

Installation Guide



Atlas Bio Series

Access Control Panels

Ver 2.0

This installation guide is used for Atlas-160 Bundle, Atlas-260 Bundle and Atlas-460 Bundle.



www.zktecousa.com

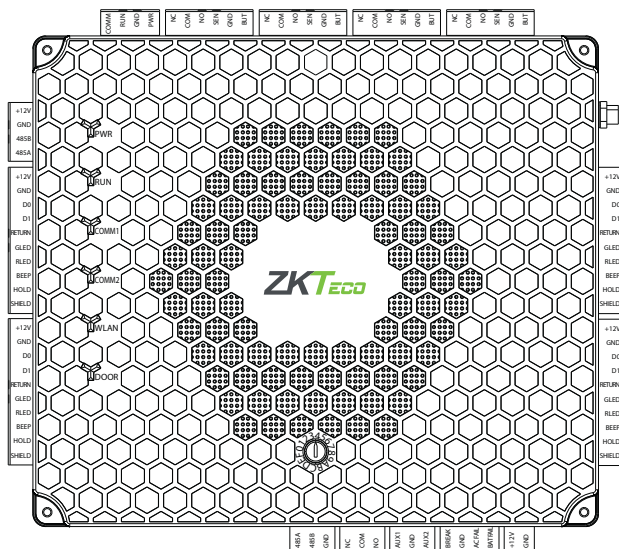
CONTENTS

What's in the Box.....	3
Optional Accessories.....	4
Safety Precautions.....	5
Product PIN Diagram.....	6
LED Indicators.....	7
Product Dimension.....	8
Installation of Panel & Cabinet.....	10
Wiring Legend.....	11
Power Wiring Diagram	12
Wiegand Connection.....	13
OSDP Connection.....	14
AHEB-0808 Connection	15
EP30CF Connection.....	16
FR1500A Connection.....	17
DIP Switch Setting for FR1500A Devices....	18
REX Connections.....	19
Lock Connection	20
AUX. I/O Connection	21
Ethernet Connection	22
Troubleshooting.....	23
Electrical Specifications	24
Introduction	27
Understanding the Atlas Series Network	28
Initial Controller Setup	29
Connect the Controller to the Network	35
Complete the Configuration	36
Add a User and Test Access	40
Adding Secondary Controllers	43
Adding the AHEB - 0808 Expansion Board	44
Adding an EP30CF Reader	46
Hanwha Wave/DW Spectrum Integration Setup..	48
ZKey Mobile Credential App.....	52
Atlas Mobile App.....	57
Special Considerations for Complex Networks	65
Where to Go Next	65

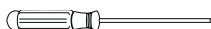


Web Management Application
Programming Guide starts at
page 27

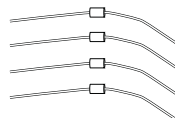
What's in the Box



4 Screws & Anchors



1 Screwdriver



4 Diodes

Optional Accessories



Wiegand Card Reader



Prox Card



Door Sensor



Exit Button



ZK9500 USB Fingerprint Scanner



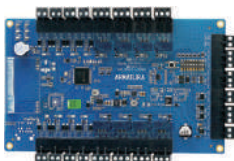
CR10E Card Enrollment Reader



EP30CF



FR1500A FP & Prox Reader



AHEB-0808



Atlas x60 Metal Cabinet

Safety Precautions

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



Do not expose to direct sunlight, water, dust and soot.



Do not place any magnetic objects near the product. Magnetic objects such as magnets, CRT, TV, monitors or speakers may damage the device



Do not place the device next to heating equipment.



Prevent water, drinks or chemicals leaking into the device.



This product is not intended for use by children unless they are supervised.



Do not drop or damage the device.



Do not disassemble, repair or modify the device.



Do not use the device for any purpose other than those specified.



Remove dust or dirt regularly. While cleaning, wipe dust off with a smooth cloth or towel instead of water.

Contact your supplier in case of any problem!

Product PIN Diagram

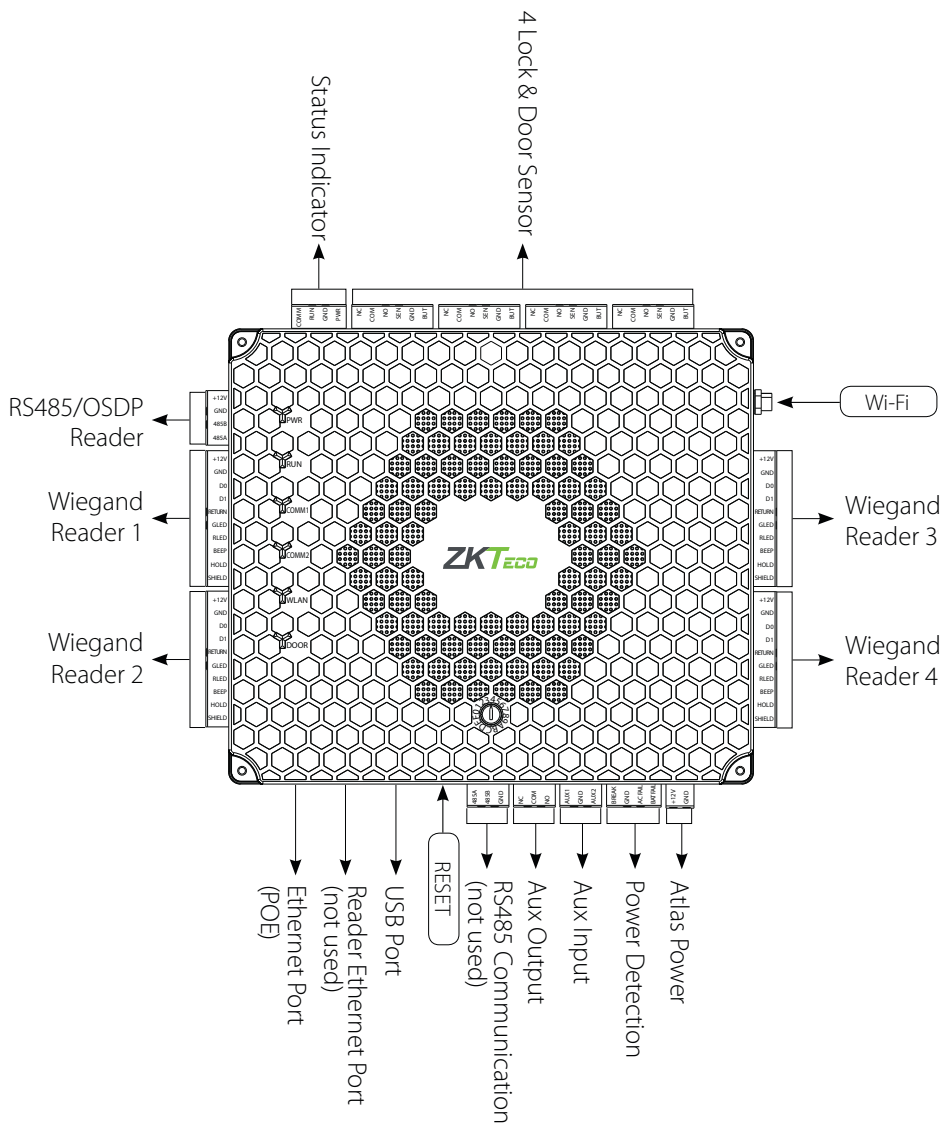


Figure 1

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

1. Press reset button for about 2-5 seconds, zk firmware will check if there is a USB disk which stores an upgrade package inserted into controller, if yes, then controller will do firmware upgrade automatically.
2. Press reset button for about 5-10 seconds, zk firmware will temporarily set IP to default 169.254.202.242.

LED Indicators



Figure 2

LINK Solid Green LED indicates TCP/IP communication is normal

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

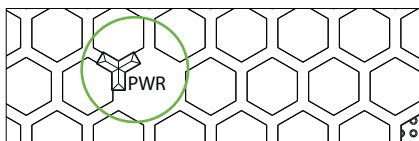


Figure 3

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

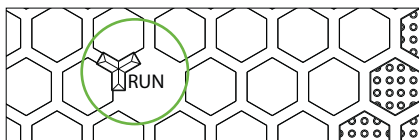


Figure 4

Flashing (RUN) Green LED indicates that panel is in its normal working state.

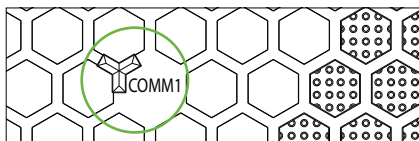


Figure 5

COMM1 Flashing Yellow indicates the system is communicating with upper-level devices (for example, the PC).

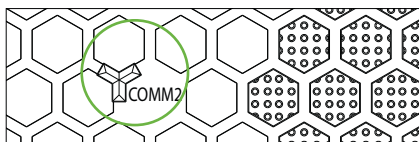


Figure 6

COMM2 Flashing Yellow indicates the system is communicating with lower-level devices (for example, readers).



Figure 7

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

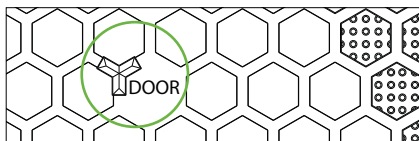
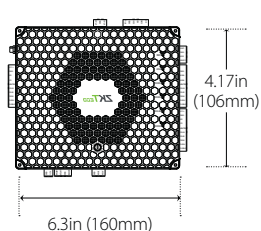


Figure 8

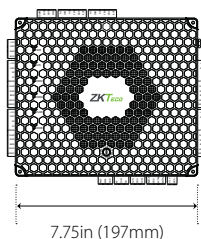
Flashing (DOOR) Green LED indicates a door opening signal (a door is opened).

Product Dimension

Atlas-160 Bundle



Atlas-260 Bundle



Atlas-460 Bundle

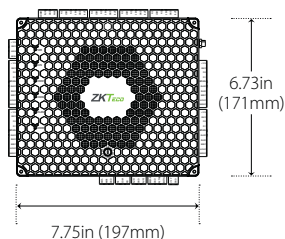


Figure 9

Model	Atlas-160 Bundle	Atlas-260 Bundle	Atlas-460 Bundle
Number of Doors Controlled	One Door	Two Doors	Four Doors
Number of Readers Supported	2 (Wiegand or OSDP Readers) 2 (Fingerprint Readers)	4 (Wiegand or OSDP Readers) 4 (Fingerprint Readers)	4 Wiegand or 8 OSDP Readers 8 (Fingerprint Readers)
Number of Inputs	4 (Exit Device, Door Contact and 2 Aux)	6 (2 Exit Devices, 2 Door Contacts and 2 Aux)	10 (4 Exit Devices, 4 Door Contacts and 2 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)

Atlas x60 Metal Cabinet

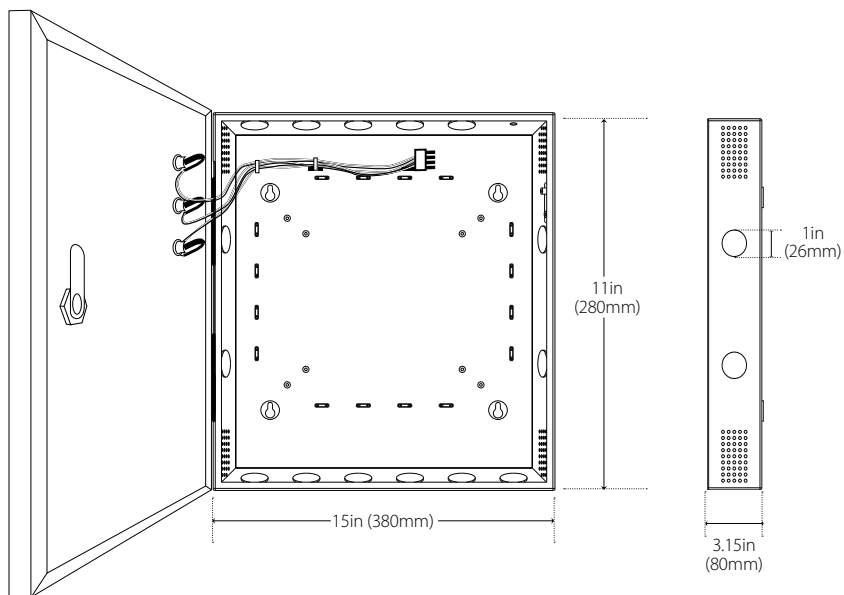
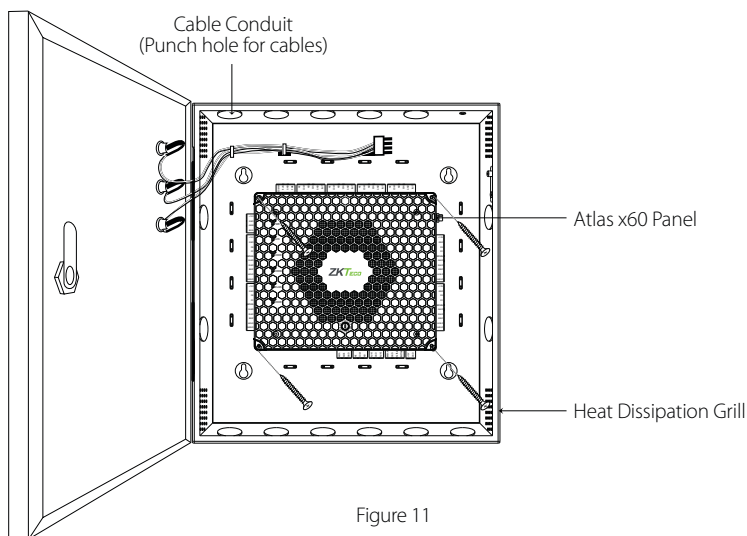


Figure 10

The surface of the metal cabinet is coated with high temperature baking paint, which can prevent rust. And the around holes are spot welded by a round metal plate. You have to frustrate them with tool when you want to put cable through.

Installation of Panel & Cabinet



Step 1

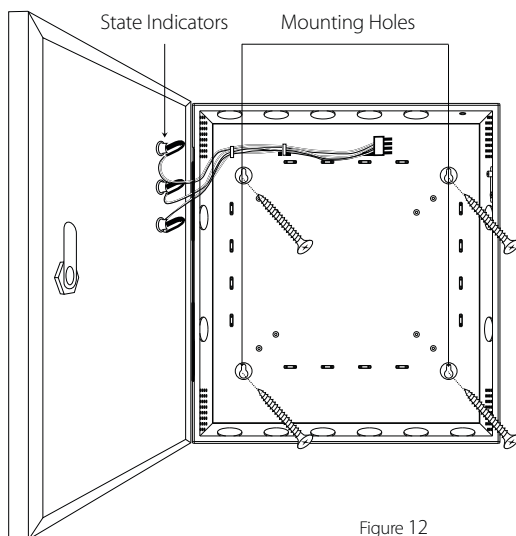
Pass the cable through holes

Step 2

Mount the Metal Cabinet

Step 3

Fasten the Panel with four screws.



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

Wiring Legend

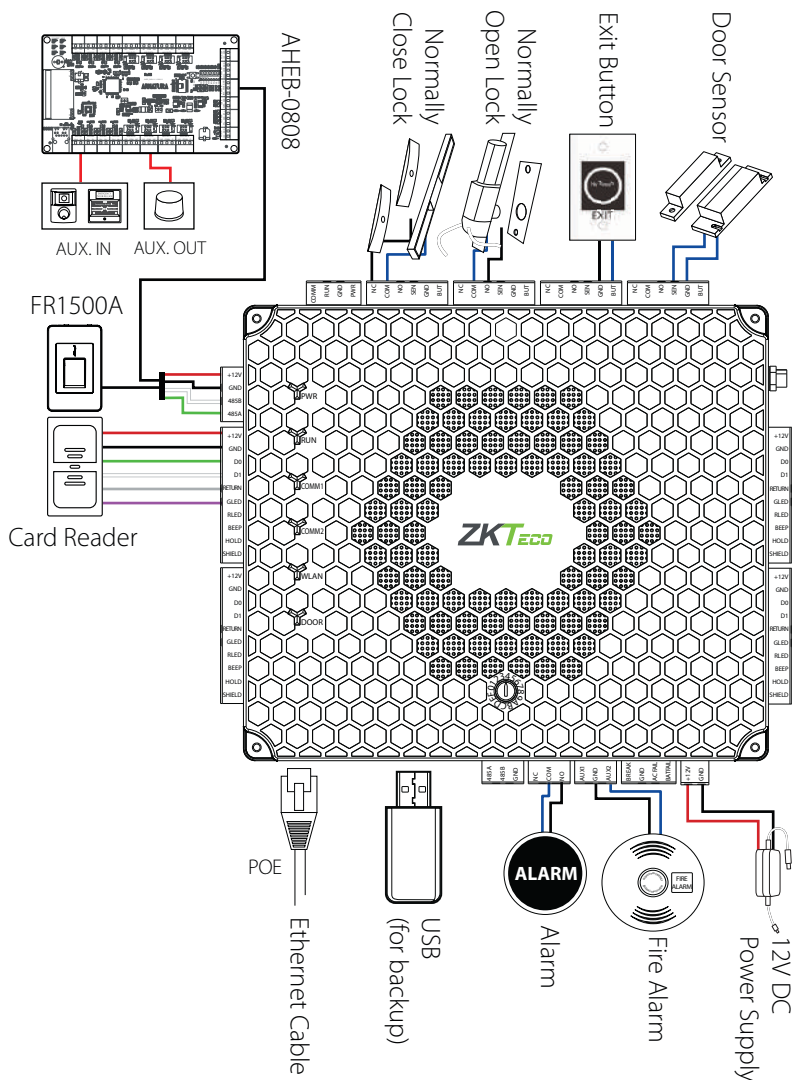


Figure 13

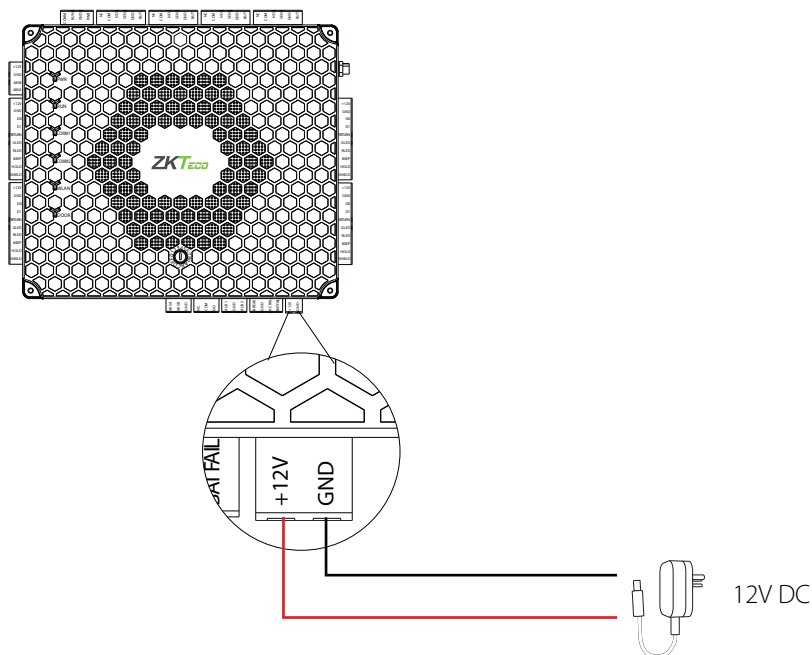
The auxiliary input may be connected to infrared motion sensors, fire alarms, or smoke detectors. The auxiliary output may be connected to alarms, cameras or door bells, etc.

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

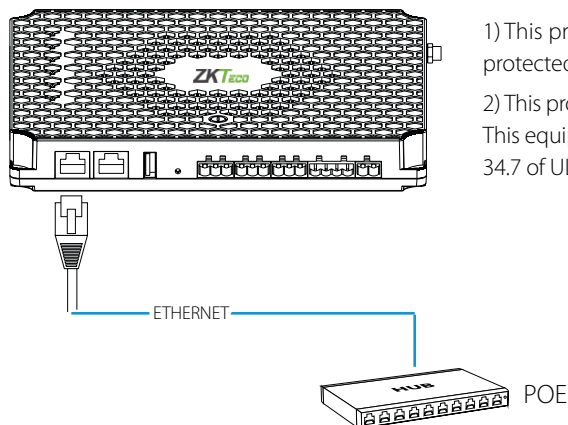
Reference to National Electrical Code, ANSI/NFPA 70 for Power over communications

Power Wiring Diagram

12V Power



POE Power



- 1) This product comes with a 12V DC surge protected Class 2 power supply.
- 2) This product comes with a POC cable source. This equipment is in compliance with section 34.7 of UL 294, 7th Edition.

Figure 14

Wiegand Connection

Wiegand card readers should be connected via the Wiegand reader ports. When scanning a card or inputting a PIN, the reader will send the card or PIN to the panel via Wiegand communication.

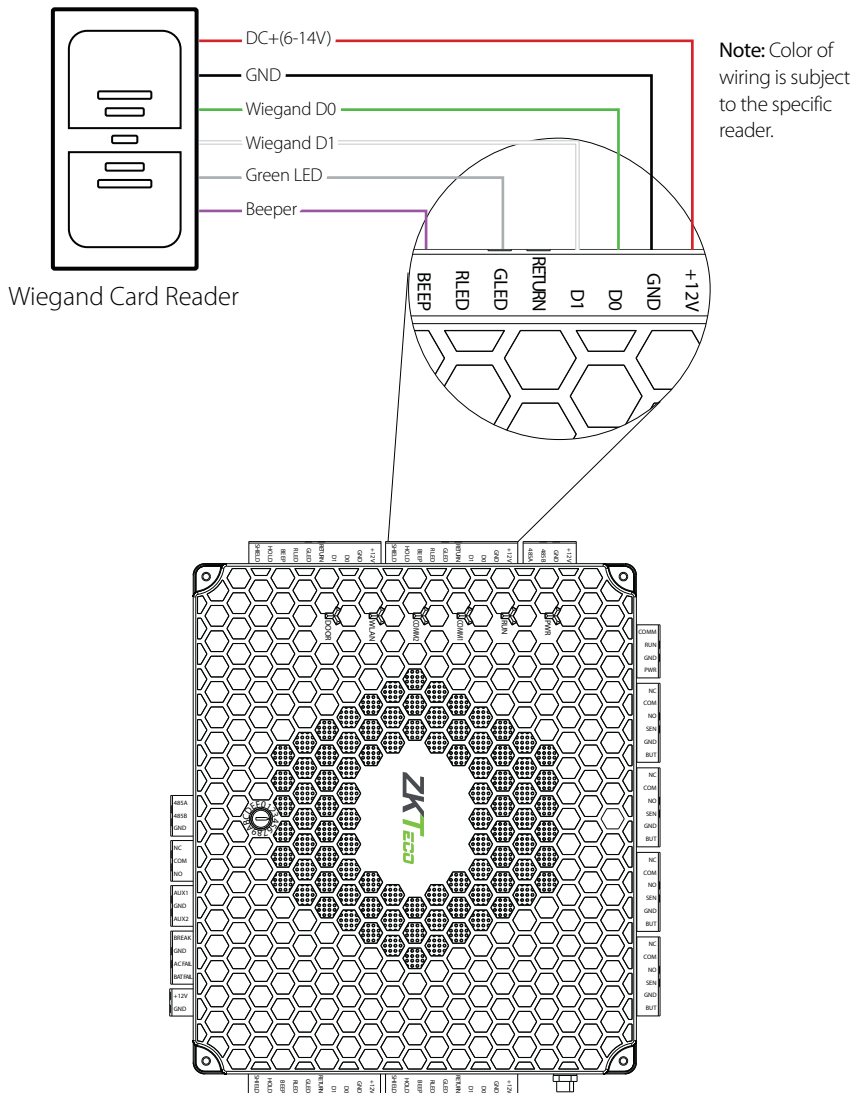


Figure 15

OSDP Connection

OSDP readers should be connected via the RS485 communication port. When scanning a card or inputting a PIN, the reader will send the card or PIN to the panel via OSDP communication.

NOTE: OSDP and ZKTeco RS485 (FR1500A readers) cannot be supported simultaneously.

OSDP Reader

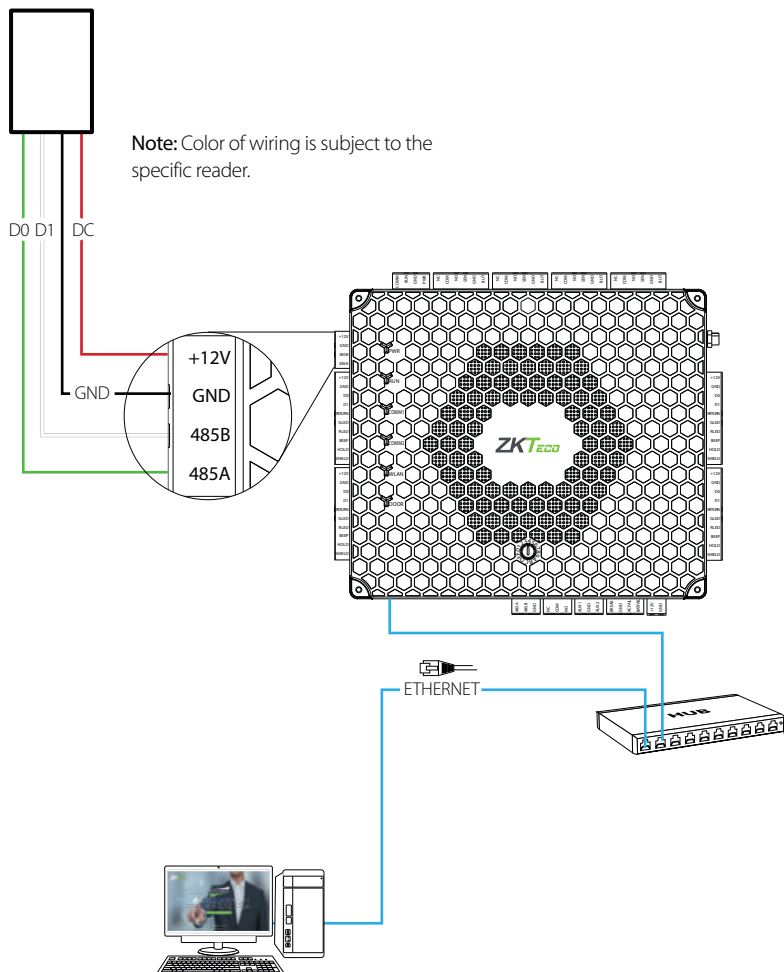


Figure 16

AHEB-0808 Connection

The AHEB-0808 expansion board should be connected via the RS485 terminal. The AHEB-0808 Supports a maximum of 8 inputs & 8 outputs. A maximum of 8 AHEB-0808 boards can be connected in a single instance.

NOTE: Set the RS485 addresses of each AHEB-0808 by the DIP switch before power is supplied.

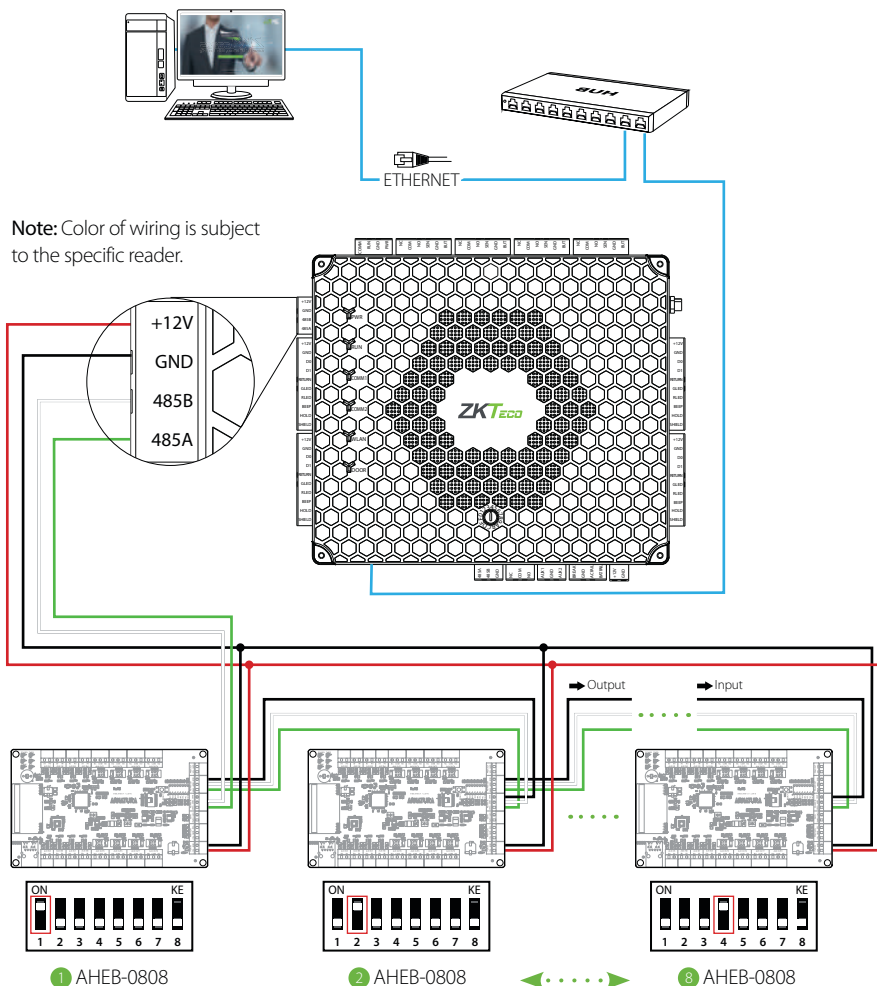


Figure 17

EP30CF Connection

The EP30CF reader is one of the most comprehensive biometric (fingerprint) + card readers available. The EP30CF supports fingerprint, proximity cards, NFC & BLE. The EP30CF connects via the RS485 terminal. When a card or fingerprint is scanned, the reader will send the output through RS485 to the panel.

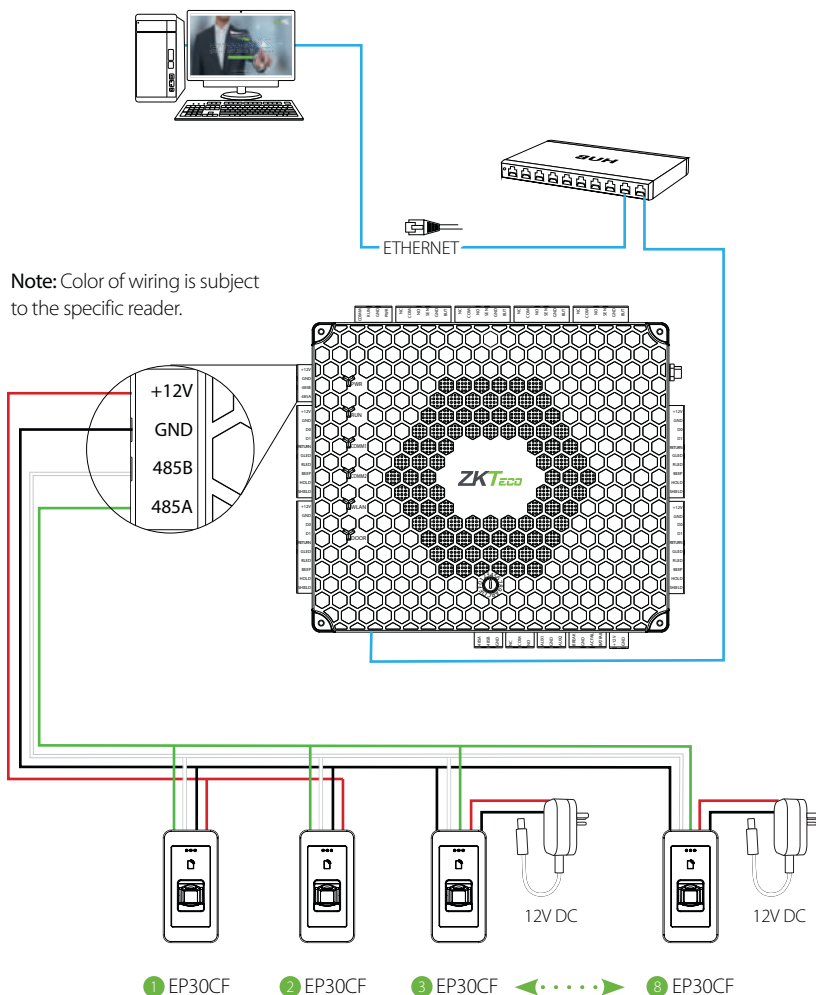


Figure 18

FR1500A Connection

The FR1500A comes in versions supporting ID, MF, iClass & HID. The FR1500A fingerprint readers should be connected via the RS485 terminal. When a card or fingerprint is scanned, the reader will send the output through RS485 to the panel.

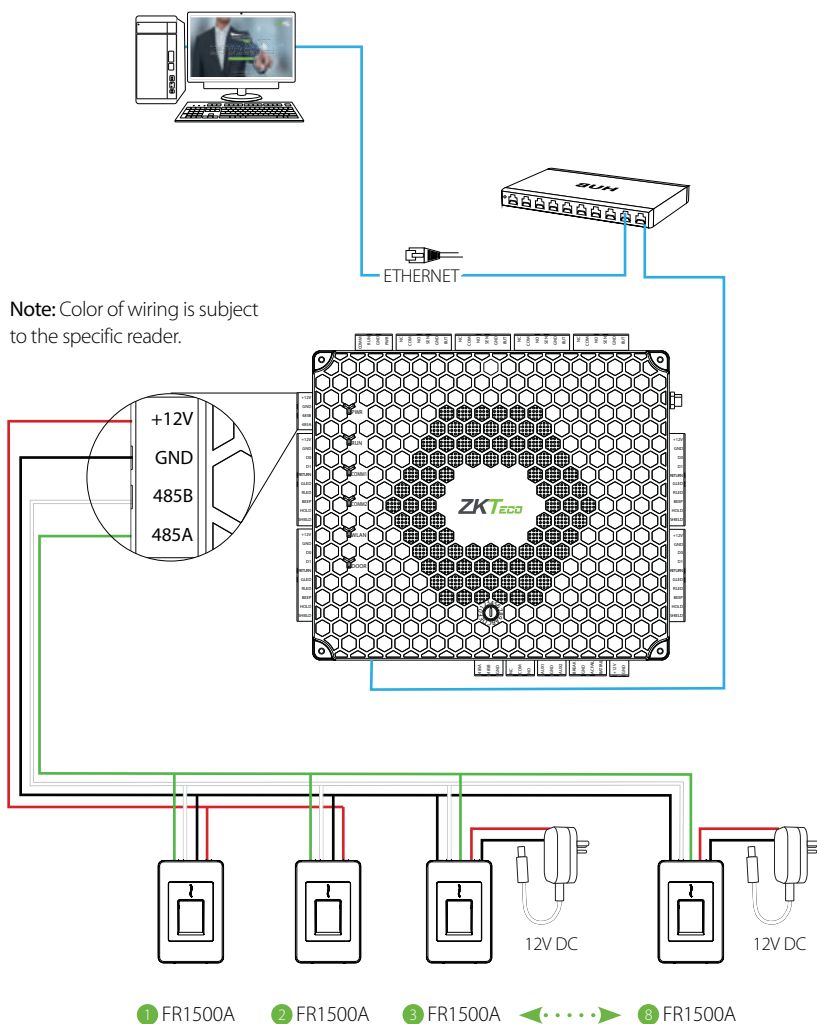


Figure 19

DIP Switch Setting for FR1500 Devices

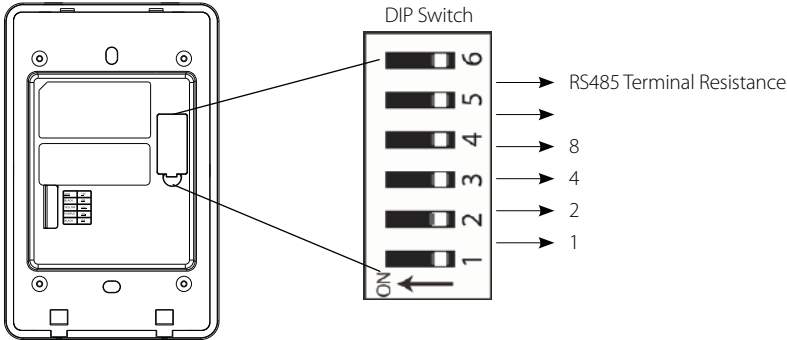


Figure 20

Address	Switch Settings	Address	Switch Settings
1		5	
2		6	
3		7	
4		8	

Important Notes

1. There are six DIP switches on the back of FR1500. Switches 1-4 is for RS485 address, switch 5 is reserved, switch 6 is for reducing noise on long RS485 cable.
2. Set the odd number for IN reader, and the even number for OUT reader (for eg. For two readers for one door-the RS485 address 1 is for IN reader, RS485 address 2 is for OUT reader).
3. If FR1500 is powered via the Atlas-460 panel, the length of wire should be less than 100 meters or 330 ft.
4. The External RS485 interface can supply maximum 500mA current, The FR1500A's startup current is 240 mA. So Atlas-460 only can only power two FR1500's.
5. If the cable length is more than 200 meters or 600 ft , the number 6 switch should be ON as below.



Distance: More than 200 meters



REX Connections

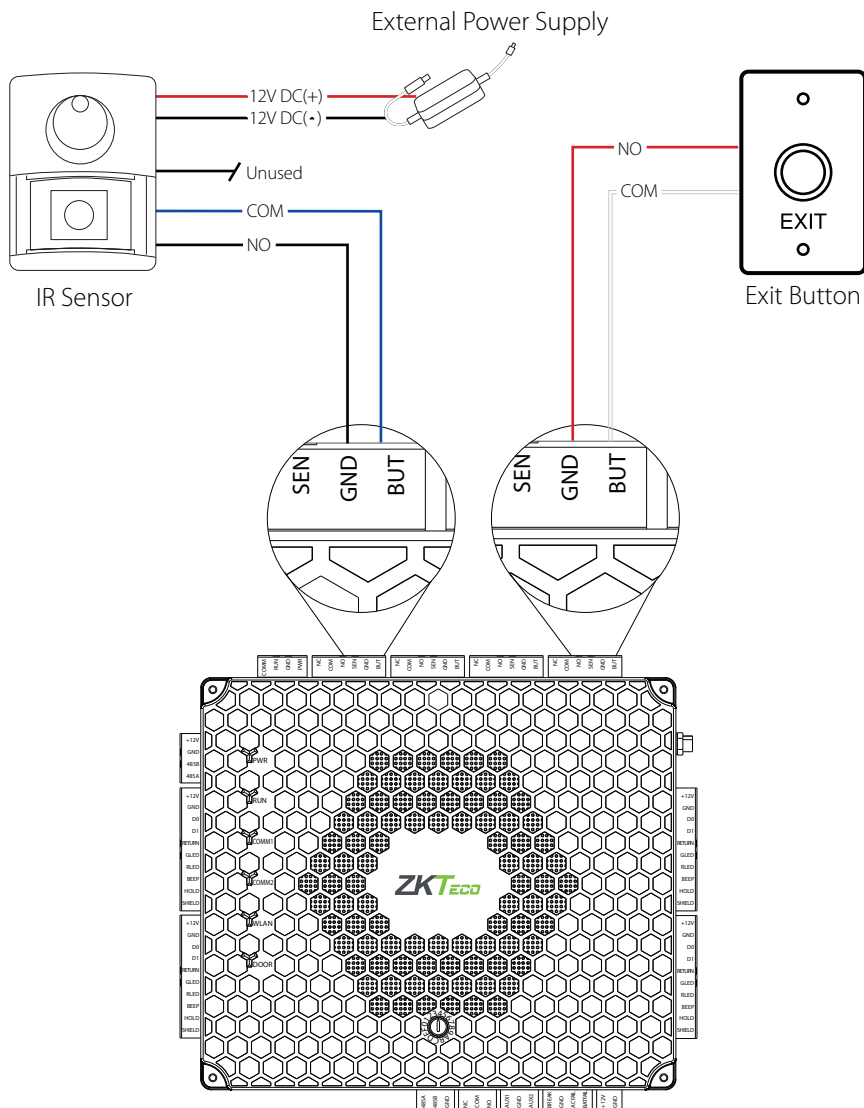


Figure 21

Lock Connection

NO: Locks always stay locked until power is provided from the board after a valid card read.

NC: Locks always stay locked until power is cut by the board after a valid card read.

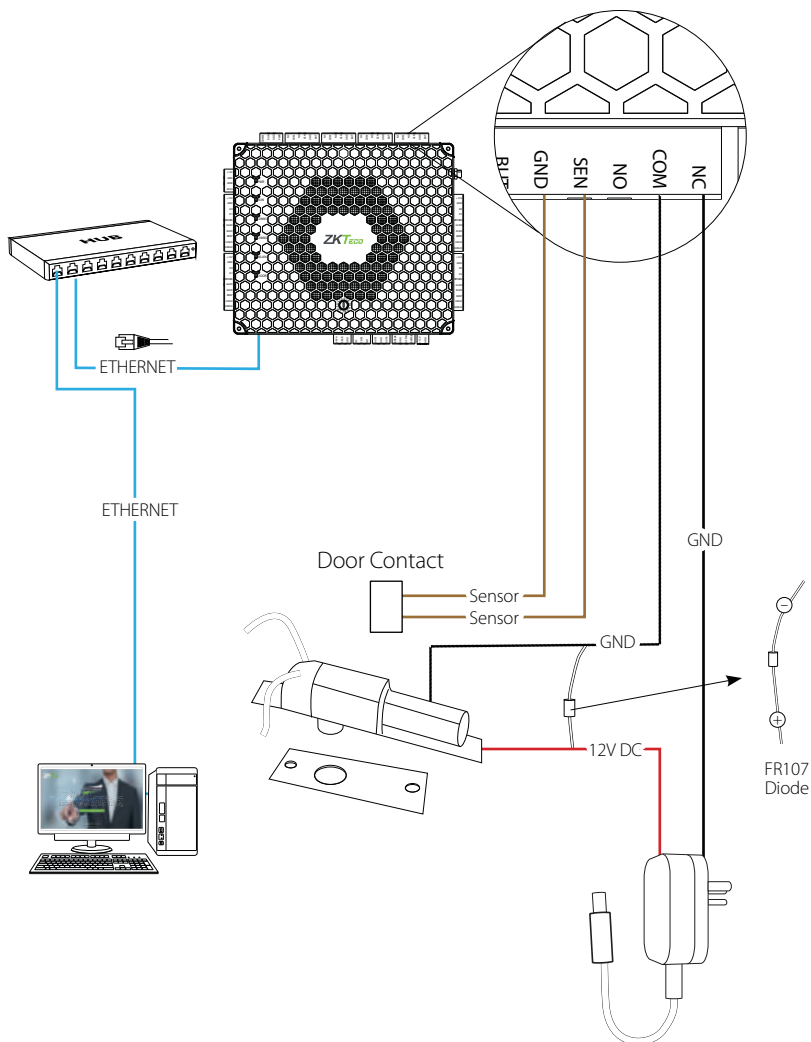


Figure 22

AUX. I/O Connection

AUX. Input Connection

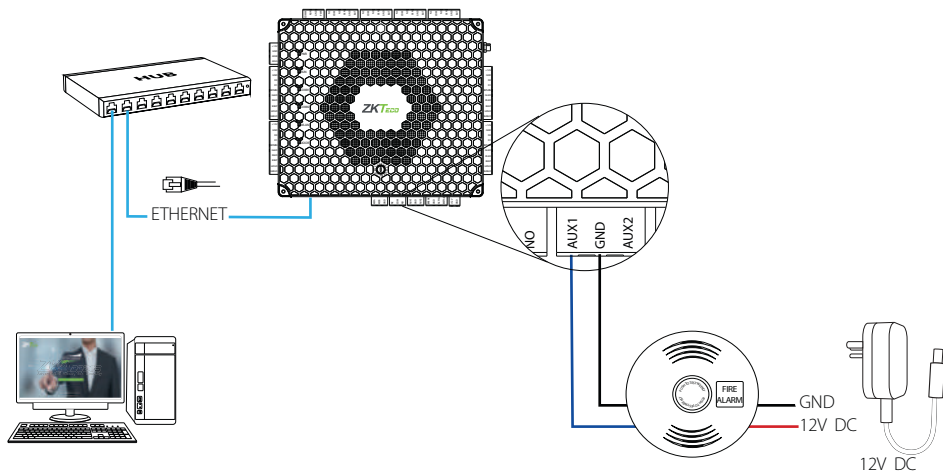


Figure 23

AUX. Output Connection

Normally, the AUX output is used to connect an external alarm which can be linked to a reader or Aux input events.

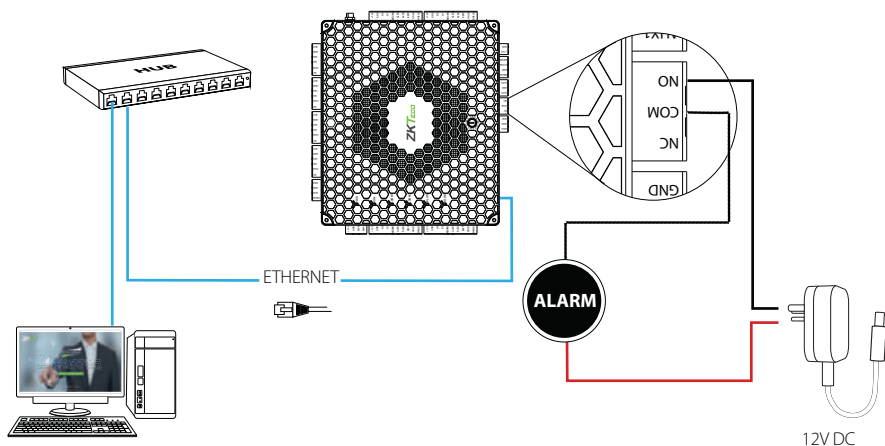


Figure 24

Ethernet Connection

LAN Connection

Important Notes:

1. Both 10Base-T and 100Base-T are supported
2. This cable distance should be less than 330 ft. (100m)
3. For cable lengths more than 330ft. (100m), use an extender or switch.

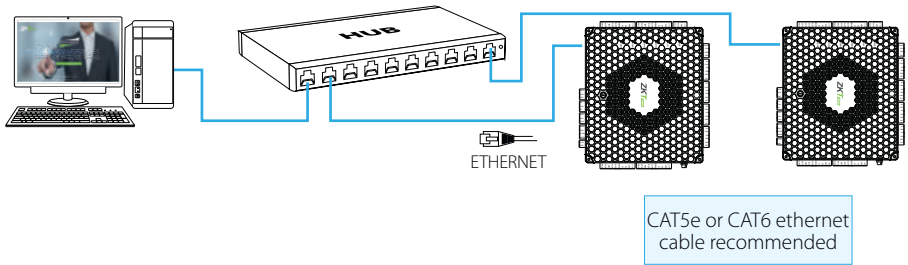


Figure 25

Direct Connection

To connect the Atlas x60 series with a PC directly, connect both devices with a straight network cable. As the Atlas x60 supports auto MDI/MDIX, it is not necessary to use a crossover type cable.

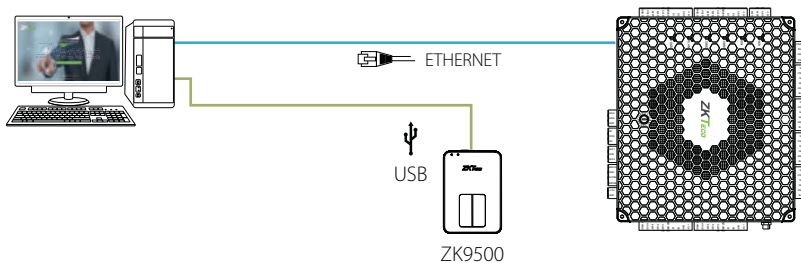


Figure 26

Troubleshooting

1. How do I connect in/out doors?

- › Connect "Out" door readers as needed, in pairs 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 "Add a User and 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.

Electrical Specifications

	Minimum	Typical	Maximum	Notes
WORKING POWER SUPPLY				
Voltage (V) DC	9.6	12	14.4	Use surge protected class 2 power supply
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	

Specifications

Communication	TCP/IP, OSDP
Baud Rate for RS485	9600-15200
Power Supply	12V DC, 3A
Users Capacity	5,000
Event Database Capacity	10,000 transactions, plus unlimited archive downloads
LED Indicator	Indicator for communication, power, status and prox card
Environment	32-113 °F (0-45°C)
Operating Humidity	20% to 80%
Number of doors controlled	Four Door (four door one way and two door two way)
Number of readers supported	4 Wiegand or 8 RS-485 or 8 OSDP
Types of readers supported	125kHz and 13.56MHz Wiegand readers, OSDP (RS-485), others upon request
Number of Inputs	10 (4 Exit Device, 4 Door Status, 2 AUX)
Number of Outputs	5 (4- Form C relay for lock and 1- Form C relay for AUX output)
Weight	Atlas-160: 9lbs (3.8kg); Atlas-260/460: 10lbs (4.2kg)
Enclosure	Metal Cabinet
Mounting	Wall Mount
Dimensions (Bundle Only)	14in. X 2.5in. X 12in. 380mm(L) X 80mm(W) X 280mm(H)
CPU	32 bit 1.2GHz
RAM	256MB
Flash	1GB
Certified	   

Atlas Series Web Management Application



Programming Guide

- Introduction.....27
- Understanding the Atlas Series Network.....28
- Initial Controller Setup.....29
- Connect the Controller to the Network.....35
- Complete the Configuration.....36
- Add a User and Test Access.....40
- Adding Secondary Controllers.....43
- Adding the AHEB-0808 Expansion Board.....44
- Adding an EP30CF Reader.....46
- Hanwha Wave/DW Spectrum Integration Setup.....48
- ZKey Mobile Credential App.....52
- Atlas Mobile App.....57
- Special Considerations for Complex Networks.....65
- Where to Go Next.....65

Introduction

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. Supported certificate formats are PEM or PFX. See “Complete the Configuration,” below.
3. Find out whether using network time protocol (NTP) to automatically update the controller clock over the Internet is possible and acceptable, as well as 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.

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 will operate on the network.
3. Connect the controller to the local network.
4. Log in to the controller with a web browser and complete essential configuration.
5. Add a user and test door access.
6. Add any secondary controllers you are installing.

Help

This guide refers you to online help topics for more detailed information. The help is available once you have connected the first controller and logged in to the Web Management Application. Open it by selecting “Help” from the menu in the upper right corner.

Understanding the Atlas Series Network

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, varies among browser applications. You can prevent this warning by installing a signed HTTPS certificate when directed, below.

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 provides a Web Management Application you can log into from a web browser. This application on the primary controller is where you will manage all configuration for the entire system.

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

Network Considerations

Ideally, all controllers should be networked on the same subnet. If you have a simple home or small office network, this will almost always be the case. For more complex networks, be sure to review the “Special Considerations” discussed at the end of this document before proceeding.

Initial Controller Setup

Connecting

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 will 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 should get an insecure site warning from the browser (see 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 become available.

Trouble Connecting: If at any point you find you cannot connect to the controller at the default IP address, or the address you configure, below, you can try a hard network reset. Find the small opening on the controller labeled "Reset." Insert a paperclip to depress the button for **5-10** seconds. The controller address will revert to the default, 169.254.202.242, until rebooted, reset, or the configuration is modified.

Running the Setup Wizard

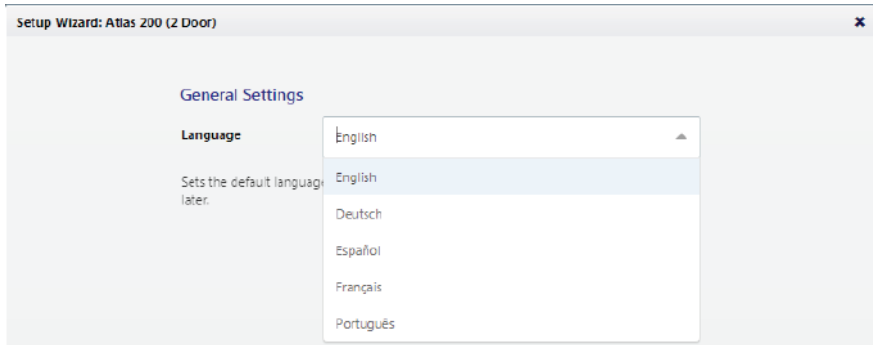
Log in using the default administrator account:

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

You will be directed to the Setup Wizard, where you will enter information required for the controller to operate.

Initial Controller Setup

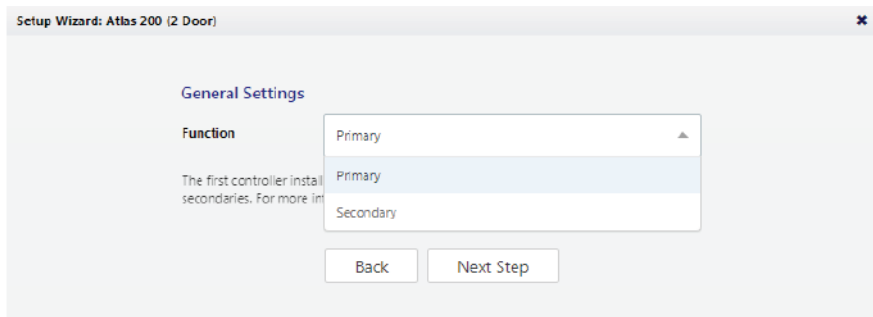
Page 1: Language



Choose a language. Your choice 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, Language does not affect the Web Management Application. It does set the language of the simplified management application on this controller, and can be changed later in the configuration of this controller.

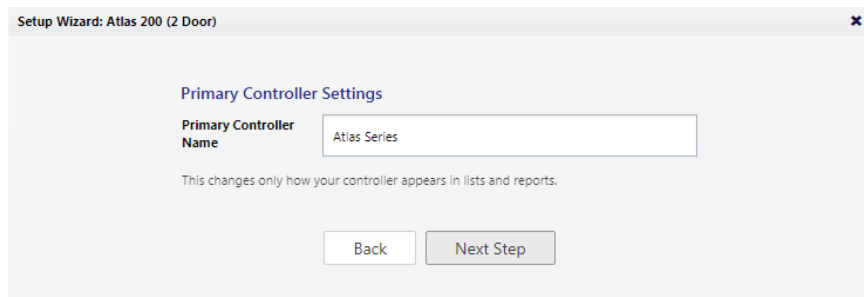
Page 2: Function



Choose whether this controller will be a "Primary" or a "Secondary". Make sure you understand the Atlas Series network, discussed above. The first controller installed should be a primary, and all others should be secondaries.

Initial Controller Setup

Page 3: Primary Controller Name (primaries only)



Setup Wizard: Atlas 200 (2 Door)

Primary Controller Settings

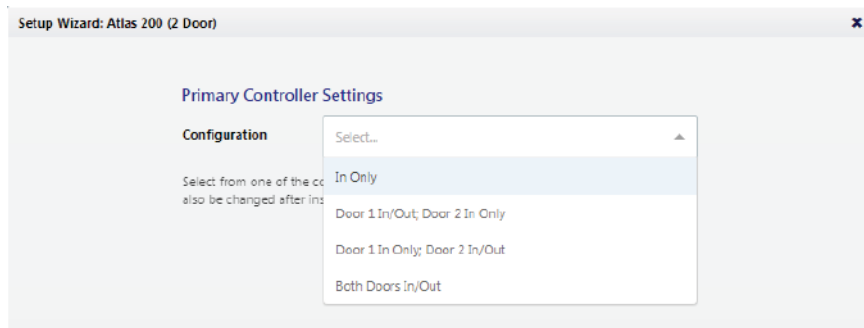
Primary Controller Name

This changes only how your controller appears in lists and reports.

The name of the controller will be used for display in the Web Management Application and in reports.

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

Page 4: Configuration (primaries only)



Setup Wizard: Atlas 200 (2 Door)

Primary Controller Settings

Configuration

Select from one of the configurations. The configuration will also be changed after installation.

- In Only
- Door 1 In/Out; Door 2 In Only
- Door 1 In Only; Door 2 In/Out
- Both Doors In/Out

This determines what your controller will be used for: controlling door entry, perhaps door exit, or as special purpose readers.

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

Initial Controller Setup

Configuration options available depend on the controller model. Each option will involve one or more of the following possibilities. Each possibility determines the function of the card, PIN, or biometric readers connected to the controller. The configuration can be modified during “Complete the Configuration,” below.

In Only - This is the most common configuration, where a reader is used to gain entry, but no credentials are required to exit (although an exit button may be configured for opening the door from the inside).

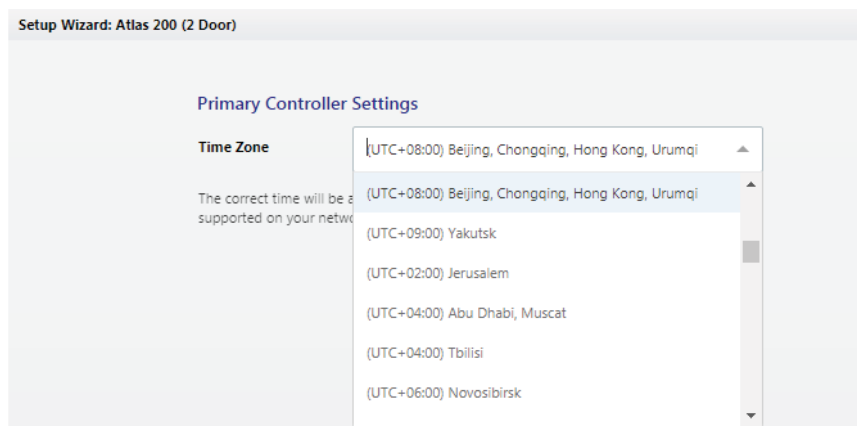
All controllers will have at least one “In” reader. It cannot be configured for another purpose, though you may choose not to use it.

In/Out - The physical door will have a reader both inside and outside. Authorization is required to pass either direction.

+ **Muster Point** - The second reader will serve as a muster point, where users can register that they have reached a safe location.

+ **Card Enrollment Point** - The second reader will be used to easily enter card numbers when adding users.

Page 5: Time Zone (primaries only)

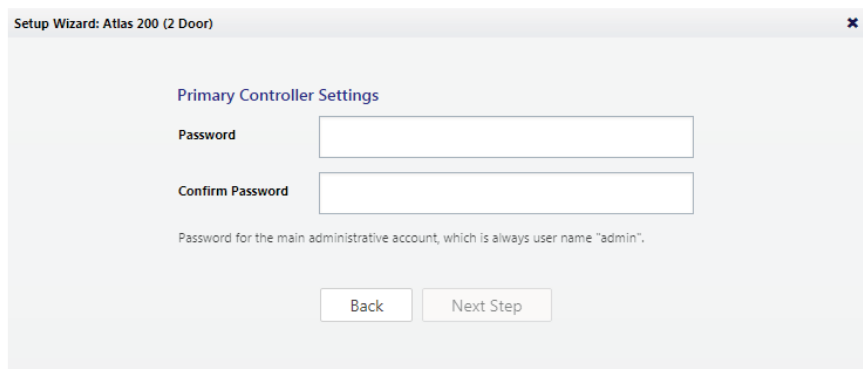


Initial Controller Setup

Select your time zone. In most cases you will never need to set the actual time; the controller will get the time from the internet using a technology called NTP. Other situations are discussed, below, under “Complete the Configuration.”

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

Page 6: Password (primaries only)



Setup Wizard: Atlas 200 (2 Door) ✕

Primary Controller Settings

Password

Confirm Password

Password for the main administrative account, which is always user name "admin".

Enter a strong password for the primary administrator account. The user name for this account is “admin” and cannot be changed.

Initial Controller Setup

Page 7: Network Interface Settings

Setup Wizard: Atlas 200 (2 Door)

Network Interface Settings

Name: Ethernet

Configure IPv4: Manually

Primary controllers must have static IP addresses, we recommend: Manually

IP Address: 192.168.0.102

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

DNS Servers:

Search Domains:

Back Next Step

The important choice here is “Configure IPv4.”

A 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 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 are logged 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.

Connect the Controller to the Network

When you "Complete Setup," 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.

Complete the Configuration

Open a web browser and enter the IP address you specified in Network Interface Settings during 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 allows ZKTeco to contact you about software updates and other information. 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 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.”)

Complete the Configuration

3. Fill in the registration information. Asterisks indicate required information. The email address you enter must be able to receive your registration information.
4. Submit your registration automatically or by email.
 - a. For automatic registration, click **Submit Online** button. You will see a progress window followed by a success message.
 - b. For email registration:
 - i. Click the **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 email message by clicking the email link or entering it in your email program. Your email must contain the registration data file as an attachment, with its original name. The subject and text of the email do not matter.

You will receive a registration confirmation file by reply email. When you do,

1. Open the email 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 should see a "Registration successful" message window.

Complete the Configuration

Fine Tune 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.) Each controller has an “I/O” sub-controller listed beneath it. The controller item 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” that doors were 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:
 - o “Change to In/Out”
 - o “Add Muster Point”
 - o “Add Card Enrollment Point”
 - o “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 optional functionality of auxiliary inputs and outputs. These settings are on the sub-controller, and are detailed in the topic, “Hardware Properties”.

Configure 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.

Complete the Configuration

For In doors, review the lock timings and behaviors under “Operation”.

Card enrollment and muster doors usually need little configuration.

See the online help topic, “Configuration: Doors”, for more advanced configuration, such as

- changing door mode on a schedule,
- anti-passback, and
- applying the same settings to multiple doors

Install a Fingerprint Enrollment Reader (optional)

If you are using biometric readers, a ZKTeco USB fingerprint enrollment reader must be installed at any computer where fingerprints will be enrolled.

1. Plug the device into any USB port.
2. Install the Fingerprint Driver software (available on the Downloads page at ZKTecoUSA.com).

Install a Signed Certificate (optional)

To provide extra security for the controller, and to avoid browser warnings when logging in, you might wish to install a signed HTTPS security certificate. For more information on what this means, and to get such a certificate, talk to your IT department.

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

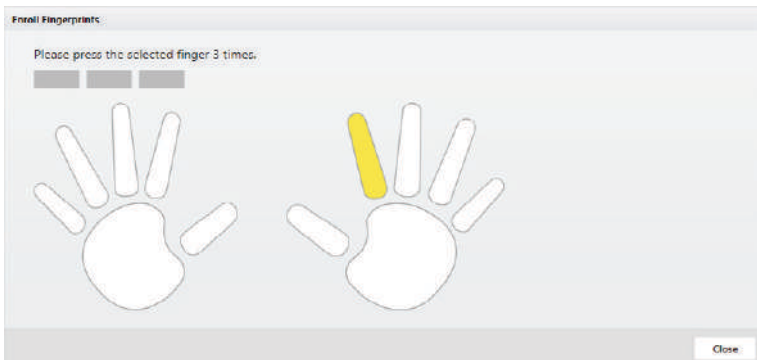
To install a certificate:

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.

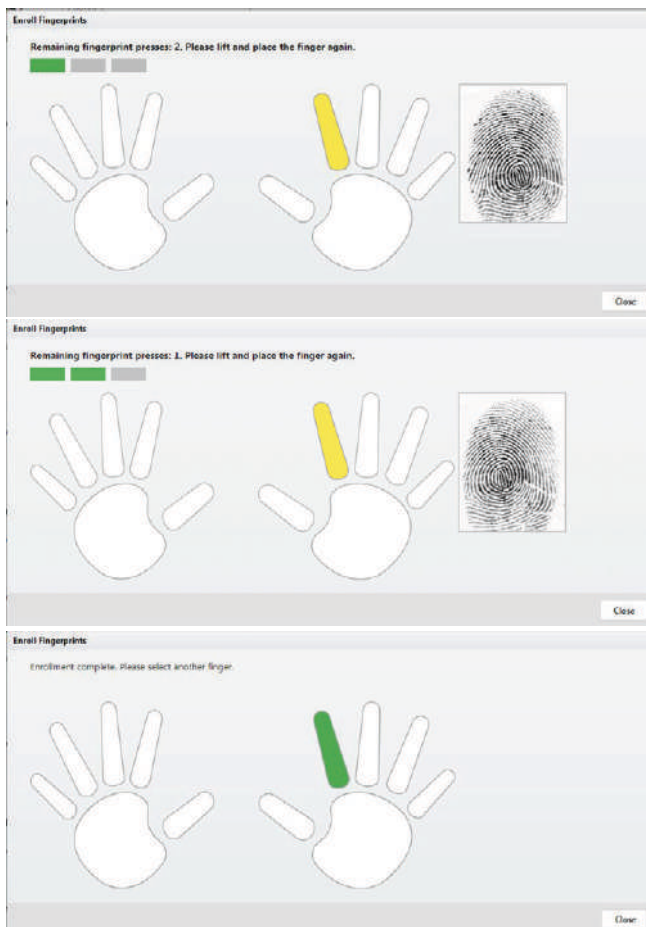
Add a User and Test Access

1. Go to "Access → Users."
2. Click **Create** on the menu bar.
3. Enter the following minimum 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 biometrics) Scroll down to "Number of Enrolled Fingerprints;" click "Enroll Fingerprints;" and follow the on-screen instructions. You must have installed a USB fingerprint enrollment reader during "Complete the Configuration."

The screenshot shows a configuration form for adding a user. At the top, there is a 'Cards' section with a table that has two columns: 'Card Number' and 'Enabled'. To the right of the table are '+ Add' and 'Remove' buttons. Below the table is the 'Number of Enrolled Fingerprints' section, which shows a count of 0 and two buttons: 'Enroll Fingerprints' (highlighted with a blue box) and 'Delete All Fingerprints'. Below this is the 'PIN' section with a text input field, an eye icon, and 'Create New' and 'Clear' buttons. At the bottom is the 'Duress PIN Type' section with a dropdown menu set to 'None' and a checkbox for 'Use Extended Door Times'.



Add a User and Test Access



- (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 the **Add** button and select 1 or more doors on the following screen.
 5. Click **Save** on the menu bar.

The card, PIN, and fingerprint you entered should now work to grant access at the specified doors, assuming you chose a compatible "Default Mode" during "Configure Doors."

Add a User and Test Access

To test access, you will (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.

First:

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.

Then:

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 should now work to grant access to the specified doors during the specified schedules, assuming you chose a compatible "Default Mode" during "Configure Doors."

Card formats that work out of the box 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 sophisticated 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."**

Adding Secondary Controllers

Step 1: Initial Setup

Follow the instructions under “Initial Controller Setup,” above, for each controller. This will configure the controller for connection to the network.

Step 2: Add 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 qualifications about Discovery.

- 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...,” 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 moments, a form will display all controllers discovered.
5. Click the link to add a controller. The create controller screen will appear.
 - a. Select a “Configuration.” (See “Initial Controller Setup,” above.)
 - b. Enter a “Name,” and select “Custom Door Names” so you can name the doors.
 - c. Leave all other settings as they are. These are the settings that were discovered.
 - d. Click **Save** on the menu bar.

Adding the AHEB-0808 Expansion Board

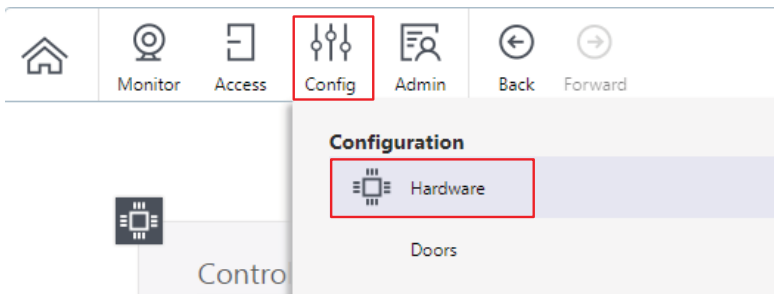
Step 1: Add the AHEB-0808 via the Web Management Application

Make sure the following steps have been completed before adding.

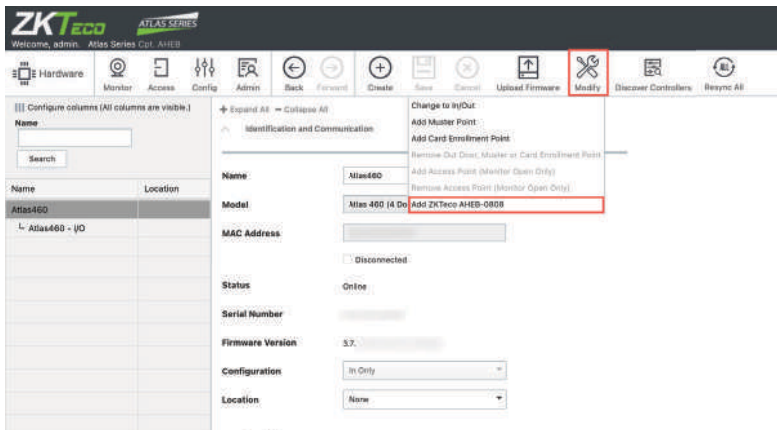
- Connect the AHEB-0808 expansion board to the controller as shown in the "AHEB-0808 Connection," above. Set the RS485 addresses of each AHEB-0808 by DIP switch before power is supplied.
- Please make sure the baudrate of the expansion board is set to **9600**.

To add the AHEB-0808 expansion boards:

1. Log in to the Web Management Application (on the primary controller).
2. Go to "Config → Hardware."



3. Click on "Modify" to add a ZKTeco AHEB-0808



Adding the AHEB-0808 Expansion Board

4. Name the board
5. Select COM1
6. Assign the OSDP address of the board and click "Add"

Modify Hardware

Add ZKTeco AHEB-0808

Enter the name, serial port and address, then click Add.

Name

Serial Port

OSDP Address

Add **Cancel**

7. After adding the board, you will then see it in the device tree and can configure the inputs and outputs as needed.

Hardware Template

☐ Hardware Template

☐ Custom Hardware Template

Inputs

Address	Name	Disabled	Normally Open	Function	Managed By	Linkage Type	Schedule
ASL 001	AHEB Input 1	<input type="checkbox"/>	<input type="checkbox"/>	Door Contact	Hardware/Door		
ASL 002	AHEB Input 2	<input type="checkbox"/>	<input type="checkbox"/>	Door Contact			
ASL 003	AHEB Input 3	<input type="checkbox"/>	<input type="checkbox"/>	Door Contact			
ASL 004	AHEB Input 4	<input type="checkbox"/>	<input type="checkbox"/>	Door Contact			
ASL 005	AHEB Input 5	<input type="checkbox"/>	<input type="checkbox"/>	Door Contact			
ASL 006	AHEB Input 6	<input type="checkbox"/>	<input type="checkbox"/>	Door Contact			

Outputs

Address	Name	Function	Managed By	Event/Condition	Trigger Rule	Push Time	Schedule
ASL 001	AHEB Output 1	Door Contact					
ASL 002	AHEB Output 2	Door Contact					
ASL 003	AHEB Output 3	Door Contact					
ASL 004	AHEB Output 4	Door Contact					
ASL 005	AHEB Output 5	Door Contact					
ASL 006	AHEB Output 6	Door Contact					


Adding an EP30CF Reader

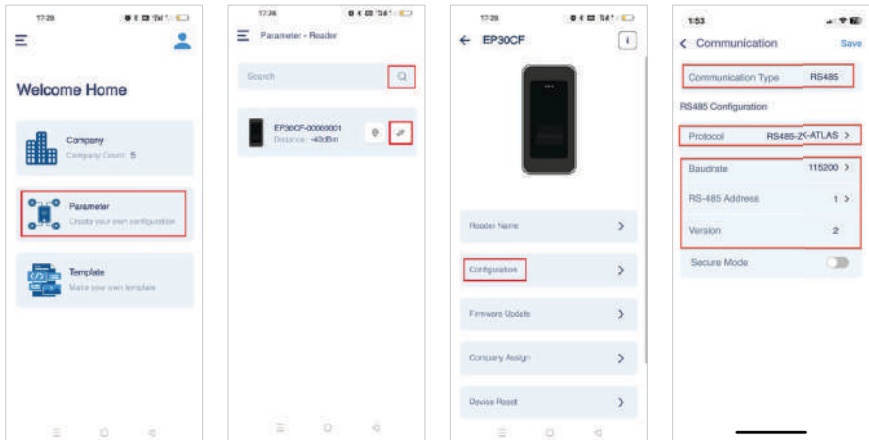
Step 1: Adding the EP30CF via the Web Management Application

Make sure the following three steps have been completed before adding.

- Connect the EP30CF reader to the controller as shown in the "EP30CF Connection," above.
- Set the RS485 addresses of each EP30CF by using **ARMATURA CONNECT** App.
- Please make sure the baudrate of the reader is set to **115200**.

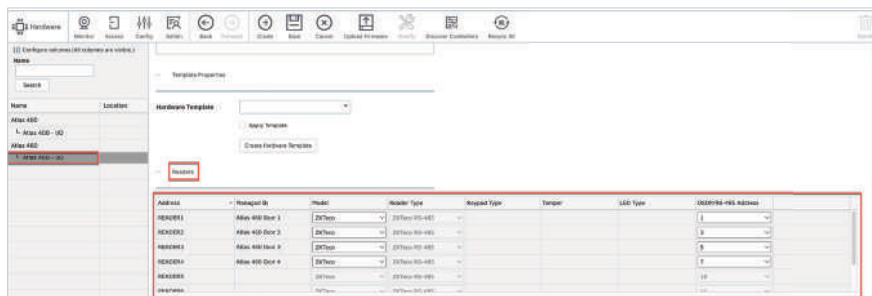
To add the EP30CF readers:

1. Log into the **ARMATURA CONNECT** App on your smartphone. Click "**Parameter**" on the Welcome Home screen to open the "Parameter - Reader" interface.
2. Find the current reader, click the  icon to enter the parameter setting interface, and click "**Configuration** → **Communication**" to set the relevant parameters, as shown in the figure below.



3. Log in to the Web Management Application (on the primary controller).
4. Go to "Config → Hardware."
5. Select the controller from the left-hand side menu and select "Readers" to open the parameter settings.

Adding an EP30CF Reader



6. In the parameter list, set Reader Type to **ZK-RS485** and enter the 485 address.
7. Click **Save** on the menu bar to save the parameter settings of the reader.
8. Click **Monitor → Event History** or click **Home** on the menu bar to view the status of the reader after completing the setup.

NOTE: For detailed operation of the **ARMATURA CONNECT** App, please refer to the relevant user manual.

Hanwha Wave/DW Spectrum Integration Setup

What you will need:

If you already have an existing Wave or Spectrum system, then you will need the following from ZKTeco USA:

- **Atlas-Vid-Lic**

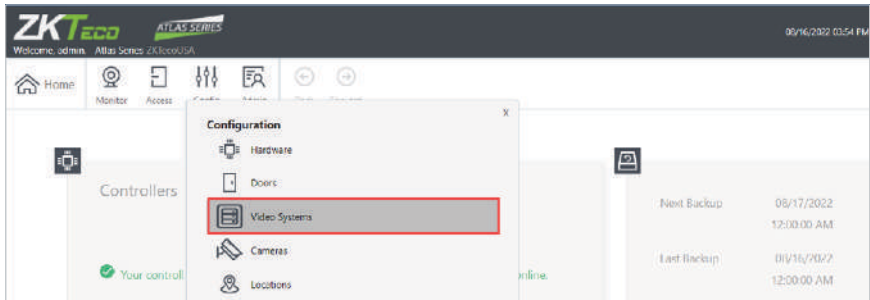
If you do not have an existing Wave or Spectrum system, then you will need the following from ZKTeco USA:

- **Atlas-Vid-Bun** (Combines Atlas-Vid-Lic & Hanwha/DW license)

The following steps are applicable after you have already set up your existing Hanwha Wave & DW Spectrum system.

Step 1: Navigate to Config and select Video Systems

1. Login to your Atlas system.
2. Go to "Config→Video Systems" to choose the system you are using.

The screenshot shows the 'Video Systems' configuration form. It has a title bar with 'Video Systems' and navigation icons. The form contains several fields: 'Model' (a dropdown menu), 'Name' (a text field with 'Hanwha Wiseret WAVE' and 'Digital Watchdog Spectrum' entered, highlighted with a red rectangle), 'Protocol' (a text field), 'IP Address' (a text field with a dropdown arrow), 'Port' (a text field), 'Username' (a text field), and 'Password' (a text field with masked characters and a 'Change' button). There are also 'Monitor', 'Access', 'Config', 'Admin', 'Back', and 'Forward' buttons at the top of the form.

Hanwha Wave/DW Spectrum Integration Setup

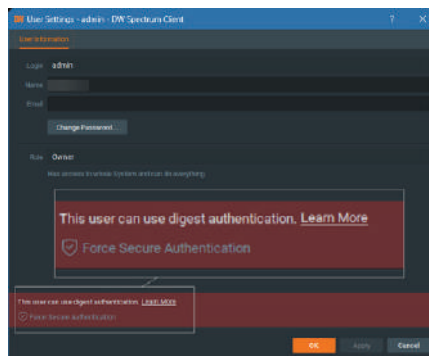
Step 2: Input the Wave/Spectrum configuration

1. Click **Create** on the menu bar to input your Wave/Spectrum configuration.

The screenshot shows the 'Video Systems' configuration page. The top menu bar includes buttons for Monitor, Access, Locking, Admin, Back, Forward, **Create** (highlighted with a red box), Save, Cancel, and Add Camera. On the left, there's a list of systems with 'Hanwha' selected. The main area is titled 'Identification' and contains a form for adding a new system. The form fields are: Model (Hanwha Wisenet DWiE), Name (empty), Status (empty), Protocol (HTTPS), IP Address (empty), Port (7001), Username (admin), Password (masked), and an 'Enabled' checkbox which is checked. A 'Change' button is next to the password field.

- Name: Input the name of your system.
- Protocol: Always use **HTTPS**.
- IP Address: IP of your Wave/Spectrum Server.
- Port: Wave/Spectrum default is **7001**.
- Username/Password: Login for your Wave/Spectrum Server.

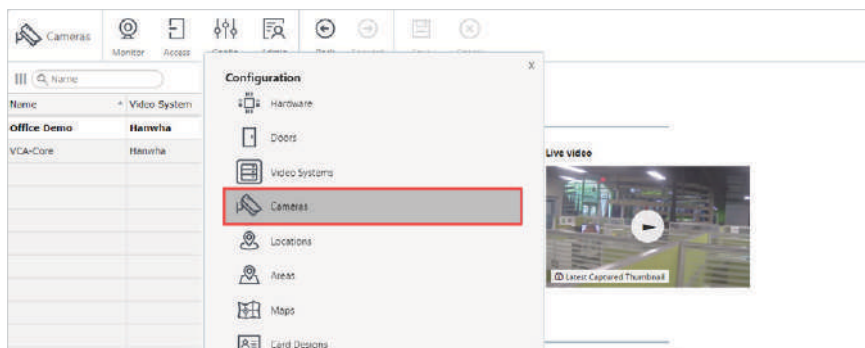
Note: If you are using Wisenet Wave or DW Spectrum version 5.0 & higher you will need to set your user settings to allow Digest Authentication.



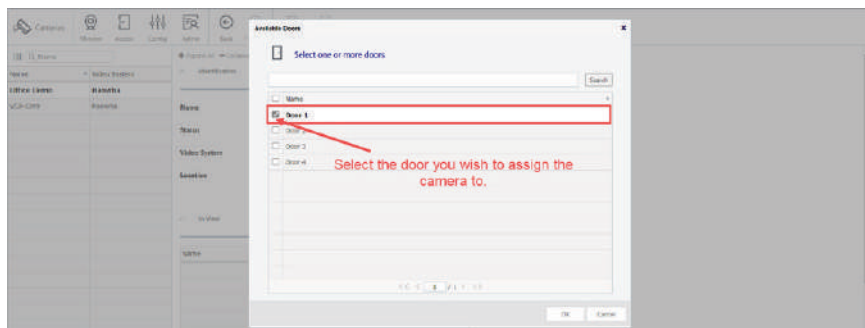
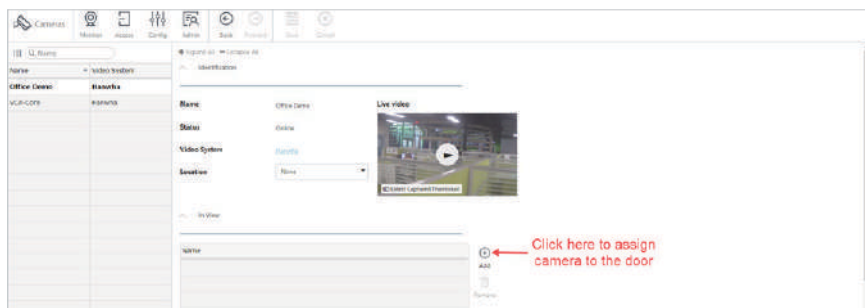
Hanwha Wave/DW Spectrum Integration Setup

Step 3: Assigning a camera to a door

1. After you have connected to the Wave/Spectrum system, you can click "Config → Cameras".



2. Click **Add** to select the door to assign the camera to.

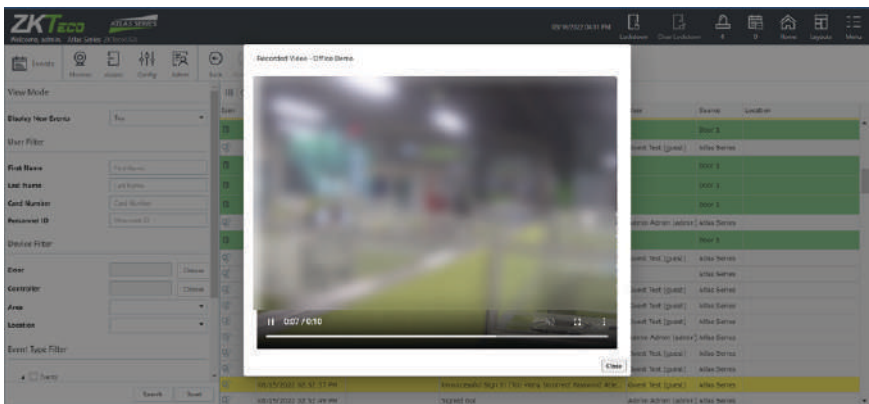
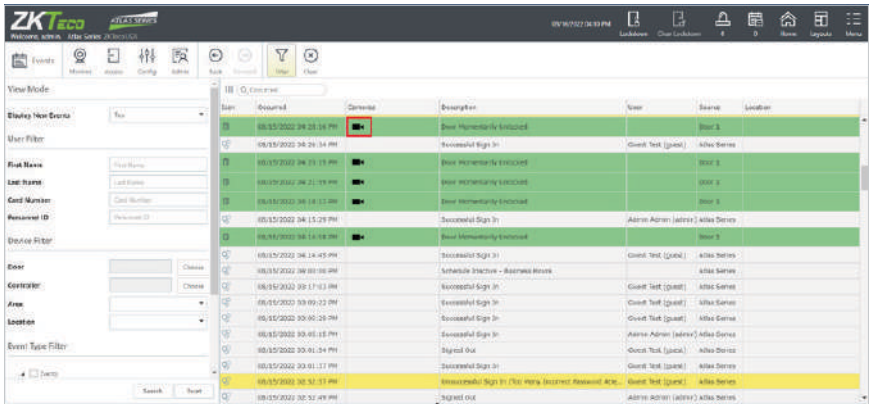


Hanwha Wave/DW Spectrum Integration Setup

Step 4: View recorded video from the Wave VMS

Now that you have configured your Wave/Spectrum connection and assigned that camera that is recording to a door, you can then click the camera icon on any new events to pull up the video.

1. Click on the  icon to view recorded video from the VMS.



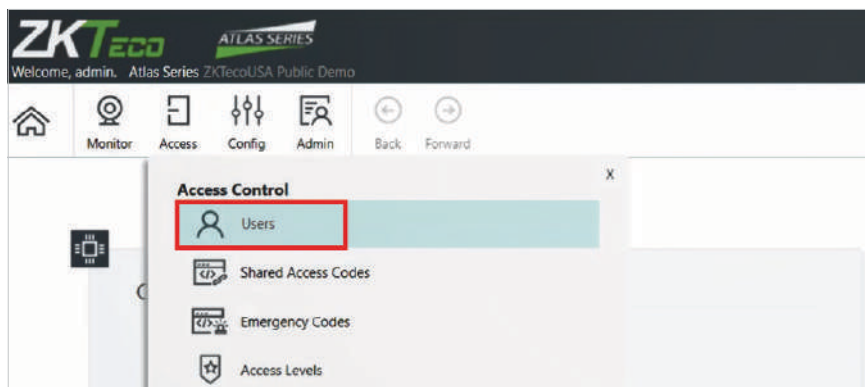
ZKey Mobile Credential App

ZKTeco provides its "ZKey" mobile app in Apple's "App Store" and in "Google Play." You must authorize each mobile device before it can access your system.

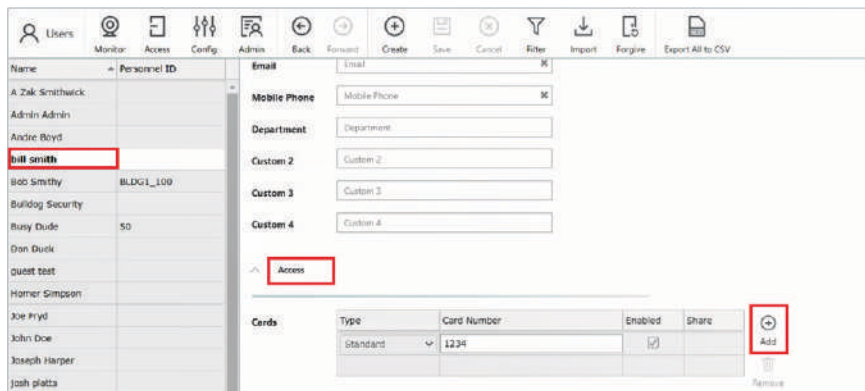
Using the Atlas built in QR generator (ZKey)

Create QR code in the Web Management Application:

1. Go to "Access → Users."



2. Select "Users" from the left-hand side menu. Scroll down to find the "Access" parameter and click **Add** to add a new card.



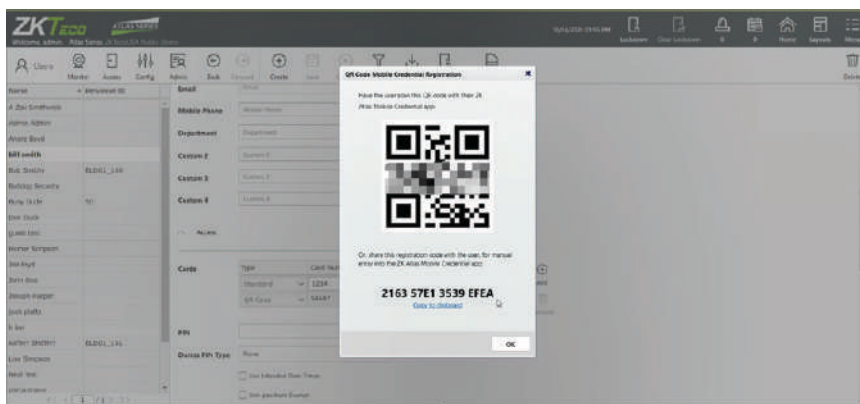
ZKey Mobile Credential App

- Set the type as "QR Code" and enter the **Card Number**. After clicking **Save** on the menu bar and click the **Share** icon. A QR code image will be displayed in the QR Code Mobile Credential Registration pop-up window.

The screenshot shows the 'Create' form for a mobile credential. On the left is a 'Users' list. The main form has fields for 'Email', 'Mobile Phone', 'Department', and 'Custom' fields. Below these is the 'Cards' section with a table:

Type	Card Number	Enabled	Share
Standard	1234	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
QR Code	54687	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Below the table are fields for 'PIN' and 'Device PIN Type'. The 'Share' icon in the 'Cards' table row is highlighted with a red box.

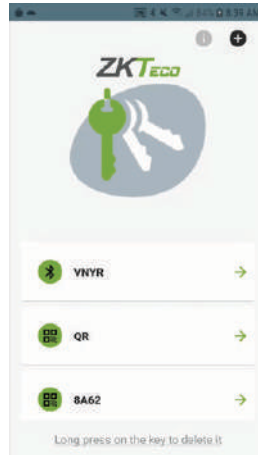
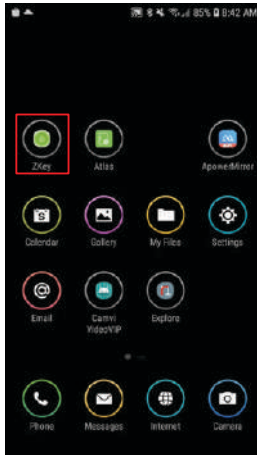


- Have the user scan this QR code with their ZKey Mobile Credential app.
- Or, click "Copy to clipboard" to share this registration code with the user, for manual entry into the ZKey Mobile Credential app.

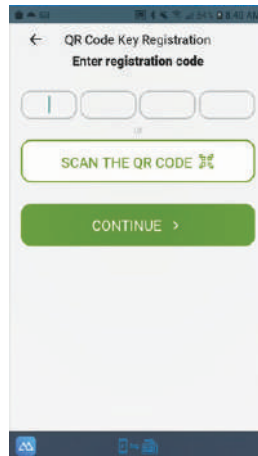
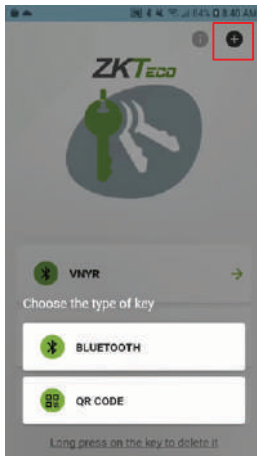
ZKey Mobile Credential App

ZKey User Guide

1. Click the **ZKey App** on your smartphone to open it.
2. You can view your credential types here.

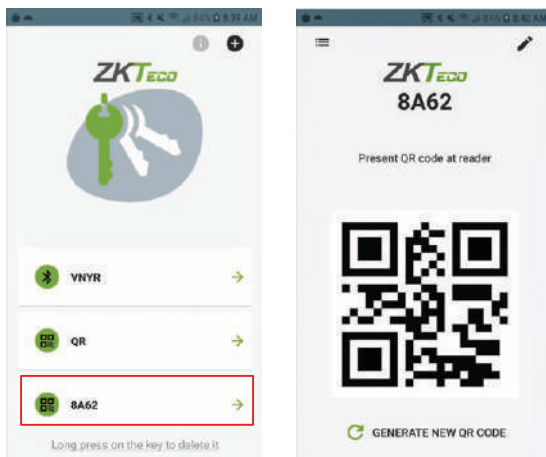


3. Click the "+" button to add a credential. You can input the registration # or scan the QR from the user profile.



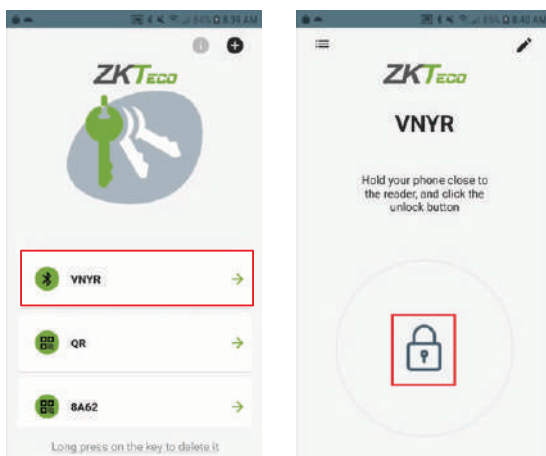
ZKey Mobile Credential App

4. You can now click on that credential and present it to the QR reader to gain access.



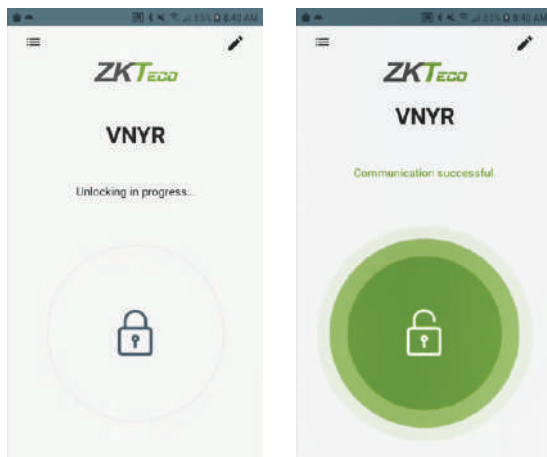
Note: It's a 1-time use and will need to be generated to be used again.

5. To use BT credential, click on it and then press the lock button.



ZKey Mobile Credential App

6. Hold the phone to the reader and wait for the signal to connect. Once communication is successful your door will open.



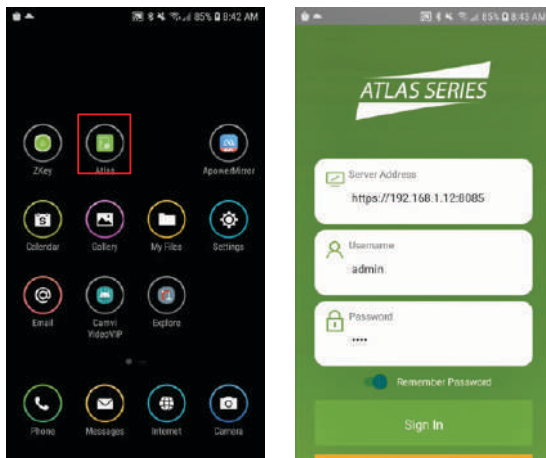
Important: The mobile device must be connected by WiFi to the same local network as the Atlas Series controllers. To connect from a distance, your network administrator must in some way open access from the Internet (such as by using a NAT) and provide the necessary "Server Address."

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.

Atlas Mobile App

Atlas Mobile App Walkthrough

1. Click the **Atlas App** on your smartphone to open it.
2. Input Server, Username, and Password in the login screen.



3. Click on "Change QR Code" and scan the QR code you have registered.

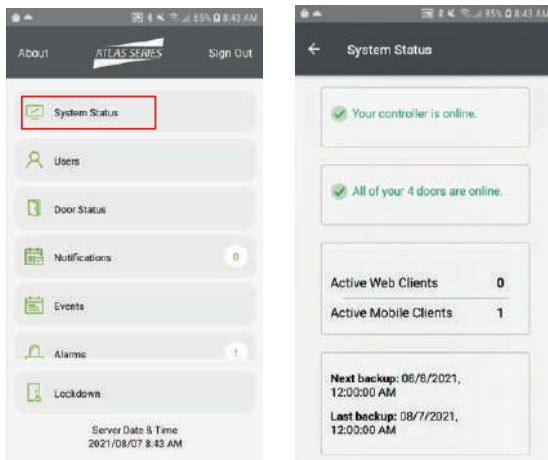


4. Press "Sign In" to log into the App.

Atlas Mobile App

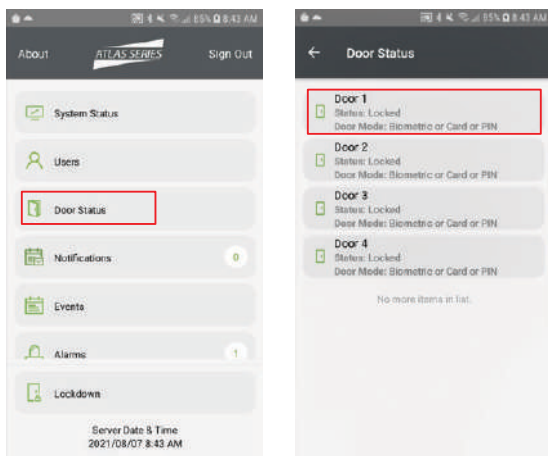
View Controllers, Doors, Activity & Backup Status

Click "System Status" to view controllers, doors, activity & backup status.



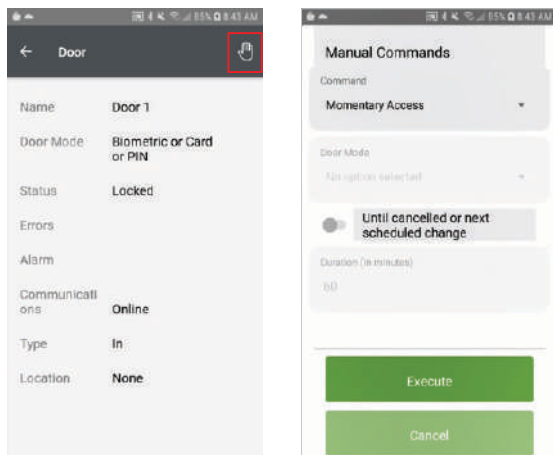
View Individual Door Status & Send Manual Commands

1. Click "Door Status" to view individual door status.
2. Select a door in the list and go to the information view screen.

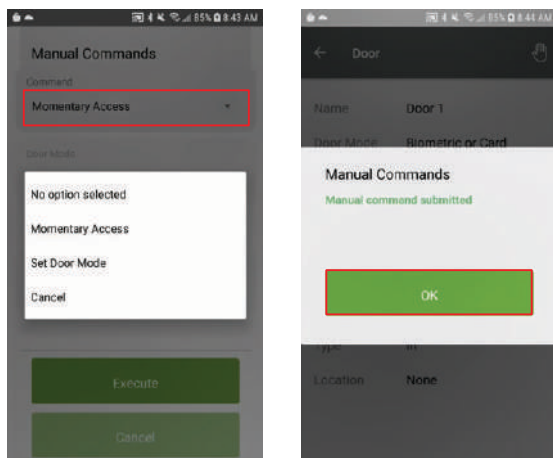


Atlas Mobile App

- Click the **Manual Commands** icon in the upper right corner of the interface.



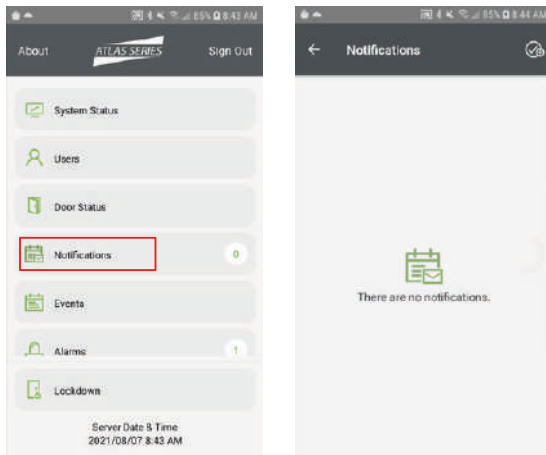
- Set the command parameters, and click "OK" to save and exit.



Atlas Mobile App

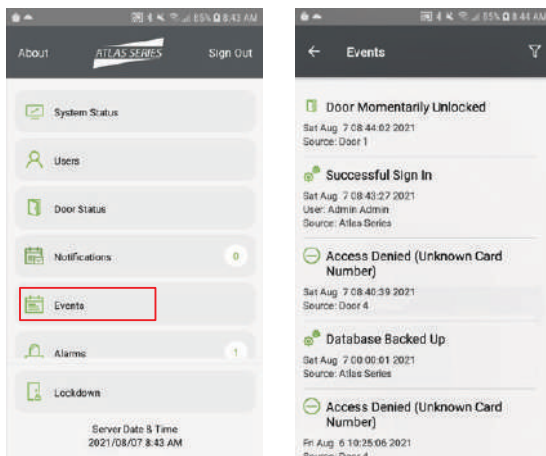
Check Your Notifications (If Any)

Click "Notifications" to check your notifications.



View & Monitor Any Events

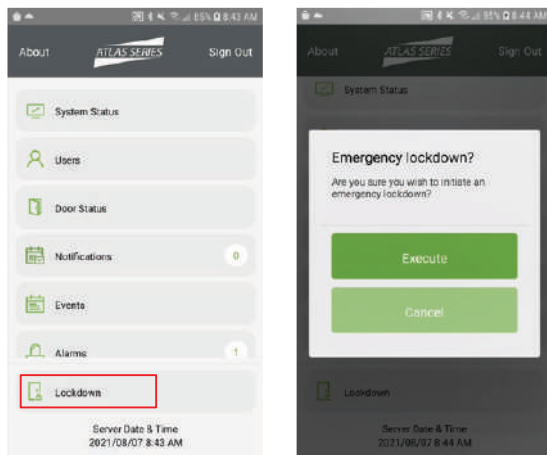
Click "Events" to view any events.



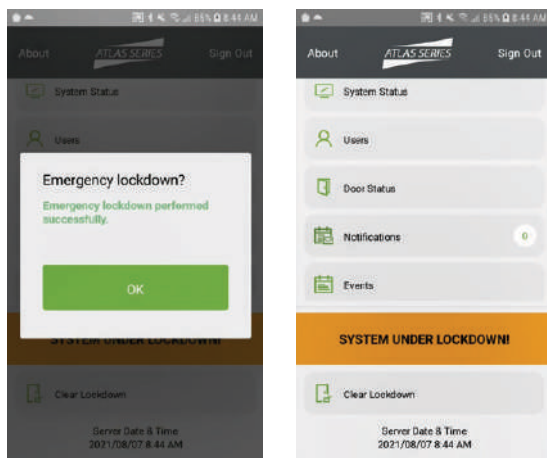
Atlas Mobile App

Activate & Deactivate an Emergency Lockdown

1. Click "Lockdown" to activate an emergency lockdown.

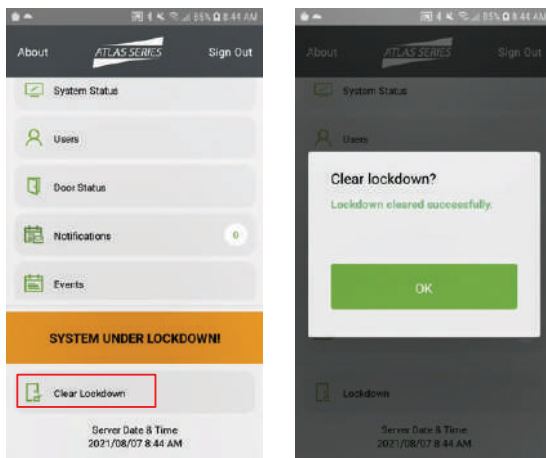


2. The interface prompts "SYSTEM UNDER LOCKDOWN!" when initiated successfully.



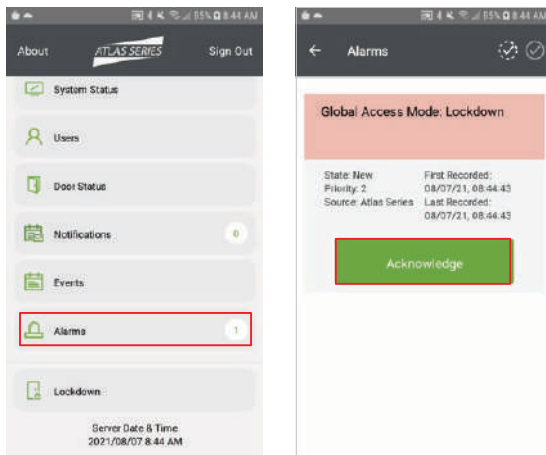
Atlas Mobile App

- Click "Clear Lockdown" to deactivate the emergency lockdown.

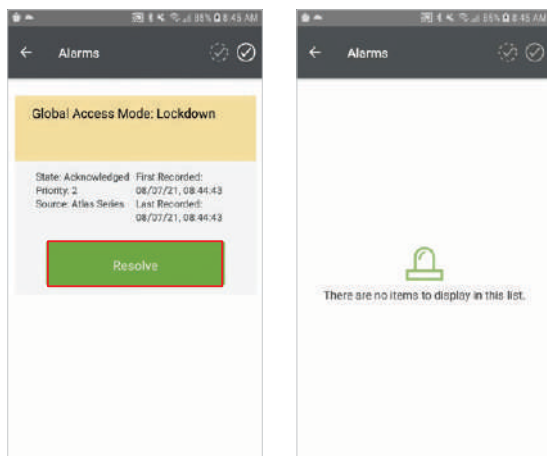


View & Manage Alarms

Click "Alarms" to view and manage alarms.

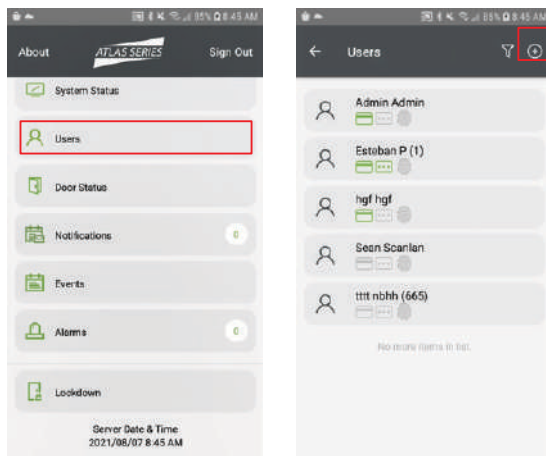


Atlas Mobile App



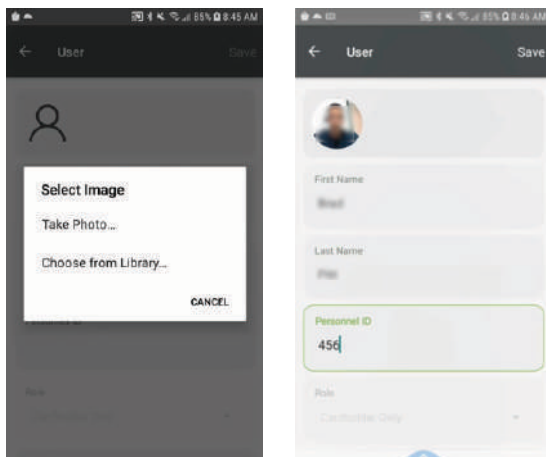
Add New Users

1. Click "Users" to enter the user list screen and click "+" to register a new user.

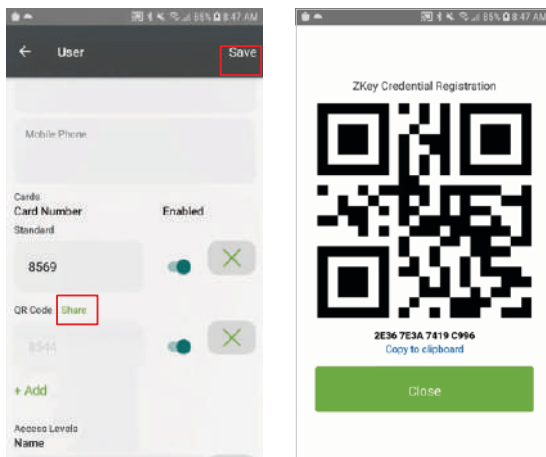


2. Enter basic user information, add card number, QR Code, set access level, and add PIM or generate one.

Atlas Mobile App



- After setting the parameters, click **"Save"** and distribute QR to user.



Edit User

Click **"Users"** to enter the user list screen and select a user.

Editing a user is done in the same way as adding a user. It will not be repeated.

Special Considerations for Complex Networks

If all Atlas Series controllers cannot be located on one network subnet, or if Discovery is blocked by network restrictions, observe the following.

- There is no difference in the way you set up the primary controller.
- During “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.

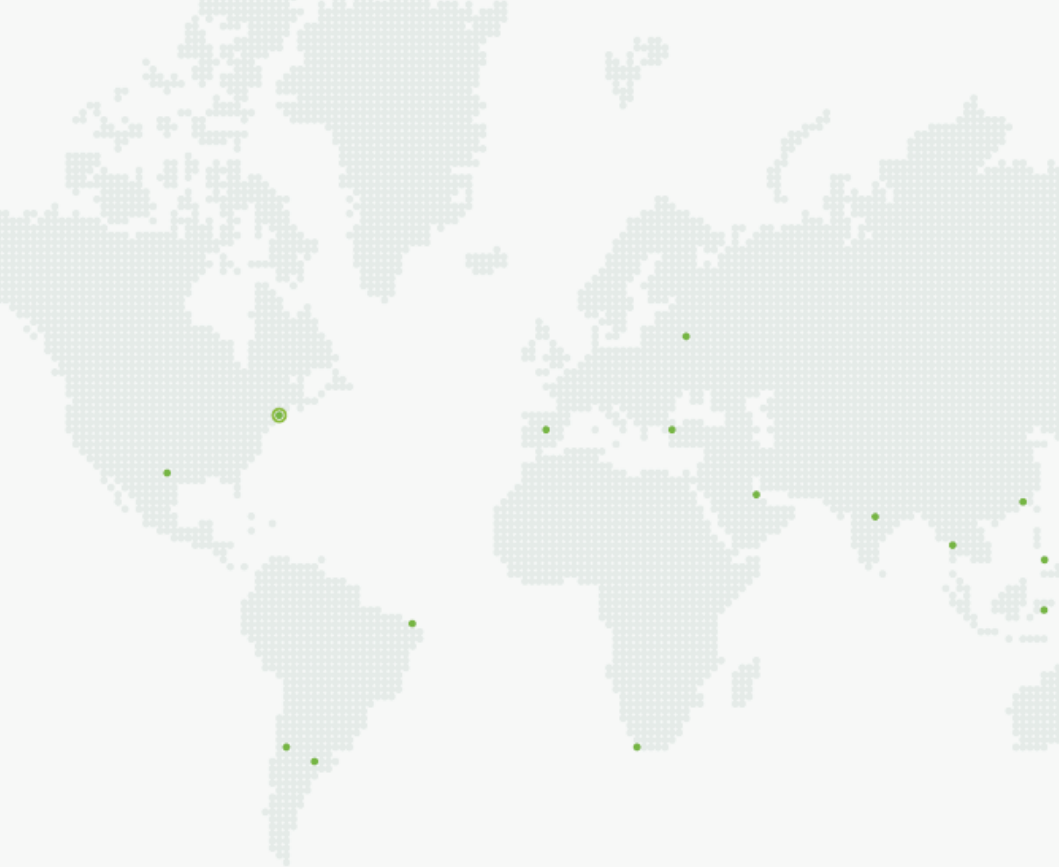
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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.



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