



Azure Access BLU-IC4 Hardware Manual

Revision E3
January 26, 2024

© 2024 Azure Access Technology, Inc.

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without written permission.

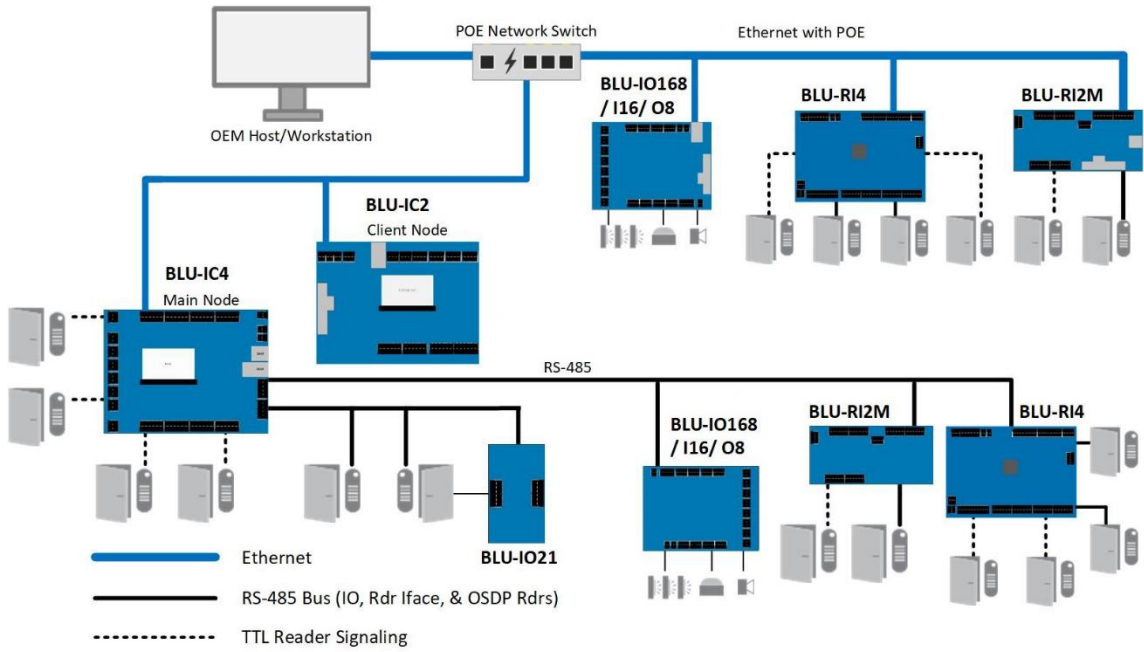
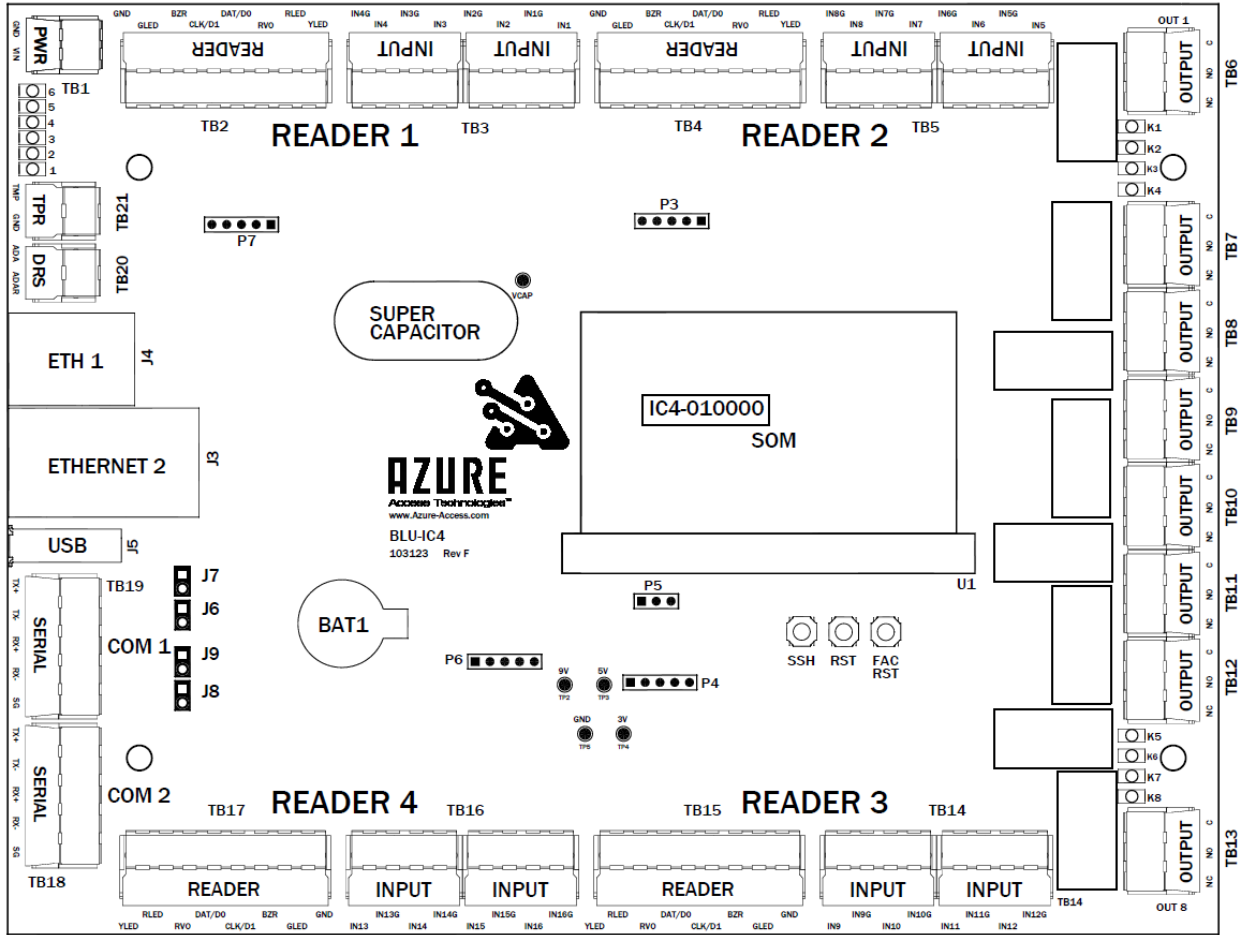
While every precaution has been taken in the preparation of this document, Author assumes no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.



BLU-IC4 Hardware Manual

4-Door Intelligent Network Controller

by Azure Access Technology



IMPORTANT INFORMATION



WARNING

HIGH VOLTAGE, AC MAIN POWER SHOULD ONLY BE CONNECTED BY QUALIFIED, LICENSED ELECTRICIANS. ALL APPLICABLE LAWS AND CODES MUST BE FOLLOWED. IF THIS PRECAUTION IS NOT OBSERVED, PERSONAL INJURY OR DEATH COULD OCCUR

Power should not be applied to the system until after the installation has been completed. If this precaution is not observed, personal injury or death could occur, and the equipment could be damaged beyond repair.

-Verify that the external circuit breaker which supplies power to the device power supply is turned off prior to installation.

-Verify that the output voltage of the power supply is within specifications prior to connection to the device.



CAUTION

Several important procedures should be followed to prevent electro-static discharge (ESD) damage to sensitive CMOS integrated circuits and modules.

-All transport of electronic components, including completed reader assemblies, should be in static shield packaging and containers.

-Handle all ESD sensitive components at an approved static controlled work station. These work stations consist of a desk mat, floor mat and an ESD wrist strap. Work stations are available from various vendors including the 3M company.

FCC Compliance Statement

This device complies with Part 15 of 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.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense. The user is advised that any equipment changes or modifications not expressly approved by the party responsible for compliance would void the compliance to FCC regulations and therefore, the user's authority to operate the equipment.

CE Compliant



Table of Contents

1	INTRODUCTION	1
1.1	General Features.....	1
1.2	Configuration	2
2	HARDWARE LAYOUT	3
2.1	Terminal Connectors	3
2.2	Jumpers	7
2.3	SOM (System on Module).....	8
2.4	USB Port	8
2.5	Factory Connectors	8
2.6	LEDs.....	8
2.7	Function Buttons	9
2.8	Memory & RTC Retention During Power Failure.....	9
2.9	Mounting.....	10
3	SYSTEM WIRING	11
3.1	Power	11
3.1.1	Primary Board Power	11
3.1.2	Powering Peripherals	11
3.2	Grounding.....	11
3.3	Communications.....	12
3.3.1	Network.....	12
3.3.2	Downstream Serial Ports	12
3.3.3	OSDP Reader Wiring.....	14
3.4	Reader Ports.....	15
3.5	Unsupervised Cabinet Tamper	15
3.6	Supervised Input Wiring.....	16
3.6.1	Input Supervision	16
3.7	Output Relays.....	17
3.7.1	Strike Wiring.....	18
3.7.2	Auxiliary Relay Output Wiring.....	18
3.7.3	Voltage Spike Suppression	18
3.8	Door / Access Point Setup	18
3.8.1	Reader	19
3.8.2	Door Contact & Exit Pushbutton/REX Inputs	20
3.8.3	Door Strike	20
4	CONTROLLER CONFIGURATION	21
4.1	Host Communications	21
4.2	Controller Clustering	21
4.3	Licenses.....	22
4.3.1	Card Database License.....	22
4.3.2	Expandable Reader License	23
4.4	Web Configuration Interface	23
4.4.1	Date & Time	24
4.4.2	Network.....	25
4.4.3	Mail	26
4.4.4	Services	27
4.4.5	Applications.....	30
4.4.6	Maintenance.....	31
4.4.7	Profile.....	32
4.5	Firmware & License Updates	32
4.6	Embedded Applications	34
4.7	Custom Logic	34
4.7.1	Internal Variables	34
4.7.2	Scripting.....	34
4.8	Elevator Control	34
4.9	Security.....	35

5	TROUBLESHOOTING	36
5.1	Communications.....	36
5.2	Reader / Keypad	36
5.3	Input Zones.....	37
5.4	Output relays	37
6	SPECIFICATIONS.....	38
7	REVISION HISTORY	40

Part I

Introduction

1 Introduction

This is high-level installation and basic usage manual for the BLU-IC4 high-speed network controller. In this manual is hardware information for installation and setup as well as configuration information to get started using the controller. More detailed information regarding firmware, configurations, features, and use can be found in the online wiki and forum.

The BLU-IC4 provides onboard hardware interfaces for four Access Points. The BLU-IC4 also supports downstream IO & Reader Interface panels connected over the network or serial ports to expand the access control system. A variety of card reader technologies are supported including proximity, smart card, biometric, bar code, and infrared readers. The BLU-IC4 reader ports support TTL readers (Wiegand / Clock & Data) and RS485 (OSDP) readers can be connected to the serial ports. A downloadable card database and event buffering allows the BLU-IC4 to work independently of monitoring software after initial programming.

Typical use of the access control system is the monitoring and control of site-access by control of door locking devices associated with card readers and PIN keypads, while maintaining logs of this access for later reporting. Many levels of further integration with building alarm and monitoring systems, time and attendance systems, and video surveillance systems are possible.

1.1 General Features

- 4 onboard reader ports for up to 4 readers, keypads, or reader/keypad combinations
 - OSDP readers are supported on the two RS485 serial ports
- Support up to 16 RS485 (OSDP) readers with expandable reader licenses
- 16 Supervised Alarm Inputs (Default config: 4 Door Contact, 4 Exit Push Button, 8 Auxiliary)
 - Configurable EOL termination-resistor values
- 8 Relay Outputs (Default config: 4 Door strike & 4 Auxiliary)
- 1 Unsupervised Cabinet Tamper Input
- Two, 4-wire RS-485 serial ports for communication to downstream reader-interface and/or IO panels
 - Supports proprietary or OSDPv2 protocol
- Two dedicated 10/100 Ethernet ports
- Full, standalone operation with local database of up to 1,000,000 cards / 100,000 events
- Up to 127 Card Formats
- 50 Access Levels Per Card
- Activation/Deactivation Time
- Inputs & Outputs are custom-mappable
- 3 LED control signals for each reader port for supporting up to 3 colors
- Customizable logic and event scripting
- Clustering
- 3rd party embedded applications

1.2 Configuration

The BLU-IC4 is configured and monitored by Host software over a network connection. The controller Clustering feature allows multiple controllers to communicate with each other, while a single controller maintains the Host connection. This reduces the load on the Host allowing for enterprise-scale installations. Once programmed, the controller/Cluster will operate independently without needing a Host connection. Events are stored on the controller(s) to be reported to the Host when a connection is re-established.

In addition to cardholders, here are examples of information is stored in the Cluster:

- Card Reader Data Output Format: Wiegand or Magnetic
- Strike Time— The duration during which the strike relay will be energized in the case of an access grant.
- Held Open Time—After an access grant and a subsequent opening of the door contact, the time in which the door contact must be closed before an alarm state is reported
- Reader Mode—The access mode in which the reader will function upon powering up or when communication has been interrupted with the Host software. The following modes are supported:
 - Card Only—An access request is made by presenting a card to the reader. The data is verified against the controller database to ensure that the card has a valid Facility Code and Card Number.
 - Card or PIN—Access requests are made either by presenting a card or by keying in a PIN (Personal Identification Number) on a keypad. A card entry is process in Card Only mode.
 - Card & PIN—A card must be read to start the access request. If the card is valid, the user is prompted to enter the corresponding PIN. The request is granted only if the card and PIN match what is in the data base.
 - Locked—No access granted. Reader ignores all cards and PIN entries.
 - Unlocked—Door strike is continuously energized and the door contact input is not monitored. Access is not controlled.
 - Facility Code—The entire card's contents are read by the controller, but only the Facility Code is checked, and if it matches a Facility Code downloaded from the Host software, access is granted.
- Anti-Passback – Card location and access rules are shared across the Cluster.
- Internal Variables – If-then logic that can execute commands/actions based on event triggers.
- Scripting – Logic scripts that change the base functionality of a function on the controller, generally to modify the access cycle or to perform unique non-access related functions. This functionality can be applied with modifying the core firmware.
- Plugin Scripts – Programs that remain resident on the controller but can have their function modified by sending a dynamic configuration to information storage areas on the controller. This allows the controller or another external system to easily affect the function of script behavior without having to modify and reload the entire script.
- Elevator Control – Elevator control is accomplished by using the BLU-O8 or BLU-IO168 panels. Using the BLU-IO168 has the added benefit of providing feedback to the inputs on the IO panel.

Part II

Hardware Layout

2 Hardware Layout

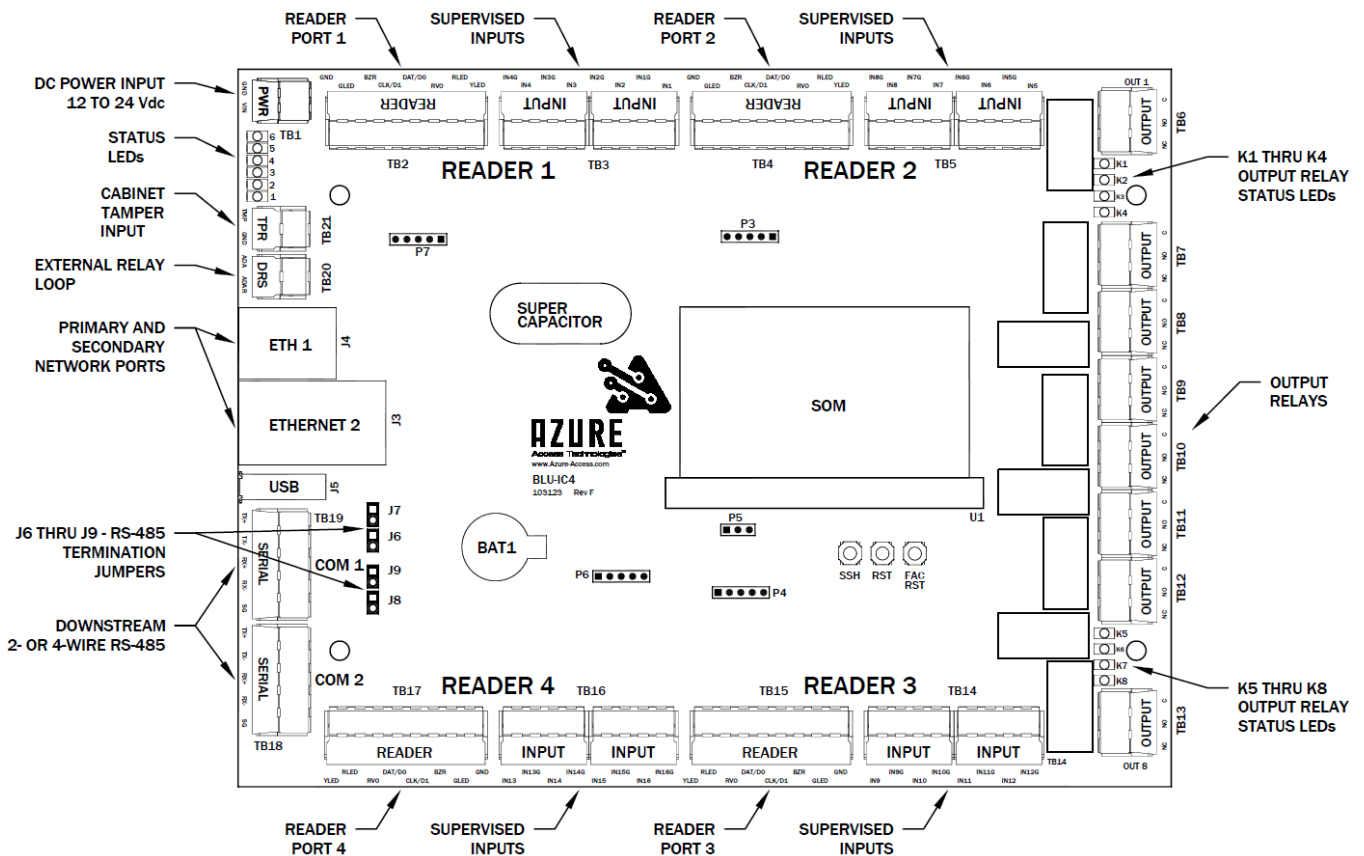


Figure 2.1: Board Diagram

2.1 Terminal Connectors

Terminal blocks are used for easy interface wiring. The connection terminals are factory equipped with removable screw-down quick connectors which are easily removed from the board by firmly grasping the connector and pulling away from the board. If pliers are used to remove the connectors, they should be of the rubber-tipped type. Take care to not damage onboard components when using any tools near the board. The proper location of the quick connectors is outlined in white on the board. Cable specs can be found in section 6 “Specifications”.

The SDK allows for custom-mapping of hardware interfaces. Any reader, input, or output can be assigned to any Access Point. Recommended wiring configurations are listed in parenthesis in the function column.

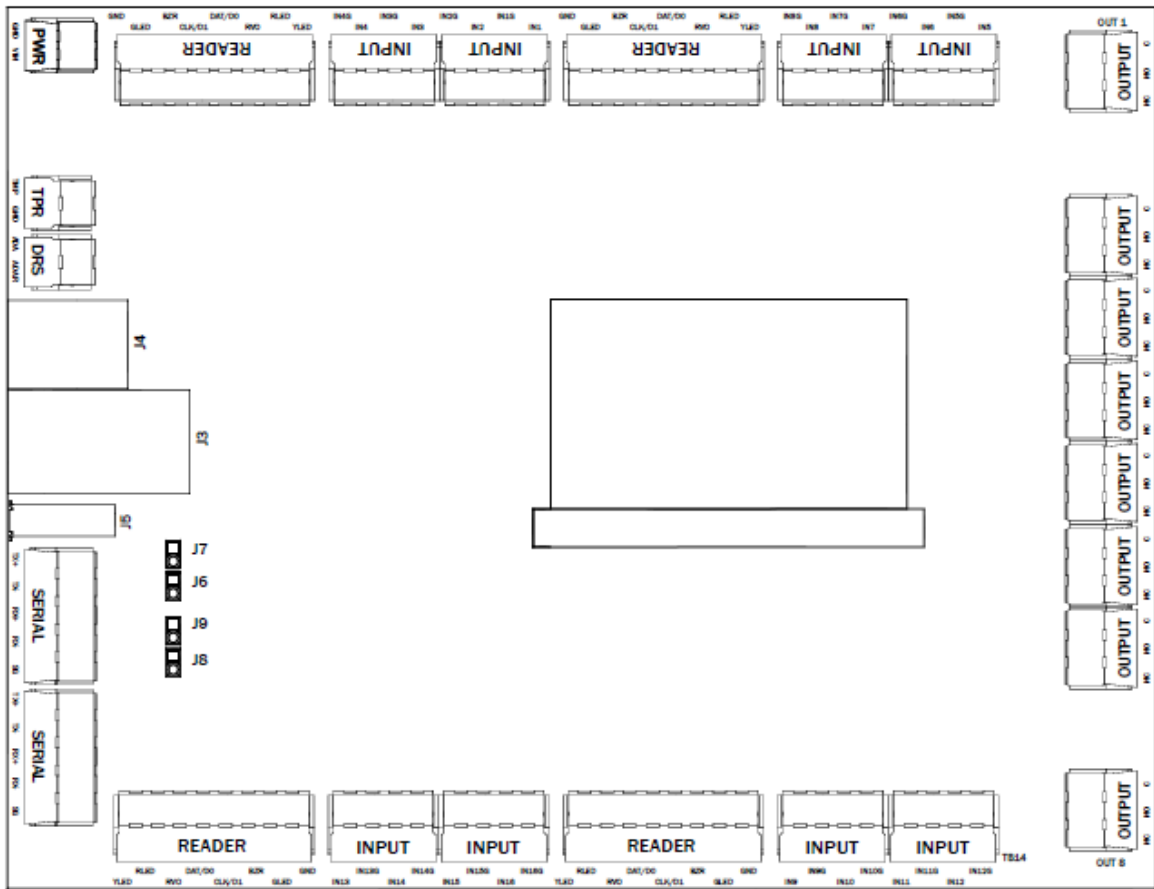
Terminal Block Wiring Connections			
Location	Type	Label	Function (Recommended Connection)
Power & Tamper			
TB1-1	Power Input	VIN	Power Input Connection
TB1-2	Ground	GND	
TB21-1	Tamper Input	TMPR	Cabinet Tamper Input (Normally Closed)
TB21-2	Tamper Input Return	GND	
TB20-1	<i>NOT USED</i>	ADA	* <i>INTERFACE NOT USED</i> *
TB20-2	<i>NOT USED</i>	ADAR	
Serial Ports			
TB19-1	Transmit Data (+)	TX+	4-Wire RS-485 COM Port 1
TB19-2	Transmit Data (-)	TX-	
TB19-3	Receive Data (+)	RX+	
TB19-4	Receive Data (-)	RX-	
TB19-5	Signal Ground	SG	
TB18-1	Transmit Data (+)	TX+	4-Wire RS-485 COM Port 2
TB18-2	Transmit Data (-)	TX-	
TB18-3	Receive Data (+)	RX+	
TB18-4	Receive Data (-)	RX-	
TB18-5	Signal Ground	SG	
Relay Output Connections			
TB6-1	Normally Open	NO	OUT1 Relay (Door 1 Strike)
TB6-2	Common	C	
TB6-3	Normally Closed	NC	
TB7-1	Normally Open	NO	OUT2 Relay (Door 2 Strike)
TB7-2	Common	C	
TB7-3	Normally Closed	NC	
TB8-1	Normally Open	NO	OUT3 Relay (Door 3 Strike)
TB8-2	Common	C	
TB8-3	Normally Closed	NC	
TB9-1	Normally Open	NO	OUT4 Relay (Door 4 Strike)
TB9-2	Common	C	
TB9-3	Normally Closed	NC	
TB10-1	Normally Open	NO	OUT5 Relay (Door 1 AUX Output)
TB10-2	Common	C	
TB10-3	Normally Closed	NC	

TB11-1	Normally Open	NO	OUT6 Relay (Door 2 AUX Output)
TB11-2	Common	C	
TB11-3	Normally Closed	NC	
TB12-1	Normally Open	NO	OUT7 Relay (Door 3 AUX Output)
TB12-2	Common	C	
TB12-3	Normally Closed	NC	
TB13-1	Normally Open	NO	OUT8 Relay (Door 4 AUX Output)
TB13-2	Common	C	
TB13-3	Normally Closed	NC	
Door 1 – Reader & Supervised Inputs			
TB2-1	Yellow LED Control	YLED	Reader 1 Device Connections (Door 1 Reader)
TB2-2	Red LED Control	RLED	
TB2-3	RVO (Reader Power)	RVO	
TB2-4	Data/Data 0	DAT/D0	
TB2-5	Clock/Data 1	CLK/D1	
TB2-6	Beeper (Buzzer) Control	BZR	
TB2-7	Green LED Control	GLLED	
TB2-8	Ground (Reader Power)	GND	
TB3-1	Input 1	IN1	Input 1 (Door 1 Door Contact)
TB3-2	Input 1 Return	IN1G	
TB3-3	Input 2	IN2	Input 2 (Door 1 REX/EPB)
TB3-4	Input 2 Return	IN2G	
TB3-5	Input 3	IN3	Input 3 (Door 1 AUX1 Input)
TB3-6	Input 3 Return	IN3G	
TB3-7	Input 4	IN4	Input 4 (Door 1 AUX2 Input)
TB3-8	Input 4 Return	IN4G	
Door 2 – Reader & Supervised Inputs			
TB4-1	Yellow LED Control	YLED	Reader 2 Device Connections (Door 2 Reader)
TB4-2	Red LED Control	RLED	
TB4-3	RVO (Reader Power)	RVO	
TB4-4	Data/Data 0	DAT/D0	
TB4-5	Clock/Data 1	CLK/D1	
TB4-6	Beeper (Buzzer) Control	BZR	
TB4-7	Green LED Control	GLLED	
TB4-8	Ground (Reader Power)	GND	
TB5-1	Input 5	IN5	Input 5 (Door 2 Door Contact)
TB5-2	Input 5 Return	IN5G	
TB5-3	Input 6	IN6	Input 6 (Door 2 REX/EPB)
TB5-4	Input 6 Return	IN6G	

TB5-5	Input 7	IN7	Input 7 (Door 2 AUX1 Input)
TB5-6	Input 7 Return	IN7G	
TB5-7	Input 8	IN8	Input 8 (Door 2 AUX2 Input)
TB5-8	Input 8 Return	IN8G	
Door 3 – Reader & Supervised Inputs			
TB15-1	Yellow LED Control	YLED	Reader 3 Device Connections (Door 3 Reader)
TB15-2	Red LED Control	RLED	
TB15-3	RVO (Reader Power)	RVO	
TB15-4	Data/Data 0	DAT/D0	
TB15-5	Clock/Data 1	CLK/D1	
TB15-6	Beeper (Buzzer) Control	BZR	
TB15-7	Green LED Control	GLED	
TB15-8	Ground (Reader Power)	GND	
TB14-1	Input 9	IN9	Input 9 (Door 3 Door Contact)
TB14-2	Input 9 Return	IN9G	
TB14-3	Input 10	IN10	Input 10 (Door 3 REX/EPB)
TB14-4	Input 10 Return	IN10G	
TB14-5	Input 11	IN11	Input 11 (Door 3 AUX1 Input)
TB14-6	Input 11 Return	IN11G	
TB14-7	Input 12	IN12	Input 12 (Door 3 AUX2 Input)
TB14-8	Input 12 Return	IN12G	
Door 4 – Reader & Supervised Inputs			
TB17-1	Yellow LED Control	YLED	Reader 4 Device Connections (Door 4 Reader)
TB17-2	Red LED Control	RLED	
TB17-3	RVO (Reader Power)	RVO	
TB17-4	Data/Data 0	DAT/D0	
TB17-5	Clock/Data 1	CLK/D1	
TB17-6	Beeper (Buzzer) Control	BZR	
TB17-7	Green LED Control	GLED	
TB17-8	Ground (Reader Power)	GND	
TB16-1	Input 13	IN13	Input 13 (Door 4 Door Contact)
TB16-2	Input 13 Return	IN13G	
TB16-3	Input 14	IN14	Input 14 (Door 4 REX/EPB)
TB16-4	Input 14 Return	IN14G	
TB16-5	Input 15	IN15	Input 15 (Door 4 AUX1 Input)
TB16-6	Input 15 Return	IN15G	
TB16-7	Input 16	IN16	Input 16 (Door 4 AUX2 Input)
TB16-8	Input 16 Return	IN16G	

Figure 2.2: Terminal Connections

2.2 Jumpers



JUMPER	SETTING	DESCRIPTION
J6	ON/OFF	RS485 termination - Serial Port 1 (COM1) • See Note 1 below
J7	ON/OFF	
J8	ON/OFF	RS485 termination - Serial Port 2 (COM2) • See Note 1 below
J9	ON/OFF	

Figure 2.3: User-installed jumper settings

Note 1: RS485 termination jumpers are shipped from the factory in the OFF (termination disengaged) position. Only turn ON termination if the controller is at the end of the serial bus. When the serial port is operating in 2-wire (half duplex) mode, only engage 1 of the port's jumpers.

2.3 SOM (System on Module)

SOM Port: U1

The SOM (System On Module) comes from the factory and should not be removed. In case replacement is necessary, align the notch at the bottom of the SOM with the connector, slide the module in at a 45-degree angle until the contact pins are fully covered by the connector, then gently press the SOM towards the board until it clicks into place. Make sure the SOM is properly installed before powering on the board.

2.4 USB Port

The USB connection port is reserved for future use and should not be connected to any device.

2.5 Factory Connectors

Connectors: P3, P4, P5, P6, & P7

These are used for factory configuration and should not be modified or connected in any way unless directed by your technical support.

2.6 LEDs

There are 6 LEDs for monitoring panel functions and diagnosing issues.

Status LEDs	
1	Controller as Main Node in Cluster – ON means connected to a Host Controller as Client Node in the Cluster – ON means connected to Main Node
2	<ul style="list-style-type: none"> LED will flash when firmware is updating or Factory Reset is occurring FAC_RST button press – ON when ready to reset to default network interface settings (signals user to release button) ENB_SSH button press – ON indicates SSH is accepting connections. 30 second time window
3	RS-485 Serial Port 1 & 2 Activity – Flashes when data is transmitted
4	
5	Internal Interface Bus Activity – Flashes when data is transmitted
6	Heartbeat LED
Ethernet Ports	
Speed (left side)	ON = 100Mbps network connection
Link (right side)	Flashing = Network activity present

Figure 2.4: Status LED definitions

2.7 Function Buttons

There are three pushbuttons to perform the following functions...

RESET

This button will perform a hardware reboot. It functions like disconnecting and re-connecting power. To perform a reboot, press the button and immediately release. The status LEDs will light up and the device will reboot.

SSH

This button will enable connection to the device by SSH. This mode is only used for advanced troubleshooting. After pressing the button, SSH will be active for 30 seconds. If there is no connection within 30 seconds, SSH will be disabled.

FAC RST (Factory Default)

This button services two functions:

Full Factory Reset – Completely reset the device to factory default configuration; completely erasing all network settings, configurations, scripts, cardholder databases, and installed applications. Firmware version will be rolled back to the version was loaded by the factory at time of shipment.

Note: As of firmware 1.19, there is a “persistent storage” memory space that can be used to retain data through a Factory Reset.

Note: Boards shipped from factory with firmware version 1.20 will automatically reinstall embedded applications installed at the factory.

To perform a factory reset:

1. Power down the board by removing the power input connector or turning off the power supply to the device and waiting for all LEDs to turn off.
2. Press and hold the FAC_RST button.
3. While continuing to hold the FAC_RST button, reconnect power.
4. After the status LEDs turn off (about 7 seconds), release FAC_RST button.
5. After about 1 minute, the device will be up and running from its factory default configuration.

Network Reset - Reset both network interfaces as well as controller web interface UI username and password to their defaults. All other configuration and saved information will be kept. This function can be used when the network configuration is unknown or it is not possible to communicate with the device using the current configuration. To perform a network reset:

1. Make sure the device is powered on a running normally.
2. Press and hold the FAC_RST button until LED 3 is lit (about 3 seconds).
3. Release the FAC_RST button.

After a few seconds, the network interfaces will be reset to their default configurations (see the “Host Communications” section for the default settings).

2.8 Memory & RTC Retention During Power Failure

The controller configuration and cardholder memory are stored in non-volatile memory which does not require constant power to retain information. In the case of sudden power failure, the controller has onboard backup power to retain volatile memory.

The RTC (Real Time Clock) is persevered through a power outage with a coin cell battery. See the “Specifications” section for more information. The coin cell battery power level is monitored and as of firmware version 1.17 a low battery condition will generate an event message.

2.9 Mounting

Four holes are provided for mounting the BLU-IC4. Mount at least 0.25 inches above the conductive surfaces. All four mounting holes are plated for connecting to Chassis (Earth) ground.

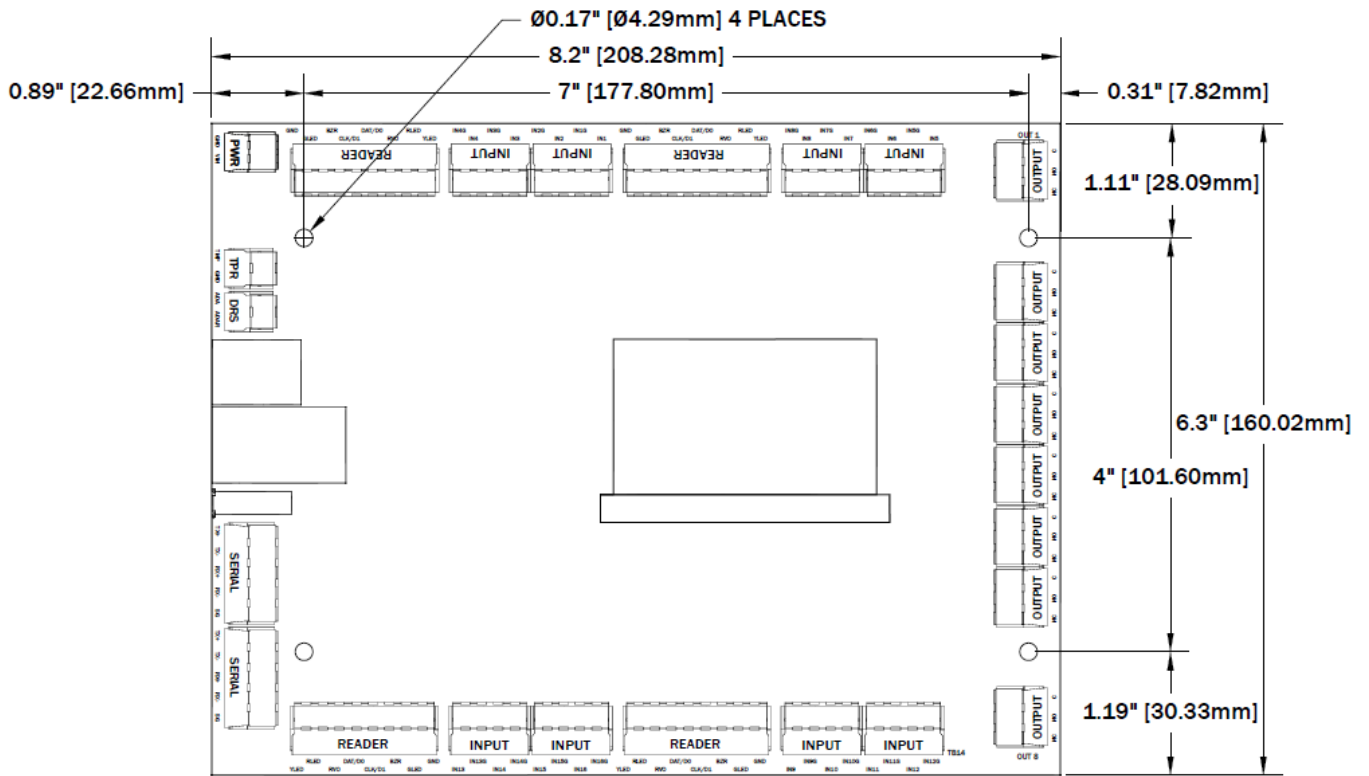


Figure 2.5: Dimensions and Mounting in inches(mm)

Part III

System Wiring & Setup

3 System Wiring

This section will provide installation and wiring instructions as well as hardware interface information as it applies to the access control system. To guard personal safety and avoid damaging equipment it is important to have a full understanding of electrical wiring best-practices and safety. The following sections provide general guidelines relating to the controller, but are not a substitute for formal training in safely handling electrical systems!

3.1 Power

3.1.1 Primary Board Power

Connector: TB1

The power connection should be 12-24 VDC and the maximum current consumption at 12VDC is 450mA. Due to large inrush currents, it is recommended to use a power supply with a “soft-start” feature. See Section 6 “Specifications” for more details on power consumption.

Take care when selecting a power supply for use with the controller. Most power supplies in the market today provide good input/output isolation, however those which do not provide isolation (or have high leakage capacitance), coupled with accidental AC power lines interchange, present serious ground fault problems for installers. With ground fault, the signal reference between subsystems may be 115 VAC (230 VAC) apart. If these subsystems are interconnected, the large potential difference will cause equipment damage or personal injury. Azure Access recommends the use of isolated, continuous power supplies only.

In the case of over-current, solid-state fuses integrated on the controller will ‘trip’ to protect the components of the panel. In many cases, the solid-state fuses will reset automatically when normal current resumes, however it may be necessary to interrupt the supply of power to allow the fuses to reset.

3.1.2 Powering Peripherals

Detailed electrical specs are in the “Specifications” section of this document (section 6).

To maximize longevity, it is not recommended to fully load all peripheral power ports when operating at the top of the operating temperature range.

Reader Port Power “RVO” (TB2, TB4, TB15, & TB17 – pin 3)

Readers can be powered directly from the four Reader Ports. The Reader Port power pin is directly connected to VIN so the voltage range can be 12-24VDC. Each port has a maximum current rating of 500mA and are auto-resetting fuse protected.

USB (J5)

The USB port is 5V and has a current maximum of 500mA.

3.2 Grounding

DC Ground

This is typically the minus (-) side of the DC output of the power supply. This is never to be connected to Safety (Earth) Ground on the AC side. It is to be connected to the DC ground input of all devices being powered by one supply. All devices’ ground connections must connect here if the device is powered by this supply.

AC Ground

Known as “Safety”, “Earth”, or “Chassis” ground. To avoid ground loop current, there must be only ONE point at which the safety ground connects to the DC ground (usually through the DC/DC power supply).

3.3 Communications

3.3.1 Network

Connectors: J3 & J4

The controller communicates with the Host and other clustered ICs over the network and can also be configured to communicate with downstream panels over the network. There are 2 dedicated Ethernet ports available. Connection to network switch should be made using standard CAT5e or CAT6 cable.

3.3.2 Downstream Serial Ports

Connectors: TB19 & TB20

Communication with downstream IO Alarm Panels, Reader Interfaces, and OSDP Readers is done through the two RS-485 Serial Ports.

RS-485 is an electrical interface standard for multi-point communication on bus transmission lines. It allows high speed data transfer over extended distance (4000 ft, 1219m). Both ports can be configured to communicate using different protocols. The Serial Ports on the controller are 4-wire but can support 2-wire devices on the bus.

Device Wiring

4-wire RS-485 consists of 5 wires; TX+, TX-, RX+, RX-, & SG (signal ground). Both TX and RX have their own differential pair. Match the polarities; connect positive (+) to positive and negative (-) to negative. Wiring recommendation of 24 AWG, shielded twisted-pair. Wiring requirements satisfied by Belden 9841 or equivalent. 2-wire devices (such as OSDP Readers) on the bus can be supported if the TX+ and RX+ are connected together, and the TX- and RX- are connected together.

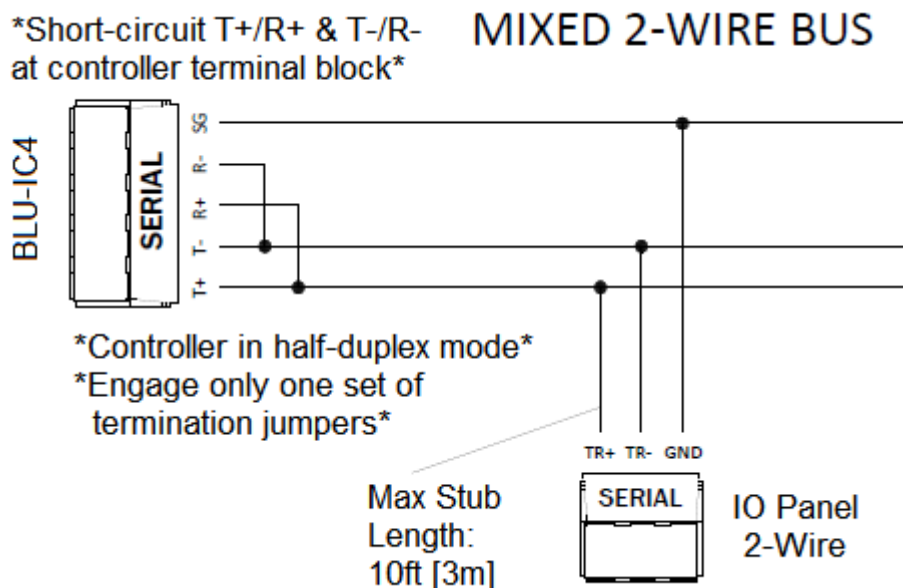


Figure 3.1 RS-485 Device Connections

Bus Configuration

There are 32 available addresses on each serial port's RS-485 bus although required system-performance may limit the number of actual devices on the bus. Communication cables for RS-485 should be laid out in a "multi-drop topology". This means that there should only be two ends to the line and devices should be located directly along this line. The controller can be located at any point along the line. T-stubs longer than 10ft and Star wiring topology will cause communication problems and must be avoided. All the devices on the bus must communicate with the same protocol, use the same baud rate, and all the downstream devices connected to the IC must have a unique address (set with DIP switches on downstream devices).

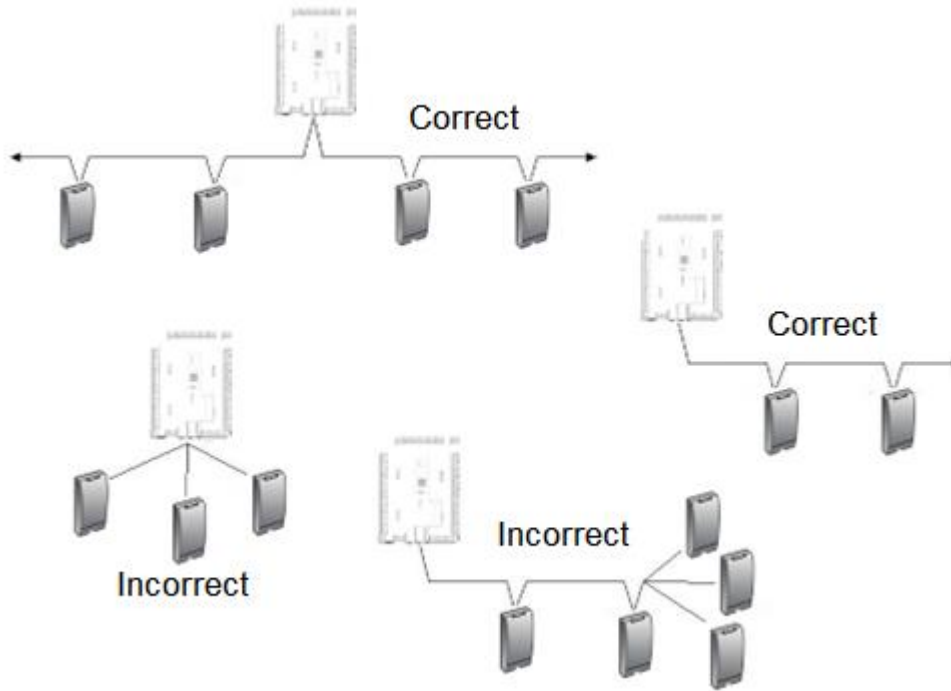


Figure 3.2: RS-485 Bus Configuration

Devices on the RS485 Serial Bus must be daisy-chained. 'T'-stubs or Star configurations are not allowed!

Termination

For the most reliable communications, the RS-485 bus must be terminated at both ends. The terminators are integrated on the board and are engaged via user installed jumpers. Never engage termination of devices in the middle of the communication bus. When the serial port is operating in 2-wire (half duplex) mode, only engage ONE 1 of the jumpers.

External termination modules (ATM-48) are not required but can be used. If using the ATM-48 termination module, DO NOT install the jumpers on the board. The wiring is as follows...

4-wire configuration:

ATM-48 Pin 1 -> T+
 ATM-48 Pin 2 -> T-
 ATM-48 Pin 3 -> R+
 ATM-48 Pin 4 -> R-

If using 2-wire RS-485 configuration, only connect pins 1 & 2 **OR** 3 & 4 since the +'s and -'s will already be connected together.

Signal Ground

When devices are powered from different power supplies, a common ground reference must be established on the RS-485 bus. This is the ground (GND) connection on the Serial port connector. Failure to have a common ground between devices may cause communication errors. If connecting the RS-485 bus with shielded wire, the shielding can be used as the signal ground connection. Or, if the environment is known to be electrically noisy, the wire's shield can be connected to safety/chassis/Earth ground and a separate wire can be used for signal ground.

Grounding Potential Difference Checks Before Connecting

Before a device is connected to an RS-485 subsystem, it must be checked for ground fault. Ground faults can damage all devices connected to the RS-485 communication line. To check if there is ground fault for a new unit, follow the steps below:

1. Apply power to all devices already successfully connected to the RS-485 line.
2. Power up the new unit, but DO NOT connect it to the RS-485 line.
3. Connect the signal ground (SG) of the RS-485 line through a 10k limiting resistor.
4. Measure the AC and DC voltage across the resistor. There should NOT be more than 1 volt across the resistor. Otherwise find and clear the fault.
5. Connect the new unit to the RS-485 line only if no ground fault is found.

3.3.3 OSDP Reader Wiring

Because the Reader Ports only support TLL readers, OSDP (or other RS-485 readers) must connect to the Serial Ports. RS-485 restrictions on wire length and bus configuration must be observed.

OSDP readers use a 2-wire RS-485 interface with a single pair of wires handling both TX & RX. To connect them to the IC's 4-wire interface, the TX+ needs to be jumpered to the RX+ and the TX- jumpered to the RX-. All devices must share a common signal ground connection; especially if being powered from different sources.

Extra reader licenses can be purchased to enable connecting up to 16 OSDP readers (8 readers per serial port). See the previous section on "Bus Configuration" for adding multiple OSDP readers to the bus.

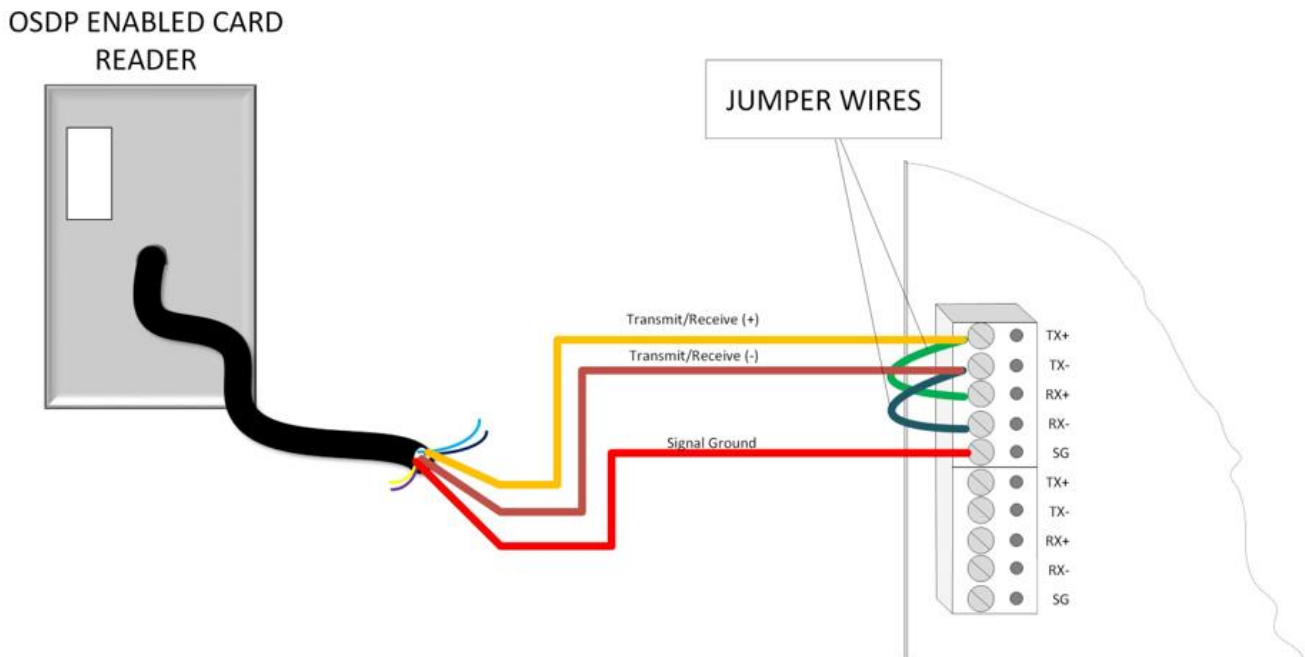


Figure 3.3: OSDP Reader Wiring

3.4 Reader Ports

Connectors: TB2, TB4, TB15, & TB17

The controller has four onboard reader ports for connecting TTL Readers (Wiegand, Clock & Data, etc). OSDP Readers that use RS-485 are connected to the Serial Ports (Section 3.3.3)

PIN	DESCRIPTION
YLED	Open-collector LED output (labeled for Yellow)
RLED	Open-collector LED output (labeled for Red)
RVO	VIN passthrough DC power for reader
DAT / D0	Wiegand "Data 0" input / Clock&Data "Data" input
CLK / D1	Wiegand "Data 1" input / Clock&Data "Clock" input
BZR	Open-collector buzzer output
GLED	Open-collector LED output (labeled for Green)
GND	Ground connection for the reader

Each reader port can support one TLL reader. TTL reader types include Wiegand, magnetic stripe, proximity, bar code, smart card, biometric, keypad, etc. A different type of reader can go on each port.

Do not exceed 500 feet (152 m) between the IC and reader. 18 AWG cable may be required for long cable lengths or for large current requirements. If twisted pair cable is used, do not wire Data 1/Clock and Data 0/Data in the same pair. There are 3 signals for controlling LEDs on the reader (up to 3 colors). Connect the shield drain wire of the cable at the GND terminal of the appropriate Reader Port. Carefully insulate the drain wire with sleeving for a reliable installation.

Power for each reader port is provided through the "RVO" pins. This pin is a passthrough of VIN (12-24VDC) and is protected with an auto-resetting fuse. The Reader Ports can each supply 500mA maximum of current. Reader power consumption needs to be accounted for in the supply's power budget. If not powering the readers through the controller's reader port, leave RVO and GND disconnected on the controller and wire the reader directly to the power supply.

For basic operation of the reader, at a minimum the Data 1/Clock and Data 0/Data wires must be connected from the reader to the controller and power supplied to the reader. LED and buzzer control lines do not have to be connected, but in this case, the LED and buzzer may not function on the reader.

3.5 Unsupervised Cabinet Tamper

Connector: TB21

The Cabinet Tamper (TMP) input only supports an unsupervised configuration. This input is wired to the enclosure and detects when the enclosure door is opened and closed. Wire this input with 24 AWG minimum. See "Unsupervised" in Figure 3.4 wiring diagram.

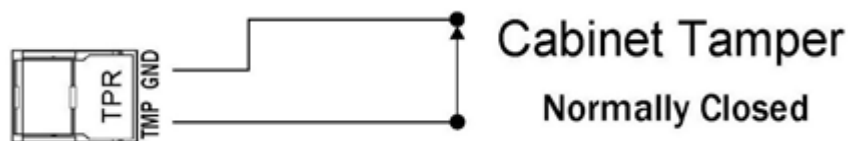


Figure 3.4: Cabinet Tamper

3.6 Supervised Input Wiring

Connectors: TB3, TB5, TB14, & TB16

The controller has 16 Supervised Alarm Inputs. These inputs are multi-purpose and are configured with the Host software. Any input can be assigned as a door contact, REX, or auxiliary alarm input (i.e. motion or glass-break sensors). With the use of end-of-line termination resistors, the alarms are monitored for not only secure and alarm states, but also the detection of fault conditions from tampering and accidental damage.

These alarm inputs can be configured as either “Normally Open” or “Normally Closed” and can also operate in an Unsupervised mode. Unsupervised configuration does not require any external, end of line resistors.

However, unsupervised mode is the least secure and damage or tampering of the line can go undetected, resulting in missed or false alarms. The unsupervised configuration should not be used in any situation that requires security. An example of unsupervised input wiring can be seen in Figure 3.9.

Input wiring requires minimum 22 AWG up to 1,000ft (304.8m) and a maximum of 30 Ohms of loop resistance.

The possible modes for each input are:

Type	Supervision	Configuration	Resistance Value
Alarm Zone	Unsupervised	NC (Normally Closed)	None
Alarm Zone	Unsupervised	NO (Normally Open)	None
Alarm Zone	Supervised	NC (Normally Closed)	300/10K
Alarm Zone	Supervised	NO (Normally Open)	300/10K
Alarm Zone	Supervised	NC (Normally Closed)	3K/4.5K
Alarm Zone	Supervised	NO (Normally Open)	3K/4.5K
Tamper Zone	Unsupervised	NC (Normally Closed)	None
Tamper Zone	Unsupervised	NO (Normally Open)	None
Tamper Zone	Supervised	NC (Normally Closed)	300/10K
Tamper Zone	Supervised	NO (Normally Open)	300/10K
Tamper Zone	Supervised	NC (Normally Closed)	3K/4.5K
Tamper Zone	Supervised	NO (Normally Open)	3K/4.5K

3.6.1 Input Supervision

Using two End-of-Line (EOL) termination resistors, the Supervised mode can detect fault conditions resulting from accidental damage or tampering. The controller will not confuse this condition with a valid secure or alarm condition. For maximum security, the end-of-line termination resistors should be placed at the END of the cable, farthest away from the controller.

Supervised inputs can be configured with the Host software to use different EOL resistor values. A handful of standard EOL resistor values are configurable as well as support custom resistor values. Resistors can be individually installed or factory-made resistor packs can be installed. All resistors used for supervision should be 1% tolerance or less. Factory-made resistor packs include the ATM-30 (300/10K Ohm) and ATM-3D (3K/4.5K Ohm). The following wiring diagrams show how to install the EOL resistors...

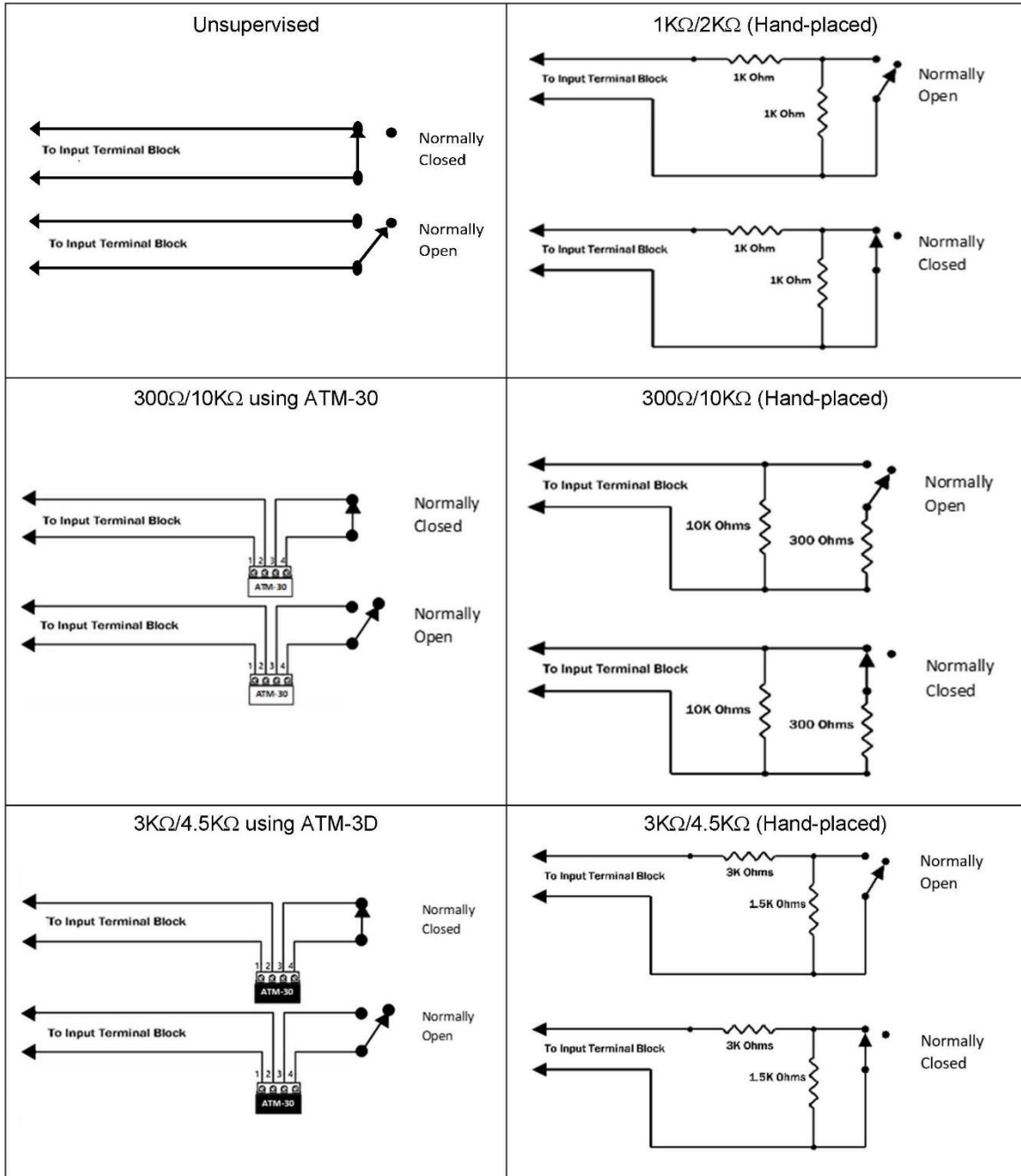


Figure 3.5: Input Supervision

3.7 Output Relays

Connectors: TB6 – TB13

There are 8 output relays onboard. These relays can either control a door strike (lock) or other electrical device connections or other miscellaneous output control. Relay functions are defined in the host software. The onboard relays can switch up to 2A @ 24VDC or 1A @ 120VAC.

The strike can be wired in a fail-safe (door unlocks on power outage) or fail-secure (door locks on power outage) manner by using either the Normally Closed (NC) or Normally Open (NO) relay contacts

3.7.1 Strike Wiring

A typical electric door strike (lock) will require around 250mA (0.25 Amps) to operate. If the locking device requires more than 2 Amps to control, another external power-switching device/relay of adequate power rating must be used. Some strikes such as magnetic strikes are inductive loads, in which case is recommended to derate the relay's rated current by 50%.

Wiring between the strike power supply, strike relay (internal or external) and the electric lock should be of sufficient gauge (16 to 18 AWG recommended) to prevent excessive voltage drop under all circumstances.

3.7.2 Auxiliary Relay Output Wiring

Aside from controlling door strikes, relay outputs can be used for controlling other audible and visual devices. Auxiliary relay functionality is configured via the Host software.

3.7.3 Voltage Spike Suppression

Due to inductive nature of a door strike, energizing and deenergizing of the relay can cause voltage spikes across the relay contacts. If no suppression is used to defend against these voltage spikes, communication problems and permanent damage to the hardware may occur.

Strike Type	Suppression Method
DC Strike	Reverse-biased DIODE with a continuous current rating of at least 1x the strike current and a breakdown voltage (Vbr) rating of at least 2x the strike voltage. Usually a 1N4001 – 1N4006 will work.
AC Strike	A Metal Oxide Varistor (MOV) will usually be included with the strike. If a MOV does not come with the strike, contact the strike manufacturer for the appropriate MOV ratings. Be sure to use a UL approved MOV.

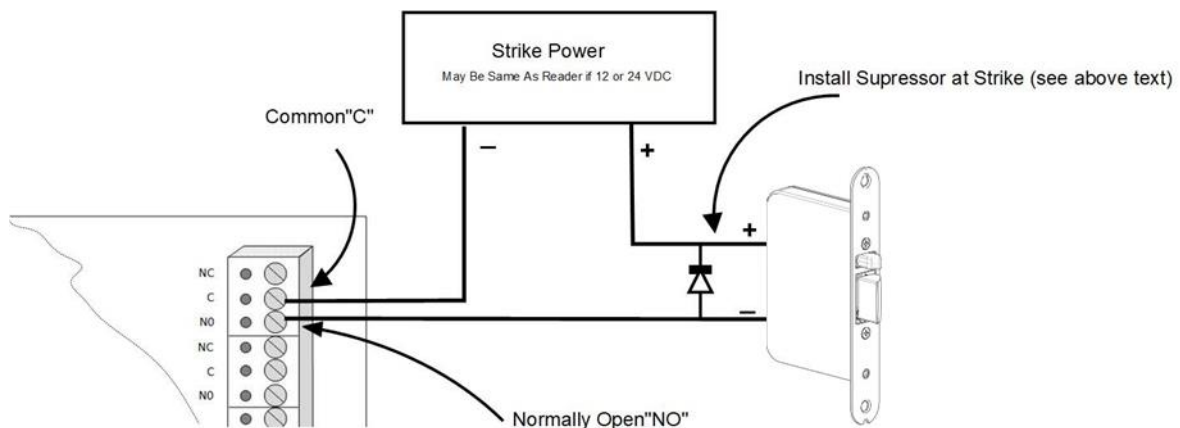


Figure 3.6: Strike Wiring Diagram (DC w/ Diode)

Both DC and AC suppression components are placed across the output device's electrical terminals.

3.8 Door / Access Point Setup

An Access Point (sometimes referred to simply as a "Door") is the grouping of at least one reader, supervised inputs, and relay outputs to yield full control and monitoring of a door/entryway. The controller can support up to 4 complete Access Points by default. More Access Points are possible with the purchase of extra reader licenses allowing for multi-dropping more OSDP readers. A "complete" Access Point consists of at least one reader, two supervised inputs (for door contact and REX), and one relay output controlling the door strike. Configuration and assignment of the Access Point's interfaces is done through the Host software. Recommended connections are listed in parenthesis in the Terminal Block table in section 2.

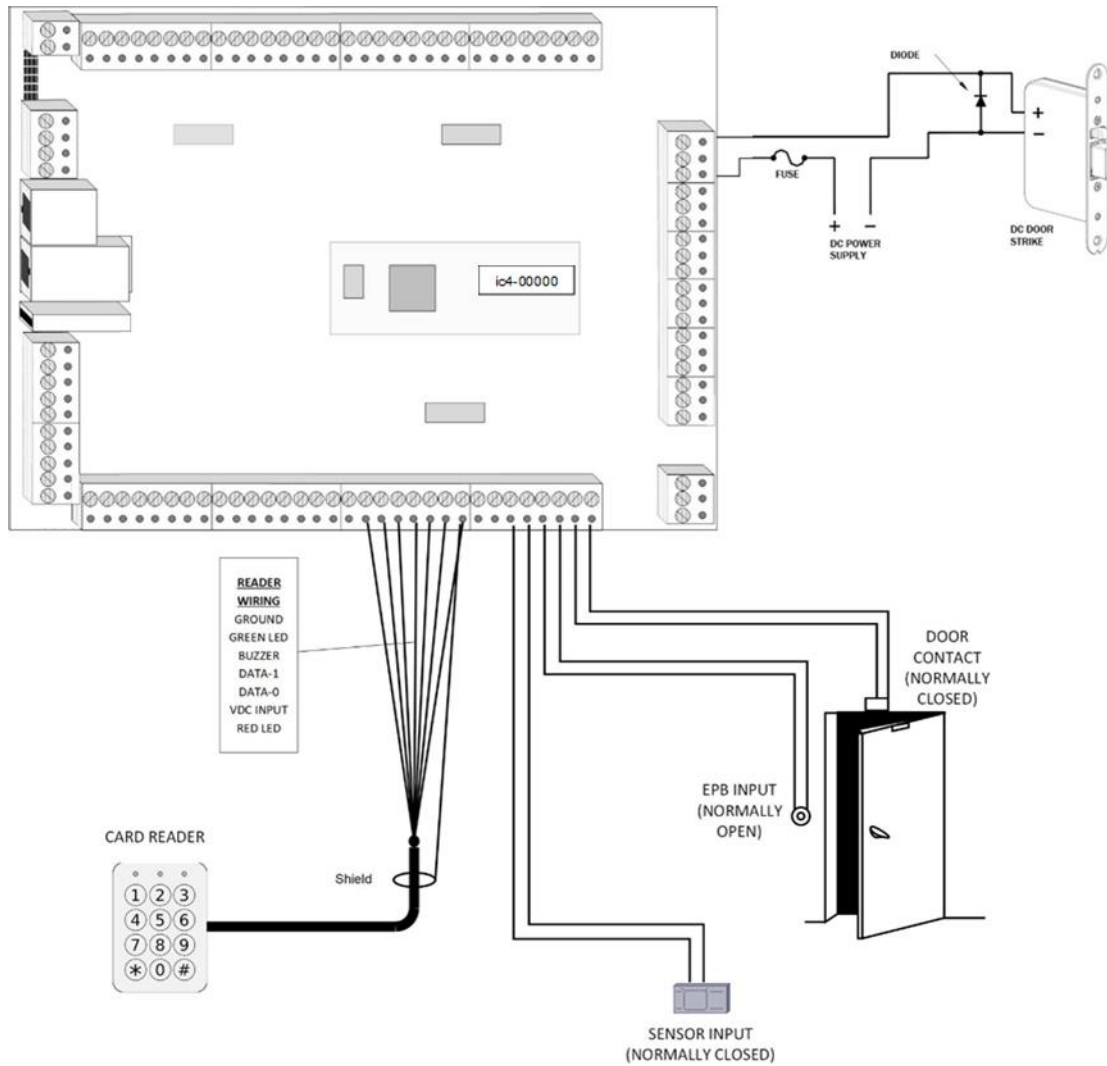


Figure 3.7: Example of wiring a complete Access Point / Door

For each reader connection there is a door contact input, exit push button input and two axillary inputs one of which is displayed here connected to a motion sensor. Refer to the Terminal Connectors table and the installation instructions for the reader that will be used for exact wiring positions.

3.8.1 Reader

An Access Point needs at least one reader to receive credentials. The controller supports both TTL and RS-485 (OSDP readers). Access Points can also use two readers in a “paired” configuration.

3.8.2 Door Contact & Exit Pushbutton/REX Inputs

The door contact input is a normally closed input used to monitor the position of the door (open or closed). This will typically be connected to a magnetic sensor in the frame of the door that will provide a short circuit when the door is closed and an open circuit when the door is opened. Door Contact inputs are required for features that require knowledge of door usage; such as Anti-Passback, Door Forced / Held Open, and more precise strike timing. Door contact inputs should be jumpered and configured as Normally Closed when not in use.

The Exit Pushbutton, sometimes referred to as a REX (Request-to-Exit/Enter) input, is a Normally Open input that is used to inform the Access Point the door needs to, or will be opening without an access request being made with a user's credential (card, pin, etc). It is usually in the form of a pushbutton, but it could also be in the form of a motion sensor or other user-activated sensor. Note that different types of sensors will require different strike timing calibrations. An input configured as an Exit Pushbutton will be disabled while reader tamper is active, and will remain inactive for 1 minute after the tamper alarm ends.

If input supervision is enabled (see Part 3.5.1 above), end of line (EOL) terminating resistors must be installed. The terminating resistors should be installed as close to sensor (away from the controller) as possible.

3.8.3 Door Strike

Door strikes come in a variety of different styles. They can come in different voltages (both AC and DC), and can operate in a Fail-Secure or Fail-Safe manner. The most common voltages are 12 & 24 Volts. A Fail-Safe door uses electrical current to keep the strike locked; meaning in the case of power failure, the strike will default to an unlocked state. A Fail-Secure strike uses electrical current to unlock the door; meaning in a power failure situation, the door will default to a locked state.

Part IV

Controller Configuration

4 Controller Configuration

4.1 Host Communications

The controller connects to the Host monitoring software over the network to receive commands and report events. Controllers communicate with the Host either individually (Standalone Mode) or as a part of a multi-controller Cluster (see section 4.2). If the connection to the Host is not available, events and other messages will be stored in the memory buffer on the controller and will be transmitted once a Host connection becomes available.

The default network interface settings are as follows...

Network Interface 1: DHCP using IPv4

Network Interface 2: Static IP using IPv4; IP Address 192.168.0.1

Network settings can be changed through the controller's web server (see section 4.4.2 for more details)

The DHCP resolves an IP address to the Hostname printed on the SOM sticker. When Network Interface 1 is unable to use DHCP, connections to the controller must be done through a static IP address. On startup, the controller will initially attempt to reach a DNS server. If this is unsuccessful, the controller will switch to using a default static IP address of **192.168.0.2**

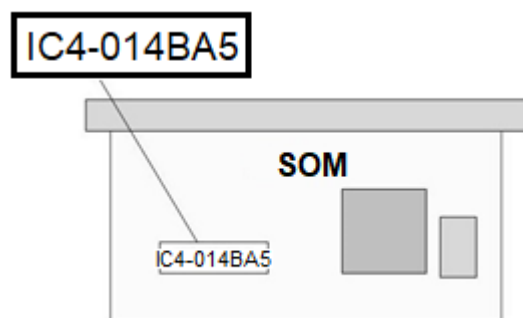


Figure 4.1: Hostname

4.2 Controller Clustering

A Cluster is a group of controllers (Nodes) that maintain communications with the Host software through a single controller. There are two types of Nodes; a Main Node and Client Nodes. Each Cluster can comprise of 1 to 32 Nodes requiring a single controller acting as the Main Node.

Main Node – This controller acts as the communication bridge between the Host and the other Client Nodes in the Cluster. In Clusters with many controllers, it is recommended that the Main Node serve the sole purpose of being a communication bridge without performing access control functions; i.e. no readers, access points, etc. For Clusters with fewer controllers, the Main Node can perform access control functions with readers, access points, etc while also being the communication bridge.

Client Node – Controller(s) that point to a Main Node. Client Nodes are responsible for access control functionality; controlling and monitoring access points/doors.

It is possible to use single-controller Clusters, where every controller maintains its own individual connection to the Host as the Main Node with no Client Nodes. This is referred to as Standalone Mode.

Controller-to-Host and Controller-to-Controller communications happens over a TCP/IP network connection. Certain functions and information such as Anti-Passback is shared throughout the Cluster. Cluster configuring is done in each controller's Services page on the web server (see section 4.4.4).

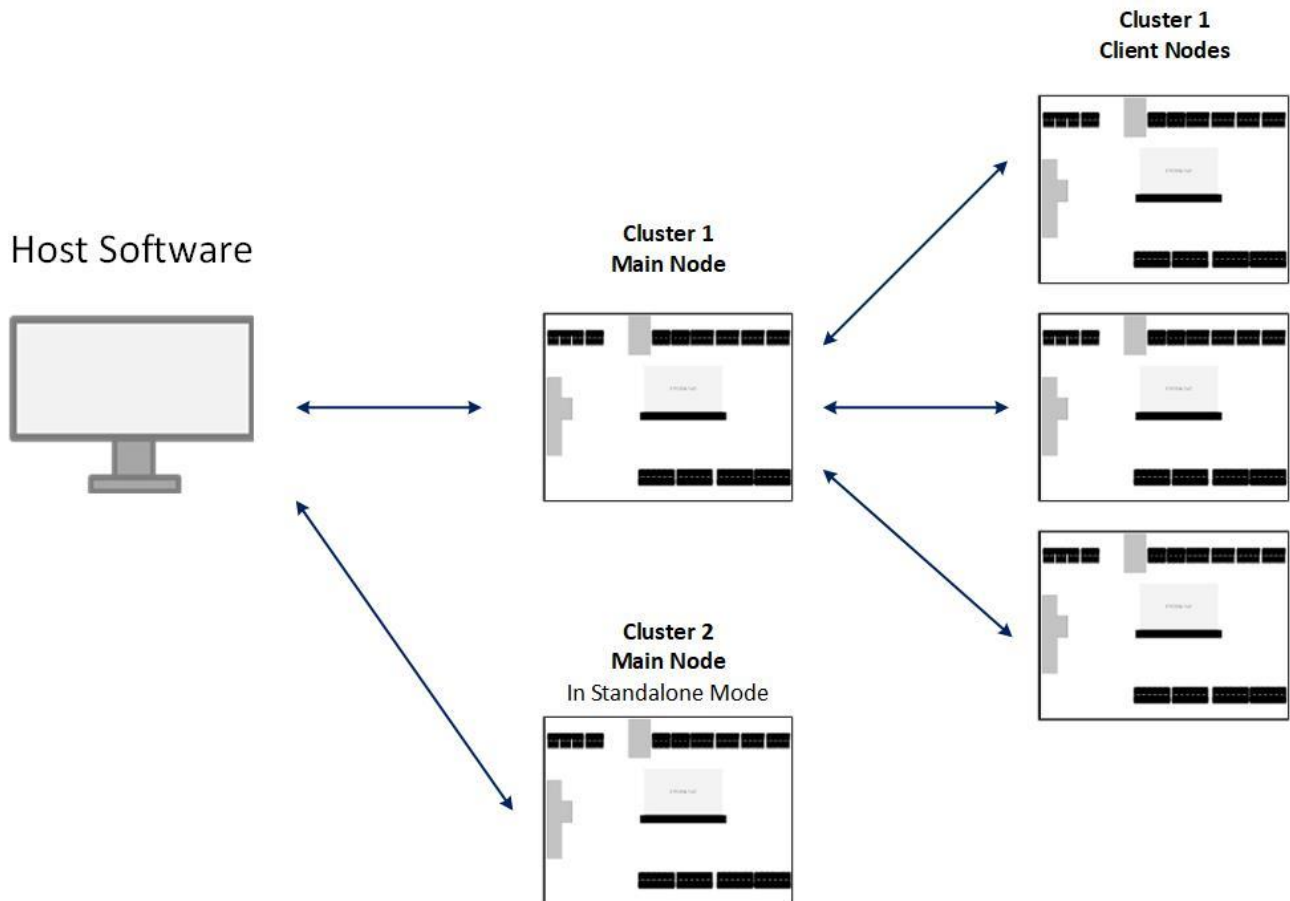


Figure 4.2: Cluster Topology

4.3 Licenses

License	
Max Cards	20000
Max Readers	8

Figure 4.3: Controller's License Values Shown on Home Page

Licenses only apply to controllers. The Card Database size and Expandable Reader count are set with licenses stored on the controller and the values can be seen on the web server Home Page. Both licenses come pre-loaded from the factory based on product ordering options. Licenses can be later upgraded in the field. Upgrade license files can be electronically delivered and then uploaded to the controller either through the web server or Host software (if update feature is supported). See section 4.5 for instructions on upgrading licenses through the web server.

The controller does not need any licensing for connecting downstream reader-interface and IO panels. Furthermore, the downstream boards themselves do not require licenses for storage or to connect readers to them. Downstream Reader Interface panels have fixed limits on the number of readers that can be connected.

4.3.1 Card Database License

The max number of cards that can be stored in the controller's database. There is no limitation on complexity of the card record. The database size license that is loaded at the factory is based on the purchase option.

Firmware earlier than version 1.17 all cards, active or inactive are counted towards the database size limit. Starting with firmware version 1.17 only active cards are counted towards the database size limit.

4.3.2 Expandable Reader License

The total number of readers that can be connected directly to the controller is set with the Reader License. By default, the BLU-IC4 comes pre-loaded with four reader licenses. As of firmware version 1.17, readers that are used as alternate, paired readers on the first four Access Points do not consume a license. More Reader Licenses can be selected at the time of purchase to come pre-loaded from the factory or purchased after initial purchase of the hardware and updated in the field.

4.4 Web Configuration Interface

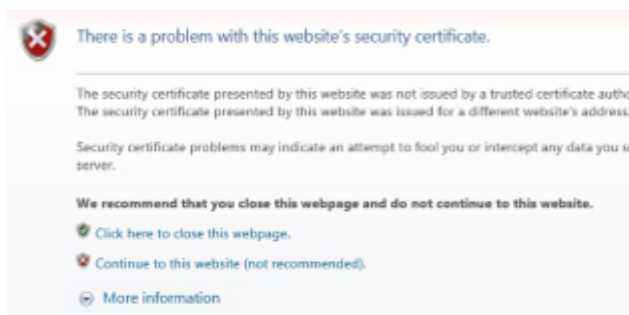
The onboard web server allows for network and certain configuration options to be applied through a web browser. In order to access the web server, enter the Hostname or IP address of the controller into a web browser in one of the following formats:

https://IC4-010001 or **https://192.168.0.2**

If TLS certificates are not recognized, an alert window will appear saying the communication connection is not secure. This warning can be ignored in order to proceed to the configuration page. TLS certificates are supported to secure web server connections (see section 4.4.4).

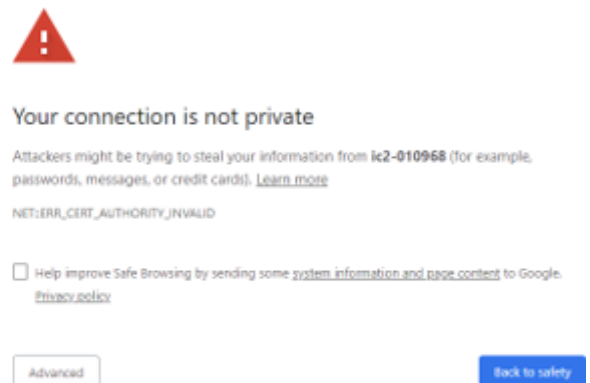
To bypass the secure-connection error, perform the follow steps depending on the web browser...

Internet Explorer:



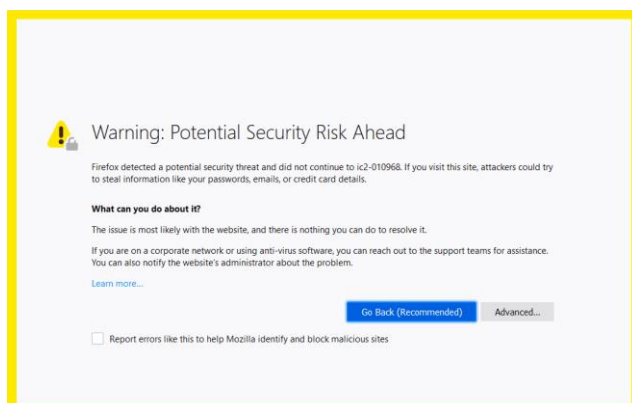
1. Click *continue to this website (not recommended)*

Google Chrome:



1. Click **ADVANCED**
2. Click *Proceed to IC2-010001 (unsafe)*

Firefox:



1. Click **ADVANCED**
2. Click *Add Exception*
3. In the new window that is displayed, enter IC-010001 as *Location*
4. Click *Confirm Security Exception*

A sign in form will appear for entering the username and password. The credentials are case-sensitive.

Username: admin

Default Password: *last 6 characters of MAC address (see Hostname sticker on SOM)*

THE DEFAULT PASSWORD SHOULD IMMEDIATELY BE CHANGED

As of firmware version 1.20, the user will be prompted to change the password following these requirements:

- Minimum length of 6 characters
- Contain at least one of each of the following: uppercase, lowercase, number, symbol

Clicking "CANCEL" of the new password prompt will keep the current password. This is not recommended!

A successful log in will redirect to the web server home page that displays core controller information such as serial number, Hostname, firmware versions, licensing, and board information. The tabs at the top of the window navigate to different configuration pages.

The following subsections describe the different web pages accessible on the web server and the configurable settings...

4.4.1 Date & Time

The screenshot shows a web interface for configuring date and time. The title is "Date and Time Configuration". There are four main configuration items, each with a text input field and a small 'x' icon to the right:

- Date:** 07/08/2019
- Time:** 10:48:40.000 AM
- Time Zone:** America/Los_Angeles
- SNTP:** time.azure-access.com

Below the Time Zone field, there is a note: "Type the region you're in or use the valid POSIX TZ string to specify the custom time zone. For example: America/Los_Angeles (PST8PDT,M3.2.0,M11.1.0)". At the bottom of the form are two buttons: "Save" and "Reset".

Date – The current date setting used by the device. This value cannot be modified

Time – The current time setting used by the device. This value cannot be modified

Time Zone – The time zone the controller should use

SNTP – It is recommended to use a Simple Network Time Protocol (SNTP) service to maintain the highest level of time precision for event data. SNTPs are available publicly over the internet or can be hosted locally on the network. To point to an SNTP server, enter its network or web address. Publicly accessible SNTP servers include: **time.azure-access.com** or **pool.ntp.org**

Save settings when complete or click **Reset** to return to default settings.

4.4.2 Network

Network #1 (00:60:ee:01:4b:a5)

IPv4 Settings

DHCP
 Static

Address

Mask

Default Gateway

Enable 802.1X security
Configure 802.1X

IPv6 Settings

Auto
 Static

Address

Prefix Length

Default Gateway

Network #2 (34:08:e1:a0:1a:72)

IPv4 Settings

DHCP
 Static

Address

Mask

Default Gateway

Enable 802.1X security
Configure 802.1X

IPv6 Settings

Auto
 Static

Address

Prefix Length

Default Gateway

Network #1 – Checking this box enables the first Ethernet port (smaller RJ45 connector designated J4)

Network #2 – Checking this box enables the second Ethernet port (larger RJ45 connector designated J3)

IPv4 Settings – Checking this box enables IPv4 addressing (most common).

IPv6 Settings – Checking this box enables IPv6 addressing.

DHCP or Static – Select the method of IPv4 address assignment to the controller.

DHCP – The DHCP server will assign the controller an IPv4 address. This requires a DNS server operating on the network. Dedicated routers or server-type operating systems can provide DNS services on the network. With DHCP, the controller can be connected to on the network with by the Hostname. The Hostname is printed on a sticker on the SOM module.

Static – The user must enter a unique IPv4 address for the controller to use.

Address / Mask / Default Gateway – Manually entered network parameters when using Static IP address.

802.1X – Controllers can use 802.1X authentication on the network. Clicking the Configure button will allow the user to enter the authentication type, username, and password. Check the “Enable 802.1X security” box to enable 802.1X.

Bridge (42:0f:d7:28:57:85)

IPv4 Settings

DHCP
 Static

Address

Mask

Default Gateway

Enable 802.1X security
Configure 802.1X

IPv6 Settings

Auto
 Static

Address

Prefix Length

Default Gateway

Bridge – Check this box to have both Ethernet ports act as a single network interface with a single IP address. This overrides individual settings for Network #1 and Network #2. The bridge is configured with the same types of network settings as the individual interfaces.

Manual DNS

Domain

Primary DNS Server

Secondary DNS Server

Third DNS Server

Save Reset

Manual DNS – Check this box to enable manually designated DNS servers on the network. This is used primarily for Static IP configurations.

Firewall (firmware 1.20) – IP rules can be put in place to prevent unauthorized access and prevent DDoS attacks to different services.

IP-Based Access Control

Description

My rule1

IP-Networks

10.0.0.0/8

Main Node

Zeroconf

NTPD

SNMP

Socket Driver

SSH

Web Config

Save Reset Cancel

Save settings when complete or click **Reset** to return to default settings.

4.4.3 Mail

The controller can send SMTP e-mail notifications via features like Scripting.

SMTP Client Configuration

Mail from address	<input type="text" value="<from>"/>
SMTP server hostname	<input type="text" value="smtp.example.com"/>
SMTP server port	<input type="text" value="587"/>
SMTP server username	<input type="text" value="<user>"/>
SMTP server password	<input type="password" value="[defined]"/> <input type="checkbox"/> Show password
Use TLS	<input checked="" type="checkbox"/>
SMTP server verification	<div style="border: 1px solid #ccc; padding: 2px;"> ▼ <div style="background-color: #f0f0f0; padding: 2px;">No</div> <div style="background-color: #0070c0; color: white; padding: 2px;">No</div> <div style="padding: 2px;">Fingerprint</div> <div style="padding: 2px;">CA certificate</div> </div>

Mail from address – The address (ex: sender@example.com) that will be displayed in the “from” field.

SMTP server hostname – Network location (Hostname or IP address) of the SMTP server on the network.

SMTP server port – The port to use to establish connection to SMTP server.

SMTP server username – The username for accessing the SMTP server.

SMTP server password – The password for accessing the SMTP server.

Use TLS – Check this box to enable encryption for message sending.

SMTP server verification (firmware 1.20) – Select verification method.

Save settings when complete or click **Reset** to return to default settings.

4.4.4 Services

Web Config

Comm Certificate	<input type="button" value="Choose file"/> <input style="width: 150px;" type="text"/>
	Note: Using default communication certificate
HTTPS port	<input type="text" value="443"/>
HTTP port	<input type="text" value="80"/>
Redirect to HTTPS	<input checked="" type="checkbox"/>

Web Config – Checking this box enables the web server on the controller that can be accessed via web browser.

Comm Certificate – Users can upload custom certificates for TLS encryption.

HTTPS port – The network port to connect to for encrypted connections.

HTTP port – The network port to connect to for unencrypted connections.

Redirect to HTTPS – Check this box to force unencrypted HTTP connections to be encrypted HTTPS connections.

Client

Main Node address localhost

Read Timeout 1000

Keepalive time 500

Note: For backward compatibility keepalive time should be less than read timeout

Keepalive interval 3000

Keepalive retry 3

Node name ic2-014BA5

Client – When box is checked, this enables the Access Control functionality on the controller allowing for readers, downstream panels, and access points to be controlled locally. This should always be enabled unless the controller is strictly acting as a Main Node communication-bridge for a multi-controller Cluster (see section 4.2).

Main Node address – When this controller is a Client Node of a multi-controller Cluster, enter the Hostname or IP address of the Main Node controller in the Cluster. If this controller is the Main Node, enter “localhost”.

Read Timeout – How long (in milliseconds) the controller should be allowed to process an entire multi-packet message after the first packet is received. This is the Client Node service’s connection to the Main Node service.

Keepalive Time – How long (in milliseconds) the controller should wait to send a Keepalive message after the last successful message exchange has occurred. This is the Client Node service’s connection to the Main Node service.

Keepalive Interval – After an unsuccessful Keepalive message, how long (in milliseconds) the controller should wait to try another Keepalive message. This is the Client Node service’s connection to the Main Node service.

Keepalive Retry – The number of times to retry the Keepalive message before considering the connection offline. This is the Client Node service’s connection to the Main Node service.

Node Name – A text string identifying the Client controller to the Main Node / Node map. This can be anything.

Main Node

Read Timeout	1000
Keepalive time	500
Note: For backward compatibility keepalive time should be less than read timeout	
Keepalive interval	3000
Keepalive retry	3
Time Server	<input checked="" type="checkbox"/>
Incoming Connection	<input checked="" type="checkbox"/>
Port	5000
WebSocket Incoming Connection	<input checked="" type="checkbox"/>
Port	5001
Outgoing Connections	<input type="checkbox"/>
Host Filter	<input type="checkbox"/>

Main Node – Checking this box configures the controller to communicate with the Host either as a Standalone controller (single-controller Cluster) or as the communication-bridge to the Host for multiple Client controllers in a Cluster.

Read Timeout – How long (in milliseconds) the controller should be allowed to process an entire multi-packet message after the first packet is received. This is the Main Node service's connection to the Host.

Keepalive Time – How long (in milliseconds) the controller should wait to send a Keepalive message after the last successful message exchange has occurred. This is the Main Node service's connection to the Host.

Keepalive Interval – After an unsuccessful Keepalive message, how long (in milliseconds) the controller should wait to try another Keepalive message. This is the Main Node service's connection to the Host

Keepalive Retry – The number of times to retry the Keepalive message before considering the connection offline. This is the Main Node service's connection to the Host.

Time Server – This enables this Main Node controller to be the Time Server for the Client Nodes in the Cluster.

Incoming Connection – This enables network connections to be initiated from another device to the controller.

Port – The network port to accept incoming network connections.

WebSocket Incoming Connection – Enable incoming WebSocket connections.

Port – The network port to accept incoming WebSocket connections.

Outgoing Connections – Checking this box will configure the controller to be the initiator of the connection to the Host or a WebSocket endpoint.

Host Filter – By default, the controller allows for up to 5 simultaneous Host connections. It is recommended to check this box to only allow authorized Host IP addresses to connect to the controller. Upon clicking the box, text boxes will appear for entering the Hostnames or IP addresses of the authorized Hosts.

 SNMP

 Zeroconf

SNMP – If enabled, the controller will advertise Simple Network Management Protocol information that is viewable using an SNMP MIB browser or other SNMP compatible devices.

SNMPv3 (firmware 1.20) – SNMPv3 can be used with a mandatory username and password and the option of using MD5 or SHA authentication.

SNMP Service


Enable SNMPv2	<input checked="" type="checkbox"/>	Enable the SNMPv2 server on this appliance
Backward compatibility with SNMPv1	<input checked="" type="checkbox"/>	
SNMPv2 Community Name	<input type="text" value="public"/>	
Enable SNMPv3	<input checked="" type="checkbox"/>	Enable the SNMPv3 server on this appliance
SNMPv3 Username	<input type="text"/>	Please enter SNMPv3 server username
SNMPv3 Password	<input type="password"/>	Please enter SNMPv3 server password
	<input type="checkbox"/> Show password	Password is required even if no authentication is used
SNMPv3 Authentication Method	<input type="text" value="No Authentication"/>	▼
System Location	<input type="text" value="ASP Location"/>	
System Contacts	<input type="text" value="ASP Contact <some@email>"/>	

Zeroconf – If enabled, the controller is discoverable on the network by tools such as Bonjour Browser. This is recommended to always be enabled.

Save settings when complete or click **Reset** to return to default settings.

4.4.5 Applications

Embedded applications can be installed to run on the controller in a containerized environment. See section 4.6 for more information.

Applications			
ID	Status	SSH	Remove
z9	Stopped	Stopped	

Upload – Upload application (*.app) file

Settings – The settings button will open a window allowing for setting a particular application to run in Exclusive Mode as well as inputting the developer certificate.

ID – The text string identifying the app. Clicking this ID will open a new window that shows some configuration options and app information. In this window, the user can start up the application, see version information, enable/disable SSH, and see what ports are mapped for the application to use.

Status – Shows whether the application is running or stopped.

SSH – Shows whether SSH is enabled or stopped.

Remove – Clicking the red trash can icon will uninstall the app from the controller.

4.4.6 Maintenance

Restart Application

Warm
Cold

Reboot System

Reboot

Download Log Files

Download

Logging Configuration

Logging level

DEBUG ▼

Save

Update Firmware

Choose File
No file chosen

Upload

Restart Application – Any restart will cause the controller to temporarily drop offline.

- **Warm** – This option will restart the Access Control application and other embedded applications on the controller while retaining the stored configuration, scripts, and user database.
- **Cold** – This option will restart all running applications and clear all data including configuration, scripts, and user database. To regain functionality, a complete configuration must be sent to the controller.

Reboot System - Completely restarts the controller as if power was cycled, while retaining the configuration. This will cause the controller to temporarily drop offline.

Download Log Files - Downloads the current logs as a text file.

Logging Configuration - Selects the level of detail for the logs. This is used by support personnel for diagnostics and troubleshooting.

Update Firmware - Allows uploading a different firmware version and uploading licenses. This should only

be performed at the direction of your solution provider. See section 4.5 for instructions on updating firmware through the web.

4.4.7 Profile

Username - Configures the username for the controller's web server. This value is always 'admin' and cannot be changed.

Change Password - Change the controller's web login password.

Change SSH Password – Change the password to connect to the controller via SSH.

4.5 Firmware & License Updates

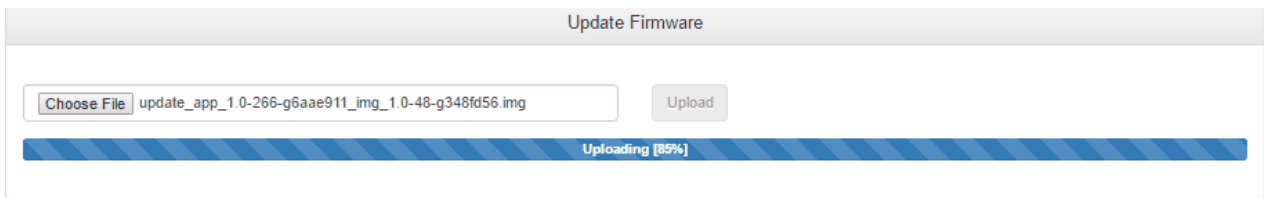
Firmware Updates

Firmware updates are provided electronically and can be loaded to a controller with no modifications to the hardware. The firmware file is uploaded to the controller using either the controller's web server or SDK/Host connection. Updates should be done as needed to make use of new features, improvements, and bug fixes.

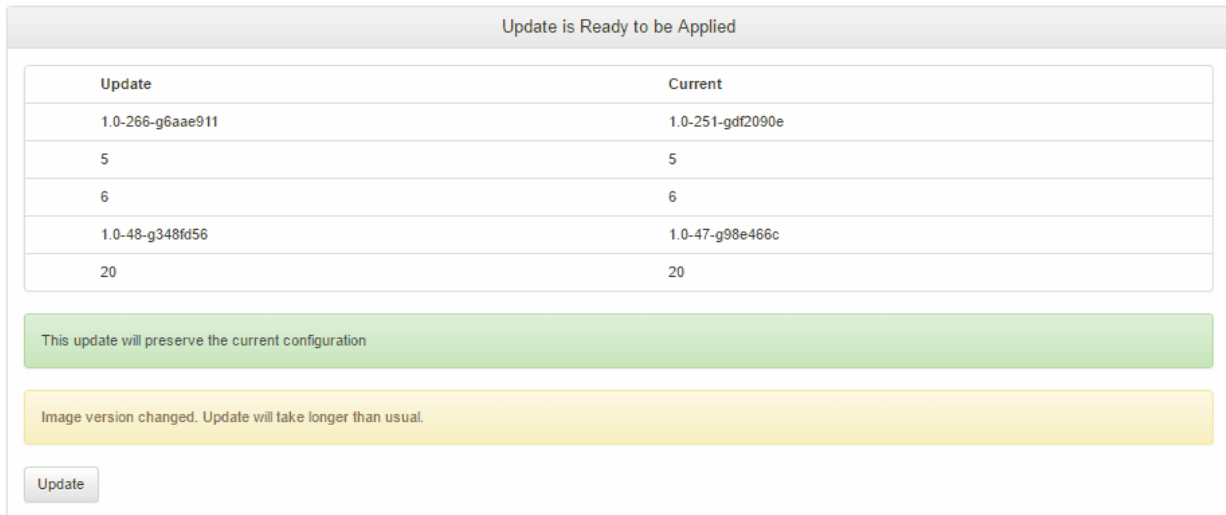
To update firmware through the controller's web server, follow this procedure:

1. Obtain the new firmware package from the Azure Access partner portal or your solution provider and save it to a PC that is visible to the controller on the network.
2. Using the PC's web browser, connect to the controller's web server and go to the "Maintenance" page (see section 4.4.5).
3. Under the "Update Firmware" section, click "Choose File" and locate the firmware file (file extension is ".img").

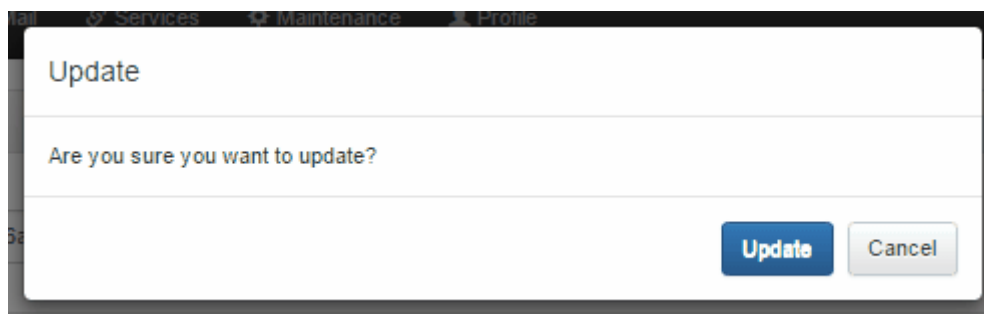
4. Click Upload and the upload of the file will begin. This will only upload the file but not apply it yet.



5. Once the image is uploaded, the information about the new firmware will be displayed.



6. Click Update to apply the update. A confirmation dialog will ask for confirmation.



7. The webpage will close. When update is finished, the LEDs will return to normal blinking patterns. This will take a couple minutes. The controller will retain its previous system and network configuration.

Note: In some cases, it may be necessary to close the browser and restart in order to access the webpage. If the webpage still cannot be accessed, it may be necessary to flush the DNS cache of the PC. See "Troubleshooting" Section for more information.

License Upgrades

See section 4.3 for details on Card Database Size and Reader Count licenses. To update a license, follow a similar procedure as updating firmware:

1. Obtain the new license file and save to PC that can access the controller on the network.
2. On the Maintenance page of the web server, under the Update Firmware section, click Choose File, then locate and select the license file (*.img).
3. Press Upload button.
4. Confirm when prompted

4.6 Embedded Applications

The controller supports running 3rd party embedded applications in a containerized environment on the board. Embedded applications can be user-developed with our available ADK (Application Development Kit), user-deployed, and user-maintained without involvement of Azure Access. Embedded applications can utilize the SDK for access control functionality as well as interact with the Linux system itself and other onboard services.

Apps can be installed and managed through the controller's web server (see section 4.4.5) or via the Host. There are two modes the embedded applications can run in; Exclusive and Non-Exclusive Mode...

Exclusive Mode – In exclusive mode, the board boots directly into the application and normal board services are hidden in the background. The application can still configure the native board services through the API. This is like Kiosk mode in the Windows OS. In exclusive mode, the application can display a custom web page when a user connects to the board's web server.

Non-Exclusive Mode – In non-exclusive mode, the application runs on the board in parallel while still exposing the controller's native web server interface and services.

Embedded applications support SSH connections for root access. Azure Access can generate a custom developer certificate for each customer to protect embedded apps from unauthorized root access.

Embedded applications can be deleted from the controller via the web server interface or the Host. When deleting the app, all app data is also deleted. Apps are also deleted when performing a Factory Reset. As of firmware 1.19, there is a "persistent storage" memory space that can retain app data through a Factory Reset.

4.7 Custom Logic

The controller has two features, Internal Variables and Scripting, that allow a user to modify the access control logic and operation of the board without requiring modifications to the core firmware. These features enable site-specific requirements to be met without involvement of Azure Access.

4.7.1 Internal Variables

Introduced in firmware version 1.16.16, Internal Variables are a user-friendly, SDK-configurable form of if-then type logic that can run on the board. This allows for certain types of API-recognized events to automatically trigger API-recognized actions. These event-triggered actions can be cascaded into complex functionality.

Internal Variables are configured by the Host and stored on the controller to be functional even when a Host connection is not active. Internal Variables can involve the controller itself as well as downstream panels connected to the controller. For a list of supported event-triggers and actions, consult with your Host solution provider.

4.7.2 Scripting

Scripting is a more advanced form of custom logic that can be loaded onto the controller. Scripting allows for modifying access control and other system functionality beyond the API-recognizable events and actions. For example, Scripting can be used to automatically send email notifications, communicate with 3rd party devices, and react to or manipulate the system environment. Scripting is also useful for creating access control logic for things like mantraps, interlocks, specialty escorts, etc.

Scripts are written in Pawn Script and then compiled and loaded onto the controller via the Host. Once a script has been developed, it can be used infinitely on any controller.

4.8 Elevator Control

The controller supports elevator control by configuring Access Points to be floors in a building. Outputs on the controller itself as well as on downstream boards can be used depending on the number of floors. Inputs can optionally be used for feedback.

4.9 Security

The controller and downstream panels support end-to-end security/encryption, from the reader to the Host, whether using network or serial connections. Encryption keys and certificates are generated with OpenSSL. Firmware is encrypted and signed for authenticity.

Network communications to the Host and web server are secured with TLSv1.3 and custom certificates are supported. Serial communications are AES encrypted with OSDP devices utilizing the OSDP Secure Channel standardization. As of firmware 1.17, custom OSDP keys can be used for OSDP Secure Channel. The controller also supports credential-level encryption mechanisms used by governments and other high-security industries; TWIC, CAC, and SSCPv2.

All of these encryption mechanisms give system-wide FIPS compliance.

PART V

Troubleshooting

5 Troubleshooting

5.1 Communications

PROBLEM – Main node device is not communicating with host software.

If the device is communicating with the software, LED1 will be lit solid if it is not lit, there is an incorrect configuration or the network is not working properly.

SOLUTION - Check communication settings

1. First check that the correct IP address or hostname has been specified in the software.
2. To verify the IP address, try to access the webpage of the device from the computer where the host software is installed.
3. Try using the ping command from the command prompt to verify that the device responds.
4. If device correctly pings but still does not communicate with software, check that the correct Mask is set in the configuration. If the host is on a different subnet but the mask of the device is set to 255.255.255.0, it may not respond. Try setting the mask to 255.255.0.0
5. If device will ping at IP address, but not at hostname, try to flush the dns cache:

TO FLUSH DNS CACHE (instructions may differ slightly due to Windows versions and may require administrator privilege)

1. Open a command prompt (Start > Run > cmd.exe > OK).
2. Type in the command `ipconfig /flushdns`

6. If device will ping at IP address, but not at hostname, check the DNS server of the network.
7. Try to restart the device
8. If the host list of the device is active, make sure the hostname of software host is listed in the host list.
9. If the device still cannot communicate, reset the network connection, reconfigure and try again

PROBLEM – Client node device is not communicating with Main Node.

SOLUTION - Check configuration settings

1. Check that the proper hostname or IP address is set in the Main Node Address configuration of the Client Node
2. Check that Main Node feature is disabled on the Client Node
3. Check that there is a proper network route between the Main Node and Client Node and that if they are not on the same subnet that the proper Network Mask and Gateway are configured.

5.2 Reader / Keypad

The reader function can be verified after communications are functioning properly. The host system must be configured for each of the readers on the controller to be used, and with the correct card format. The card format is determined by the actual cards that will be used. After configuring the card format at the host, placing a card in front of the reader should generate an access message on the host computer. If the message is "Access Denied" the reason for the message will indicate further steps to be performed. "Access Denied – Wrong Facility Code" will also display the actual facility code on the card. This information should

then be entered to the host computer system. "Access Denied – Not in File" will display the actual card number of the presented card. This card should then be added into the employee database of the host system." Access Denied – Access Level Error" indicates that the cards are entered into the system but the Access Level assigned to the card does not allow access to the particular door at this time.

On readers with integral keypads, the keypad may be verified by setting the reader into the Card and PIN mode. After presenting a valid card, the reader should flash the yellow LED (if installed reader supports 3 color LEDs). This indicates the reader is waiting for a Pin entry. Enter a valid PIN using the keypad and press the "ENTER" key. Access should be granted.

PROBLEM - Device is online, but readers are not responding.

SOLUTION - Check configuration settings

1. Check that the readers are configured. If readers are configured properly and are communicating, LED2 will blink rapidly indicating that the Reader Interface Layer is active in the case of onboard readers. For OSDP/serial readers, LED3 or LED4 should be blinking rapidly indicating activity on the Serial 2 or 3 connection.

SOLUTION - Check wiring.

1. For Wiegand readers, check that Data-1 and Data-0 lines are not reversed.
2. Check that the ground wire of the reader is properly connected. If the reader is being powered from a separate source, the ground should be connected in order to provide signal ground reference.

5.3 Input Zones

All alarm inputs should next be verified. Opening the Door Contact input should generate an immediate "Forced Open" alarm. Closing the Exit Push Button input should release the strike relay. The Exit Push Button input will not function if the reader interface is in tamper (Tamper Contact=Open) and also one minute after the tamper condition is secured. The reader may also be configured (via the host) to not activate the strike relay when the Exit Push Button is depressed. In all cases the reader should not report "Forced Open" immediately after pressing the Exit Push Button. The Aux Alarm inputs (if used) can be verified next. Some system will not allow use of the second Aux alarm. Opening the Aux alarm input should result in a message on the host system. Unused Aux alarm inputs should be terminated.

PROBLEM - Inputs do not respond.

SOLUTION - Check configuration settings

1. Check that the inputs are properly configured in the software. Each input of the controller can be reconfigured by software and is not necessarily using the default function.

5.4 Output relays

The internal strike relays should energize any time a valid card (or PIN) is presented and the message "Access Granted" appears on the host. The reader may be set to the "Unlocked" mode at the host to permanently energize the relay for test purposes. Any external, high-security, ADA-11 relay modules should also be verified.

PROBLEM - Outputs do not respond.

SOLUTION - Check configuration settings

1. Check that the outputs are properly configured in the software. Each output of the controller can be reconfigured by software and is not necessarily using the default function.

PROBLEM - One Pass command does not function

SOLUTION - Check reader inputs

1. Check that the door contact of the reader is secure (closed). If the controller detects that the door is already open, it will not energize the strike relay.

Part VI

Specifications

6 Specifications

Specifications are subject to change without notice

Primary Power (VIN)	<p>DC/DC: 12 to 24 VDC \pm 10%</p> <ul style="list-style-type: none"> 12VDC board operating current: 430mA max 12VDC “peak inrush”** current: 2A 12VDC full-load (powering VOUT & RVOs) current: 2.32A max 24VDC board operating current: 170mA max 24VDC “peak inrush”** current: 1.54A 24VDC full-load (powering VOUT & RVOs) current: 2.17A max <p>** “Peak inrush” current occurs immediately when applying power and then falls rapidly as the super capacitor starts to charge. Power supplies with “soft-start” feature are recommended, otherwise the power supply must be rated to handle the “peak inrush” current. Some power supplies without “soft-start” feature still worked when rated at least x2 operating max, still below “peak inrush” current rating.</p>
Reader Power (RVO)	VIN Passthrough; 500mA per port. Add to VIN current
RTC Coin Cell Battery (BAT1)	CR1225; 3V; 48mAh capacity recommended
USB	5VDC, 500mA maximum (add 270mA to Primary Power current)
Host Communication	Two independent Network Interfaces; 10BaseT/100Base-TX
Downstream Serial Com (x2)	RS-485; 4-wire (full-duplex) plus Signal Ground; 2-wire (half-duplex) compatible; 9,600 to 115,200 baud
Cabinet Tamper	1 unsupervised digital input for cabinet tamper
Alarm Inputs (x16)	Unsupervised or Supervised, configurable End-Of-Line resistor values. 1K/2K, 3K/4.5K, 300/10K are supported by default. Custom values available. Use 1 %, ¼ W resistors.
Output Relays (x8)	Dry, Form-C contacts; 2A @ 24VDC / 1A @ 120 VAC
Reader Ports (x4)	<p>Reader Power (VDC): See “Reader Power (RVO)” above</p> <p>TTL Data Inputs: Supports Wiegand, Clock & Data, and F/2F</p> <p>Buzzer Output: Open collector; 18VDC max; sink 50mA max</p> <p>LED Outputs (x3): Open collector; 18VDC max; sink 50mA max</p>

Cable Requirements	<p>DC Power: 18 AWG minimum; 1 twisted pair</p> <p>Ethernet: Cat 5 minimum</p> <p>RS-485: 24 AWG. 1 shielded twisted pair. 4000 ft. (1,219m) max @ 9600 baud; Belden 9841 or equivalent cable</p> <p>Reader Data (TTL): 4 to 8 wires; 500 ft. (152 m) max; 18 to 22 AWG depending on cable length; non-twisted pairs</p> <p>Inputs: 1 twisted pair; 22 AWG minimum; 1000 feet (304.8 m); 30 Ω max loop resistance</p> <p>Relay Outputs: 16 to 18 AWG. Use sufficient gauge to avoid voltage loss</p>
Environmental	<p>Temperature: -40 to 85°C operating and storage; Indoors</p> <p>Humidity: 5 to 95% RHNC.</p>
Mechanical	<p>Dim: 8.2 in. (208.28 mm) W x 6.3 in. (160 mm) L x 1.06 in. (26.93 mm) H</p> <p>Weight: 0.53 lbs. (240.4g)</p>

Part VII

Revision History

7 Revision History

REVISION HISTORY

Rev	Date	Description of changes	Editor
X.2	4/3/2020	Initial draft	Sean C
A	4/27/2020	Initial Release	Sean C
A.1	7/21/2020	New table of content, overall layout edits, added table of figures	Sean C
A2	11/10/2020	Organize sections/table of contents, content mods, update specs	Evan Z
A3	11/12/2020	Update Layout and content	Sean C
A4	11/17/2020	Update content	Evan Z
A5	11/20/2020	Update content and new Input supervision diagrams	Sean C
B	8/24/2021	Major Update: New Cluster Labeling	Sean C
B1	9/21/2021	Major Update to reflect new PCB design	Evan Z
B2	10/14/2021	New OSDP Wiring & Door Wiring Diagram	Sean C
B3	11/5/2021	Linked table of content & multiple updates	Sean C
B4	3/28/2022	Formatting and updated images	Evan Z
B5	5/18/2022	Update images and formatting fixes. Fix Terminal Block Connection table	Evan Z
E1	8/4/2023	<ul style="list-style-type: none"> • Add firmware version 1.16.16, 1.17.0, and 1.19.0 information • Updated RS485 Bus Diagram Images • Updated section 4.1 • Move "Clustering" to section 4.2 and improve information • Add section 4.3 "Licensing" • Update section 4.4 "Web Server Configuration" • Add section 4.5 "Firmware & License Updates" • Add section 4.6 "Embedded Applications" • Add section 4.7 "Custom Logic" • Add section 4.8 "Elevators" (remove section 3.7.4) • Add section 4.9 "Security" • Update specifications table 	Evan Z
E2	8/17/2023	Update factory reset description	Sean C
E3	1/26/2024	Update for firmware 1.20 <ul style="list-style-type: none"> • Update FACTORY RESET pushbutton behavior • Update section 4.4 Web Server Configuration <ul style="list-style-type: none"> ▪ First log in requires web server password change ▪ Network Page – Firewall settings ▪ Mail Page – server verification ▪ Services Page – SNMP 	Evan Z