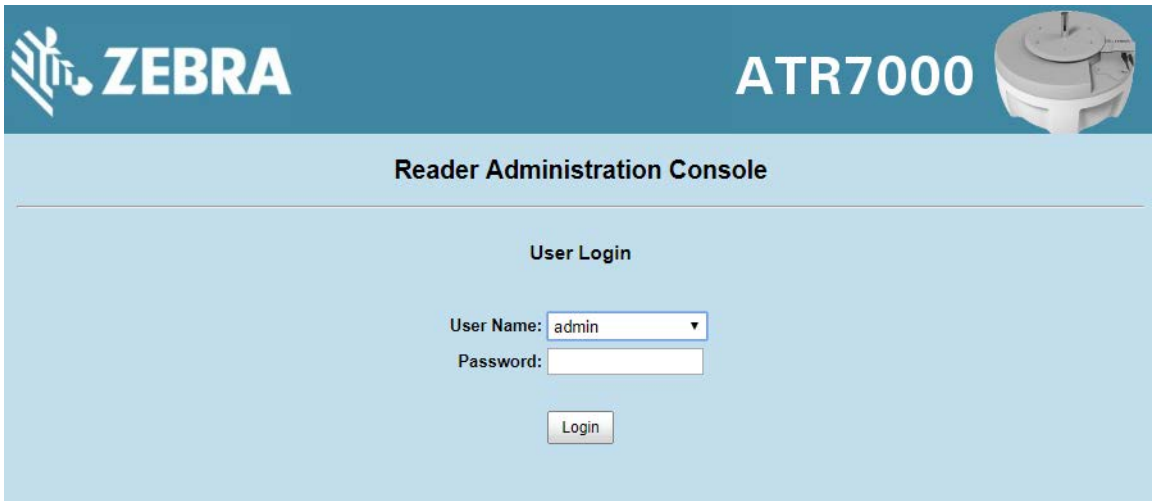
2. Select **FTP/FTPS/SCP Server**.
3. Enter the FTP/FTPS/SCP location where the files are located.
4. Enter the **User Name** and **Password** for the FTP/FTPS/SCP server login.
5. An SSH key-based authentication is possible in the case of an SCP-based firmware update. In this case, the password is not required, provided the reader's public SSH key has already been added to the authorized_keys file of the SCP server serving the files. For more information on how to import SSH keys, refer to SSH Key Management.
6. Click **Start Update**. The reader starts the update process and displays the update status as follows:
   - The reader continuously blinks the power/status LED red.
   - The reader power/status LED remains steady orange.
   - The reader power/status LED settles to a steady green to indicate that the update is complete.
7. When the update completes, the reader reboots and returns to the login screen.

Verifying Firmware Version

To verify reader update success:

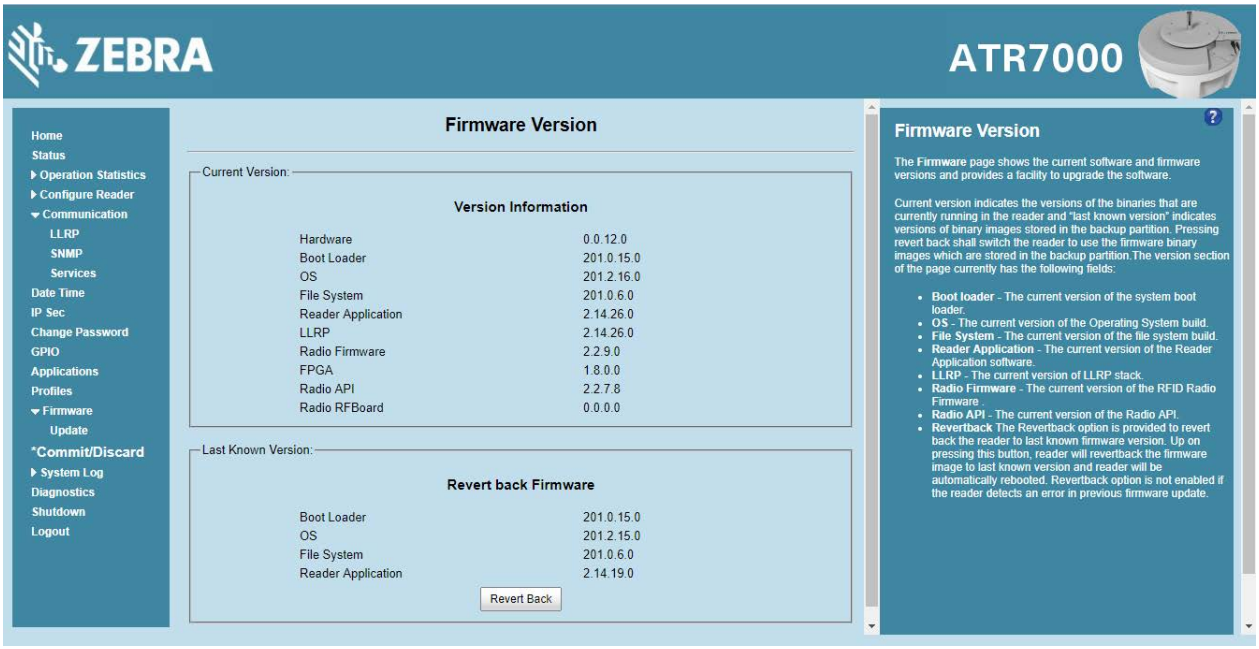
1. Log into the reader. In the **User Login** window, enter **admin** in the **User Name:** field and enter **change** in the **Password:** field.

Figure 70 User Login Window



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

Figure 71 Firmware Version Window



Technical Specifications

Technical Specifications

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

Table 7 Technical Specifications

Item	Description
Physical and Environmental Characteristics	
Dimensions	19 in. Diameter x 6.34 in. Height (48.26 cm Diameter x 16.10 cm Height)
Weight	11.1 lbs ± 0.1 lbs (5.03 kg +/- 0.05 kg)
Visual Status Indicators	Multi-color LED: Power, Activity, Status, and Applications
Mounting	Pole mounted. VESA mount option supports 100 mm x 100 mm and 75 mm x 75 mm with M4 screws.
ATR7000 Environmental Specifications	
Operational Temperature	-4° to +131° F / -20° to +55° C
Storage Temperature	-40° to +158° F / -40° to +70° C
Humidity	5 to 95% non-condensing
Shock and Vibration	MIL-STD-810G
Seal	IP 51
Connectivity	
Communications	10/100 BaseT Ethernet (RJ45) w/ PoE+ support, USB Host (Type A)
General Purpose I/O	2 inputs, 3 outputs, optically isolated (terminal block) External 24 VDC power available for GPIO
Power Input	PoE+ (802.3at) 48 VDC PoE + or 24 VDC Universal Power Supply
Antenna Elements	14 (internal)

Table 7 Technical Specifications (Continued)

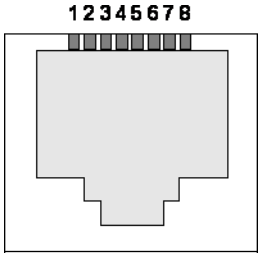
Item	Description
Hardware/OS and Firmware Management	
Memory	Flash 512 MB; DRAM 256 MB
Operating System	Linux
Firmware Upgrade	Web-based and remote firmware upgrade capabilities
Management Protocols	RM 1.0.1 (with XML over HTTP/HTTPS and SNMP binding)
Network Services	DHCP, HTTPS, FTPS, SFPT, SCP, SSH, HTTP, FTP, SNMP and NTP
Network Stack	IPv4, IPv6
Security	Transport Layer Security Ver. 1.2, FIPS 140-2 Level 1
Air Protocols	EPCglobal UHF Class 1 Gen2, ISO 18000-6C
Frequency (UHF Band)	902 MHz to 928 MHz
Beam Scanning Range	Azimuth 0-360 degrees, Elevation 0-60 degrees
Transmit Power Output	16dBm to +36dBm EIRP
Max Receive Sensitivity	-88dBm
Power Consumption	22W, Operational; <4W, Idle
IP Addressing	Static and Dynamic
Host Interface Protocol	LLRP v1.0.1
API Support	Host Applications – .NET, C and Java EMDK; Embedded Applications – C & Java SDK
Warranty	
For the complete Zebra hardware product warranty statement, go to www.zebra.com/warranty.	
Recommended Services	
Support Services	Zebra One Care Select and Zebra One Care On Site
Advanced Services	RFID Design and Deployment Services

Cable Pinouts

10/100bT Ethernet / PoE Connector

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

Figure 72 Ethernet Connections



USB Debug Connector

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

Figure 73 USB Debug Connector

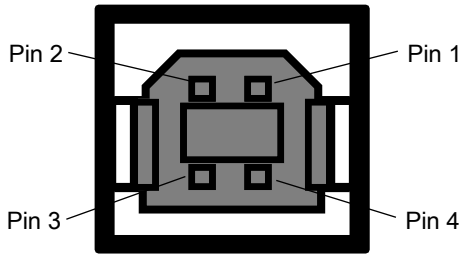


Table 8 USB Debug Port Connector Pinout

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 74 USB Host Connector (J22)

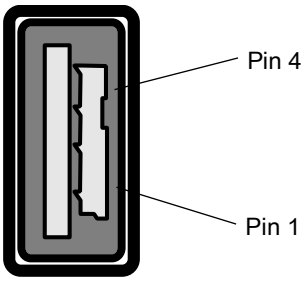


Table 9 USB Host Port Connector (J22) Pinout

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

GPIO Port Connections

The ATR7000 GPIO connector pinouts include the following:

Figure 75 ATR7000 RFID Reader GPIO Connection

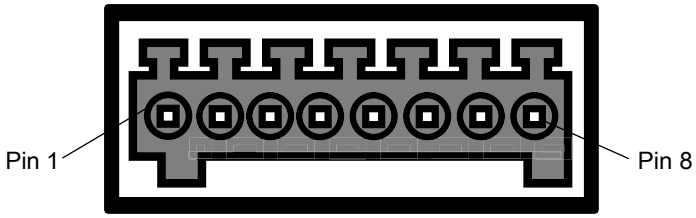


Table 10 ATR7000 GPIO Pin Outs

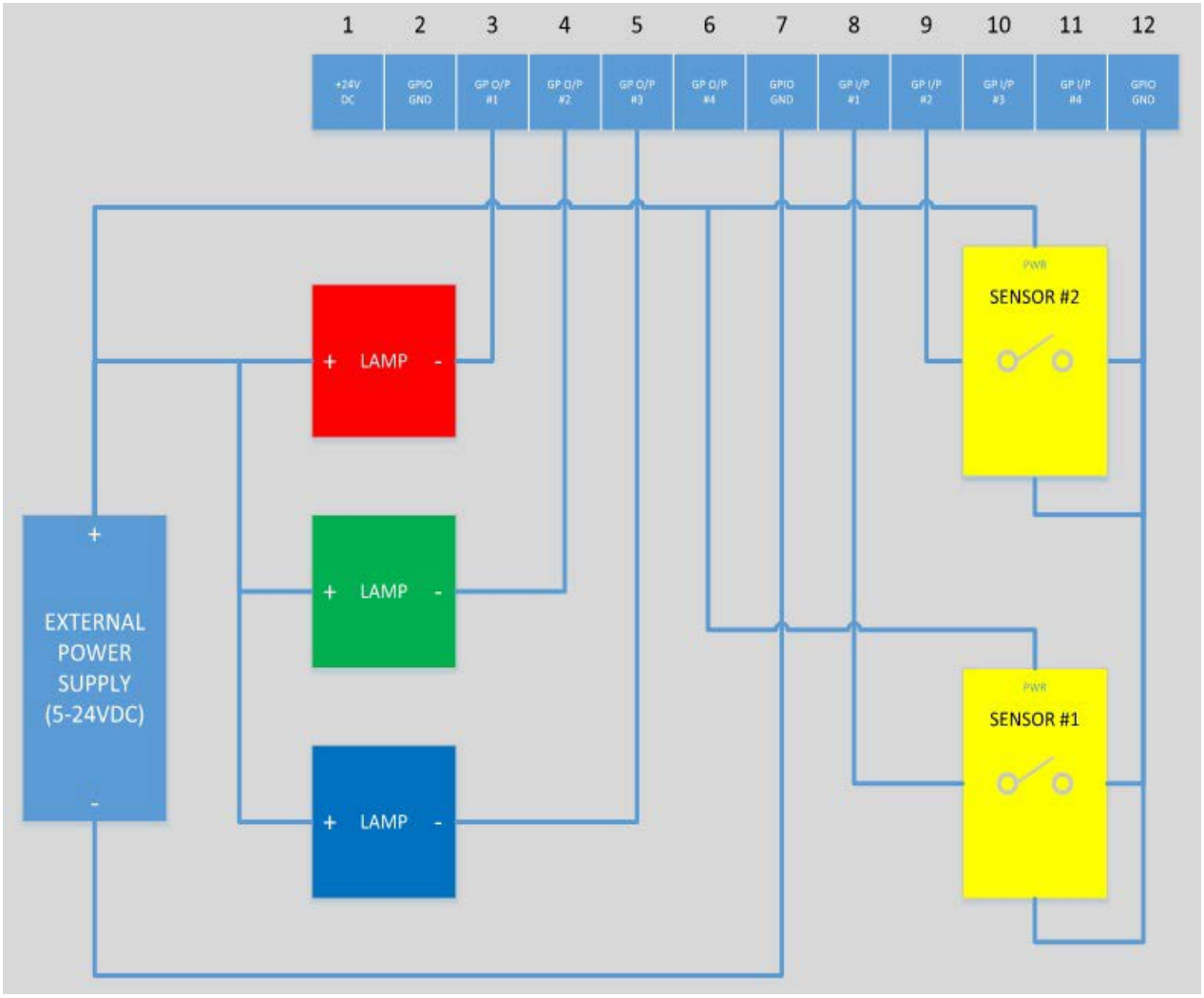
Pin #	Pin Name	Direction	Description
1	+24V DC Power	O	Supplies +24V DC at up to 1 Amp
2	GP output #1	O	Signal for GP output #1
3	GP output #2	O	Signal for GP output #2
4	GP output #3	O	Signal for GP output #3
5	GND	-	Ground connection
6	GP input #1	I	Signal for GP input #1

Table 10 ATR7000 GPIO Pin Outs (Continued)

Pin #	Pin Name	Direction	Description
7	GP input #2	I	Signal for GP input #2
8	GND	-	Ground connection

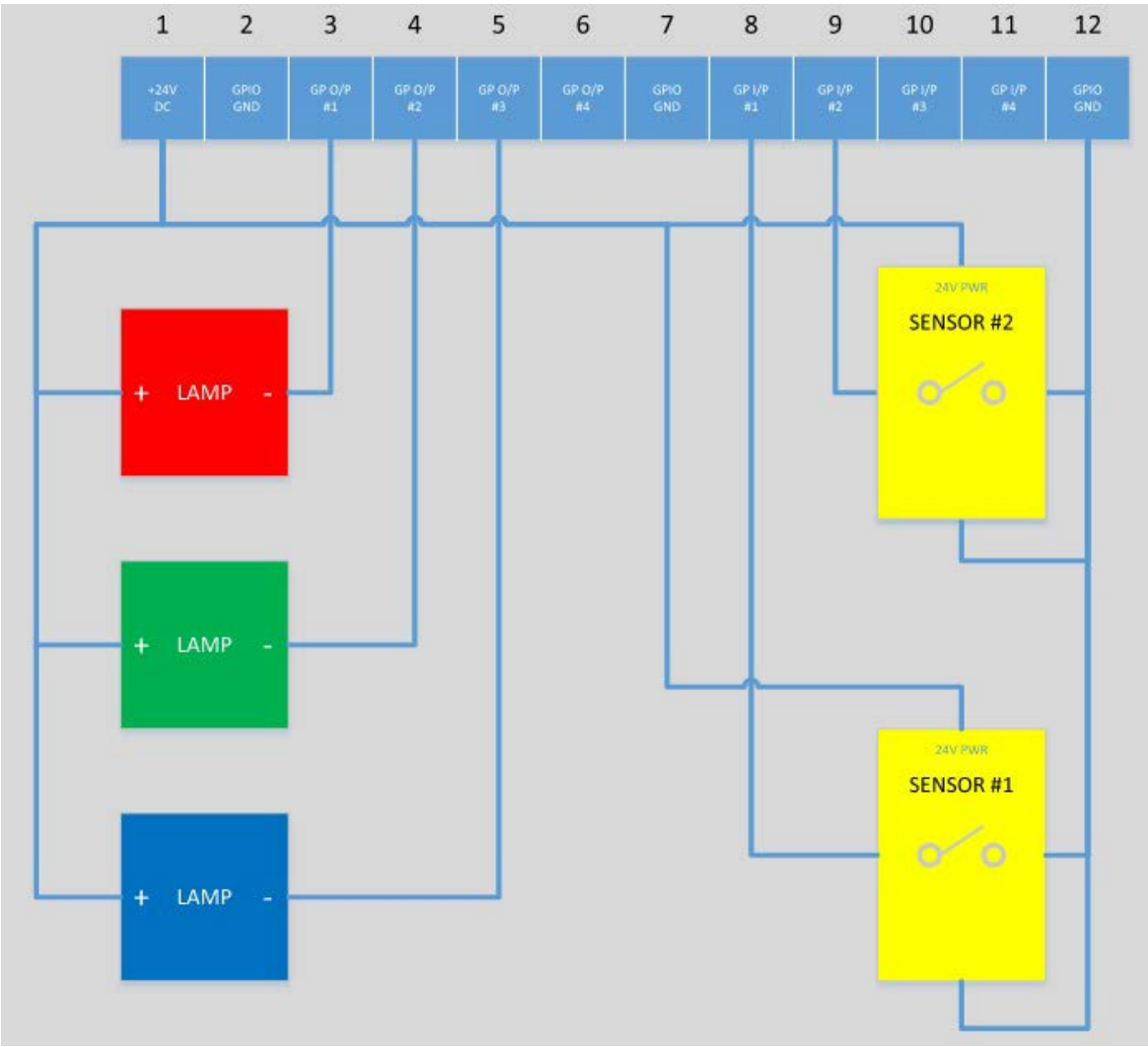
The following figure provides an example of a typical GPIO setup with the power derived from an external power supply.

Figure 76 ATR7000 GPIO Setup Example with Power Derived from External Power Supply



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

Figure 77 ATR7000 GPIO Setup Example with Power Derived from GPIO 24V Pin



Static IP Configuration

Introduction

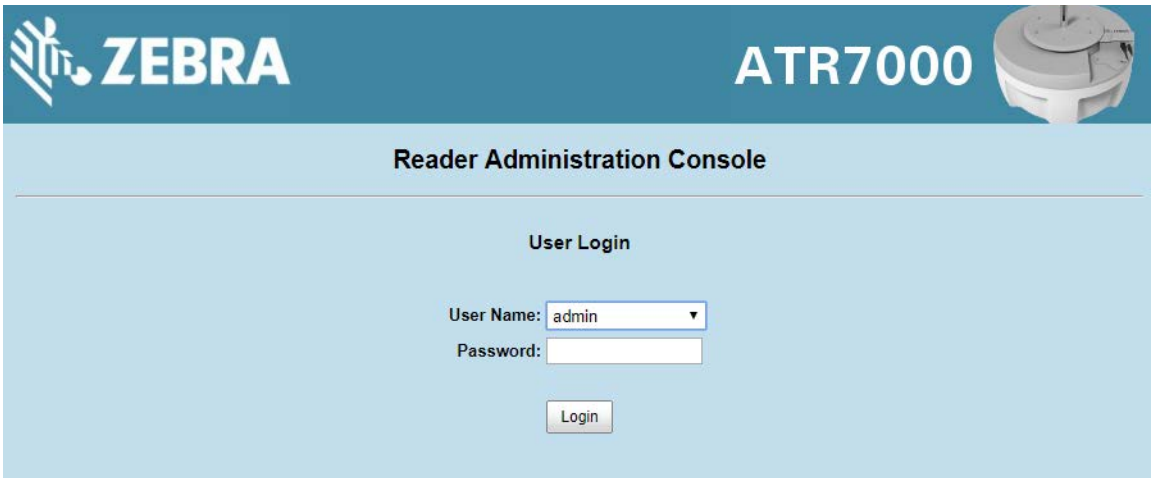
This chapter describes three methods of setting the static IP address on an ATR7000 RFID reader.

Reader IP Address or Host Name is Known

To set the Static IP using the web console:

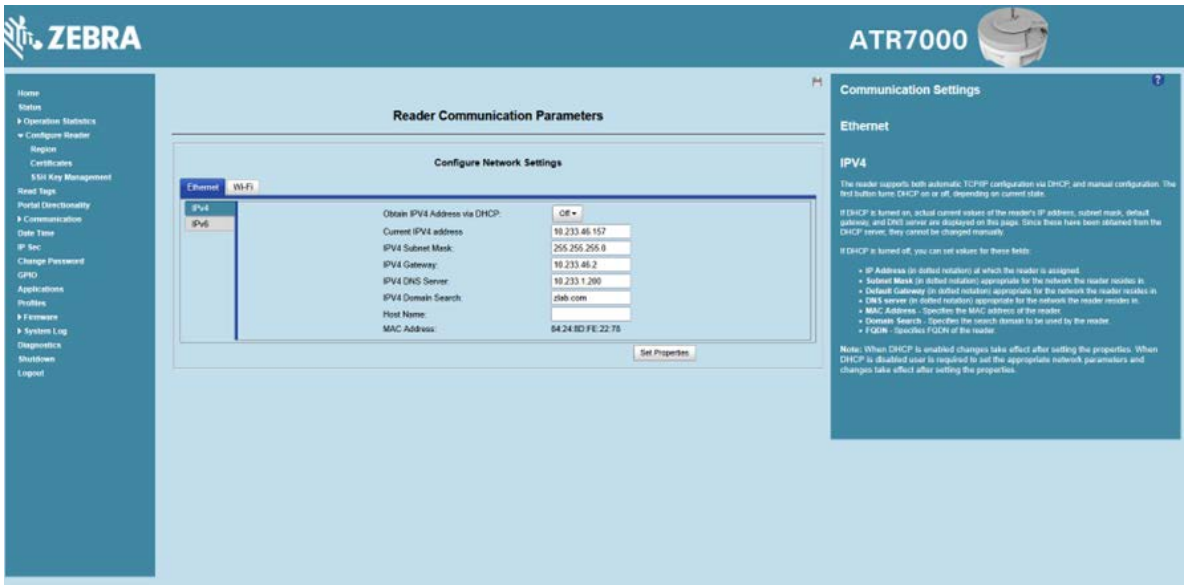
1. Browse the device using the host name, for example: ATR7000CD3B1E.
2. Log in to the device.

Figure 78 Reader Administration Console Login Window



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

Figure 79 Reader Communication Parameters Window



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

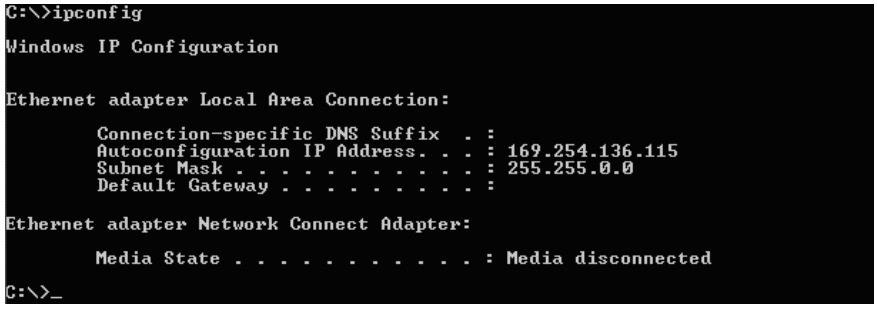
6. The message **Reader IP Address config has changed. Needs reader reboot to take effect** appears. Reset the device and use the reader with the static IP network.

Reader IP is Not Known (DHCP Network Not Available)

To set the Static IP using the web console:

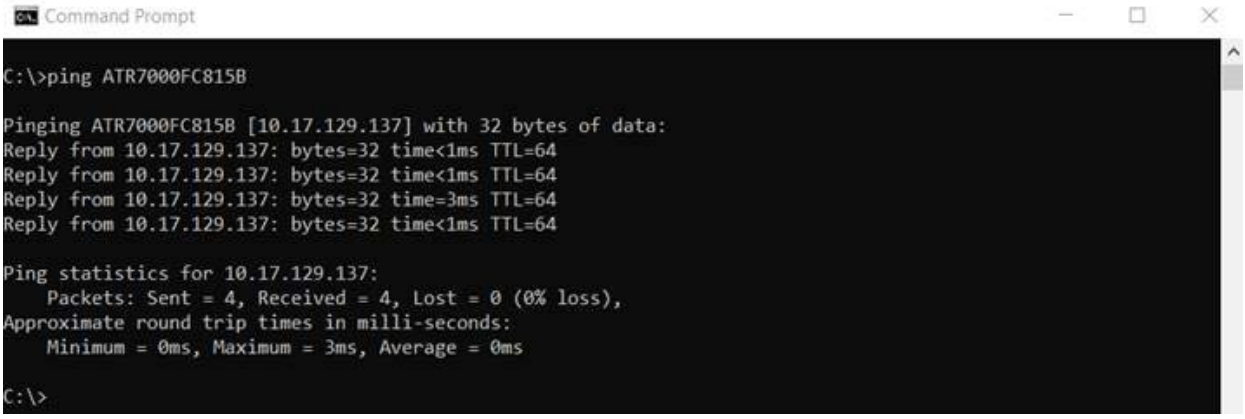
1. Connect the device and a PC running Windows XP to the same network that doesn't have a DHCP server, or connect the device directly to the PC.
2. Ensure both the device and PC Ethernet jack use at least one LED to indicate network connection detect.
3. If the PC uses an assigned static IP, update it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

Figure 80 Obtain IP Address



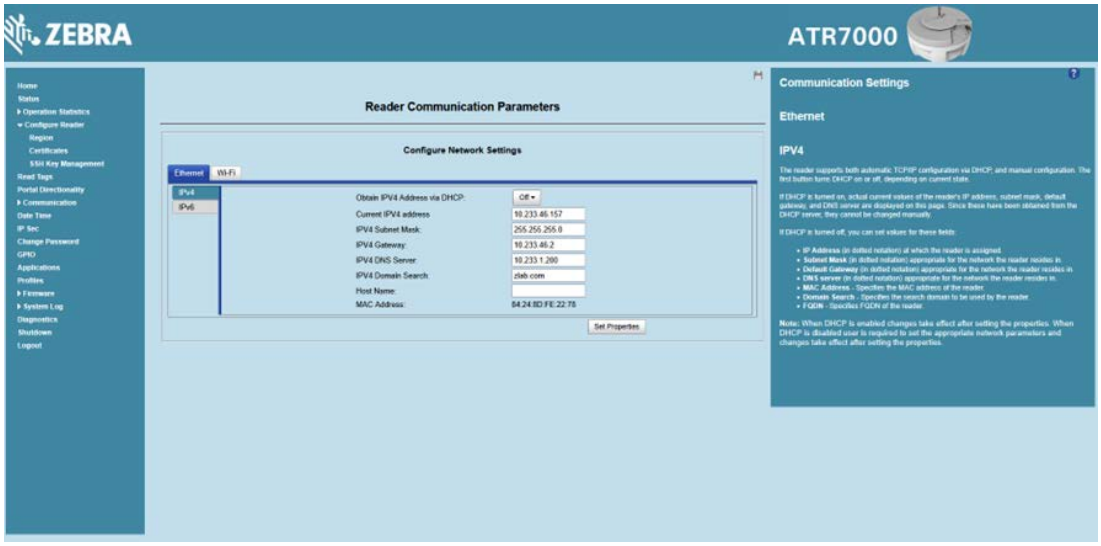
4. When possible, ping the host name of the device.

Figure 81 Ping the Host Name



5. Use a browser to connect to the device with the host name, for example: ATR7000CD3B1E, or use the IP address obtained from ping replies (for example, 169.254.62.74).
6. Log onto the device.
7. Click **Communication**.
8. Set **Obtain IP Address via DHCP** to **Off** and enter all required information.

Figure 82 Reader Communication Parameters Window



9. Click **Set Properties**.

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

Radio Modes

The supported modes are exposed as a list of individual **UHFC1G2RfModeTableEntry** parameters in regulatory capabilities as shown in Table 11. The **Mode Index** column refers to the index used to walk the **C1G2UHFRFModeTable**. Refer to the EPCglobal *Low Level Reader Protocol (LLRP) Standard*.

Table 11 Radio Modes for FCC/IC 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 Confor m-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

*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 11 Radio Modes for FCC/IC 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 Confor m-ance
11	64/3	60000	4	PR_ASK	1500	25000	25000	0	Dense	false
12	64/3	60000	4	PR_ASK	1500	12500	23000	2100	Dense	false
13	64/3	60000	4	PR_ASK	2000	25000	25000	0	Dense	false
14	64/3	60000	4	PR_ASK	2000	12500	23000	2100	Dense	false
15	64/3	64000	4	PR_ASK	1500	25000	25000	0	Dense	false
16	64/3	64000	4	PR_ASK	1500	12500	23000	2100	Dense	false
17	64/3	64000	4	PR_ASK	2000	25000	25000	0	Dense	false
18	64/3	64000	4	PR_ASK	2000	12500	23000	2100	Dense	false
19	64/3	80000	4	PR_ASK	1500	12500	18800	2100	Dense	false
20	64/3	80000	4	PR_ASK	2000	12500	18800	2100	Dense	false
*21	64/3	variable	variable	PR_ASK	variable	6250	25000	variable	variable	false
22	64/3	320000	1	PR_ASK	1500	12500	18800	2100	Dense	false
23	64/3	320000	1	PR_ASK	2000	12500	18800	2100	Dense	false
24	64/3	30000	8	PR_ASK	1500	25000	25000	0	Dense	false
25	64/3	30000	8	PR_ASK	1500	12500	23000	2100	Dense	false
26	64/3	30000	8	PR_ASK	2000	25000	25000	0	Dense	false
27	64/3	30000	8	PR_ASK	2000	12500	23000	2100	Dense	false
28	64/3	32000	8	PR_ASK	1500	25000	25000	0	Dense	false
29	64/3	32000	8	PR_ASK	1500	12500	23000	2100	Dense	false
30	64/3	32000	8	PR_ASK	2000	25000	25000	0	Dense	false
31	64/3	32000	8	PR_ASK	2000	12500	23000	2100	Dense	false
32	64/3	40000	8	PR_ASK	1500	12500	18800	2100	Dense	false
33	64/3	40000	8	PR_ASK	2000	12500	18800	2100	Dense	false

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

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

Copying Files To and From the Reader

Introduction

The ATR7000 RFID reader supports the SCP, FTP, and FTPS protocols for copying files.

SCP

The following examples illustrate SCP use:

scp SourceFileName rfidadm@MyReaderIP:/apps

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

Data Protection

Introduction

The ATR7000 RFID reader stores data in transition when it detects a network condition that prevents the reader from sending data. This applies to RFID tag data that the reader application is transmitting to the outbound TCP socket, and is no longer owned by the RFID application because it was sent to the network layer for transmission.

When the reader cannot queue RFID data in the outbound TCP socket when an LLRP connection is already established, it stores all outbound LLRP messages in the data protection queue. The queue can store up to 66,000 messages, which represents more than 5 minutes worth of data when reading 200 tags/second (the nominal data rate in DRM (dense reader mode) configuration). If the network is still unavailable when the data protection queue is full, the oldest messages are discarded to accommodate the most recent tag reports.

This feature can not be disabled and operates regardless of the physical network interface used.

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 an "admin" account. The password chosen should satisfy the following criteria:

- Should contain minimum of 8 and 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 recommended that a strong password be set for this account before readers are deployed.

The reader does not enforce password rotation, but the reader administrator recommends rotating all passwords periodically, for example, once every 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 recommended that all required services be enabled with secure mode. For example, Choose HTTPs for web server instead of HTTP, Secure FTP over unencrypted FTP, etc.

If any service is not required, such as SSH shell access to the reader, it may be turned off. Refer to the Services section for details on reader services and configurations.

Update Default Self-Signed Certificate

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

Secure IoT Connector Interface

It is recommended that endpoints to which reader connections are made for IoT use cases be secured with trusted certificates and mutual TLS authentication enabled.

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

Note that the 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 the addCAcert RM command. Refer to addCAcert, deleteCAcert and listCAcerts command documentation in the FX Series Reader Interface Control Guide.

Refer to the Certificate Configuration section in the Zebra IoT connector documentation for details on how to set certificates on the reader for endpoint connection security.

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

Enable TLS Security for LLRP

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

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 recommended that administrators keep track of the 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, which can be used to programmatically check for the currently installed certificate details, including its expiry.

Update Custom Trusted CA Certificates to Reader Trusted Certificate Store

The reader has a trusted CA certificate store that may be updated with custom CA certificates. The reader can use such CA certificates to trust remote endpoints before connecting to them, provided the same CA issues the certificates.

The reader currently supports only RM commands for managing such CA certificates. Refer to 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 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, FTPS 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 your deployment supports 802.1x EAP, it is recommended that you enable it. Refer to the 802.1x EAP Configuration section for details.

Disable Serial Port

The external serial and serial-to-USB ports on FX9600 and ATR7000 should 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

10/100BaseT Ethernet 10, 19

A

administrator console 38
- applications 83
- committing changes 86
- communication settings 69
- configure network services 73
- configure network settings 69
- configuring system log 88
- discarding changes 86
- firmware version 85, 86
- GPIO 82
- IPV6 sec 80
- login 42
- main screen 44
- managing login 82
- reader diagnostics 89
- reader profiles 84
- scan control 16, 69
- set password 81
- setting date and time 79
- shutting down 89
- status 46
- system log 87

air link 118
applications 83

C

cable pinouts
- ethernet 110
- GPIO 111
- USB 110, 111
- USB debug 110
- USB host 111

commit region change 14
committing changes 86
communication
- ethernet, wired 30

communication settings 69
configure
- LLRP 70
- reader 52
- region 53
- SNMP 72
- static IP 114
- static IP via web console 114, 116

configuring network
- ethernet 69
- services 73

connecting
- to reader 40
- via host name 41

connection
- communication 30
- ports 18
- wired ethernet 30

country list 14, 43

D

data protection 121
date 79
deployments 39
discarding changes 86

E

ethernet
- pinouts 110
- POE 31
- port 19
- setup 30, 31
- wired 30

event statistics 50

F

firmware

version 85, 86
firmware update 85, 86, 103
prerequisites 101
first time login 11, 42

G

GPIO 10, 19
pinouts 111
GPIO control 82

H

host communication
ethernet, wired 30
host name connect 10

I

initiating reads 16, 69
installation
communication connection 30
IP address 40
IP ping 40

L

LED 20
LLRP
configure 70
radio modes 118
log 87
configuring 88
login 42
first time 42
managing 82

M

multiple reader deployments 39

N

NXP
statistics 49

O

obtain reader IP address 40

P

Password 11, 103, 106
password 11, 42, 103, 106
changing 81
pinouts
ethernet 110
GPIO 111
USB 110, 111
USB debug 110
USB host 111
POE 10, 19, 31, 110
ports 18
descriptions 19
ethernet 30
power 10, 19
POE 31
port 19
profiles 84

R

reader
configuration 52
connecting 40
GEN2 statistics 48
profiles 84
statistics 47
event 50
NXP 49
status 46
reading tags 33
initiating 16, 69
reboot 39
region 43
region configuration 53
region control 43
region setting 14
region settings 14
reset 19
RFID
FX reader 17
RJ45 19

S

set region 14, 43
setting date 79
setting time 79
setup
wired ethernet 30
wired ethernet AC outlet 30
wired ethernet, power-over 31
shutdown 89
side panel 10
SNMP
configure 72
software update 103
specifications 108
start-up 11

static IP configuration 114
via web console 114, 116
Statistics 50
statistics 47
event 50
GEN2 48
NXP 49
status 46
system log 87
configuring 88
system time 79

T

tags
reading 33, 69
technical specifications 108
time 79
troubleshooting 96

U

unpacking 22
updating firmware 85, 86, 103
prerequisites 101
updating software 103
USB
debug pinouts 110
host pinouts 111
pinouts 110, 111
user ID 42
user name 11, 103, 106
user password 42

V

version control 85, 86

W

wired ethernet 30

Z

zero-configuration networking 42