Installation Guide

Atlas Prox Series

Access Control Panels

Ver 1.0

This installation guide is used for Atlas-100 Bundle, Atlas-200 Bundle and Atlas-400 Bundle.

ZKTeco

www.zktecousa.com

Copyright © 2020 ZKTeco USA. All rights reserved.

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for safe operation of the machine/unit/equipment that personnel have read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/ amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement / better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible:

- In case the machine/unit/equipment mal-functions due to any non-compliance of the instructions contained in this manual.
- In case of operation of the machine/unit/equipment beyond the rate limits.
- In case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zktecousa.com.

If there is any issue related to the product, please contact us.

ZKTeco

Address:	ZKTeco USA LLC 1600 Union Hill Rd Alpharetta, GA 30005
Phone:	+1 862-505-2101
E-mail:	sales@zktecousa.com
Website:	www.zktecousa.com

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly and logistics/shipping, all under one roof.

Since 1998, the founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally-leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of "**Atlas Prox Series**".

All figures displayed are for illustration purpose only. Figures in this manual may not be exactly consistent with the actual products.

Table of Contents

Atlas Series Web Management Application

Programming Guide

1. Important Safety Precautions

The following precautions are to keep user's safe and prevent any damage. Please read carefully before installation.

1. **Read, follow, and retain instructions -** All safety and operational instructions must be properly read and followed before bringing the device into service.

2. **Do not ignore warnings -** Adhere to all warnings on the unit and in the operating instructions.

3. **Accessories -** Use only manufacturer-recommended or product-sold accessories. Accessories not recommended by the manufacturer must not be used.

4. **Precautions for the installation –** Do not place this device on an unstable stand or frame. It may fall and cause serious injury to persons and damage to the device.

5. **Service -** Do not try to service this unit yourself. Opening or removing covers may expose you to hazardous voltages or other hazards.

6. **Damage requiring service -** Disconnect the system from the main AC or DC power source and refer service personnel under the following conditions:

- When cord or connection control is affected.
- When liquid was spilled, or an item dropped into the system.
- If exposed to water and/or inclement weather (rain, snow, etc.).
- If the system is not operating normally under operating instructions.
  Just change controls defined in operating instructions. Improper adjustment of other controls may result in damage and involve a qualified technician to return the device to normal operation.
- When system or cabinet is damaged.

7. **Replacement parts -** When replacement parts are needed, service technicians must only use replacement parts provided by the supplier. Unauthorized substitutes can result in burn, shock or other hazards.

8. **Safety check -** On completion of service or repair work on the unit, ask the service technician to perform safety checks to ensure proper operation of the unit.

9. **Power sources -** Operate the system only from the label's power source form. If the sort of power supply to use is unclear, call your dealer.

10. **Lightning -** External lightning conductors can be installed to protect against electrical storms. It stops power-ups destroying the system.

11. The devices should be installed in areas with limited access.

2. What's In The Box

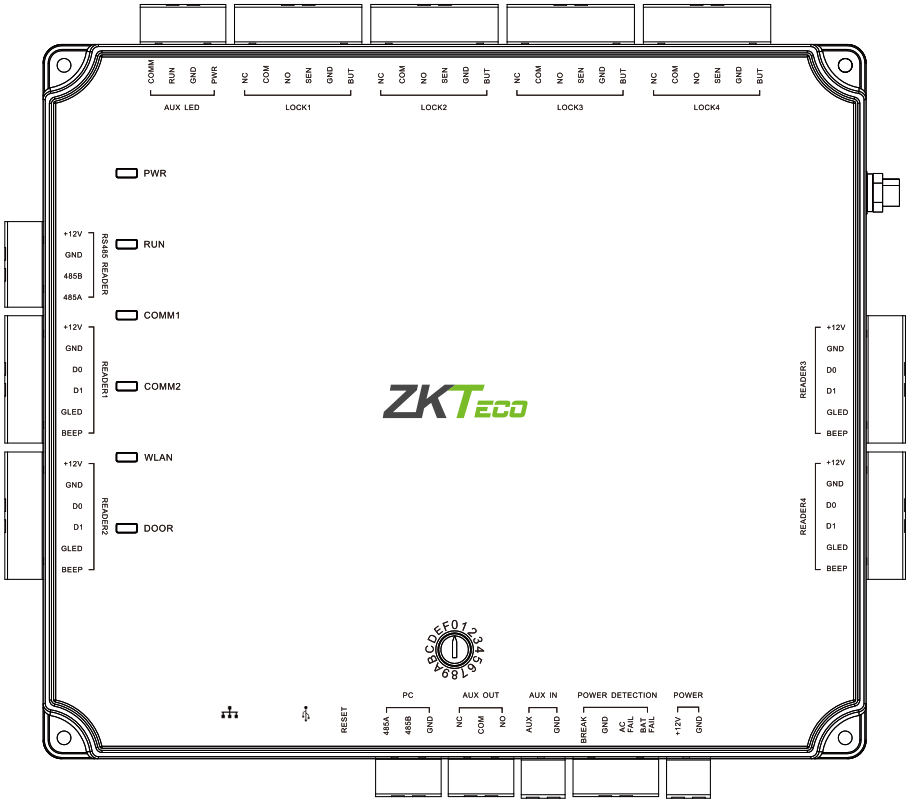
The Box comes with:

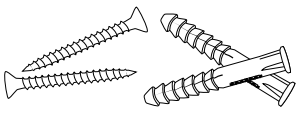
- 1 Panel
- 4 Screws & Spacers
- 1 Screwdriver
- 1 Installation Guide
- 1 Terminal Instruction Paper
- 4 Diodes

Check for visible damage to the packaging. If something has been damaged during transport, please inform the related agency.

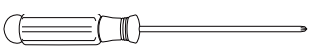
Please unpack the unit carefully. This is an electronic device that must be handled with care in order to avoid damage. Do not attempt to put the device into service if the components are damaged.

If any parts are missing, please inform your customer service representative or the sales representative of the purchase agency. Store it and other packaging materials for future use. If the unit has to be returned, use the original packaging.

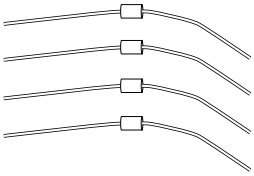




4 Screws & Spacers



1 Screwdriver



4 Diodes

2.1 OPTIONAL ACCESSORIES

Wiegand Card Reader

Prox Card

Door Sensor

Exit Button

Alarm

CR10E Card Enrollment Reader

Atlas x00 Metal Cabinet

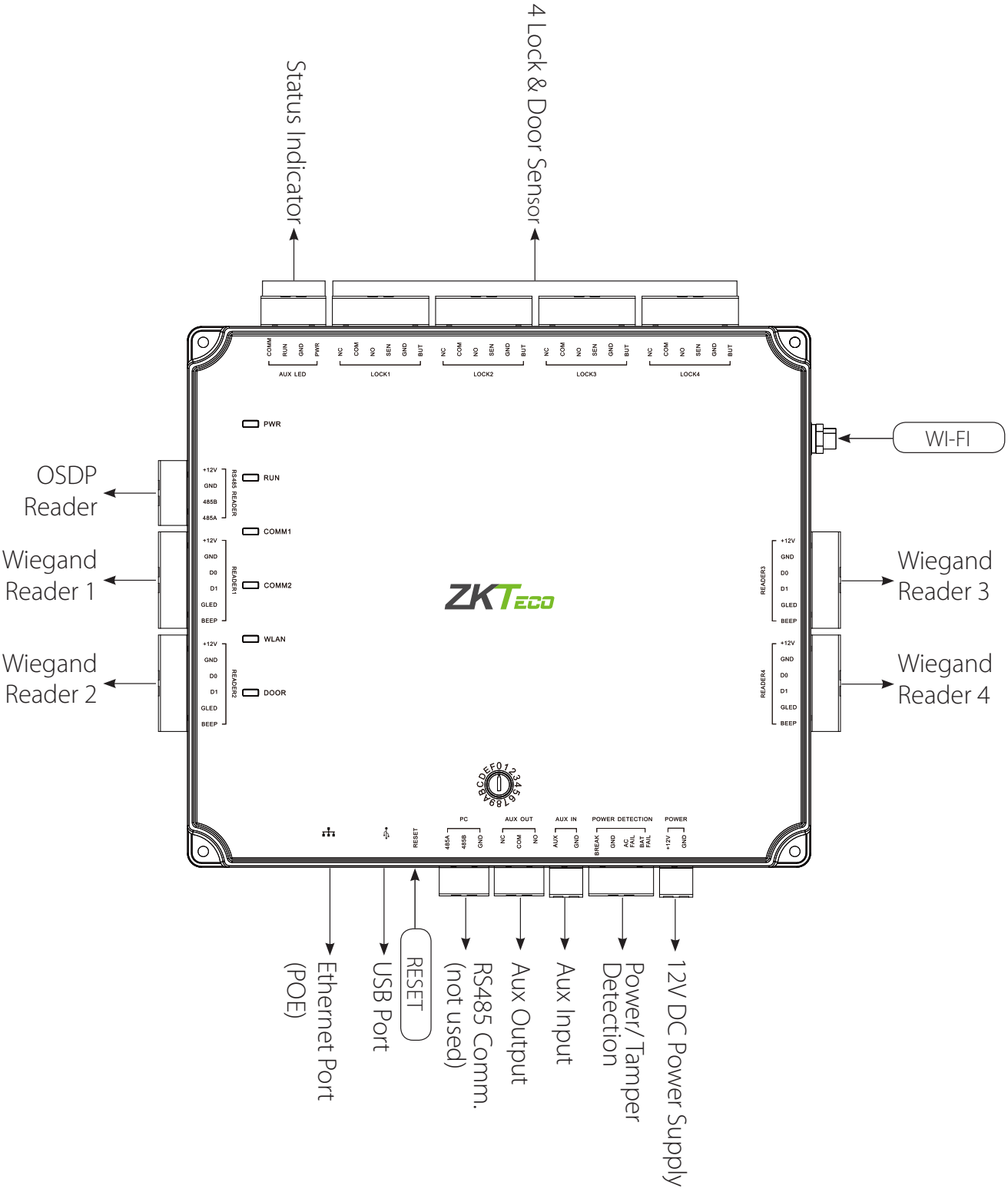
3. Overview

3.1 INTRODUCTION

The Atlas Series Access Controller is a new-generation wireless access controller product developed by ZKTeco. It is the best, simple and affordable biometric access control panel available out in the market. It can controls either one, two or four doors, and has web based software for monitoring. The access control panel is PoE powered and communicates over ethernet/TCP-IP and also via Wi-Fi. Built-in Web Application provides advanced access control features including User Enrollment & Management, Door Control & Monitoring, Lockdown, Reporting, Maps, Anti-Passback, First-Card Opening, Multi-Card Opening, Card Design and Duress PINs.

3.2 APPEARANCE

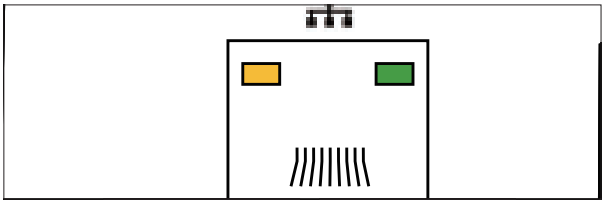
3.3 PRODUCT PIN DIAGRAM



The function of reset button (once reset button is pressed, LED will blink fast):

1. Press the Reset button for 2 to 5 seconds. The ZK Firmware will check if an USB disk is inserted to the Controller. If the disk is inserted, the Controller upgrades the firmware automatically.
2. Press the Reset button for 5 to 10 seconds and the ZK firmware will temporarily set the IP to default IP: 169.254.202.242

3.4 LED INDICATORS



LINK Solid Green LED indicates TCP/IP communication is normal

Flashing (ACT)Yellow LED indicates data communication is in progress

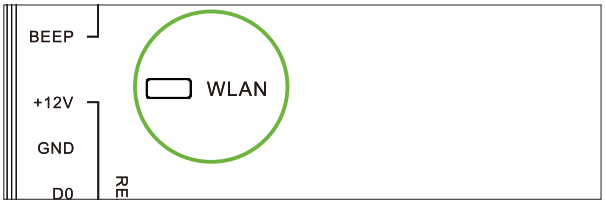
Solid (POWER) Red LED indicates the panel is powered on.

Flashing (RUN) Green LED indicates that panel is working normally.

COMM1 Flashing Yellow indicates the system is communicating with high-level devices (Example: PC).

(Not Used)

COMM2 Flashing Yellow indicates the system is communicating with low-level devices (Example: Readers).



Flashing (WLAN) Green LED indicates the system is communicating in wireless (Wi-Fi) mode.

Flashing (DOOR) Green LED indicates a door opening signal (a door is opened).

4. Specifications

4.1 PRODUCT SPECIFICATIONS

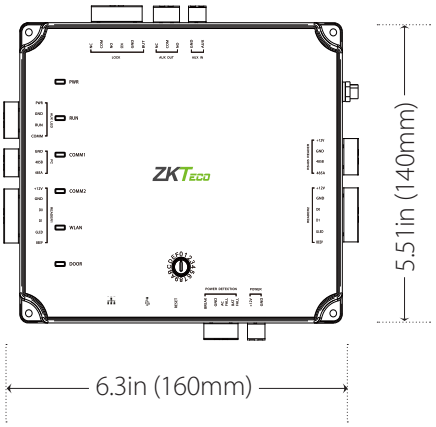
Electrical	**Communication**	TCP/IP, OSDP, WiFi, Wiegand
	Power Supply	12V DC, 3A
General	**Authentication**	Fingerprint/ Card/ PIN
	CPU	32 bit 1.2GHz
	RAM	256MB
	Flash	1GB
	Operating Temperature	32-113 °F (0-45°C)
	Operating Humidity	20% to 80%
	LED Indicator	Indications for Communication, Power, Status and Prox Card
	Weight	Atlas-100: 9lbs (3.8kg); Atlas-200/400: 10lbs (4kg)
	Enclosure	Metal Cabinet
	Mounting	Mounted inside Cabinet
	Dimensions (Panel Only)	**Atlas-100 :** 6.3in. X 5.51in. (160mm X 140mm) **Atlas-200/400 :** 7.75in. X 6.73in. (197mm X 171mm)
	Dimensions (Cabinet Only)	14in. X 2.5in. X 12in. 380mm(L) X 80mm(W) X 280mm(H)
	Certified	CE FC RoHS ETL
Capacity	**Max User [(1:1) or (1:N)]**	5,000 (one template per finger)
	Max Template [(1:1) or (1:N)]	5,000 (one template per finger)
	Max Cards	5,000
	Max Password	5,000
	Event Database Capacity	10,000 transactions, plus unlimited archive downloads
	Number of doors controlled	Four Doors (Four doors-one way and Two doors-two ways)
	Number of readers supported	Upto 4 Wiegand or 8 OSDP
	Number of Inputs	9 (4 Exit Device, 4 Door Status, 1 AUX)
	Number of Outputs	5 (4- Form C relay for lock and 1- Form C relay for AUX output)
Interfaces	**Types of readers supported**	125kHz and 13.56MHz Wiegand readers, OSDP, other readers can be configured upon request

4.2 ELECTRICAL SPECIFICATIONS

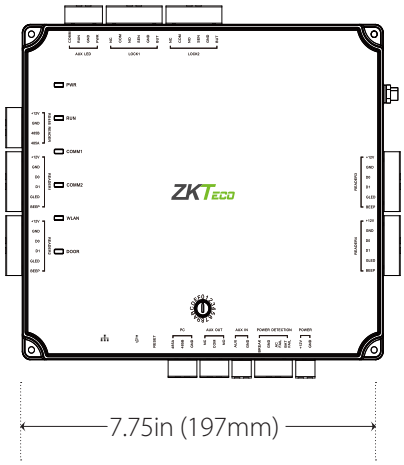
	Minimum	Typical	Maximum	Notes
WORKING POWER SUPPLY				
Voltage (V) DC	9.6	12	14.4	Use regulated DC power adaptor only
Current (A)			2	
ELECTRONIC LOCK RELAY OUTPUT				
Switching Voltage (V)		12V	30V	Use regulated DC power adaptor only
Switching Current (A)		2	3	
Auxiliary relay output				
Switching Voltage (V)		12V	30V	Use regulated DC power adaptor only
Switching Current (A)		1.25	1.5	
SWITCH AUX. INPUT				
VIH (V)		TBD	30V	
VIL (V)		TBD		
Pull-up resistance (Ω)		4.7k		The input ports are pulled up with 4.7k resistors
WIEGAND INPUT				
Voltage (V)	10.8	12	13.5	
Current (mA)			500	
ZK ELECTRIC LOCK				
Voltage (V) DC	10.8	12	13.2	
Current (mA)			500	

4.3 PRODUCT DIMENSION

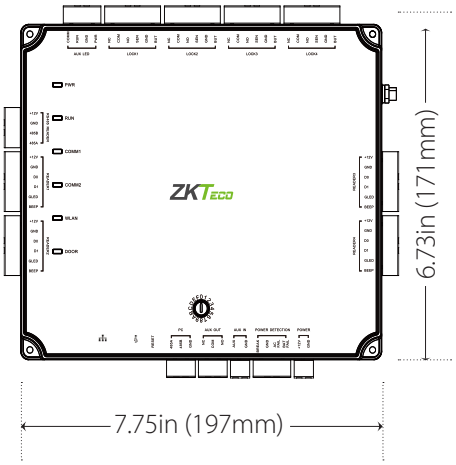
Atlas-100



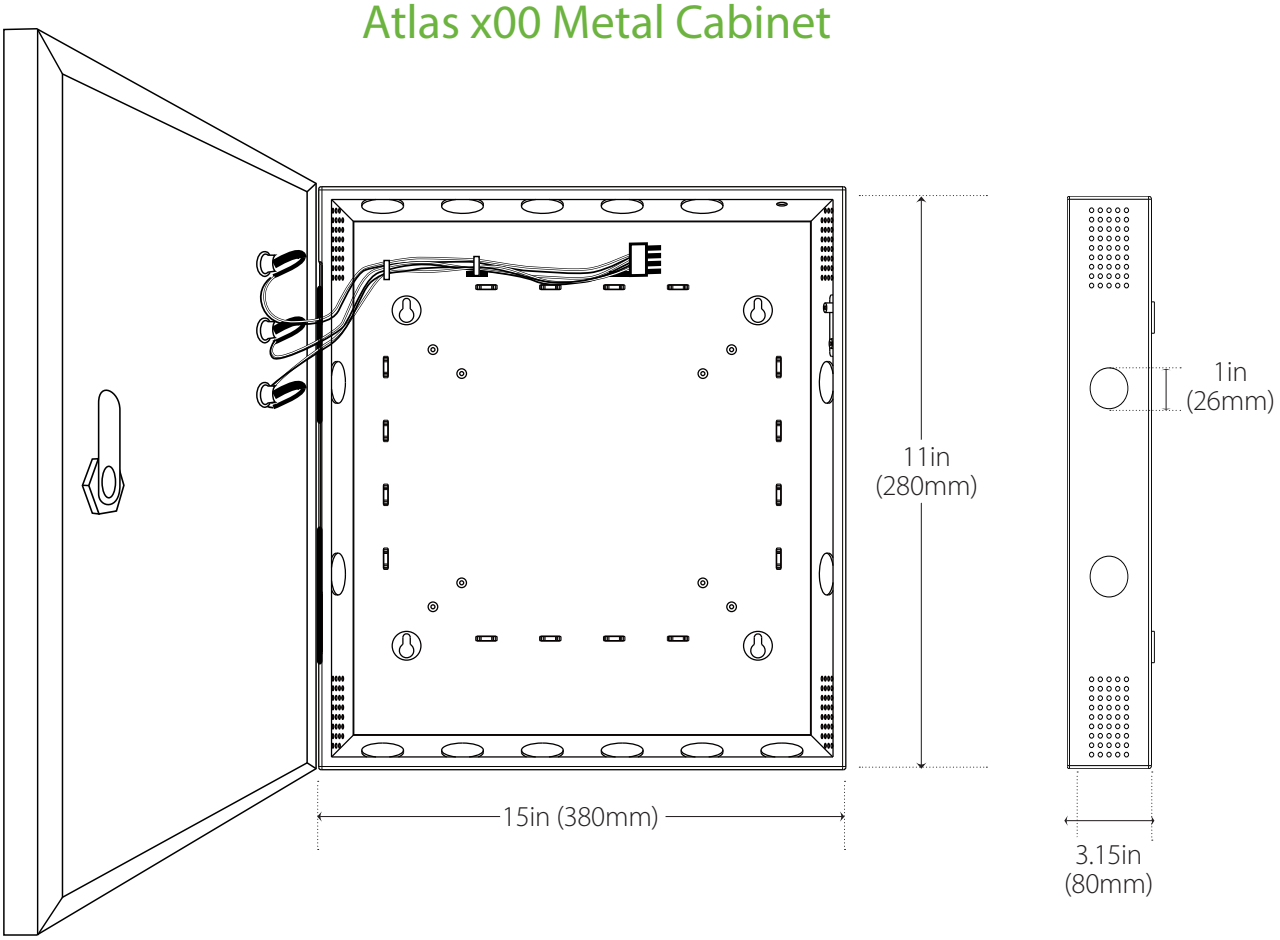
Atlas-200



Atlas-400



Atlas x00 Metal Cabinet



The surface of the metal cabinet is coated with high temperature baked paint to prevent rust. The holes on the cabinet are spot welded by a round metal plate. You have to remove the welded metal plate to insert the cable.

4.4 I/O SPECIFICATIONS

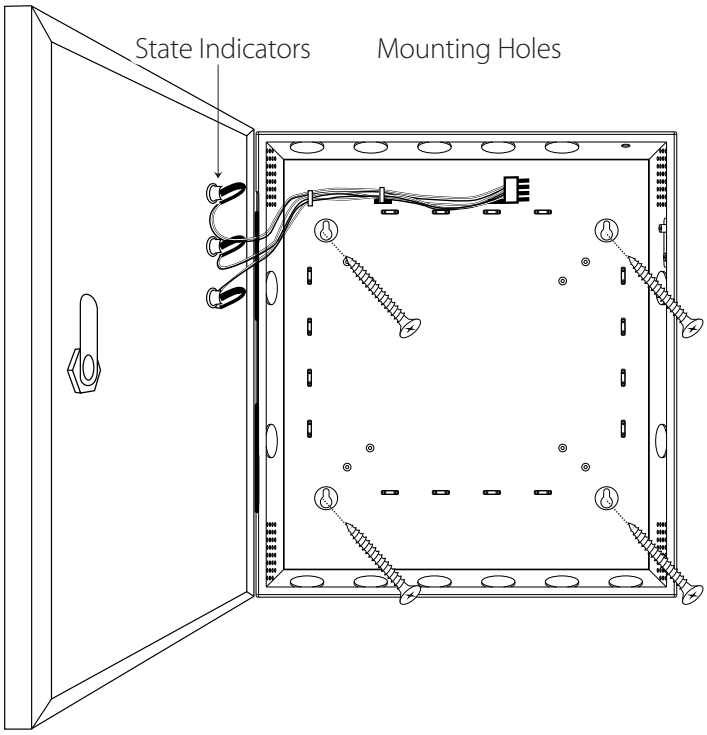
Model	Atlas-100	Atlas-200	Atlas-400
Number of Doors Controlled	One Door	Two Doors	Four Doors
Number of Readers Supported	2 (Wiegand Readers) or 2 (OSDP or Fingerprint Readers)	4 (Wiegand Readers) or 4 (OSDP or Fingerprint Readers)	4 (Wiegand Readers) or 8 (OSDP or Fingerprint Readers)
Number of Inputs	3 (Exit Device, Door Contact and 1 Aux)	5 (2 Exit Devices, 2 Door Contacts and 1 Aux)	9 (4 Exit Devices, 4 Door Contacts and 1 Aux)
Number of Outputs	2 (1 Form C relay for lock and 1 Form C relay for Aux output)	3 (2 Form C relays for locks and 1 Form C relay for Aux output)	5 (4 Form C relays for locks and 1 Form C relay for Aux output)

4.5 CONNECTION INTERFACES

Description	Related Content
Connecting the Power Cord after installation	Power Wiring Diagram
Connecting the Panel to the INTERNET	Ethernet Connection
Connecting Wiegand Reader to the Panel	Wiegand Connection
Connecting OSDP reader to the Panel	OSDP Connection
Connecting Exit Devices to the Panel	Door Sensor & Exit Button
Connecting Electric locks to the Panel	Lock Connection
Connecting Input and output Devices to the Panel	AUX I/O Connection

5. Installation Setup

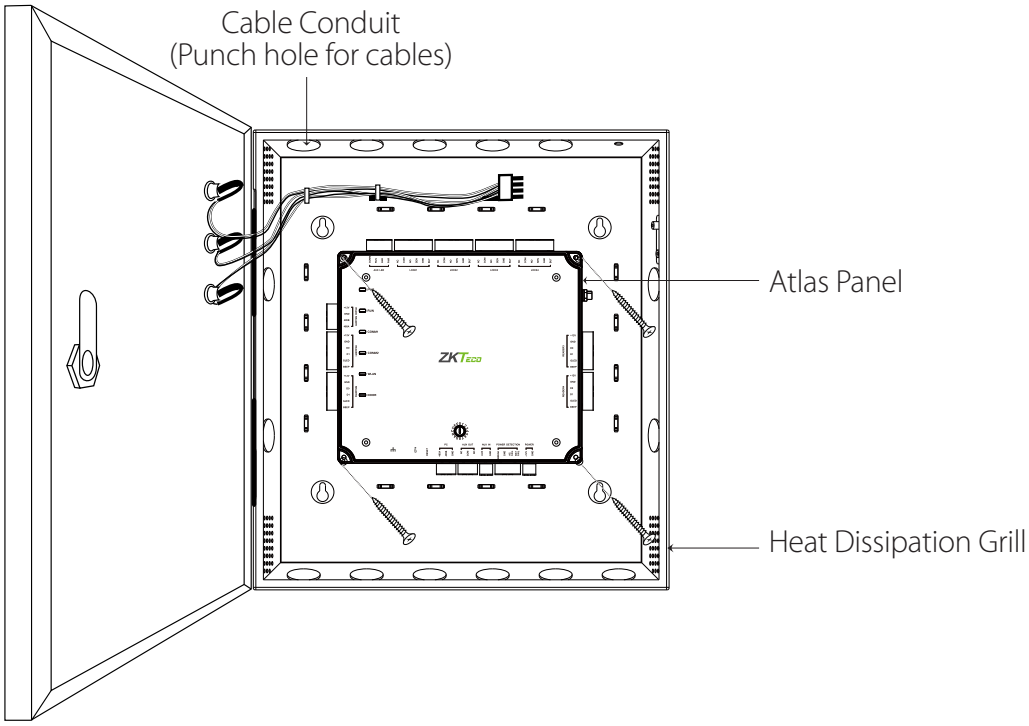
5.1 INSTALLATION OF PANEL & CABINET



Step 1
Drill Holes according to the Cabinet Holes

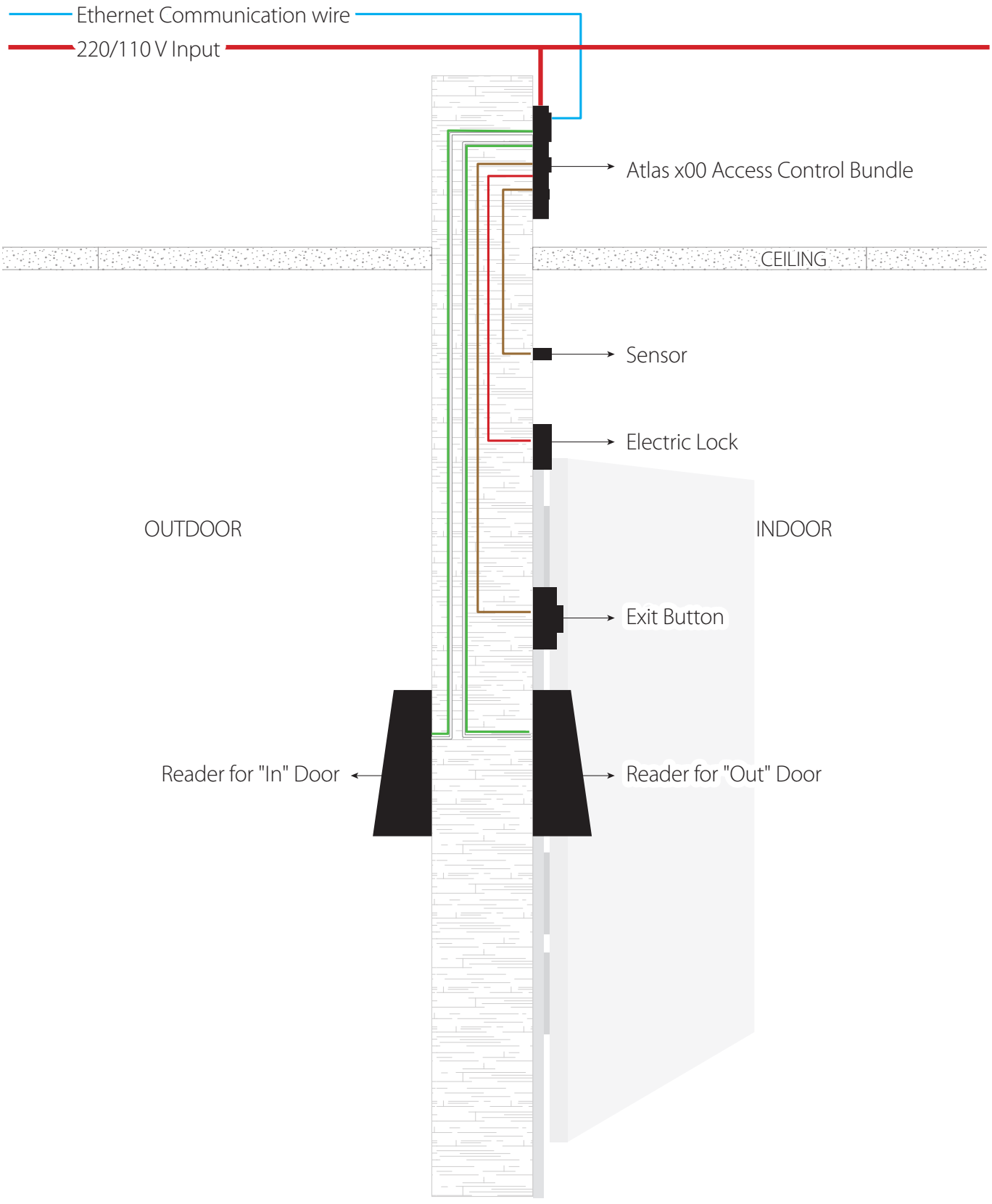
Step 2
Mount the cabinet using screws

Step 3
Screw the Panel inside the cabinet



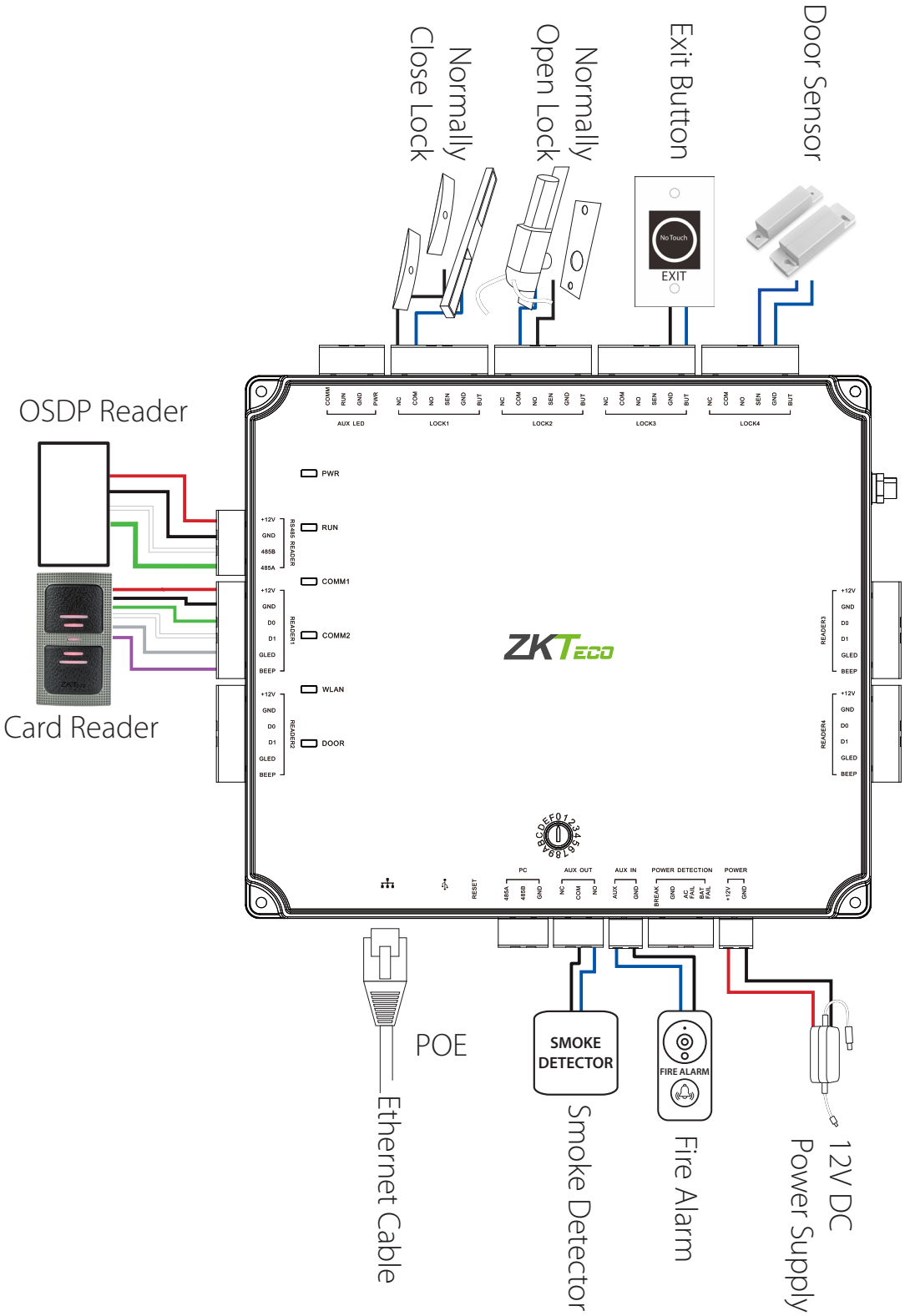
We recommend drilling the mounting plate screws into solid wood base (i.e. stud/beam). If a stud/beam cannot be found, then use the supplied Spacer (anchors). Wiring methods shall be in accordance with National Electrical Code, ANSI/NFPA 70. Do Not Connect to a Receptacle controlled by a Switch.

5.2 INSTALLATION SITE (DIAGRAM)



6. Connections

6.1 OVERALL CONNECTION DIAGRAM



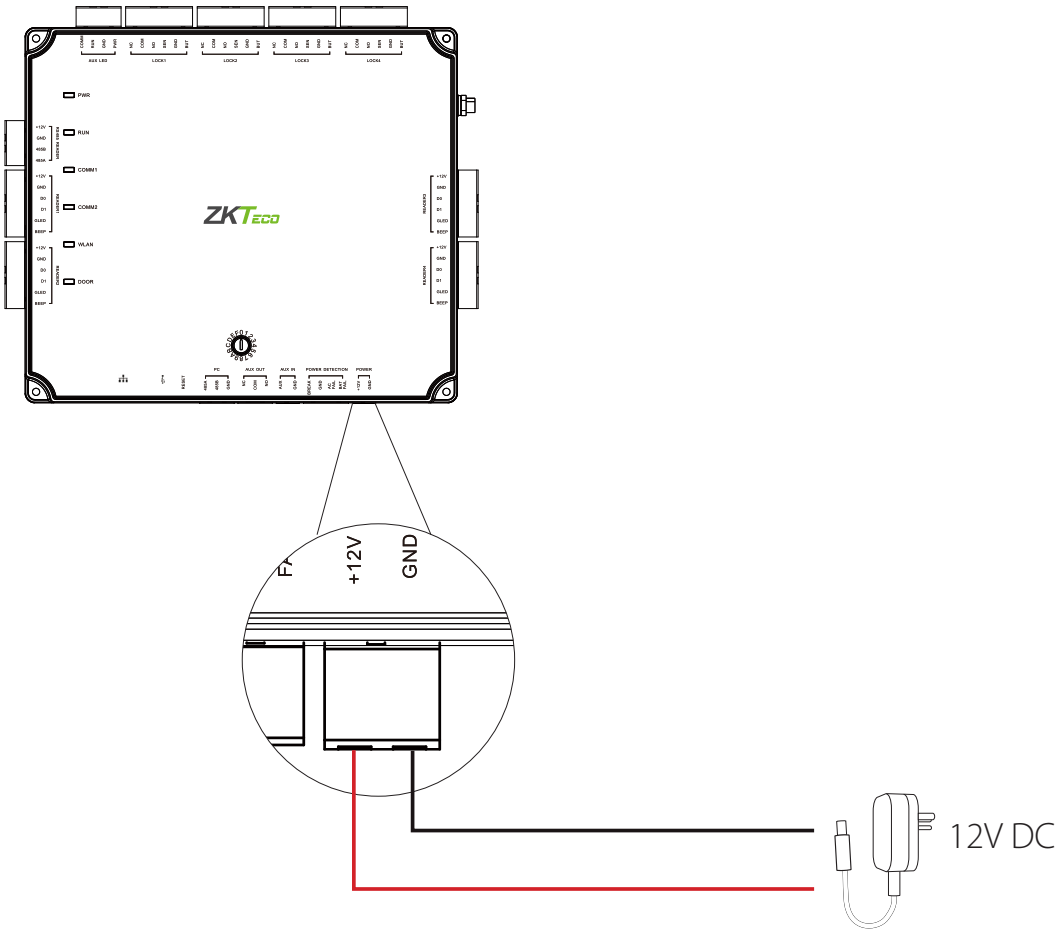
The auxiliary input may be connected to infrared motion sensors or smoke detectors. The auxiliary output may be connected to alarms, cameras or door bells, etc.

Wording "Compliance with IEEE 802.3 (at or af) is not required"

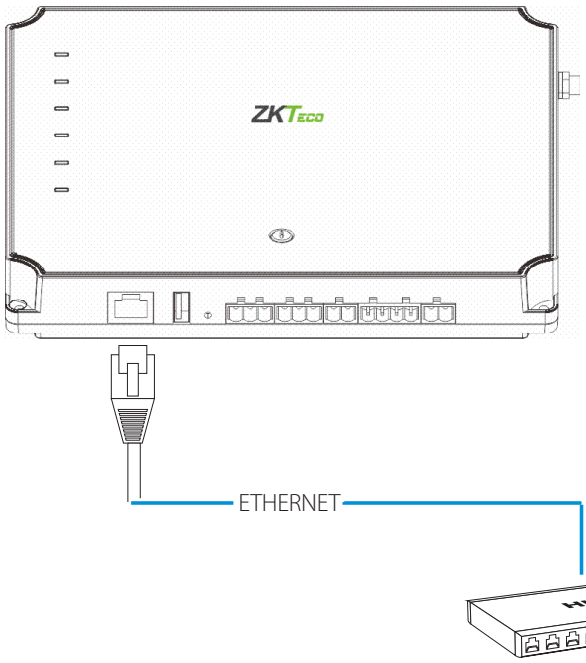
Reference to National Electrical Code, ANSI/NFPA 70 for Power over communications

6.2 POWER WIRING DIAGRAM

Power cable is connected to +12V and GND.



POE Power Supply



1) The product is supplied with 12V DC from the surge protected Class 2 power source.

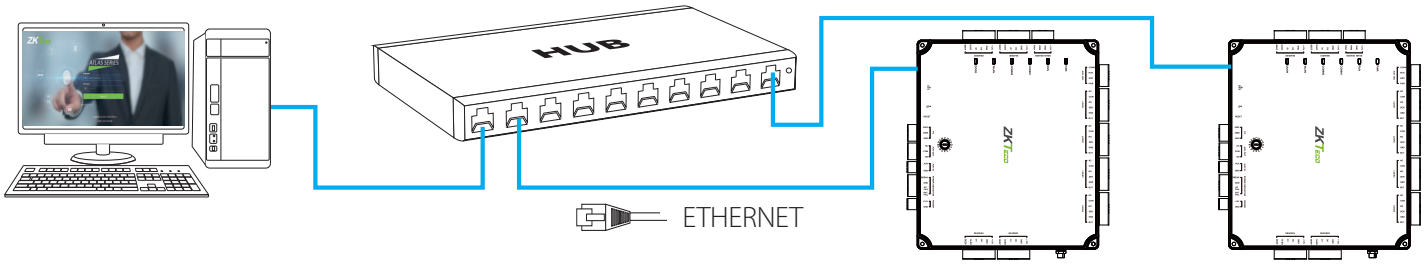
2) The product supports the Power Over Communication cable source. The Power sourcing equipment for POE shall be in compliance with section 34.7 of UL 294, 7th Edition.

6.3 ETHERNET CONNECTION

LAN Connection

Important Notes:

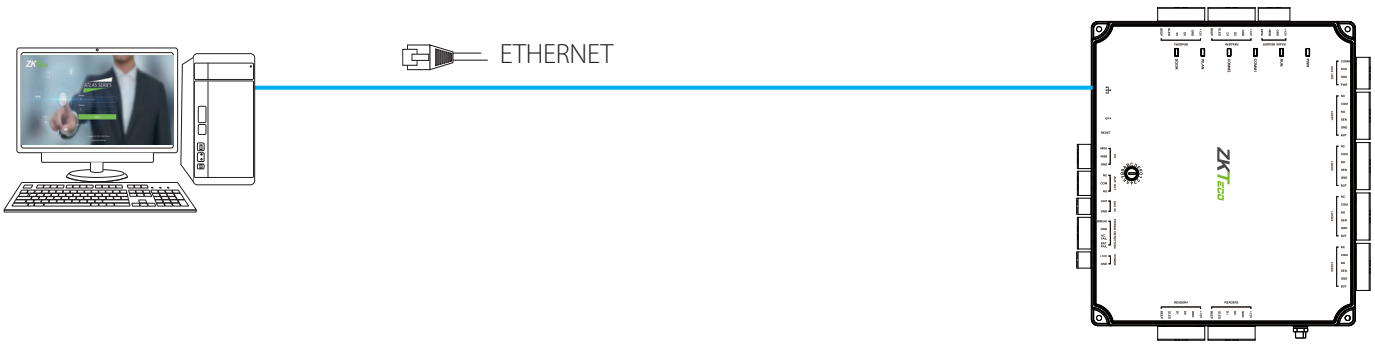
1. Both 10Base-T and 100Base-T are supported.
2. This cable distance must be less than 330 ft. (100m)
3. For cable length of more than 330 ft. (100m), use HUB to amplify the signal.



CAT5e or CAT6 Ethernet cable recommended

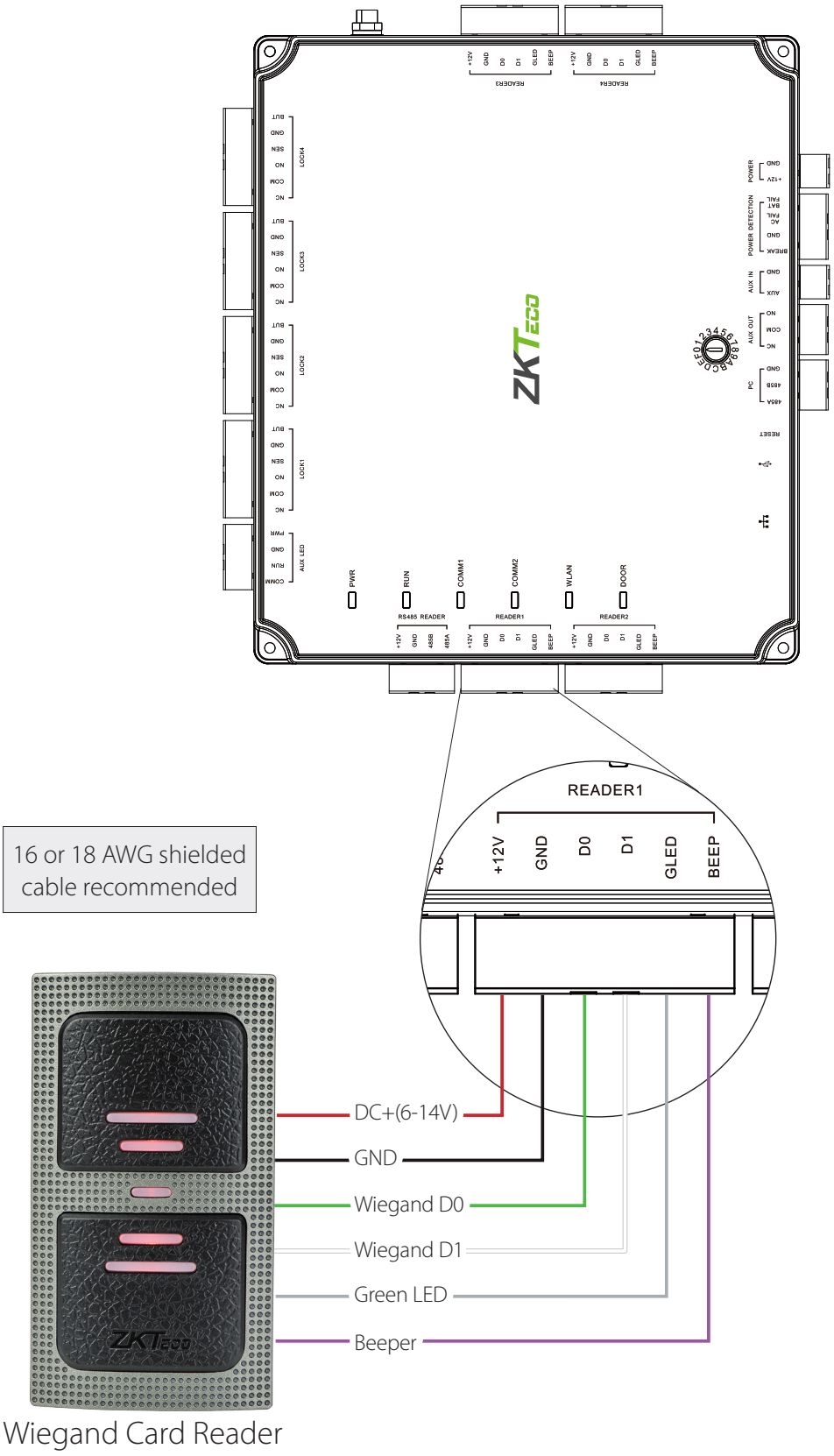
Direct Connection

To connect Atlas-460 with a PC directly, connect both with a straight network cable. As the Atlas-460 supports auto MDI/MDIX, it is not necessary to use a crossover type cable.



6.4 WIEGAND CONNECTION

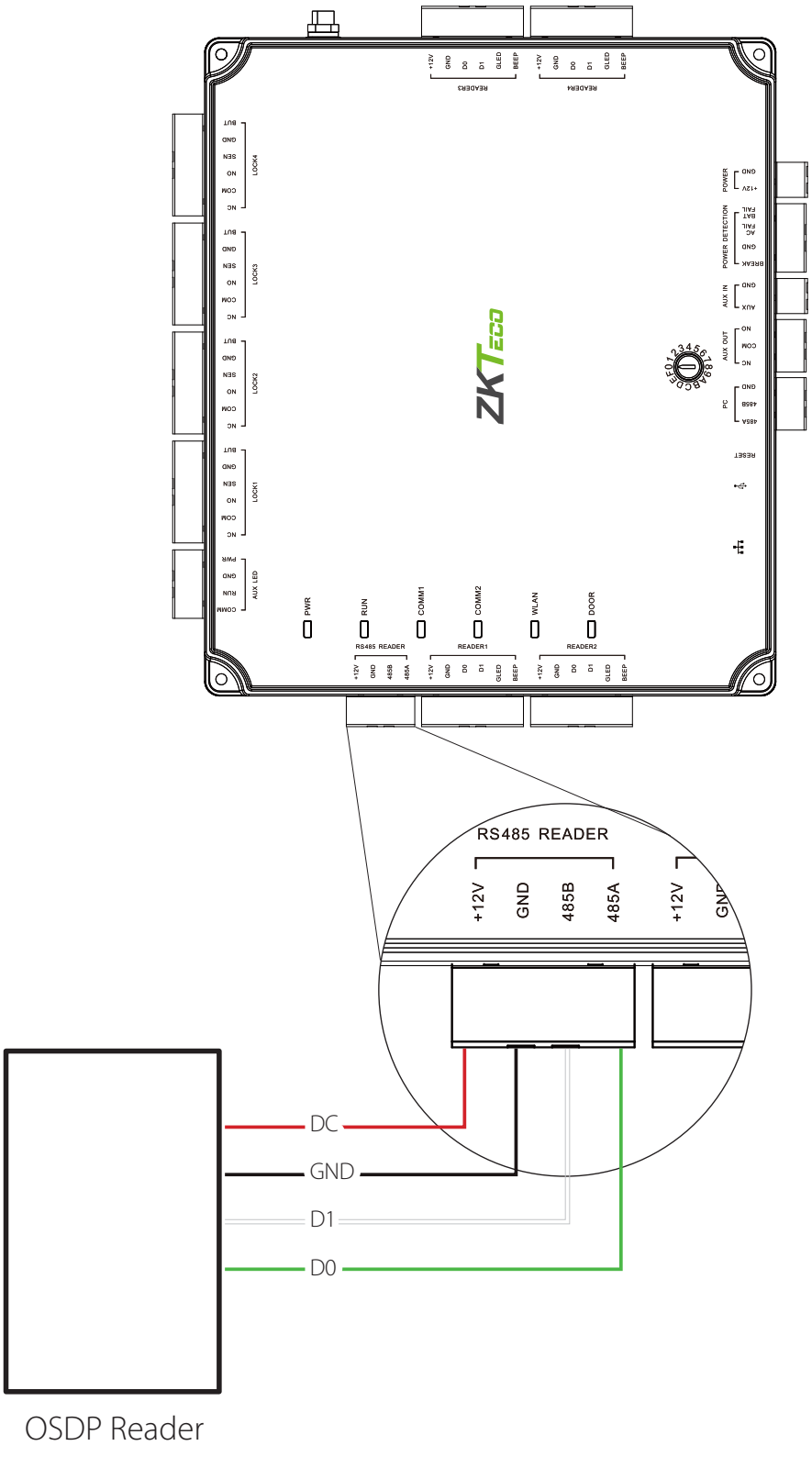
Wiegand card reader connects to the wiegand terminal while authenticating. The Wiegand card reader sends the credentials to the panel via wiegand communication. The panel's firmware decides whether to open the lock in accordance with access control levels.



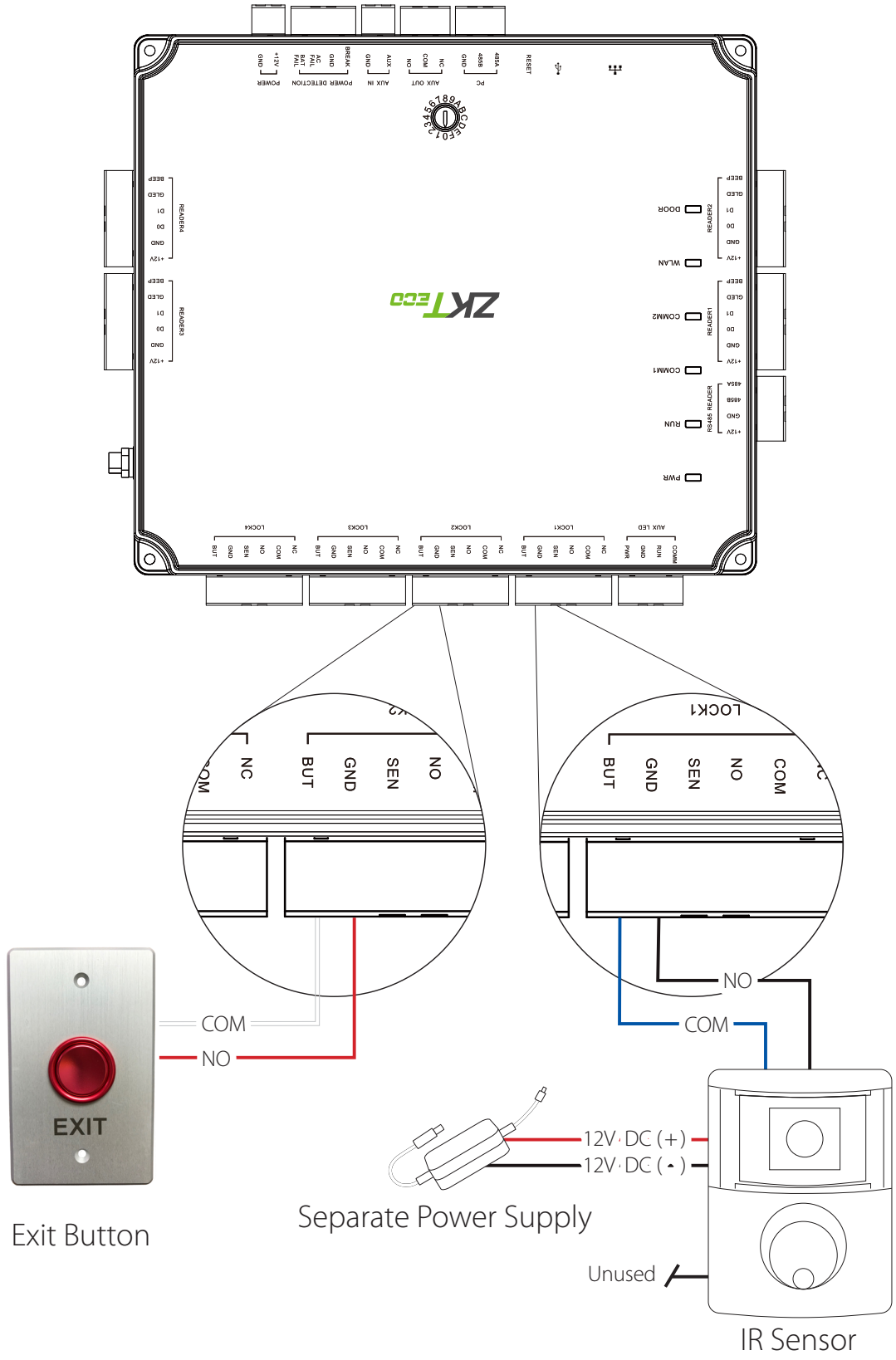
Wiegand Card Reader

6.5 OSDP CONNECTION

OSDP card reader connects to RS485 terminal while authenticating. The OSDP reader sends the credentials to panel via OSDP communication. The panel's firmware decides whether to open the lock in accordance with access control levels.



6.6 DOOR SENSOR & EXIT BUTTON (REX CONNECTION)

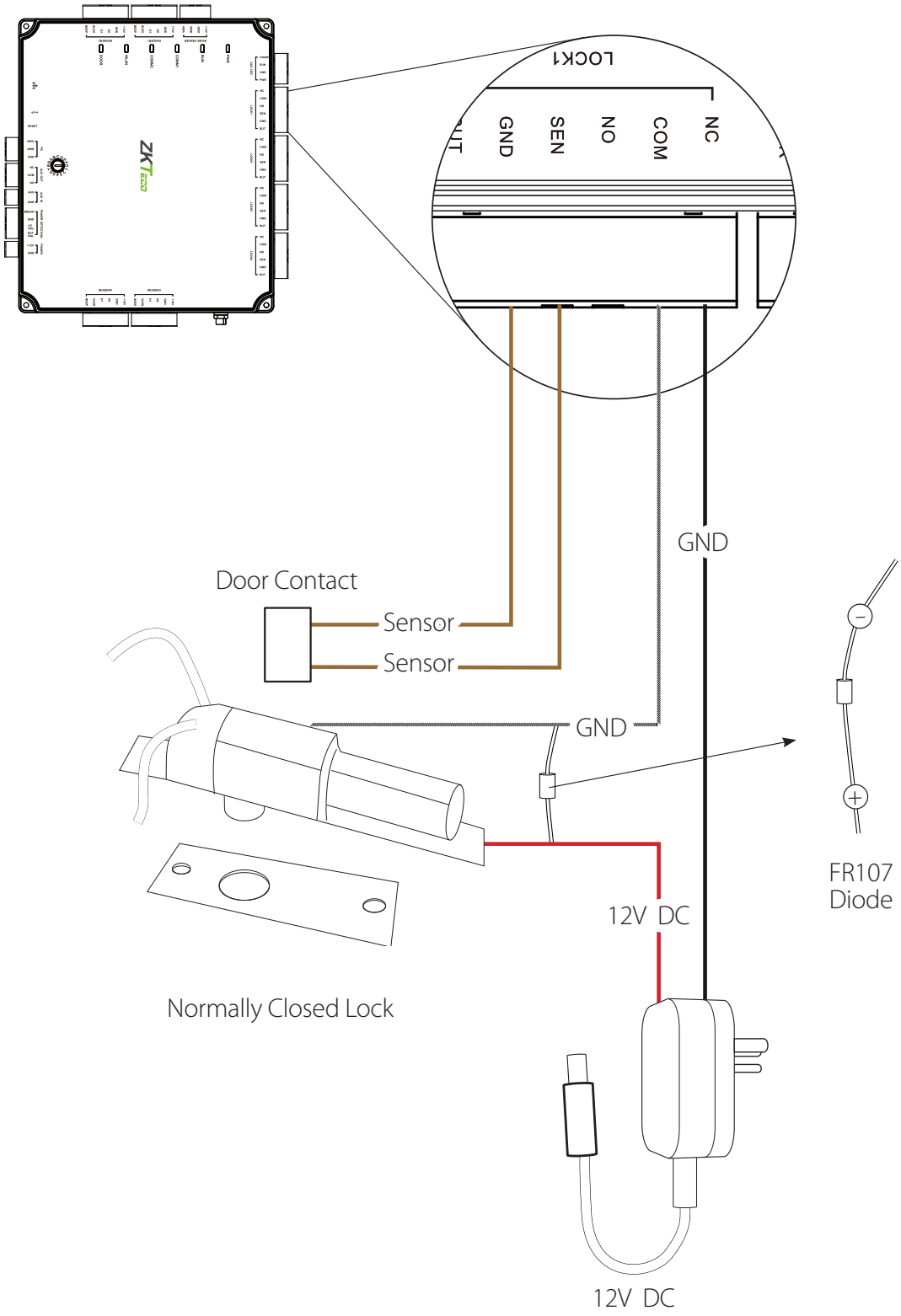


NOTE: Please make sure you are following your state and local building codes when wiring your REX & IR Motion Sensors.

6.7 LOCK CONNECTION

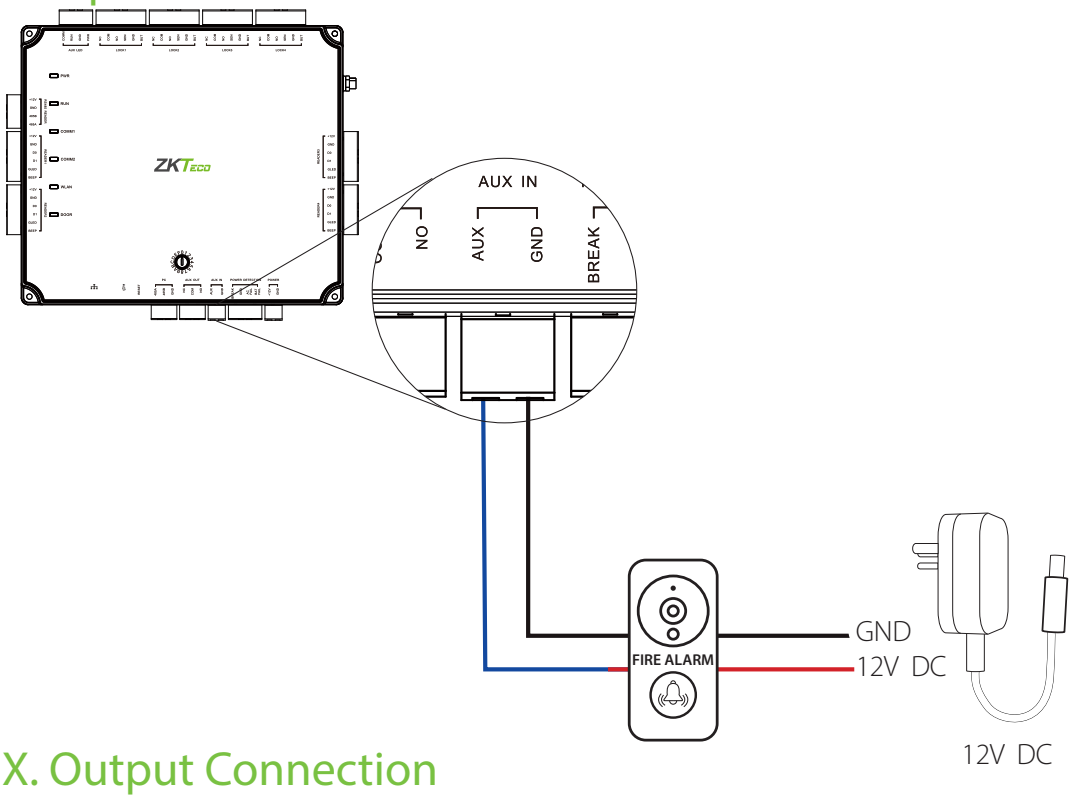
Normally Open (NO): When not in use, there is no contact between the circuits. No current is flowing through the relay and the door is opened when the relay is activated by a current flow.

Normally Closed (NC): The circuit is closed unless otherwise specified. Current flows through the relay and the door is opened when the relay is activated by blocking the current flow..



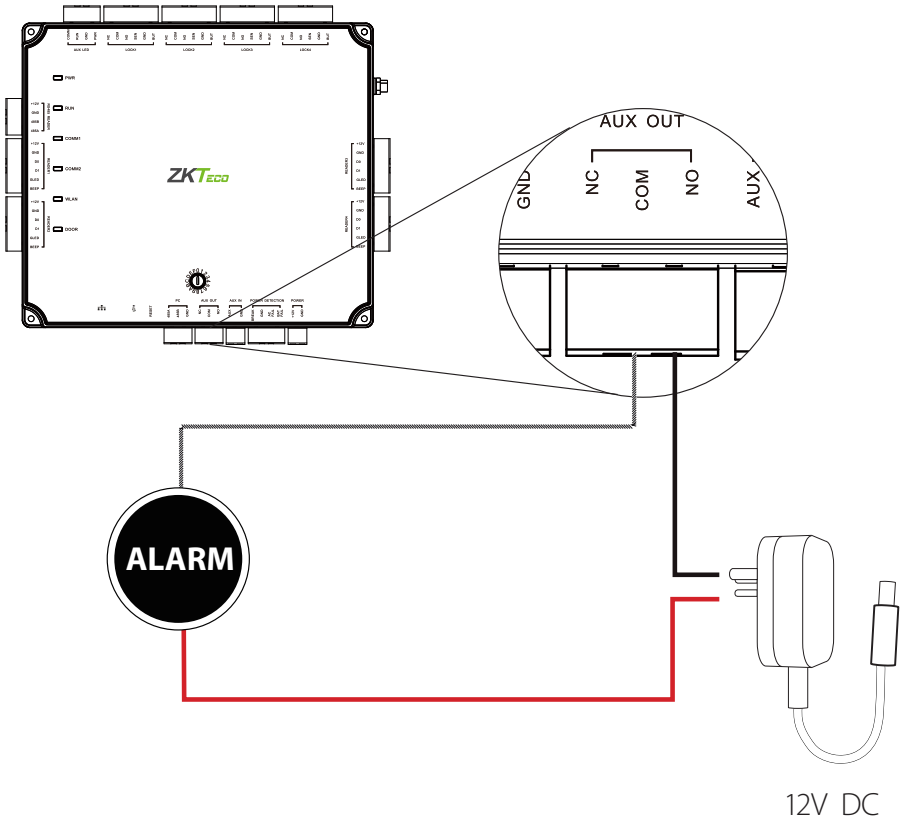
6.8 AUX I/O CONNECTION

AUX. Input Connection



AUX. Output Connection

Normally AUX. Output is used to connect external alarm which can be linked to reader input and AUX. Input. You may choose to have certain devices send signals to external devices, such as alarm sirens, when selected events occur.



Atlas Series Web Management Application

1. Understanding the Atlas Series Network

All Atlas Series systems have a single "Primary" controller. Many "Secondary" controllers may be added to support additional doors. All secondary controllers maintain a connection to the primary, and the primary provides all data and configuration, the secondaries need to operate.

The primary controller has a **Web Management Application** you can log into from a web browser. Through this application you can configure the entire system.

Important: The primary controller must support biometrics if any biometric controller is used in the system.

Requirements

1. Obtain an available static IP address and configuration from the network administrator.
2. (Optional) Obtain a signed HTTPS certificate. This provides some additional security and avoids web browser warning messages. The supported certificate formats are PEM or PFX. Check "**Optional Installations**" for more details.
3. Make sure whether using Network Time Protocol(NTP) to automatically update the controller's clock over Internet is possible and acceptable. Also make sure whether non-standard time servers are used (such as Corporate time servers).With a typical small network, it is safe to assume NTP will work with default Atlas Series settings.

Help

This guide provides you online help for the detailed operation of the controller. The help is available once you have connected the primary controller and logged in to the Web Management Application. Open the help guide by selecting "**Help**" from the menu in the upper right corner.

Procedure

1. Understand how an Atlas Series system networks together by reading the brief section, "**Understanding the Atlas Series Network**".
2. Connect a computer directly to a controller and run the initial configuration program. This step must be completed before the controller operates on the network.
3. Connect the controller to the local network.
4. Log in to the Web management application and complete the basic configuration.
5. Add a user and test door access.
6. Add any secondary controllers as per requirements.

Expected Browser Warnings

Your browser will display an insecure site warning each time you log in to the Web Management Application. The exact text of the warning, and the way to resolve it, may vary among browser applications. You can still open it by clicking "Go on to the webpage (Not recommended)" present under "Details" option (may vary in different browsers). The preferred supported browsers are Google Chrome, Mozilla Firefox, Microsoft Edge, etc. You can prevent this warning by installing a signed HTTPS certificate when directed, as shown in "**Install a Signed Certificate (Optional)**":

Network Considerations

Ideally, all controllers should be connected on the same subnet. If you have a simple home or small office network, this will be the case. For more complex networks, be sure to review the "**Special Considerations for Complex Networks**" discussed at the end of this document before proceeding.

2. Initial Controller Setup

1. Connect the controller to DC power.
2. Connect an Ethernet cable directly from your computer to the controller.
3. If your computer is set to use a static IP address, you need to temporarily change it to one in the range 169.254.202.xxx, or to DHCP. If you normally use DHCP, skip this step. If you do not know, try assuming you use DHCP, which is common.
4. Open a web browser and enter the default controller address: **169.254.202.242**. You might get an insecure site warning from the browser (check "**Expected Browser Warning**" above). After resolving the warning, you will be directed to the Web Management Application login screen. Note that it might take a minute for the connection to be available.

Trouble Connecting: If you cannot connect to the Controller at the default IP Address or the configured address, you can try "Hard Network Reset". Find the small opening on the controller labeled "Reset." Insert a paperclip to press the button for 5-10 seconds. The controller address will revert to the default IP 169.254.202.242. It remains the same untill the controller is rebooted or reset or modified.

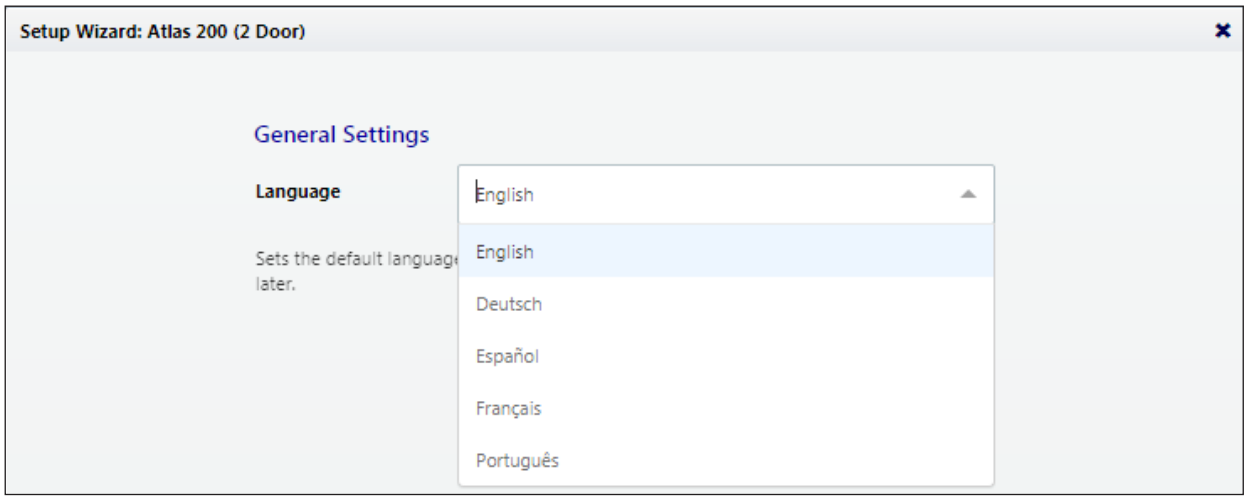
3. Running the Setup Wizard

Log in using the default administrator account:

- **User name:** admin
- **Password:** admin

You will be directed to the Setup Wizard, where you have to enter the required information for the Controller operation.

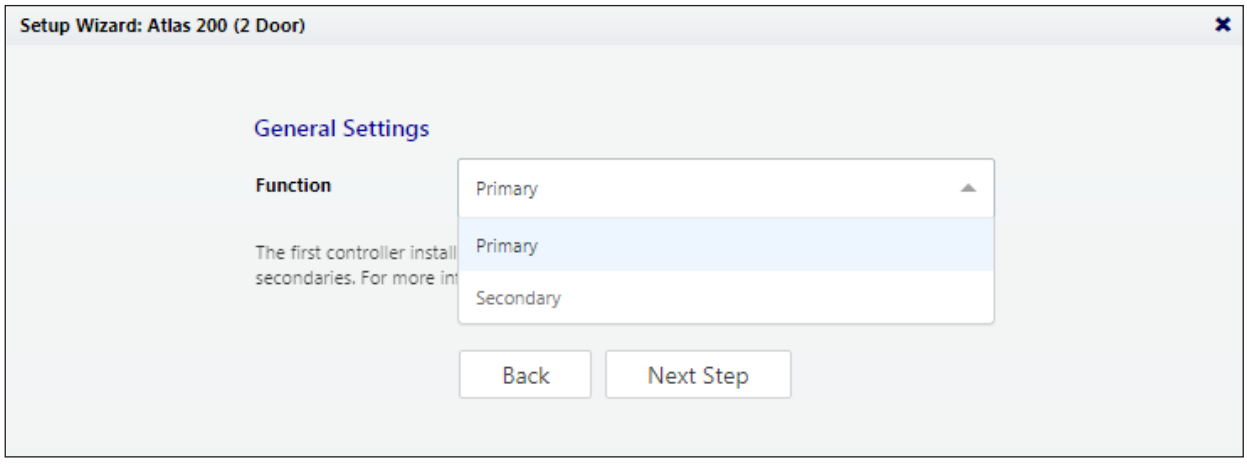
Page 1: Language



Choose a language of your choice which will be used for this wizard. It will also become the default language of the Web Management Application. This can be changed later in the hardware configuration of the primary controller.

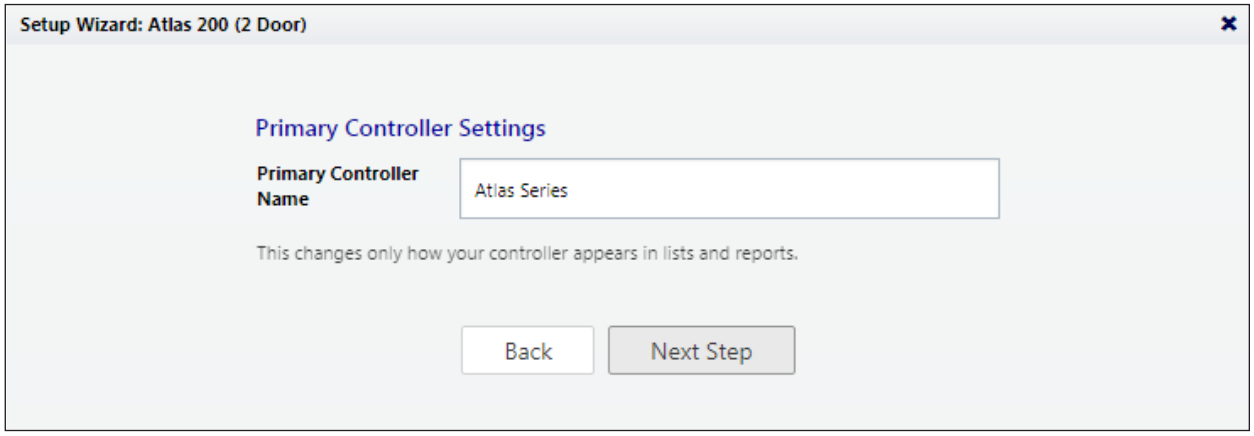
Note: For secondary controllers, the language does not affect the Web Management Application. It sets the language of the simplified management application and can be changed later while configuring the controller.

Page 2: Function



Choose whether this controller is a "Primary" or a "Secondary". Make sure you understand the Atlas Series network, discussed above. The first installed controller must be the Primary controller and all others are Secondary controllers.

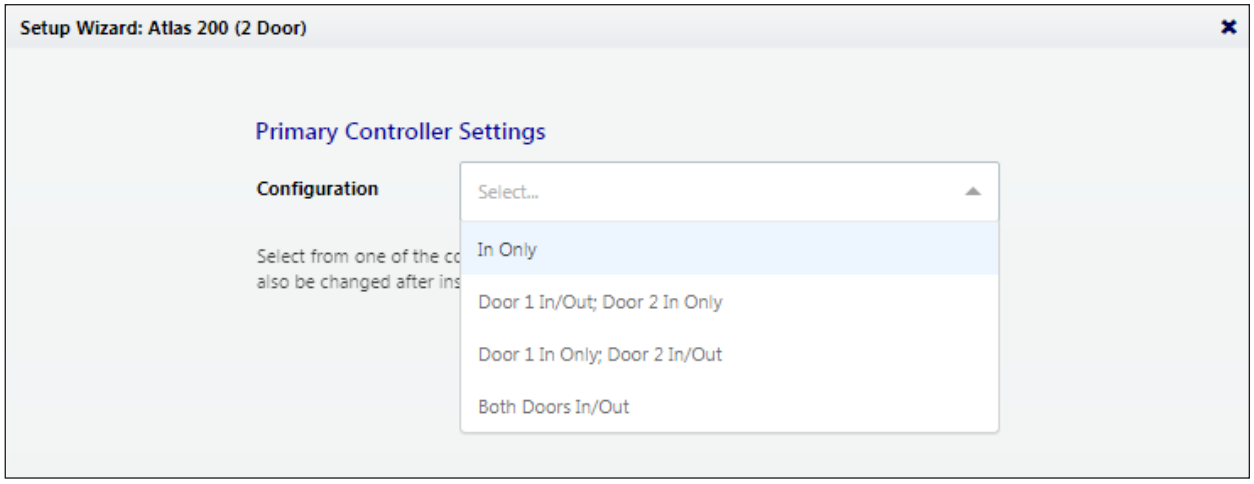
Page 3: Primary Controller Name (Primary controller Only)



Enter the Name of the controller to display in Web Management Application and reports.

Note: The Secondary controllers are named when they are connected to the system in the Web Management Application.

Page 4: Configuration (Primary controller Only)



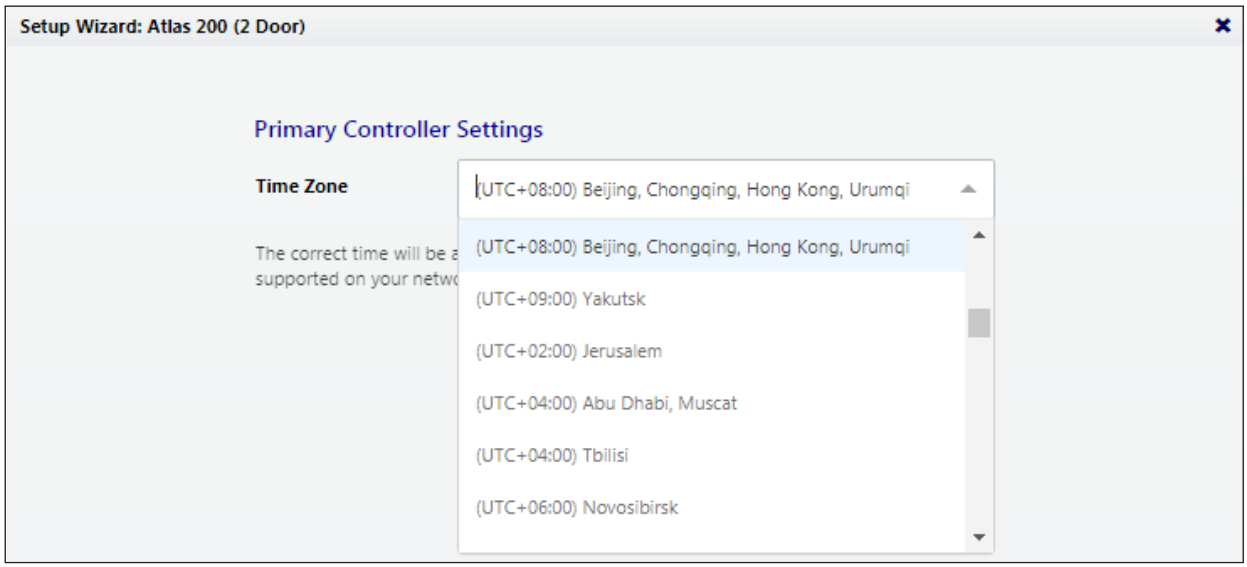
This determines the functionality of the primary controller such as controlling Door entry, controlling Door exit, Special purpose readers etc.

Note: The Secondary controllers are configured when they are connected to the system.

The available configuration options depend on the Controller model. Each option involves one or more of the following possibilities. Each possibility determines the functions of the readers connected to the controller. The configuration can be modified during "**Hardware Configuration**".

- **In Only** - This is the most common configuration, in which a reader is used to obtain access to enter, but no credentials are required to exit (although an exit button may be configured for opening the door from inside). All controllers will have at least one "In" reader. It cannot be configured for another purpose, though you may choose not to use it.
- **In/Out** - The physical door will have a reader both inside and outside. Authorization is required to access in either direction.
- **Muster Point** - The reader will serve as a muster point, where users can register that they have reached a safe location.
- **Card Enrollment Point** - The reader will be used to easily enter the card numbers when adding users.

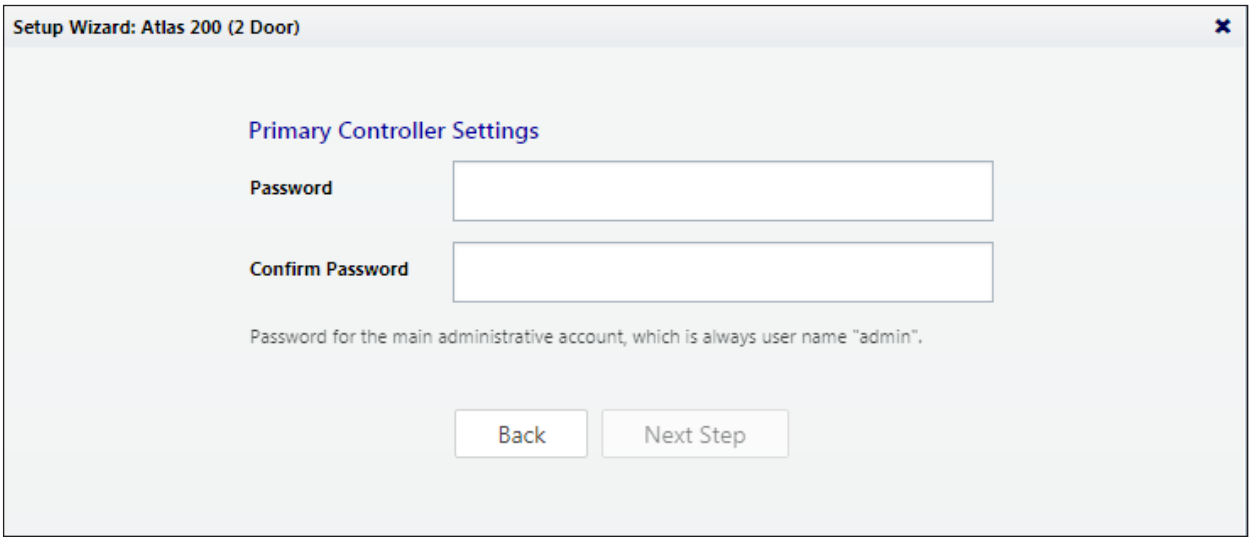
Page 5: Time Zone (Primary controller Only)



Select your time zone. In most cases you never need to set the actual time; the controller will get the time from the internet using NTP protocol. Other possibilities are discussed, under "**Review Time Setting (optional)**".

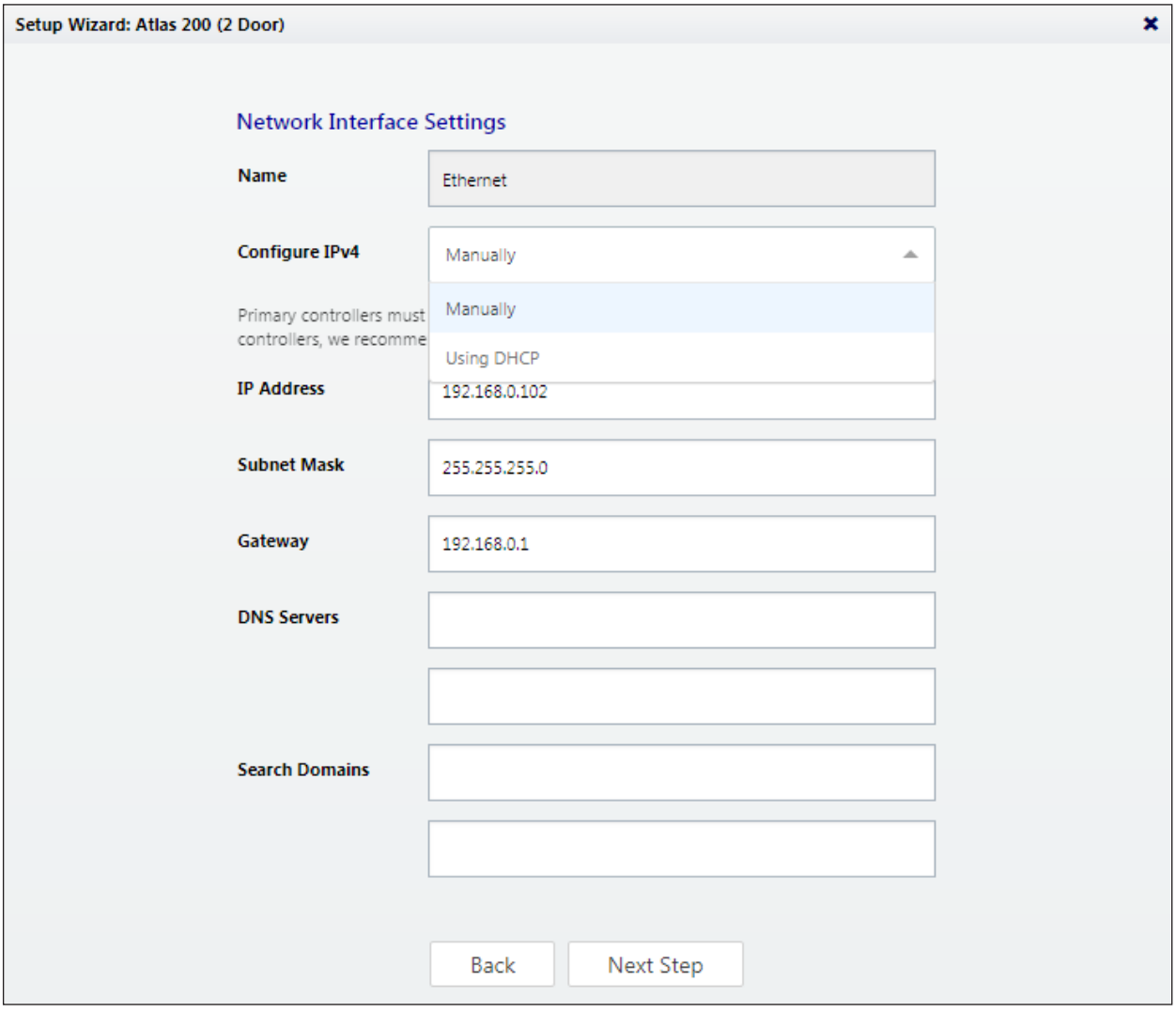
Note: The Secondary controllers get their time and time zone from the primary controller.

Page 6: Password (Primary controller Only)



Enter a strong password for the primary administrator account. The user name for this account is **"Admin"** and cannot be changed.

Page 7: Network Interface Settings



The important option here is **"Configure IPv4".**

The primary controller must have a static IP address. This is because secondary controllers need to know how to find the primary on the network. Additionally, the users need a consistent address to log in to the **Web Management Application.**

To assign a static IP address, choose **"Manually"** and enter the IP address and configuration specified by the network administrator.

Using "DHCP" is probably the right choice for secondary controllers, unless you have a complicated network as discussed below under **"Special Considerations for Complex Networks"**.

Wireless Networking: If your controller model supports WiFi, you still need to set up a wired connection, here. You can add your wireless connection once you log in to the Web Management Application. See the online help topic, "**Administration: Network**".

Page 8: Review

All your entries are displayed for review. Click either "**Back**" or "**Complete Setup**".

After completing setup, you may disconnect the direct Ethernet cable.

4. Connecting the Controller to the Network

When configuration of "**Setup Wizard**" is done, the controller will reboot itself automatically. If it is already installed, then simply reconnect it's Ethernet port to the local area network.

Otherwise, disconnect the controller and complete the physical installation. Connect it to the local area network via Ethernet.

Open a web browser and enter the IP address you specified in **Network Interface Settings** during the initial setup. This will direct you to the login screen of the Web Management Application. Enter "**admin**" as the user, and use the password you set during initial configuration. The application Dashboard will appear. Expect to see green status, indicating everything has completed correctly to this point.

Review Time Settings (optional)

By default, the primary controller will use Network Time Protocol (NTP) to automatically update the controller clock over the internet. This might not work due to local policies or because your controller does not have internet access.

If you need to change this configuration go to "**Admin → Date and Time**"

- To disable NTP, uncheck "**Update Date and Time Automatically**". When this box is not checked, you can manually set the time by checking "**Set Server Time to Current Browser Time**" and clicking Save.
- If you wish to use NTP, but with customized NTP servers, there is space to enter those server addresses. The default servers are: "0.pool.ntp.org", "1.pool.ntp.org", "1.pool.ntp.org" and "3.pool.ntp.org."
- You can also turn off the use of Daylight Savings Time.

Registration

Registration is required if you ever need to reset your system password, and optionally allowing ZKTeco to contact you about software updates and other information. You will also have access to free technical support only after you register the panel. Follow these steps to register for the first time or to update your registration information.

1. Registration can be started in two ways:
   - When you log in for the first time, click Register Now in the "**Register Your Product**" pop-up window, or
   - Select "**Menu → About**" and click the Register button. (If you have previously registered, the link is "**Update Registration**")
2. Click New Registration button in the next pop-up window. (If you have previously registered, the button is "**View/Update Registration**")
3. Fill in the registration information. Asterisks indicate required information. The e-mail address you enter must be able to receive your registration information.
4. Submit your registration automatically or by e-mail.

   a. For automatic registration, click Submit Online button. You will see a progress window followed by a success message.

   b. For e-mail registration:

      i. Click Offline Registration button. Read the instructions in the following window.

      ii. Click Download registration file link, and save the registration data file to your computer.

      iii. Create and send an e-mail message by clicking the e-mail link or entering it in your e-mail program. Your e-mail must contain the registration data file as an attachment, with its original name. The subject and text of the e-mail don't matter.

You will receive a registration confirmation file by a reply e-mail.

1. Open the e-mail and save the attachment to your computer.
2. Click Upload Confirmation button. (If you have already exited from registration, then return to this option by selecting "**Menu → About**" and clicking the Register button.)
3. Find and open the registration confirmation file you saved.

You can see a "**Registration successful**" message window.

5. Hardware Configuration

Configuration is discussed in detail in the online help topic, "**Configuration: Hardware**". Topics mentioned below are found within that section.

Go to "**Config → Hardware**". The list on the left shows all controllers. (At this point, you should see one, the primary controller.) Each controller has an "I/O" sub-controller listed beneath it. The controller manages general controller configuration, while the sub-controller manages detailed configuration of the readers, inputs, and outputs.

Click the controller and review the configuration. Note under "**Managed Doors**" the doors are automatically created to match the controller configuration you chose earlier. Every reader is represented as a door, whether its function is in, out, card enrollment point, or muster point. You might need to:

- Add more readers using the "**Modify**" button on the menu bar. Details about this operation are in the topic, "**Modifying Controller Configuration**". The Modify options are:
  - "Change to In/Out"
  - "Add Muster Point"
  - "Add Card Enrollment Point"
  - "Remove Secondary, Muster, or Card Enrollment Point"
- Change the default connection type for readers (Wiegand, OSDP, or ZKTeco RS-485). These settings are on the sub-controller, and are detailed in the topic, "**Hardware Properties**". The defaults vary by model and are listed in the topic, "**Models and Configurations**". Note that OSDP and ZKTeco RS-485 cannot be combined on the single RS-485 port.
- Change the connection properties of inputs and outputs and configure the optional functionalities of auxiliary inputs and outputs. These settings are on the sub-controller and are detailed in the topic "**Hardware Properties**".

6. Configuring the Doors

Go to "**Config → Doors**". Every reader is represented as a door, whether its function is in, out, card enrollment point, or muster point.

For In and Out doors, change the "**Default Mode**" to set the door's normal locking state.

For In doors, review the lock timings and behaviors under "**Operation**".

Card enrollment and muster doors usually need few configuration steps.

See the online help topic "**Configuration: Doors**", for more advanced configuration, such as

- Changing door mode on a schedule
- Anti-passback
- Applying the same settings to multiple doors

7. Optional Installations

Install a Signed Certificate (optional)

To provide additional security to the controller, and to avoid browser warnings when logging in, you may want to install a signed HTTPS security certificate. For more information to get a certificate, talk to your IT department.

Even if you do not install a signed certificate, all communications will still be encrypted.

To install a certificate:

1. Obtain a certificate file in .PEM or .PFX format and copy it to your computer.
2. Select "**Admin → Web Server Settings**".
3. Click Upload Certificate.
4. Complete the prompts to select and upload the certificate file.

8. User Test Access

To test access, you have to

1. Create an access level
2. Create a user
3. Give the user card, PIN, and/or biometric credentials and
4. Assign the access level to the user.

8.1 CREATING ACCESS LEVEL

1. Go to "**Access → Access Levels**".
2. Click "**Create**" on the menu bar.
3. Enter a "**Name**" for the access level.
4. Click the "**Add**" button.
5. In the pop-up window, select one or more doors that this access level will provide access to, and click "**OK**".
6. On the "**Access Levels**" screen, notice that each door has been added to the list with a schedule during which access will be granted. The default schedule, "**24/7**", provides access at all times. Schedules are explained further in the online help.
7. Click "**Save**" on the menu bar.

8.2 ADDING A USER

1. Go to "**Access → Users**"
2. Click Create on the menu bar.
3. Enter the following required information:
   - First Name
   - Last Name
   - (To test cards) Scroll down to "**Cards**" click the Add button, then enter the number of a card.
   - (To test PINs) Scroll down to "**PIN**" and either enter a 4 digit number or use the "**Create New**" button to generate a random value.
4. Scroll down to "**Door Access**". Click Add and select 1 or more doors on the following screen.
5. Click Save on the menu bar.

8.3 ASSIGNING ACCESS LEVEL

1. Go to "**Access → Users**".
2. Scroll down to "**Access Levels**". Click the Add button and select the access level you created, above.
3. Click Save on the menu bar.

The card, PIN, and fingerprint you entered works to grant access to the specified doors during the specified schedules, assuming you chose a compatible "**Default Mode**" during "**Configure Doors**".

The supported card formats are Wiegand (26, 34, 37, or 50 bits) and Corporate 1000 (35 bit). For other formats, see the online help topic, "**Configuration: Card Formats**".

More advanced ways to grant access to users are discussed in the online help under the main topic, "**Access Control**".

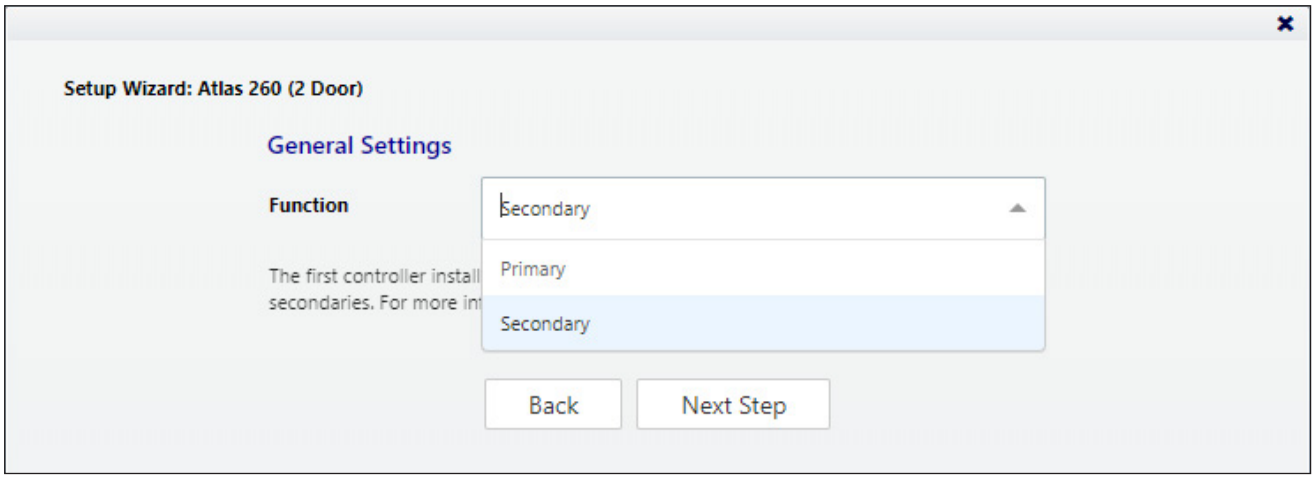
Card numbers can be more easily entered by using enrollment points. See the online help topic, "**Features and Tasks: Card Enrollment Points**".

The number of digits for PINs can be changed in "**Admin → System Settings**".

9. Adding Secondary Controller

Step 1: Initial Setup

Follow the instructions under "**Initial Controller Setup**" and "**Running the Setup Wizard**", above, for each controller. You need to select '**Secondary**' under **Function** option in the **General Settings** while running the setup wizard as shown in the image below. This will configure the controller to connect to the network.



Step 2: Adding the Controller in the Web Management Application

Secondary controllers can be automatically found and added by the Web Management Application. This is called "**Discovery**".

There are two important criteria to discover the secondary controllers.

- When using Discovery, you should connect and discover controllers one at a time. This is the only way you can differentiate them.
- Discovery only works if all controllers are networked on the same subnet. If you have a simple network, this will almost always be true. In a larger corporate environment, you might need to add secondary controllers manually. See "**Special Considerations for Complex Networks**" below.

To discover secondary controllers:

1. Log in to the Web Management Application (on the primary controller).
2. Go to "**Config → Hardware**".
3. Click Discover Controllers on the menu bar.
4. In a few seconds, a form will display all discovered controllers.
5. Click the link to add a controller. The create controller screen will appear.
   a. Select "**Configuration**" (See "**Initial Controller Setup**", above.)
   b. Enter a "**Name**" and select "**Custom Door Names**" to name the doors.
   c. Do not change other settings.
6. Click Save on the menu bar.

Adding Secondary Controller manually:

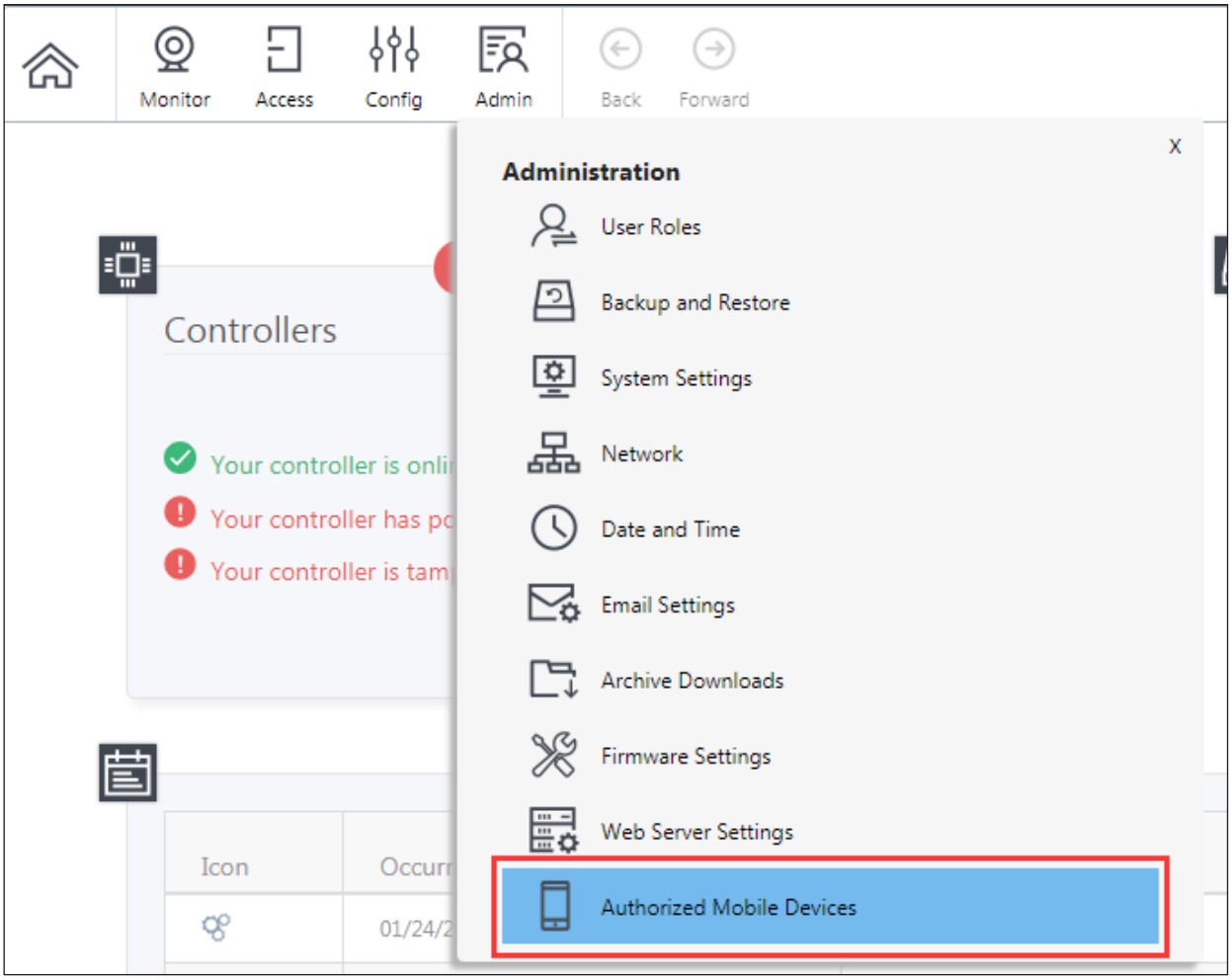
1. Click Create on the menu bar. The create controller screen will appear.
2. Select a Model.
3. Select a Configuration.
4. Enter a Name, and select Custom Door Names so you can name the doors in the box, below.
5. Enter the Controller's IP Address.
6. Leave the Port number as the default, i.e., 443.
7. Click Save on the menu bar.

10. Mobile App

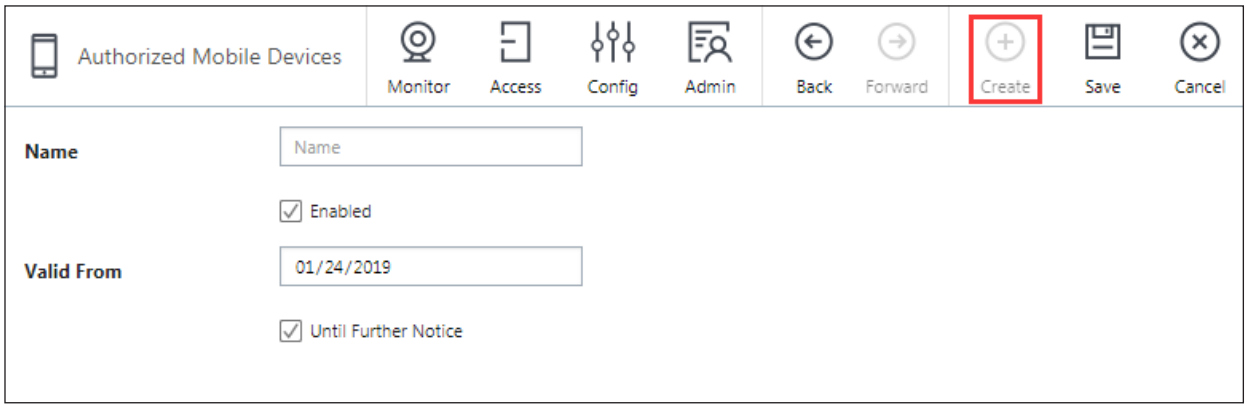
Download and install "**ZK Atlas**" Mobile App from "App Store" or "Google Play Store".

Before using the mobile App you must authorize mobile through the Web Management Application as shown below:

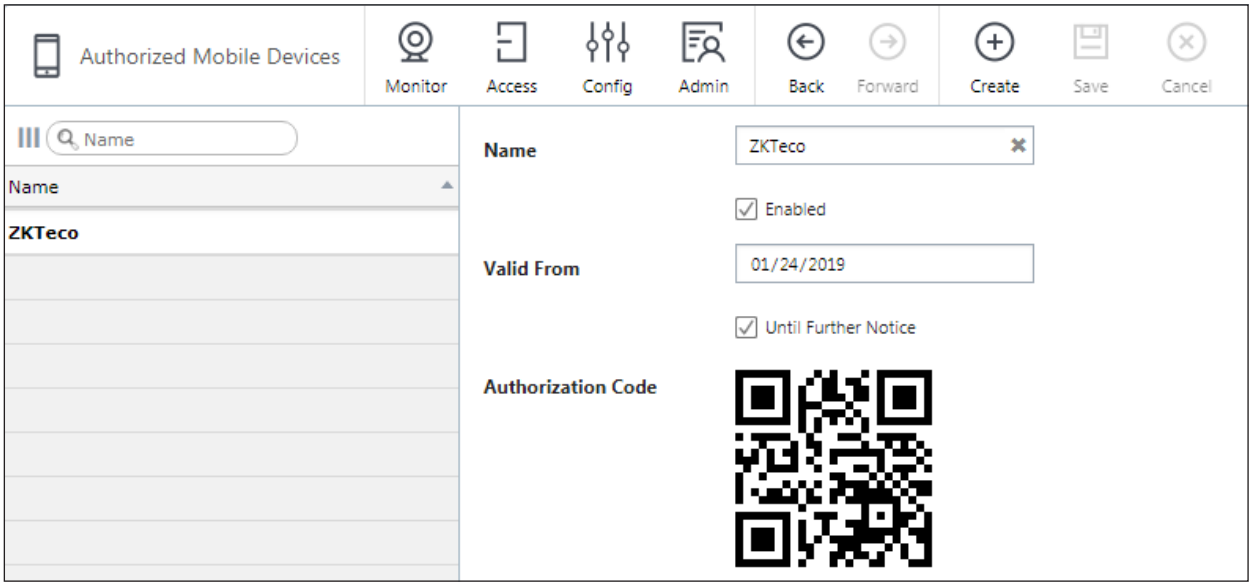
1. Go to "**Admin → Authorized Mobile Devices**"



2. Create and Save an authorization.



3. An authorization code will be generated.
   - Scan the QR code with the mobile, or
   - Right click the image to save the file and e-mail to the mobile user.



On the mobile device:

1. Run the **"ZK Atlas"** mobile App and press Scan QR Code.
2. You might have to confirm that Atlas may use the camera. Then the photo viewfinder will appear. Point the square scanning area at any copy of the authorization QR code. A picture will be taken automatically when the QR code fits the scanning area, showing the message, "**Authorization code successfully located.**"
3. On the "**Sign-In**" screen,. Enter the "**Server Address**" of the primary Atlas Series controller. Enter your Atlas Series "**Username**" and "**Password**". Press Sign In

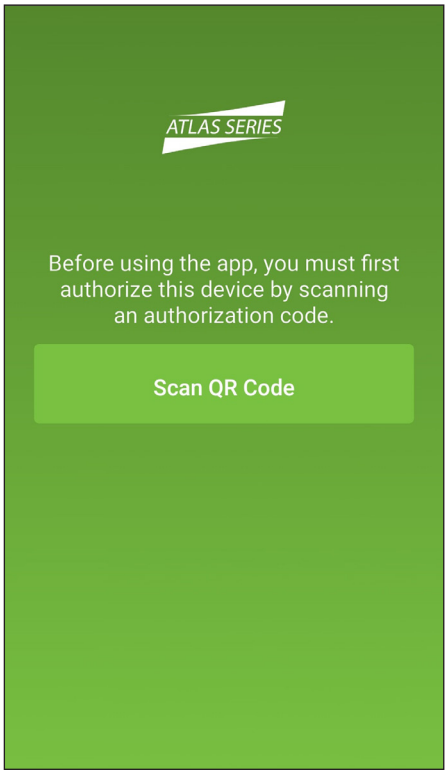


Fig. 1

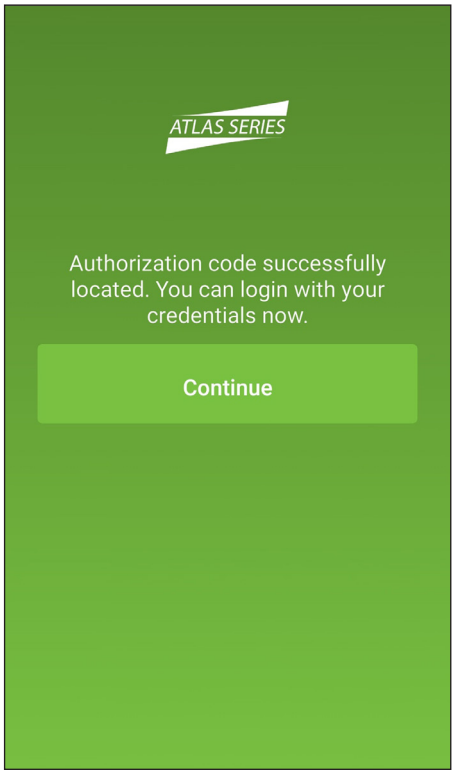


Fig. 2

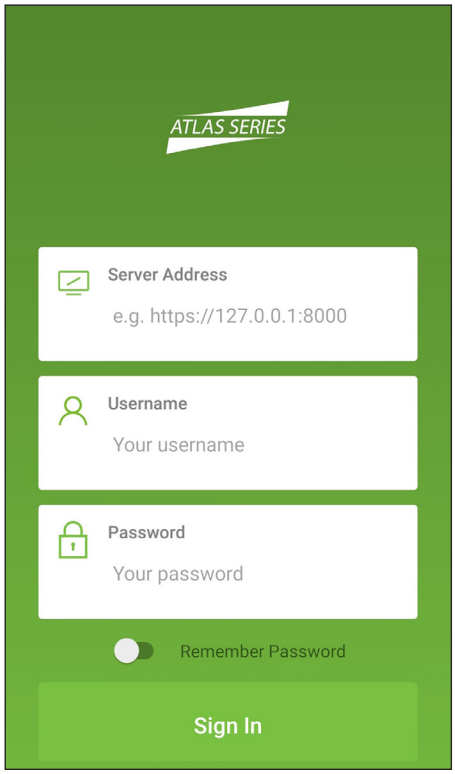


Fig. 3

4. Once signed in, you will see a list of everything you can do, including viewing alarms or status and initiating emergency lockdown.

Important: The mobile device must be connected to WiFi of the same local network to which the Atlas series controllers are connected. To connect from a distance, your network administrator must access the internet using NAT and provide the necessary "Server Address."

Each authorization code can authorize only one mobile device. You may delete and add authorizations as needed to support several devices. The number of devices you can authorize is limited by your license.

11. Special Considerations for Complex Networks

If all controllers of the Atlas Series can not be located on a single network subnet, or if Discovery is hindered by network restrictions, observe the following:

- There is no difference in the way you set up the primary controller.
- While "**Initial controller Setup**" of secondary controllers on other subnets, do not select DHCP as normally recommended. Assign these controllers static IP addresses.
- Manually add these secondary controllers in the Web Management Application. Log in and read "**Manually Adding Secondary Controllers**" in the help topic, "**Configuration: Hardware: Adding Controllers**"

Where to Go Next

A complete user manual is available through the Management Application by selecting "**Help**" from the menu in the upper right corner.

The help's "**Introduction**" page will guide you to more information on operating the application, changing the configuration of controllers and doors, setting up door access, using emergency features, and more.

ETL Certification

Resistance to attack Level I

Line security Level I

Endurance Level I

Standby Power Level I

12. Troubleshooting

1. How do I connect two-way doors?

› Connect "Out" door readers as needed, in pair with "In" door readers according to the following table.

Model	"In" Reader	Pairs with "Out" Reader
1-door	1	2
2-door	1	3
	2	4
4-door	1	5 (RS485 connection)
	2	6 (RS485 connection)
	3	7 (RS485 connection)
	4	8 (RS485 connection)

› Connect door locks and sensors to the port for their "In" door.

› See "**Initial Controller Setup**" in the "Programming Guide" for configuration instructions and additional options.

2. What does it mean when I get "Access Denied (Unknown Format)?"

› Your D0 and D1 wiring might be reversed.

› The type of card you swiped might not be recognized. See "**Adding a User**" and "**User Test Access**" in the "Programming Guide."

3. How do I connect a third party reader or a stand-alone reader to an Atlas x60 panel?

› Connect the wiegand output to the WD0 and WD1 of the stand-alone readers on the panel's reader port.

Note: The board can only supply 12 V DC, 300mA power so an external power supply may be required.

4. What kind of wire is recommended for the panel?

› 16 or 18 AWG twisted shielded wire is recommended.

5. What is the default IP of the panel?

› 169.254.202.242 - This is a "link local" IP address. See "**Initial Controller Setup**" in the "Programming Guide" for link local usage.

6. How long is the device under warranty?

› 2 Years from original purchase date, replacement/repair of hardware under ZK standard warranty requires an evaluation of the failed system by a ZK Technical Support specialist, and the issuance of a Technical Support RMA number.

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

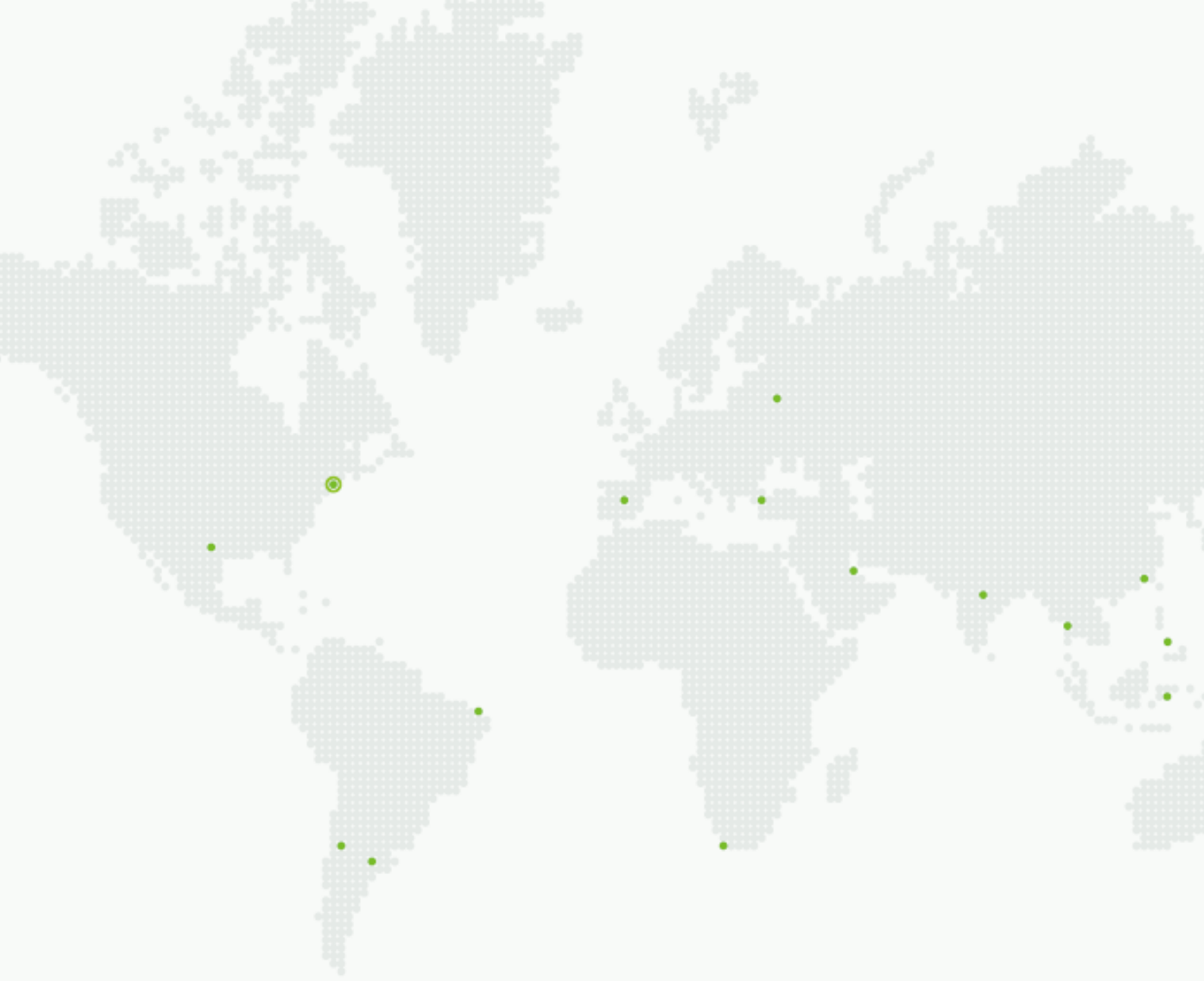
Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.



ZKTeco USA - a division of ZKTeco
1600 Union Hill Road,
Alpharetta, GA, 30005 USA
Tel: (862)505-2101
www.zktecousa.com

Date: Jan. 2020