Armatura Horizon Series Access Controller QSG

Doc Version: 1.0.0

Contents

1	Horizon Series Panel Configuration and Setup	3
2	Access Controller Wiring	4
3	Adding Time Zones	8
4	Setting Access Levels	9
5	Adding Devices	10
6	Configuring Readers	14
7	Adding Doors to Access Levels	19
8	Adding Personnel and Assigning Access Levels	20
9	Verifying Access	23

1 Horizon Series Panel Configuration and Setup

Configuration and Setup Flow Chart:



Based on your requirements, select the appropriate operation method below:

- 1. Wiring
- 2. Adding Time Zones
- 3. Setting Access Levels
- 4. Adding Devices
- 5. Configuring Readers
- 6. Adding Doors to Access Levels
- 7. Adding Personnel and Assigning Access Levels
- 8. Verifying Access

2 Access Controller Wiring

Please click on the corresponding option to view the device wiring guide based on your device type:

- 1. Power
- 2. Network
- 3. Locks
- 4. Exit Buttons and Door Sensorsr
- 5. Readers

• Power

The Armatura Horizon Controller is powered through a 12V-24V DC power adapter or PoE, whichever is available. The wiring is as shown below:



Recommended Power Supply

Note:

Recommended Power Supply: 12V-24V DC ±20%, minimum 1.5A.

Consider utilizing an AC adapter with a higher current rating to allocate power efficiently among multiple devices.

Network

Connect the device to the software via Ethernet cable plugged into the network. An example is provided below:

Horizon Series Configuration Guide





Default IP Address: 192.168.1.201 Subnet Mask: 255.255.255.0

Important Notes:

1. When connecting to the ARMATURA One software in a LAN, ensure that the IP addresses of the server (PC) and the device are in the same network segment.

2. For dual Ethernet interfaces, the default IP address for the primary NIC is 192.168.1.201, and for the expansion NIC, it is 192.168.2.202.

• Locks

The panel supports both Normally Opened (NO) and Normally Closed (NC) locks. For NO Lock, it is connected to the 'NO' and 'COM' terminals, while the NC Lock is connected to the 'NC' and 'COM' terminals. Importantly, the device does not share power with the lock. Below is an example of how the NC Lock is connected:



Note:

To safeguard the access control panel against self-induced electromotive force produced by an electronic lock during switching off/on, it is crucial to connect a diode in parallel (please use FR107 provided with the system) with the electronic lock. This diode will dissipate the self-induced electromotive force during onsite connection, ensuring the secure application of the access control system.

• Exit Button and Door Sensor

1. A door sensor is employed to detect the open/close status of a door. This sensor switch enables the access control panel to identify door openings and activate an alarm output when necessary.

2. An exit button serves as a switch specifically designed to effortlessly open a door. When activated, the door promptly swings open. Typically, the exit button is conveniently installed at a height of approximately 55.12 inches (1.4m) above the ground, providing easy access for users.





• Readers

Select the Reader Connection Method Based on the Respective Device Type:

1. <u>RS-485/OSDP</u>

2. Wiegand

• RS-485/OSDP



Note:

For communication distances greater than or equal to 984ft (300m), follow these steps to ensure proper functioning:

1. Configure the EOL resistor of 485 using the dip switch to enable the terminal.

2. Additionally, connect a 120-ohm terminal matching resistor between the 485+ and 485- terminals of the last terminal device.

• Wiegand





3 Adding Time Zones

The system offers a default access control time zone named [24 Hours Accessible], but you also have the flexibility to create a new time zone based on your specific requirements. See the options below:

- 1. Click on [Access Control] > [Time Zones] > [New] to access the time zone setting interface.
- 2. After making the desired settings, click [OK] to save, and it will be displayed in the list.

	ARMATURA ONE	III Access 🐵 🕲 admin	
		Time Zone Name Remarks	
		Time Zone Name'	
		O Reference + New Delete	
	Time Zones	Time Zone Name F F F F F F F F F F F F F F F F F F F	
		24 Hour Accessible 2	
		0 2 4 6 8 10 12 14 16 18 20 22 24 Su	
	Set Access By Person		
	Cot Access R. Donation		
	Set Access by Departine	0 2 4 6 8 10 12 14 15 18 20 22 24	
	Interlock		
		$\mathbf{r} \qquad \qquad$	
		0 2 4 6 8 10 12 14 16 18 20 22 24 Sa	
	Multi-Person Group		
		Compatible with all devices	
	Multi-Person Opening Dr	Compatible with only Armatura Controller	
8			
Đ		Save and New OK Cancel	
	Pad Resource 🗸 👻	< < 1-1 >>> 50 rows per page Y Jump To 1 // Page Total of 1 records	

4 Setting Access Levels

The system includes an access level named [General], and users also have the option to create a new access level based on their specific requirements. See the example below:

1. Click on [Access Control], then select [Access Levels], and click [New] to access the Add Levels editing interface.

2. Define the Threat Level for this access level.

3. Click [OK] to prompt the system to 'Immediately add doors to the current Access Control Level'. Next, click [OK] to add doors, or click [Cancel] to return to the access levels list. The newly added access level will be displayed in the list.

Th	eat Level Start Date End	Date 🗌 Doc	r Name			New		×	
		New		×	Level Name*				
	I evel Name*	1			Time Zone*	24-Hou	r Accessible		
		<u>'</u>			Area"	Area N	ame		
	Time Zone*	24-Hour Accessible			Set Valid Time	0			
	Area [*]	Area Name	~		Threat Level			~	
Ale						Nam			Q OK Clear
	Set Valid Time						Name	Threat Re	marks
	Threat Level		~					Level	
					OK		Low		
						п	Alert	2	
		Cancel					Higher		
		Califer					< 1-5	> > 50 ro	ws per page 🖌 Jump To 👖

5 Adding Devices

• Authorized Devices

In the [System] > [Communication Management] > [Authorized Device] section, click the [New] button to add a new authorized device. Input the serial number and then click the [OK] button to confirm.

ARMATURA ONE	s	ystem						
»	合 <i>I</i>			agement / Authorized devi				
*				9, Đ				
20	÷		- New					
\Leftrightarrow			Device Serial Number		New			Whether to authorize
6			CN30422260	Product name*	AH	~	X7LIYvpor	
		host-matt	CN30122200	Protocol mode	best-mqtt	Ť	X7LIV/mor	
			01130122200	Serial Number*				
			74402138000	Remarks			M6wDRKg	
			CN30422170				X7LIYvpor	0
				_				
				0	Cancel			

• Export Key File

1. In the [System] > [Communication Management] > [Authorized Device], click [Export Key File] Button.

- 2. Active Time Key File Validity: Key value can be set between 1 and 72 Hours.
- 3. After clicking the Export button, the browser will initiate the download of a .zip file.

ARMATURA ONE	S	ystem			
»	合 /	System /	Communication management / Au	thorized device	
×	Devi	ce Name	Q, D		
20	Ð	Refresh	Export Key File		
۲		Protocol mod	e Device Serial Device se Number	cret	Product name
G		best-mqtt	Export	Key i ile	×
		best-mqtt	Number of selected devices Active Time	2 hpur(s	s)(1-72)
		best-mqtt			
		best-mqtt	Export	Close	

• Importing Key File to the Controller

1. Open your web browser and enter the controller's IP address in the URL bar as follows: https://" [controller's IP address]".



2. Open [Network] > [Connection].

3. Click on the [Server] Tab: The default protocol for the server is MQTTs, and the address is the server address. The default port is 1884.

4. Click the [Upload] button to upload the .zip file downloaded in [Step 2]. Once the upload is complete, you will receive a prompt indicating the operation has succeeded. Finally, click the [Save] button to save the changes.

ARMATURA		🧕 armatura 👻
Overview	Connection	
🔅 Network 🔺	Server Secondary Controller	
Connection		
Ethernet	• Port 1864	
Wian	Key File Upload	
Access Filter	ProductKey Lhy2uF0EZM24WUnTVVF	
Certificate	DeviceName CN80122200004	
Parameters	DeviceSecret Y300uCq5uaFjJrgRL8sr	
Maintenance v	Host Certificat	
System v	Please down hid the certificate and upload it to "Device Management" menu on software Download	
	Softward After upp-dring the key file, the servens certificate will be automatically imported View Rave	
<u><=</u>		

• Check Authorization

1. After successful connection via MQTT, the Module column will display 'acc'.

ARMATURA One		System							
»									
*	Dev	vice Name		Q, D					
20	÷	• Refresh +	- New 🖸 Expo	rt Key File					
۲		Protocol mode	Device Serial Number	Device secret	Product name	Product code	Module	Whether to authorize	Remarks
þ		best-mqtt				-	acc	Ø	
		best-mqtt		Mentiden or ang			acc	0	
		best-mqtt						8	
		best-mqtt					acc	0	

• Adding a Device to the Software

1. Click on [Access] > [Device] > [Device] > [Search] to open the Search interface.

2. After clicking [Search], the list of Access Control Devices along with the total count will be displayed.

ARMATURA ONE	Access								e
	🛆 / Access /								
Device ^								~ Q , O	
Device	O Refresh			Export Q	Search 2 Cont				
					Search				Version
	Search N	e found? <u>Down</u>	load Search Tools	s to Local Disk					7.8.3033 Feb 7 2021
Reader	Total Progress		100%		Searched devices count Number of devices adde	:5 d:5			
	IP Address		Device Type		Serial Number		Reset		
Auxiliary Output	IP Address	MAC Address	Subnet Mask	Gateway Address	Serial Number	Device Type	Set Server	Operations	0.0.6 May 13 2022
			255.255.254.0		MOTORNY			Add [0.0.6 May 10 2022
Daylight Saving Time			255.255.255.0		-	11.05		This device has been added	0.0.5 Apr 24 2022
			255.255.255.0		100500-000-00	-	Mp. 74 10 11 100	This device has been added	0.0.6 May 18 2022
		-						This device has been added	
			266 266 266 0	-	and the second second		March 101 Log Date	This device her been added	
Real-Time Monitoring			200.200.200.0					This device has been added	
Topology Management ¥ Access Control ×									
Reports Y					Close				
Pad Resource ~	< < 1.6	> > 50) rows per page	Ƴ│ Jump To	1 /1 Page	Total of 6 records			

3. Click the [Add] button next to the Device to add it.

4. Click on [Set up] > [RS-485 Port Setting] to configure the RS-485 port of the device.

	ARMATURA ONE		Access								G	•
		«		Device / D	levice							
-	Device		Device Name		Seria	al Number		IP Address	6	More 🗸 🔍	Ð	
	Device		O Refresh	+ New	🗓 Delete	C Export	Q Search	북화 Control ▼	📀 Set up 🔹	Solution View and Get Device Info	o 🔫 🌐 Con	nmuni
	I/O Board		Device Name		Serial Number	Area Name	Network Conr Mode	nection IP Ad	Set Bg-Verification	on Options Zone	Register Device	Fin
	Door		D 384382	a (+0000040	Area Name	Wired	10 H	Set as Registrati Modify the Finge	on Device rorint Identification Threshold	3	AC
	Reader		0 34366	a 1	1407/08080-0	Area Name	Wired	10.6	Set Device In/Ou	ut State	8	AC
	Auxiliary Input		0 34343		000017800	Area Name	Wired	998	Set cloud server	parameters	8	AC
	Event Type		· 6····	a)		Area Name	Wired	94	Set date time	rd.	Э	AC
	Daylight Saving Time		0 34.942	u (0.040234888	Area Name	Wired	98	Set face param	nanement	3	AC
	Device Monitoring								Set the timing sk	eep time		
	Alarm Monitoring								Set Fiep paralitie	iers		
۵	Access Control								Set up NTP serv	er		
8	Advanced Functions	*							RS-485 Port Set	ting 7		
	Reports	*										

RS-485 Port Setting							
RS-485 Port 1							
Protocol	Armatura RS-485	~					
Baudrate	9600	~					
RS-485 Port 2							
Protocol	OSDP	~	0				
Baudrate	9600	~	0				
RS-485 Port 3							
Protocol	OSDP	~					
Baudrate	9600	~					
9	OK Cancel						

6 Configuring Readers

• Configure the Reader Parameters Using the Armatura One Software

To configure the parameters of the reader, click [Access] > [Device] > [Reader], as shown in the figure below.

Edit		×
Name*	10.8.51.195-2-In	
Number*	3	
In/Out"	⊚ In ⊖ Out	
Door Name*	10.8.51.195-2	
Operate Interval*	2	
Verification Mode*	∰′∰′⊚́/⊜≀⊟	്
Communication Type*	Wiegand/RS485 v	
RS-485 Port	RS-485 PORT3 🗸 🗸	
Wiegand/RS485"	2 ~	
Wiegand Format	Auto ~	
Software Backgound Appro	Disable Enable	

Note:

If the reader is not encrypted, the default communication type is Wiegand/RS485. In this case, only the port and Wiegand/RS485 address need to be configured.

Edit		×
Name*	10.8.51.195-2-In	
Number*	3	
In/Out"	⊙ In ⊖ Out	
Door Name*	10.8.51.195-2	
Operate Interval*	2	
		- 1
Verification Mode*		ß
Communication Type*	RS485 ~	
RS-485 Port	RS-485 PORT3 V	
RS485 Address*	2	
Encrypt	Encrypt v	
Communication Password		
Wiegand Format	Auto ~	
ОК	Cancel	

Note:

To ensure proper encryption of the reader, set the communication type to either Wiegand or RS485, depending on the actual wiring configuration. The encryption option should be selected as either the default password or encryption and remember to set a secure password.

• Download and Install the App



1. Make sure your mobile device is connected to the internet through either a mobile data or Wi-Fi network.

- 2. Open Google Play (Android) or the App Store (iOS) on your mobile device.
- 3. Search for the ARMATURA CONNECT app.
- 4. Download and install the app on your mobile device.

5. After completing the account activation process, you can log in to the ARMATURA CONNECT App using your account and password.



Note:

For instructions on obtaining an account and password, kindly refer to the ACMS User Manual.

• Viewing the Reader Information

- 1. Make sure Bluetooth is enabled on your mobile device.
- 2. Click \equiv > [Parameter] to enter the parameter setting interface.
- 3. Click \bigcirc to locate the reader. This will make the reader beep so you can locate it.

4. Click \mathscr{O} to access the reader parameter settings screen, where you can configure relevant reader parameters.

5. Click i to view reader information, including device name, company, serial number (S/N), firmware versions, module firmware, microchip firmware, BLE firmware, and BLE MAC address.

10:33	🎯 🕸 🔤 "Sil Sil 🥅	10:31	0 ⊀ ¶	al Sal 💷	10:05	toria and the state of the sta
ARMATURA CO	ONNECT	Parameter	r - Reader 2		← EP10C-000	00001 😐 📋
🎧 Home	Q	Search		Q		
Company		💼 🥫 Test-	1		Device I	nformations
	S	Distance	00000001	9	Device Name:	EP10C
😧 Parameter 🗨			8	4	Company:	
🗅 Template					S/N:	000000001
	R	EP10C-	00000001	Ø	Firmware:	RD Ver 14.0.5 Apr 19 2022
O Sign Out		Distanc	e: -86dBm 🛛 🚩	0	Module Firmware:	133NEW_V1.06
					Microchip Firmware:	01
					BLE Firmware:	BGM220S V1.4.21
					BLE MAC:	84:71:27:8A:1E:14
						ОК
					Company Assign	n >
ARMATURA CONNECT Copyright © 2022 Arma	T 1.4.19 Itura LLC.				Device Reboot	>
Ξ		Ξ			Ξ	

• Configure the Reader Parameters Using the App

1. Click on [Configuration] and then navigate to [Communication].

2. Configure the Communication Type, Protocol, Baud Rate, and RS-485 Address options to match the parameters set in the Armatura One software.

3. To save the reader configuration parameters, click [Save], then click [Apply].

11:25 0 ≮ □ 'fill fil □ ← EP10C-00000001 i	14:57	6% 15:16
 L	Communication Type RS-485 >	Communication • >
ADVATURA	Protocol OSDP >	Function
	Baudrate 9600 >	Confirmation There are some parameters that
Reader Name Test-1 >	RS-485 Address 2 >	do not apply to this reader, please confirm
Configuration >	Version 2	Discard Apply
Firmware Update >	Install Mode	
	Secure Mode	
Company Assign >		is some new parameter which have not apply to
Device Reboot		reader, By clicking 'Apply', can able to update this options.
= 0 <		

• Monitoring the Reader Status in the Armatura One Software

1. After completing the reader configuration, log into the Armatura One software.

2. To check the reader status, click on [Access] > [Device] > [Reader]. If the reader status displays as online, it means the reader is ready for normal usage.

ARMATURA ONE	A	cess									ی ک	🖲 🔕	admin
	$\Delta \prime$	Access / Device / F	Reader										
•	Read	ler Name	Door Name			२. ⊖ ⊞							
۰	Ð	Refresh + New	🗓 Delete 🛛 🗍 Fir	mware Upgrade									
8		Reader Name	Door Name	RS-485 Port	Number	Communication Type	Communication Address	In/Out	Status	Off-site Approval Bound camera	Verification Mode	Serial Number	Firmware Ver:
		<u>10.8.51.195-1-In</u>	10.8.51.195-1			Wiegand/RS4				-'8)()()()()()()()()()()()()()()()()()()(
		10.8.51.195-1-Out	10.8.51.195-1			RS485		Out			∰/∰/@/⊕/⋿		
		<u>10.8.51.195-2-In</u>	10.8.51.195-2			Wiegand/RS4			Office		∰/∰/@/⊕/⋿		
		10.8.51.195-2-Out	10.8.51.195-2			RS485		Out	Office		<u>∰'⊜'</u> ©'⊖'⊟		
		<u>10.8.51.195-3-In</u>	10.8.51.195-3			Wiegand/RS4			omine		<u>∰'⊜'</u> ©'≙'≡		
		10.8.51.195-3-Out	10.8.51.195-3			RS485		Out	Office		`∰'([®] ')®'(≜')≡		
		<u>10.8.51.195-4-In</u>	10.8.51.195-4			Wiegand/RS4			Offic		∰/∰/©/⊕/⊟		
		10.8.51.195-4-Out	10.8.51.195-4			RS485		Out			∰/∰/@/ ≙ /⋿		
		<u>10.8.51.4-1-In</u>	10.8.51.4-1			Wiegand/RS4			от		∰/ <u>⊕</u> /@/⊕/⋿		
		10.8.51.4-1-Out	10.8.51.4-1	3	2	Wiegand/RS4	2	Out	Online	8	<u>⊕'⊜'</u> ©'⊖'⊟	1	RD Ver 14.7.

7 Adding Doors to Access Levels

1. To reach the access levels interface, click on [Access] > [Access Control] > [Access Levels].

2. Select the appropriate access levels and click [Add Door] to assign them to the respective door.

	«		ccess / Acces	ss Control / Ac	cess Level	s		
🚔 Device	•	Access	Levels					<
Access Control	^	Level N	Name		Time Zo	ne		Q, Ð
Time Zones	/	Ð	Refresh +	New 🗓 De	elete	Be Door Contro	ol 🗸	
Holidays		Area N	ame Time Zone	Door Count T	Threat Leve	Start Date	End Date	Operations
Access Levels		Área N	a 24-Hour	4				r 🛙
Set Access By Levels		Area N	a 24-Hour	8				é B
Set Access By Person		Area N	a 24-Hour	0				c 🛙
Set Access By Depart	me							
« 🖒 /					Add Door			×
« C / Acce	Door	Name	S	erial Number	Add Door	Q ()		×
 ≪ △ / ▲ Device ✓ Acce ▲ Access Control ▲ 	Door	Name	S	erial Number	Add Door	Q, ←) cted(0)		X
	Door Alterr	Name native Door Name	Si Owned Device	erial Number	Add Door Sele	Q O	Owned Device	X Serial Number
 Charlen 1 Device Access Control Access Control Time Zones Holidays 	Door Alterr	Name native Door Name 10.8.16.49-4	Owned Device 10.8.16.49	erial Number Serial Number	Add Door Sele	Q O	Owned Device	X Serial Number
 Control Access Control Time Zones Holidays Access Levels 	Door Alterr	Name	Owned Device 10.8.16.49 10.8.16.49	erial Number Serial Number	Add Door	Q O	Owned Device	X Serial Number
 Control Device Access Control Time Zones Holidays Access Levels Set Access By Levels 	Door Alterr	Name	Owned Device 10.8.16.49 10.8.16.49 10.8.16.49	erial Number	Add Door	Q O	Owned Device	X Serial Number
 Control Device Access Control Access Control Time Zones Holidays Access Levels Set Access By Levels Set Access By Person 	Door Alterr C	Name	Owned Device 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49	erial Number	Add Door	Cted(0) Door Name	Owned Device	X Serial Number
 Device Access Control Time Zones Time Zones Holidays Access Levels Set Access By Levels Set Access By Departme 		Name Door Name 10.8.16.49-4 10.8.16.49-3 10.8.16.49-2 10.8.16.49-1	Owned Device 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49	erial Number	Add Door	Q Door Name	Owned Device	X Serial Number
 Device Access Control Access Control Time Zones Holidays Access By Levels Set Access By Levels Set Access By Departme Interlock 	Door Alterr C C C C C C C C C C C C C C C C C C	Name Door Name 10.8.16.49-4 10.8.16.49-3 10.8.16.49-2 10.8.16.49-1 10.8.16.130-4	Owned Device State 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49	erial Number	Add Door	Q Door Name	Owned Device	X Serial Number
 Control Access Control Time Zones Time Zones Holidays Access Levels Set Access By Levels Set Access By Departme Interlock Linkage 	Door Altern O O O O O O O O O O O O O	Name Door Name 10.8.16.49-4 10.8.16.49-3 10.8.16.49-3 10.8.16.49-3 10.8.16.49-1 10.8.16.130-4	Owned Device State 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.130 10.8.16.130 10.8.16.130	erial Number	Add Door	Q O	Owned Device	X Serial Number
 Control Device Access Control Time Zones Holidays Access By Levels Set Access By Departme Set Access By Departme Interlock Linkage Advanced Functions 	Door Alterr C C C C C C C C C C C C C C C C C C	Name Door Name 10.8.16.49-4 10.8.16.49-3 10.8.16.49-2 10.8.16.49-1 10.8.16.130-4 10.8.16.130-3 < 1-12	Owned Device State 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.49 10.8.16.130 10.8.16.130 10.8.16.130 > > 50 rows p	erial Number	Add Door	Cted(0) Door Name	Owned Device	X Serial Number

8 Adding Personnel and Assigning Access Levels

• Add Personnel in the Software

1. To add personnel, select: [Personnel] > [Personnel Management] > [Personnel] > [New].

«										
Personnel	Personnel ID	Name	More \lor Q	. 0						
Personnel	± 8	A Refresh	+ New 🗊 Delete	ළි Dismissal ළි	Adjust Department	ది Change Pos	ition 🖸 Export 🗸 🖆 Import 🗸			
Department	Department Name(1) test(1)	Personnel	D First Name Last Name	e Department Name	Person Type	Backstage comparison	Card Number Mobile Credential			
Position		<u>3190258</u>	ааа	Department Name	Employee	No	5177873			
Dismissed Personnel		-					000 100 5000			
Temporary Personnel		<u>1007</u>		test	Employee	NO	3891895923			
Custom Attributes										
Parameters										
Disabled										
Face Template Extraction										
Personnel Push Log										

2. In the new personnel interface, input the Personnel ID, Department, First Name, Last Name, and other relevant details.

3. You can select one or any of the following verification methods:

- Face
- Card
- <u>Fingerprint</u>

• Adding Face

- [Browse]: Click [Browse] to select a local photo to upload.
- [Capture]: Capture a facial image using the webcam or device as enrollment reader.
- [Use as Face Template]: Enable this option to use as a face template by checking the box.

		1	New			×
Username 123	Basic information	n Browse	Capture	☑ Use as Face Ter	nplate	
Basic information	(Optimal Size 260*390).					
Credential	Personnel ID*	123		Department*	Department Name	
Access Control	First Name			Last Name		
Time Attendance	Gender			Mobile Phone		٢
Elevator Control						
Plate Register	Certificate Type			Certificate Number		•
		Save and New	OK Cancel			

Note:

Personnel Images: The software offers an image preview function that supports various common picture formats, including JPG, JPEG, BMP, PNG, GIF, etc. To ensure the best display, we recommend using an image size of 120×140 pixels.

• Adding Card

If you know the card number, you can manually enter the card. Otherwise, click on the button to select a reader. Swipe the card at the selected reader to input the card number.

Note:

This reader should be connected to the panel via Wiegand/RS-485/OSDP.

			New								
	Gender			Mobile Phone		•					
	Certificate Type			Certificate Number		٢					
Username	Birthday			Email		•					
1230399	Hire Date			Position Name							
Basic information	Device Verification Password		۲	Card Number		166					
Credential	Threat Level			Mobile Credential							
Access Control											
Time Attendance	Credential										
Elevator Control	◎ 0 第 0	80 🕀 O	<u>}</u> 0								
Plate Register	Registration method Finger	rint Scanner									
Channel Settings	Duress Fingerprint 🛛 🚬										
Save and New OK Cancel											

• Registering a Fingerprint

1. Move the cursor to the fingerprint icon position. A registration pop-up or driver download box will appear. Click on [Register].

2. Click [Fingerprint Scanner] if using a fingerprint reader; otherwise, click '[Remote Registration]' for using remote standalone device.

3. Select a finger and press it on the sensor three times. Once the fingerprint is successfully registered, a message 'Fingerprint registered successfully' will appear on the interface.

4. Click [OK] to finalize the registration process.

	New x	
	Credential	
Username 1230399	Registration method Fingerprint Scanner Fingerprint Remote Registration	
Basic information	Register progress	
Credential		
Access Control		
Time Attendance	\ / / Left Right	
Elevator Control		
Plate Register	Access Control	
Channel Settings	E Add Select All Unselect All Levels Settings	
	Save and New OK Cancel	

5. To configure Personnel Permission Settings, click on [Access Control], then select [General].

- New

 Access Control

 Username

 t28038

 Basic information

 Credential

 Maccess Control

 Time Attendance

 Elevator Control

 Pater Ringster

 Channel Setting

 Mandance Area

 Save and New

 OK

 Cancel
- 6. Click [OK] to save the settings.

9 Verifying Access

1. Use your configured permissions for door access: Swipe your card, perform a face scan, or verify your fingerprint on the device to gain access to the door.

2. If access is granted, you can view the event log in the software by navigating to [Access] > [Reports] > [All Transactions].

ARKATURA One	Access									Ŕ	ø ()) 🗈 😩	admin
≣	🖒 / Acce	ess / Reports / J	All Transactions										
-	Time From	2023-04-26 13:57:29	To 2023-07	-26 23:59:59	Personnel ID		Device Na	ame		More 🗸 🔍 🕙	0		
٥	🕂 Ref	resh 🖸 Export	🔀 Export ph	iotos									
8	Event ID	Time	Area Name	Device Name	Event Point	Event Description	Media File	Personnel ID	First Name	Last Name	Person Type	Card Number	Depar
Ē		2023-07-24 15:37:	Area Name	10.8.51.4		Disconnected							
		2023-07-24 15:37:	Area Name	10.8.51.195		Disconnected							
	5160	2023-07-24 15:34:	Area Name	10.8.51.4		Successfully conn							
	5158	2023-07-24 15:34:	Area Name	10.8.51.4		Wlfi is connected							
	5159	2023-07-24 15:34:	Area Name	10.8.51.4		Unable to connect							
	5157	2023-07-24 15:34:	Area Name	10.8.51.4		Successfully conn							
	5155	2023-07-24 15:34:	Area Name	10.8.51.4	10.8.51.4-1	Reader online							
	5156	2023-07-24 15:34:	Area Name	10.8.51.4	10.8.51.4-1	Reader online							•



ARMATURA LLC www.armatura.us E-mail:sales@armatura.us Copyright © 2023 ARMATURA LLC. All rights reserved.