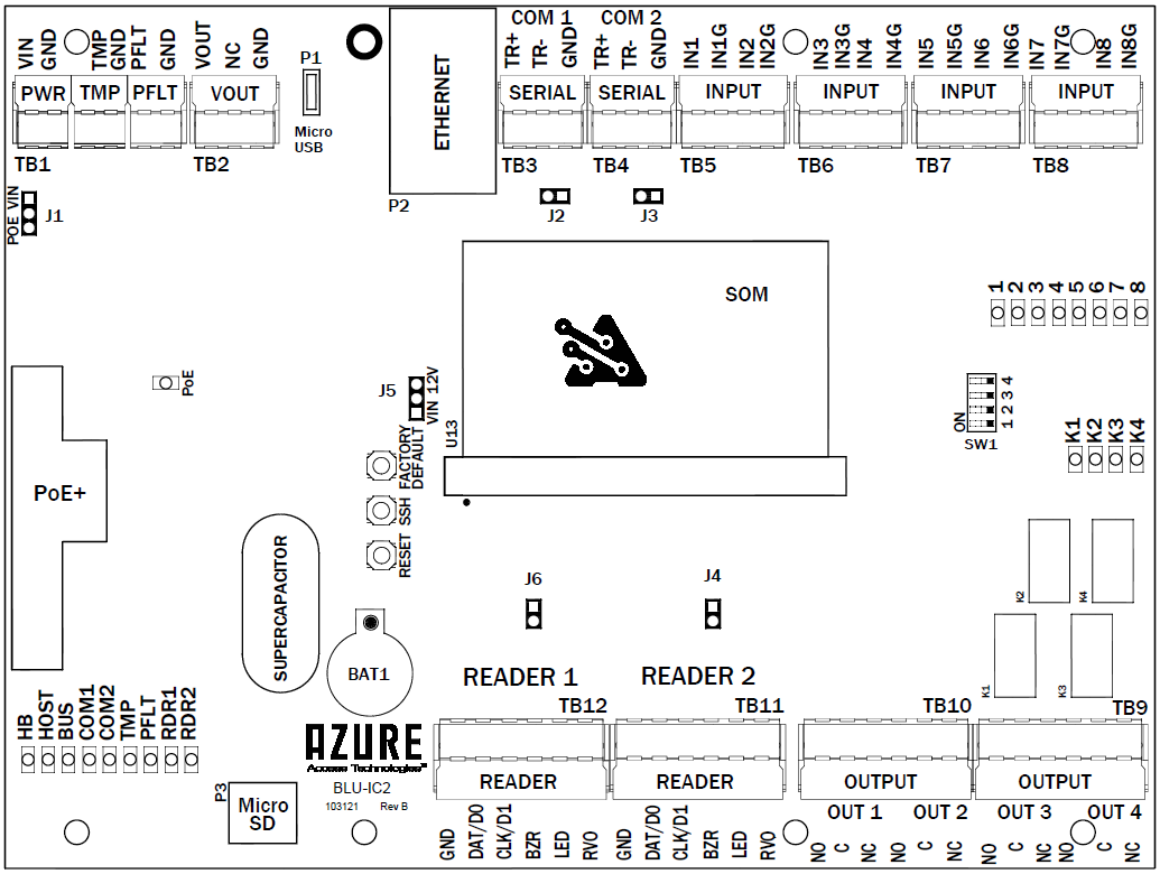
NOP-IC2 Hardware Manual

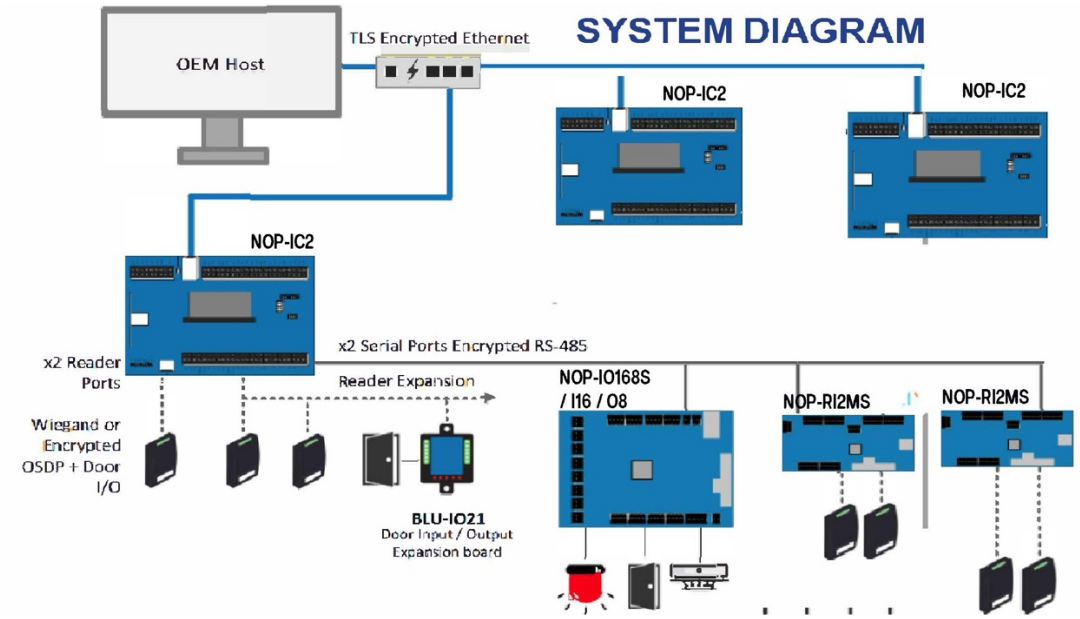
Revision C3
January *, 2026

NOP-IC2 Hardware Manual

2-Door Intelligent Network Controller

by Azure Access Technology





IMPORTANT INFORMATION

W A R N I N G
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.

C A U T I O N
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 Compliant
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

UL & ULC Recognized
- UL 294
- UL 294B
- UL 1076 & ULC/ORD 1076
- UL 2610

OSDP Verified – Secure Profile (as of firmware ver 1.21.0)

Table of Contents

Part I
Introduction

1 Introduction

This is high-level installation and basic usage manual for the NOP-IC2 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 NOP-IC2 provides onboard connectivity for two Access Points. The NOP-IC2 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 NOP-IC2 reader ports support both TTL (Wiegand / Clock & Data) or RS485 (OSDP) readers. A downloadable card database and event buffering allows the NOP-IC2 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

- 2 onboard reader ports for up to 2 TTL readers or up to 16 RS485 (OSDP) readers (with expanded licenses)
- 8 Supervised Alarm Inputs
  - Configurable EOL termination-resistor values
- 4 Relay Outputs
- 1 Unsupervised Cabinet Tamper Input
- 1 Unsupervised Power Fault Input
- Two, 2-wire RS-485 serial ports for communication to downstream reader-interface and/or IO panels
  - Supports proprietary or OSDPv2 protocol
- One 10/100 Ethernet connection
  - Second Ethernet connection possible with USB-to-Ethernet adapter
- Full, Stand-Alone 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
- 1 LED Output per reader port (tri-state control)
- 1 Buzzer Output (open collector) per reader port
  - Buzzer output can be repurposed for 2-wire LED control
- Customizable logic and event scripting
- Clustering
- 3rd party embedded applications
- Backup power to retain data and real time clock through power outages

1.2 Configuration

The NOP-IC2 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, her 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.
- 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 NOP-IO168S panels. Using the NOP-IO168S has the added benefit of providing feedback to the inputs on the IO panel.

Part II
Hardware Layout

2 Hardware Layout

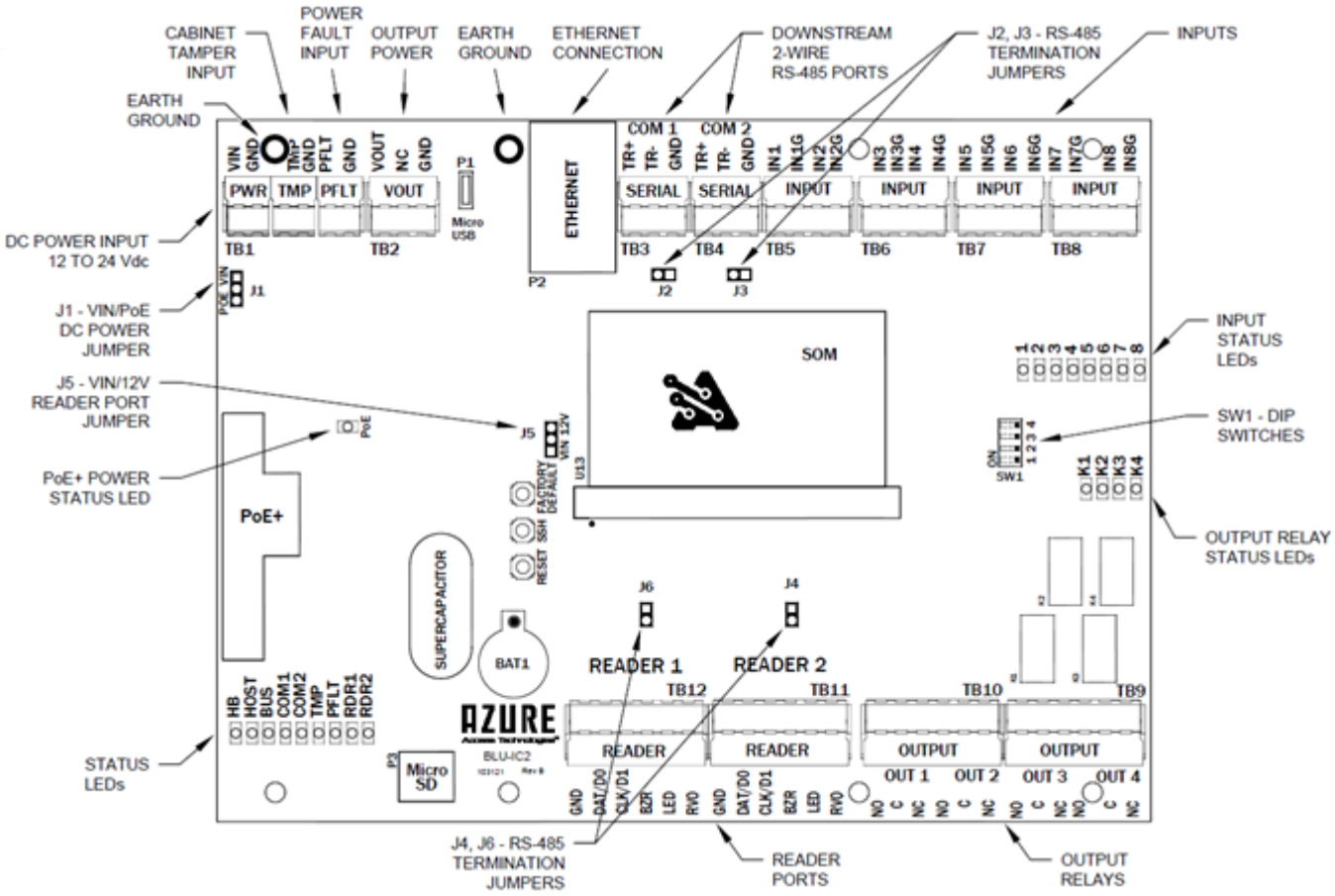


Figure 2.1: Board Diagram

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”.

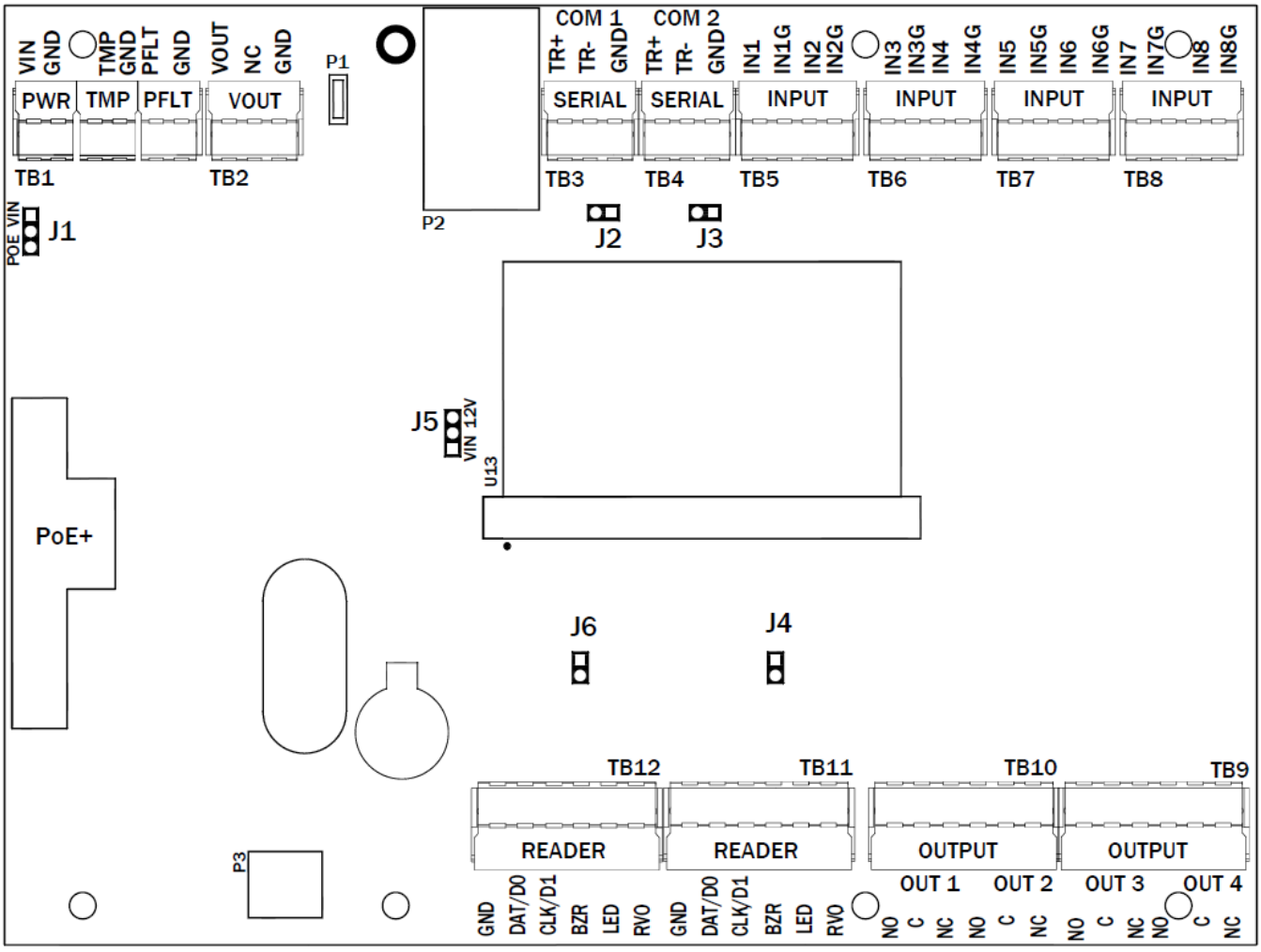
The SDK allows for custom-mapping of hardware interfaces. Any reader, input, or output can be assigned to any Access Point. Recommended wiring configurations are listed in parenthesis in the function column.

Terminal Block Wiring Connections			
Location	**Type**	**Label**	**Function (Recommended Connection)**
Power, Tamper, & Power Fault			
TB1-6	Power Input	VIN	Main Power 12 - 24 Vdc
TB1-5	Ground	GND	
TB1-4	Tamper Input	TMP	Cabinet Tamper Input
TB1-3	Tamper Input Return	GND	
TB1-2	Power Fault	PFLT	Power Supply Fault
TB1-1	Power Fault Return	GND	
TB2-3	AUX Power	VOUT	Vin or 12 Vdc if PoE+ is used
TB2-2	No Connection	-	
TB2-1	Ground	GND	
Serial Ports			
TB3-1	Signal Ground	SG	2-Wire RS-485 COM Port 1
TB3-2	Transmit/Receive Data (-)	TR-	
TB3-3	Transmit/Receive Data (+)	TR+	
TB4-1	Signal Ground	SG	2-Wire RS-485 COM Port 2
TB4-2	Transmit/Receive Data (-)	TR-	
TB4-3	Transmit/Receive Data (+)	TR+	
Reader Ports			
TB12-1	Reader Power Ground	GND	Reader 1 (Door 1 Reader) Host can configure to connect to Wiegand / Clock & Data or OSDP Readers
TB12-2	TTL: Data/Data 0 RS485: TR-/B	DAT/D0	
TB12-3	TTL: Clock/Data 1 RS485: TR+/A	CLK/D1	
TB12-4	Beeper (Buzzer) Control	BZR	
TB12-5	Green LED Control	LED	
TB12-6	VDC (Reader Power)	RVO	
TB11-1	Reader Power Ground	GND	Reader 2 (Door 2 Reader) Host can configure to connect to Wiegand / Clock & Data or OSDP Readers
TB11-2	TTL: Data/Data 0 RS485: TR-/B	DAT/D0	
TB11-3	TTL: Clock/Data 1 RS485: TR+/A	CLK/D1	
TB11-4	Beeper (Buzzer) Control	BZR	
TB11-5	LED Control	LED	
TB12-1	Reader Power	RVO	

Supervised Inputs			
TB5-4	Input 1	IN1	Input 1
TB5-3	Input 1 Return	IN1G	
TB5-2	Input 2	IN2	Input 2
TB5-1	Input 2 Return	IN2G	
TB6-4	Input 3	IN3	Input 3
TB6-3	Input 3 Return	IN3G	
TB6-2	Input 4	IN4	Input 4
TB6-1	Input 4 Return	IN4G	
TB7-4	Input 5	IN5	Input 5
TB7-3	Input 5 Return	IN5G	
TB7-2	Input 6	IN6	Input 6
TB7-1	Input 6 Return	IN6G	
TB8-4	Input 7	IN7	Input 7
TB8-3	Input 7 Return	IN7G	
TB8-2	Input 8	IN8	Input 8
TB8-1	Input 8 Return	IN8G	
Relay Outputs			
TB10-1	Normally Open	NO	Relay OUT 1
TB10-2	Common	C	
TB10-3	Normally Closed	NC	
TB10-4	Normally Open	NO	Relay OUT 2
TB10-5	Common	C	
TB10-6	Normally Closed	NC	
TB9-1	Normally Open	NO	Relay OUT 3
TB9-2	Common	C	
TB9-3	Normally Closed	NC	
TB9-4	Normally Open	NO	Relay OUT 4
TB9-5	Common	C	
TB9-6	Normally Closed	NC	

Figure 2.2: Terminal Connections

2.2 Jumpers



JUMPER	SETTING	DESCRIPTION
J1 Labeled "PoE VIN"	PoE VIN 	12-24V DC/DC Power supply. **DEFAULT**
	PoE VIN 	PoE+ (Power over Ethernet) Power Source *Not Applicable with NOP-IC2
J2	ON/OFF	RS485 termination - Serial Port 1 (COM1)
J3	ON/OFF	RS485 termination - Serial Port 2 (COM2)
J4	ON/OFF	RS485 termination - Reader Port 2 (RDR2)
J5 Labeled "VIN 12V"	 VIN 12V	12V regulated power for Reader Ports (RVO); Only use this setting when VIN >= 20VDC
	 VIN 12V	VIN passthrough power for Reader Ports (RVO); Use VIN passthrough if using PoE power source
J6	ON/OFF	RS485 termination - Reader Port 1 (RDR1)

Figure 2.3 User-installed jumper settings

Note: RS485 termination jumpers (J2, J3, J4, & J6) 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.

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 Micro USB

The USB port (P1) can be used as a secondary network interface with a USB-to-Ethernet adapter. This network is limited to only operate in DHCP mode.

2.5 MicroSD Card

The micro-SD card socket (P3) is reserved for future use and should not be used.

2.6 LEDs

There are 24 LEDs for monitoring panel functions and diagnosing issues.

Status LEDs	
HB	Heartbeat Offline – 200ms ON, 800ms OFF Online – 800ms ON, 200ms OFF
HOST	RS-485 Serial Port – Flashes when data is received
BUS	Internal Bus Activity – Flashes repeatedly while data is being exchanged
COM1	RS-485 Serial Port 1 & 2 Activity – Flashes when data is transmitted
COM2	
TMP	Cabinet Tamper & Power Supply Fault ON = Alarm OFF = Secure
PFLT	
RDR1	Reader Port 1 & 2 OSDP Reader – Flashes when communicating with reader Wiegand Reader – Flashes when receiving card data
RDR2	
Alarm Zone Inputs LEDs	
1 – 8	Supervised Input 1-8 Statuses ON = Alarm OFF = Secure Flash = Fault • Every 4 seconds the LED is pulsed to its opposite state for 0.1 seconds

Output Relays	
K1 – K4	Relay OUT 1-4 (K1 through K4) ON = Energized OFF = De-Energized
Ethernet (P2)	
Speed (left side)	ON = 100Mbps network connection
Link (right side)	Flashing = Network activity present
PoE Power	
PoE PWR	ON = PoE power active (Power over Ethernet) **Not Applicable for NOP-IC2**

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 all of the status LEDs (HB, HOST, BUS, COM1, COM2, TMP, PFLT) 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 for 5 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).

Exit Embedded App Exclusive Mode – Restore access to default web server so application can be deleted.

1. Hold FAC_RST button for at least 5 seconds.
2. While still holding FAC_RST, press SSH button and then release both buttons at the same time.

2.8 Dip Switches

The controller has 4 DIP switches that are reserved for future use.

2.9 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.

2.10 Mounting

Eight holes are provided for mounting. Mount at least 0.25 inches above the conductive surfaces. Two mounting holes are plated for connecting to Chassis (Earth) ground.

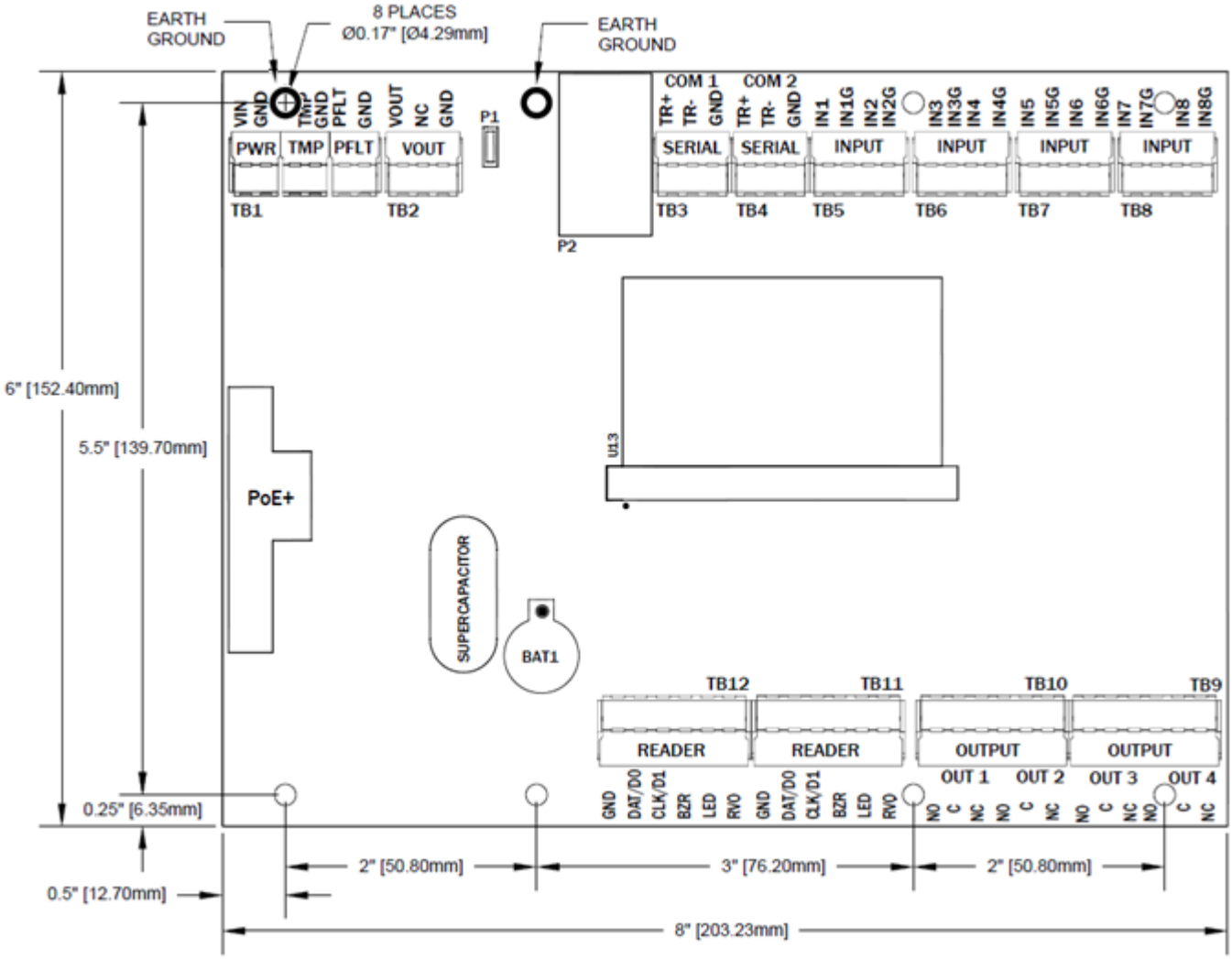


Figure 2.5: Mounting Holes [inches (mm)]

Part III
System Wiring & Setup

3 System Wiring & Setup

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

When operating on 12VDC, the controller has a peak current consumption of 700mA when charging a depleted super capacitor and a normal operating max of 320mA. 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 on 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 line interchange, presents 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 panel 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

The controller has multiple output ports for distributing power to peripheral devices. Each port has its own voltage and current specs and have over-current protection.

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

Auxiliary Output Power "VOUT" (TB2)

The VOUT port can be used to power peripheral devices such as strikes, IO modules, readers, etc. This port is a direct passthrough from the primary power VIN (same voltage as VIN), as power supply. This port has a 1 Amp current maximum.

Reader Port Power "RVO" (TB11 – pin 6) & (TB12 – pin 6)

Readers can be powered directly from the two reader ports. The RVO voltage is jumper selectable to be either passthrough from VIN or a regulated 12VDC. The regulated 12VDC setting is only to be used when VIN > 20VDC. Each port has a maximum of 500mA and the combined current maximum between both reader ports is 600mA.

USB (P1)

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

Connector: Dedicated Ethernet (P2) & USB (P1)

The controller communicates with the Host, other clustered ICs, and downstream boards over the network via a dedicated 10/100 Ethernet port (P2) or USB-to-Ethernet adapter (P1). Connection to network switch should be made using standard CAT5e or CAT6 cable. Network connections are TLS 1.3 encrypted with support for TLS 1.3 connections to downstream boards supported as of controller firmware 1.21 and downstream board firmware 1.26

3.3.2 Downstream RS-485 Serial Ports

Connectors: TB3 & TB4

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). The controller can be configured to communicate with downstream IO or Reader Interface panels on two available RS-485 ports (COM1 & COM2). The controller supports a 2-wire bus setup. Both ports can be configured to communicate using different protocols.

Note: COM1 & Reader Port 1 share an internal serial bus and COM2 & Reader Port 2 share another internal serial bus. Therefore, COM 1 & OSDP readers on Reader Port 1 must use the same baud rate and protocol and have unique addressing between them. COM 2 & OSDP readers on Reader Port 2 must also share the same baud rate and protocol and have unique addressing between them.

Device Wiring

2-wire RS-485 consists of three wires; TR+, TR-, & SG (signal ground). Both TX and RX are done on the same pair of wires. 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.

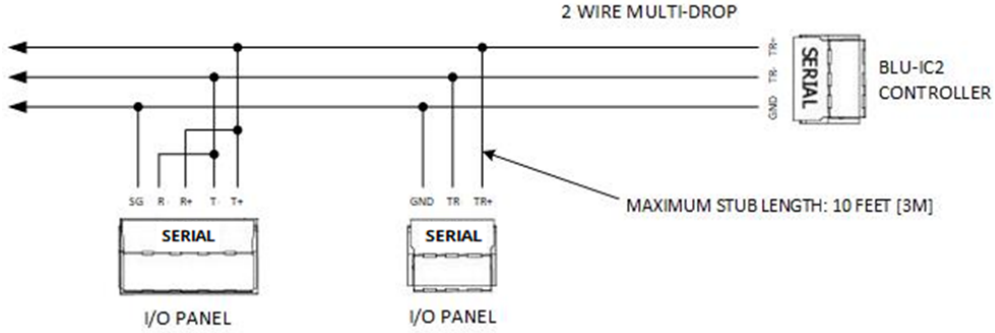


Figure 3.1: Device Wiring

Bus Configuration

There are 32 available addresses on each serial port's RS-485 bus. To maintain performance, up to 8 reader interfaces and/or I/O boards should be connected to each serial port, for a total of 16 devices between the two serial ports. When using IO21's paired with OSDP readers, up to 16 devices (combinations of OSDP readers and IO21's) can be connected to each port, for a total of 32 OSDP reader and IO21 devices. 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 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)

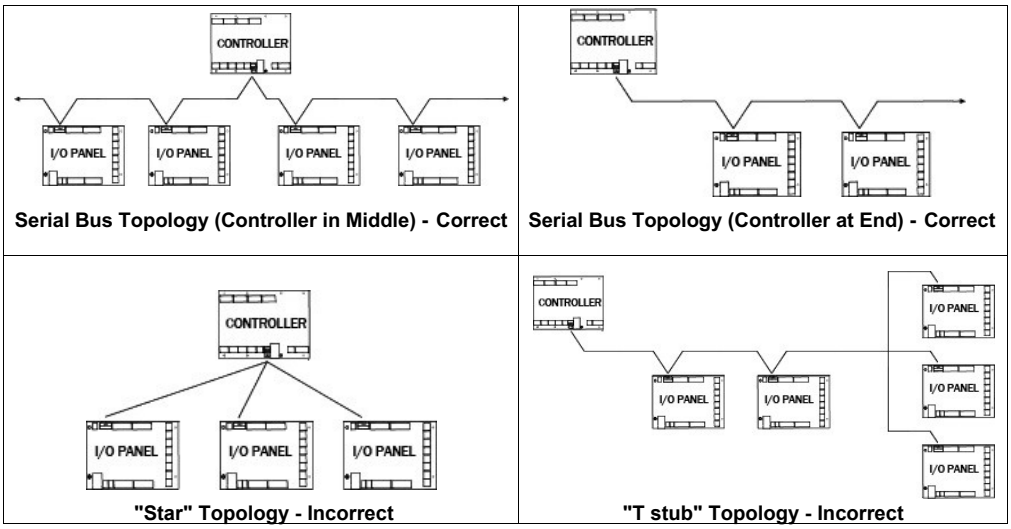


Figure 3.2: RS-485 Bus Topologies

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.

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:
ATM-48 Pin 1 -> TR+
ATM-48 Pin 2 -> TR-

Signal Ground (SG)

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.

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.

3.4 Unsupervised Cabinet Tamper & Power Fault

Connector: TB1

The cabinet tamper (TMP) and power fault (PFLT) inputs only support unsupervised configurations. The cabinet tamper input is wired to the enclosure and detects when the enclosure door is opened and closed. The power fault input is wired to the power supply and detects when there is an issue with the power supply. Wire these inputs with 24 AWG minimum. See “Unsupervised” in Section 3.6.1 wiring diagram.

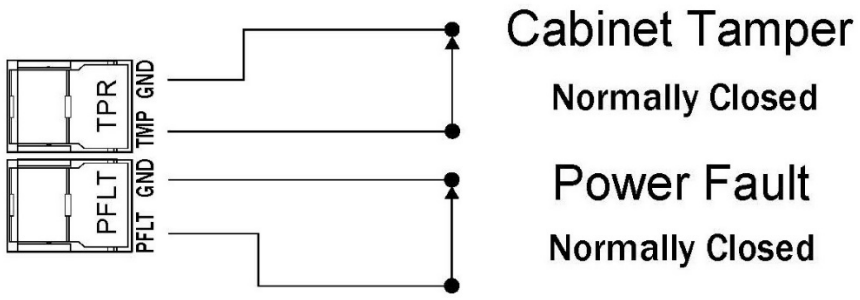


Figure 3.3: Cabinet Tamper & Power Fault Wiring

3.5 Reader Ports

Connector: TB11 & TB12

The controller has two onboard reader ports that support both TTL (Wiegand, Clock & Data, etc) and RS-485 (OSDP) readers. The RS-485 reader bus is a true RS-485 port meeting TIA-485-A.

Power for each reader port is provided through the “RVO” pins and is selected with a user-installed jumper. Power supplied on RVO is either a passthrough of VIN (12-24VDC) or a regulated 12VDC. The reader ports have over-current protection in the form of auto-resetting fuses and can supply up to 500mA per port. When using the 12V regulator for RVO, the total COMBINED maximum current limit is 600mA. 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.

PIN	DESCRIPTION
GND	Ground connection for the reader
DAT / D0 / TR-	TTL or RS-485 reader data connections (see 3.4.1 and 3.4.2 below)
CLK / D1 / TR+	TTL or RS-485 reader data connections (see 3.4.1 and 3.4.2 below)
BZR	Open-collector buzzer output. Can also be used for 2-wire LED control
LED	Tri-state LED signal
RVO	Reader power; jumper selectable to either be VIN passthrough or a regulated 12VDC

3.5.1 TTL Readers

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.

TTL readers usually utilize all pins on the reader port. The wiring to a TTL reader should be made using 24 AWG minimum, shielded cable with up to 6 conductors. Do not exceed 500 feet (152 m) between the controller 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. Connect the shield drain wire of the cable at the GND terminal of the appropriate reader connector on the controller. Carefully insulate the drain wire with sleeving for a reliable installation.

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.

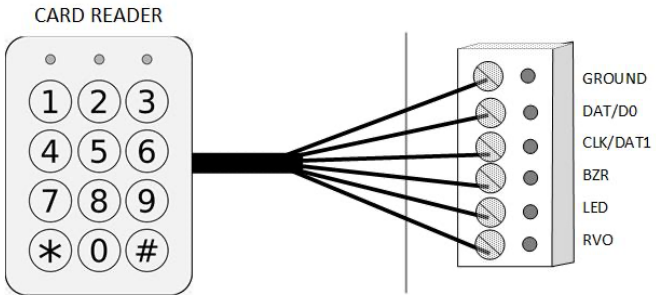


Figure 3.4: TTL (Wiegand / Clock & Data) Reader Wiring

3.5.2 RS-485 (OSDP) Readers

Both reader ports on the controller can communicate with RS-485 readers; OSDP being the most popular. The Reader Port is a true RS-485 port; meeting all the electrical standard requirements and capable of cable lengths of up to 4,000ft (1,219m).

In this section, “OSDP reader” will be used to represent what is really any RS-485 reader. The OSDP protocol standard expands the functionality of readers by enabling a large (and growing) command set.

RS485 readers (OSDP) use a 2-wire interface (transmit and receive on same wires). Always observe polarity of the lines; connecting positive (TR+) to D1 and negative (TR-) to D0. When powering the reader from an external power supply, it is still required to connect the reader’s Ground or Signal Ground to the GND connection on the reader port for reliable communications. “Star” wiring or “T stubs” longer than 10ft must never be used!

If necessary, OSDP readers can be connected to the Serial Ports instead of the Reader Ports. Extra reader licenses can allow for up to 16 OSDP readers (8 readers per port).

Note: Internally, COM1 & Reader Port 1 share a serial bus and COM2 & Reader Port 2 share an internal serial bus. Therefore, COM 1 & Reader Port 1 must use the same baud rate and protocol and COM 2 & Reader Port 2 must share the same baud rate and protocol. There must also not be any addressing conflicts on the shared buses.

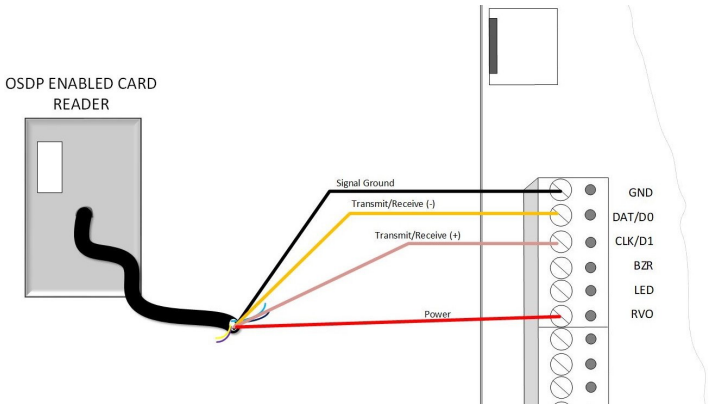


Figure 3.5: OSDP Reader Wiring

3.6 Supervised Alarm Inputs

Connector: TB3 – TB8

The controller has 8 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.

3.6.1 End of Line (EOL) Termination Resistors

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...

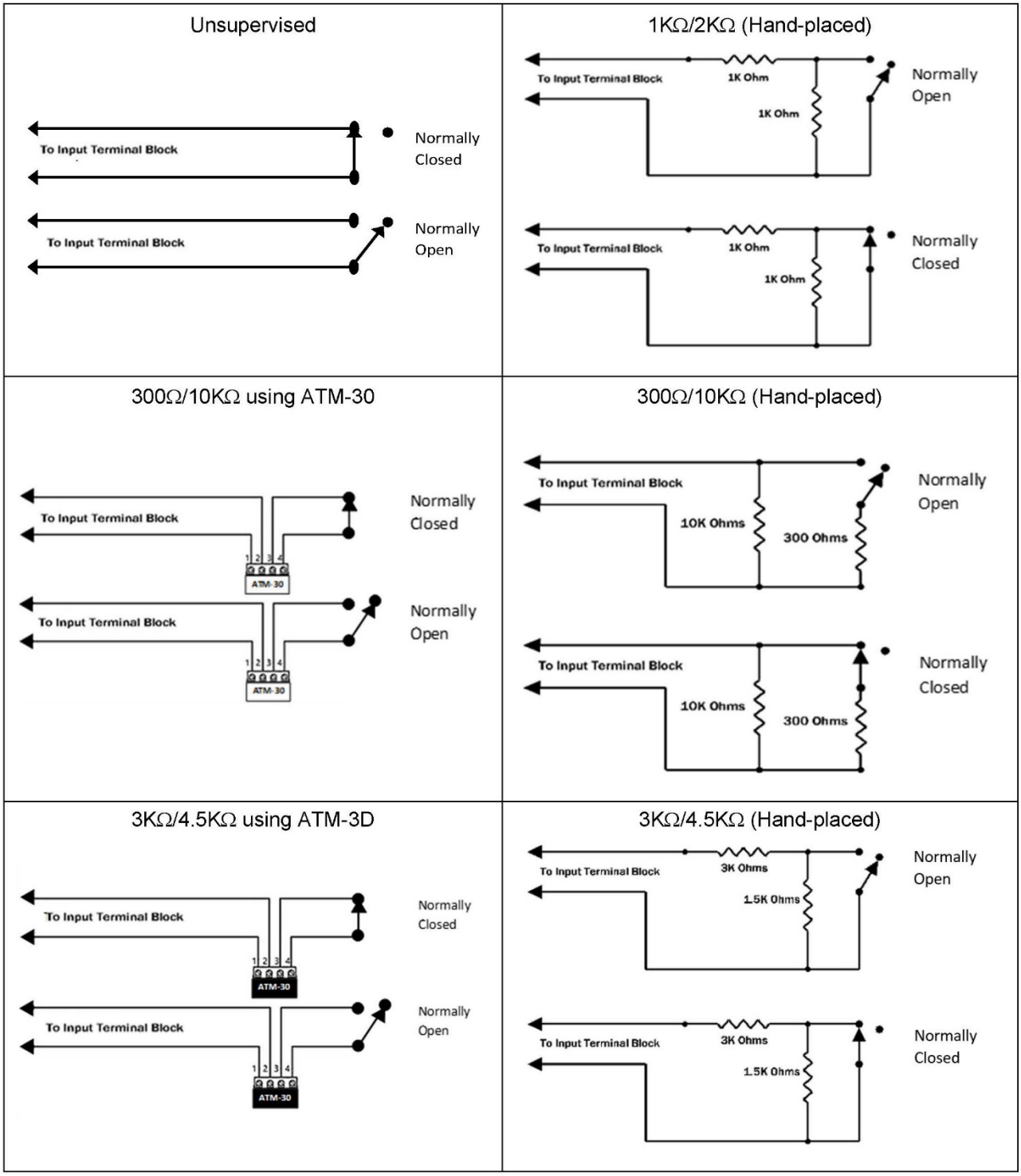


Figure 3.6: Input Supervision

3.7 Output Relays

Connector: TB9 & TB10

The controller has four 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 @ 30VDC or 0.5A @ 120VAC.

3.7.1 Door 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.

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.

3.7.2 Auxiliary Output Relay

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.

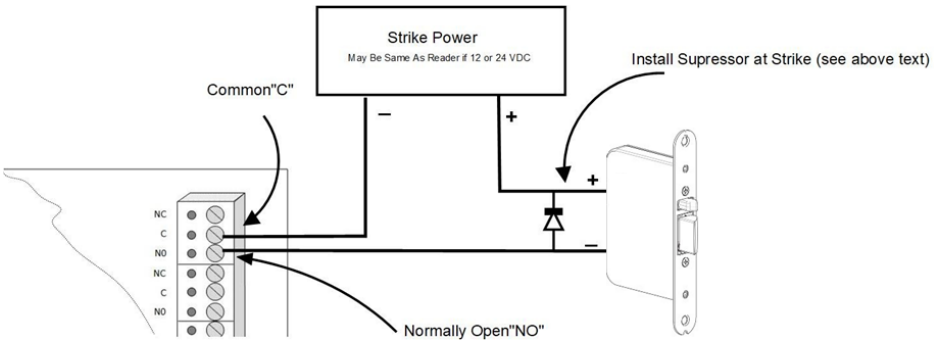


Figure 3.7: Strike Wiring Diagram (DC w/ Diode)

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

3.8 Door / Access Point Setup

An Access Point (sometimes referred to simply as "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 supports 2 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 Terminal Connections table in section 2.

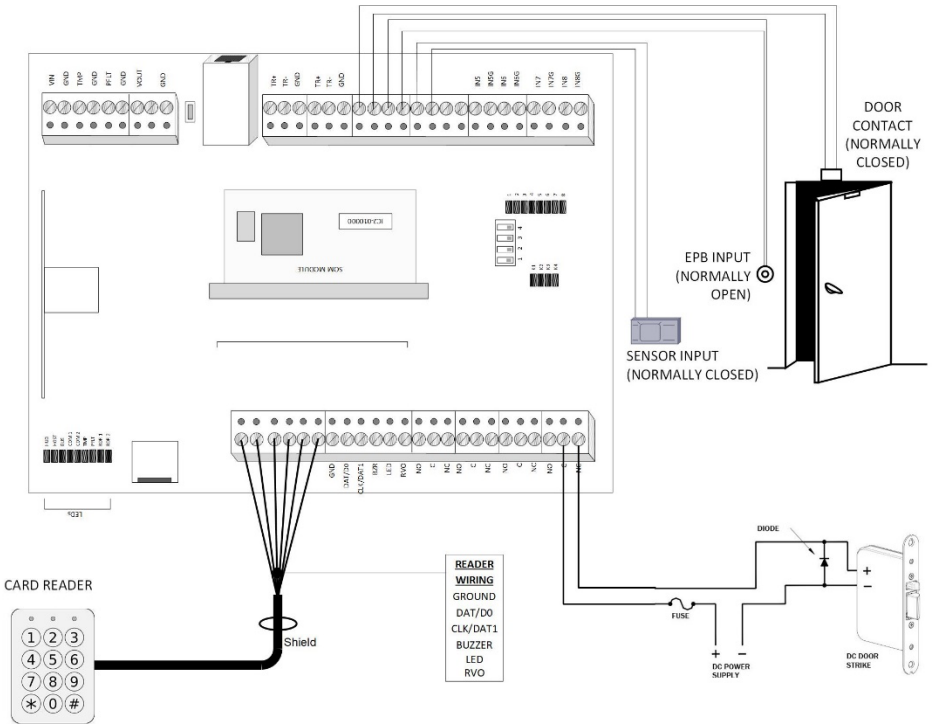


Figure 3.8: Door / Access Point Wiring

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 Door Forced / Held Open, and more precise strike timing.

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.

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 DHCP using IPv4. Network settings can be changed through the controller's web server (see section 4.4)

The DCHP resolves an IP address to the Hostname printed on the SOM sticker. When the network interface 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 for 60 seconds, the controller will switch to using a default static IP address of **192.168.0.2**

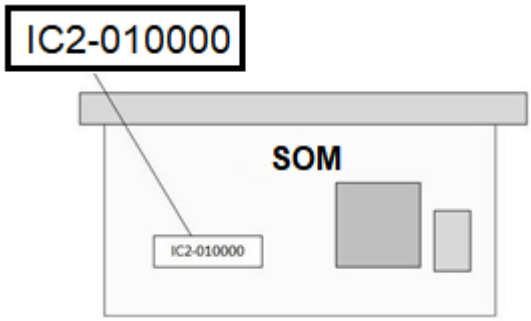


Figure 4.1: Hostname

4.2 Licensing

Figure 4.2: 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.

4.2.1 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.

4.2.2 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 NOP-IC2 comes pre-loaded with two reader licenses. As of firmware version 1.17, readers that are used as alternate, paired readers on the first two 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.

4.3 Web Server Configuration

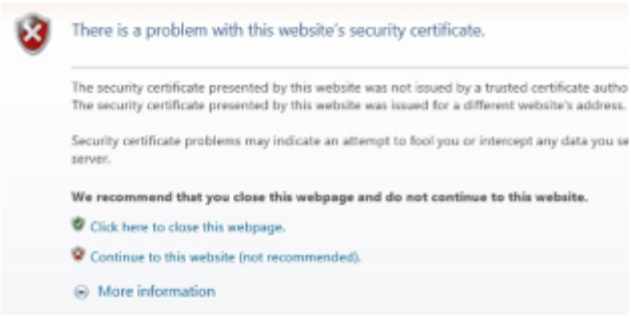
The onboard web server allows for network and certain configuration options to be applied through a web browser. To access the web server, enter the Hostname or IP address of the controller into a web browser in one of the following formats:

https://IC2-0100001 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).

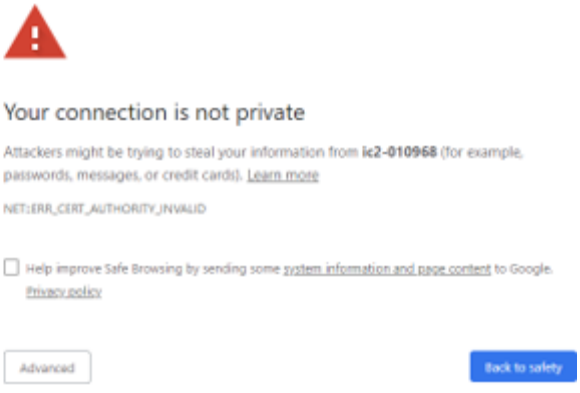
To bypass the secure-connection error, perform the follow steps depending on the web browser…

Internet Explorer:



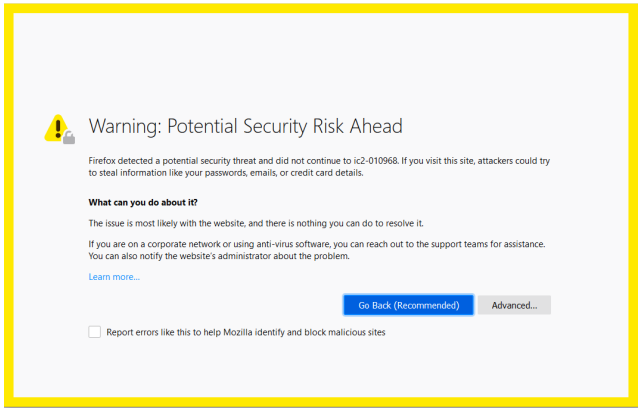
1. Click con*tinue to this website (not recommended)*

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 IMMEDIETLY BE CHANGED

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

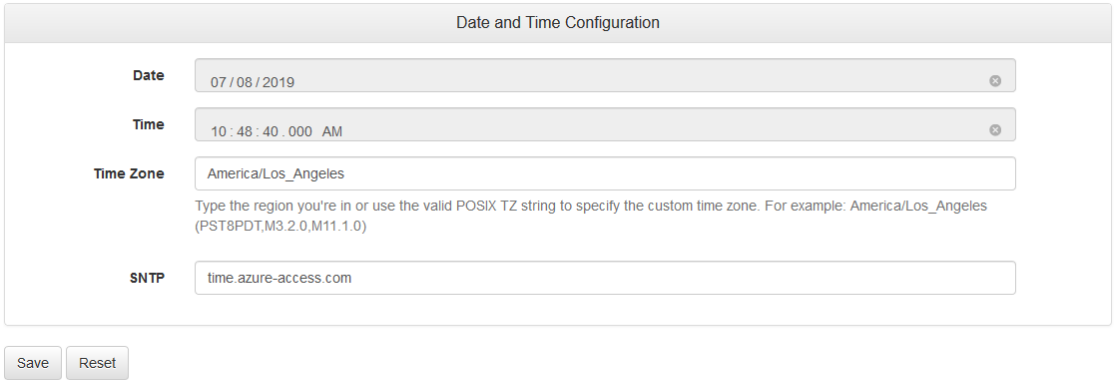
- Minimum length of 6 characters
- Contain at least one of each of the following: uppercase, lowercase, number, symbol

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…

4.3.1 Date & Time



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

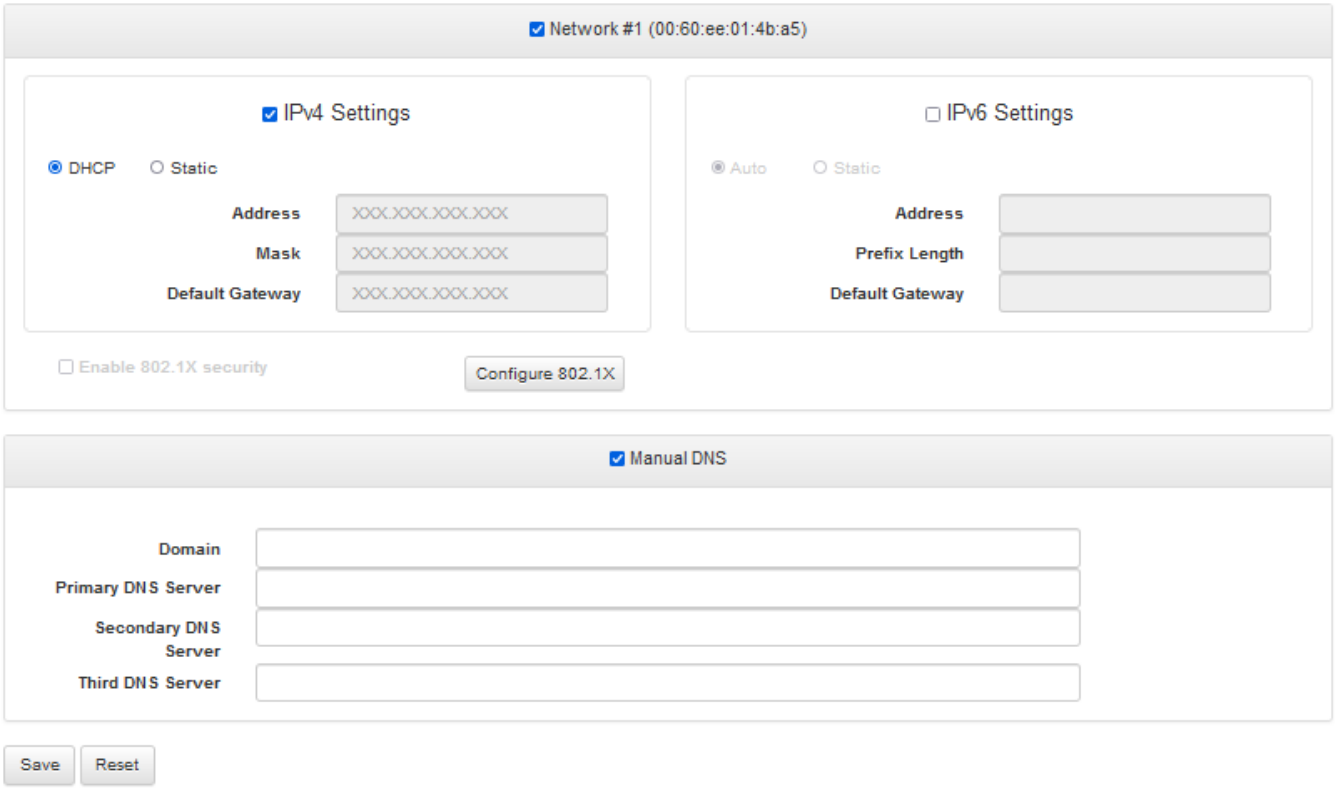
Time – The current time setting used by the device. This value cannot be modified

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.

4.3.2 Network



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.

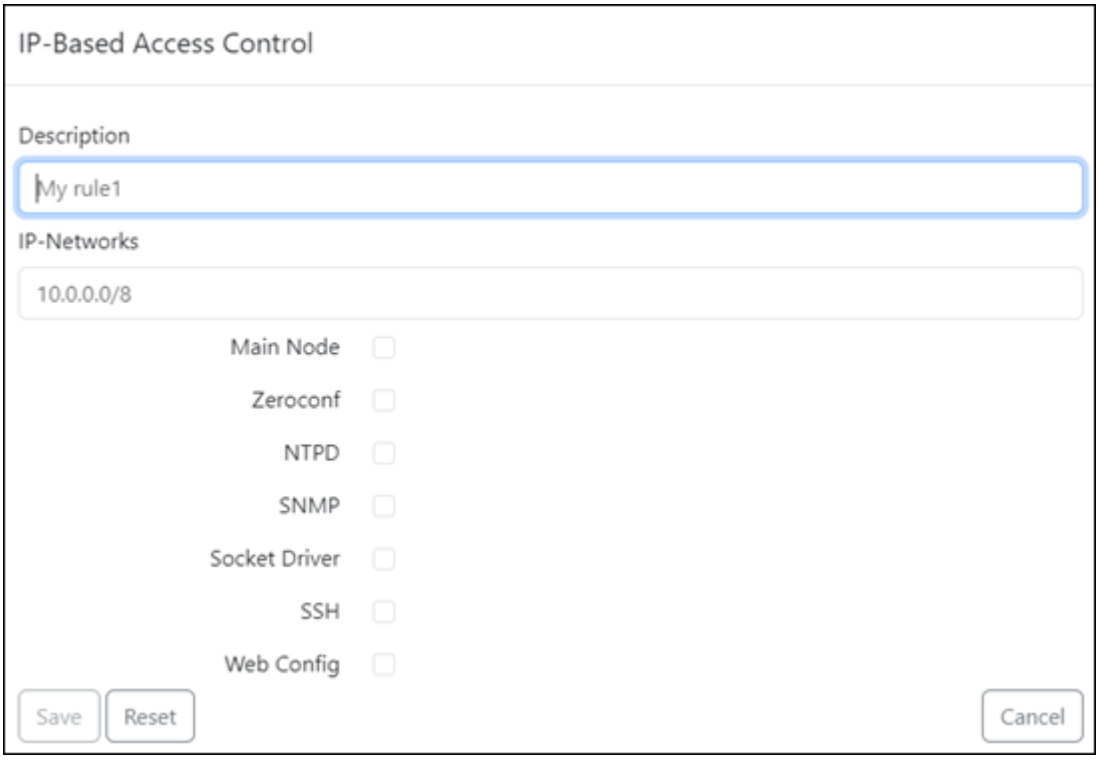
> **DHCP** – The DHCP server will assign the controller an IPv4 address. This requires a DNS server operating on the network. Dedicated routers or server-type operating systems can provide DNS services on the network. If a DNS server is unavailable after 60 seconds, the board will use the default static IP address 192.168.0.2
>
> With DHCP, the controller can be reached on the network with the Hostname. The default Hostname is printed on a sticker on the SOM module.
>
> **Static** – The user must enter a unique IPv4 address for the controller to use along with subnet mask, gateway, etc.

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.

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

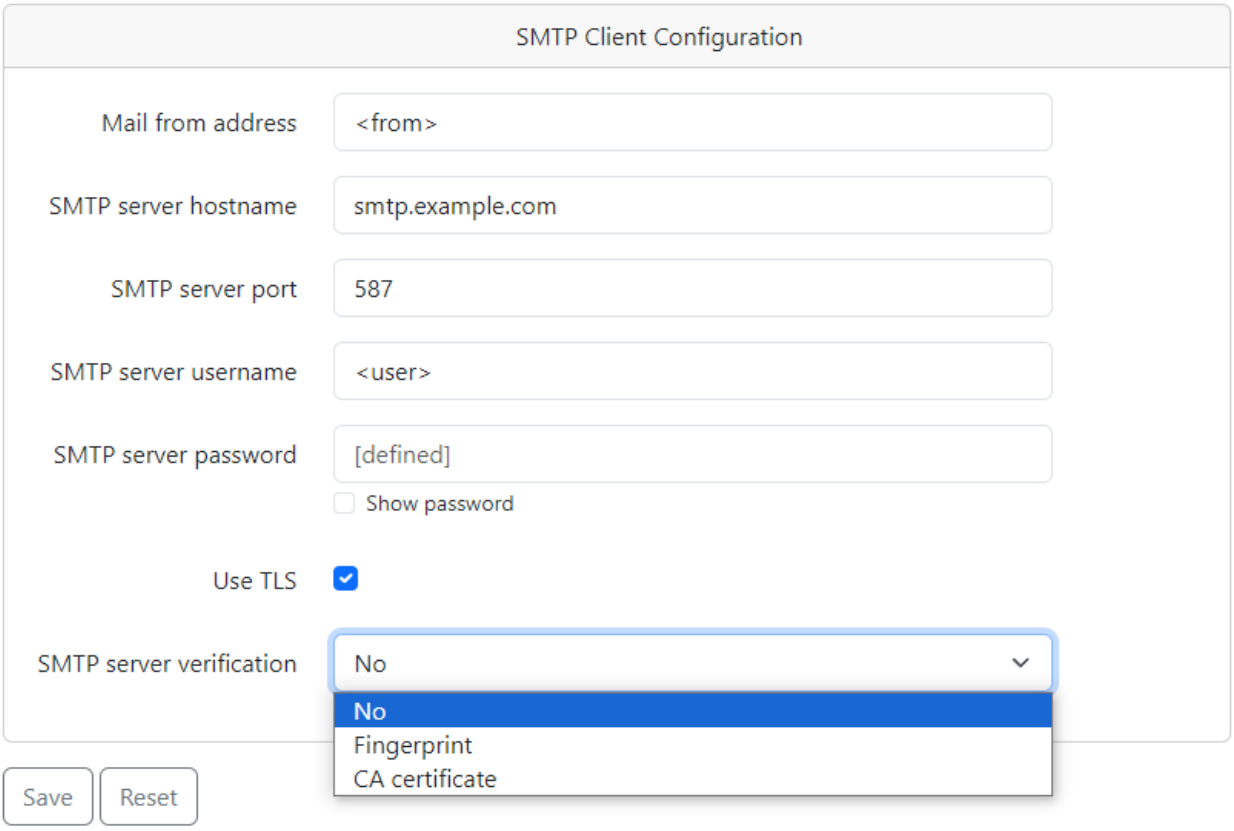
Firewall (firmware 1.20) – IP rules can be put in place to prevent unauthorized access and prevent DDoS attacks to different services.



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

4.3.3 Mail

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



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.

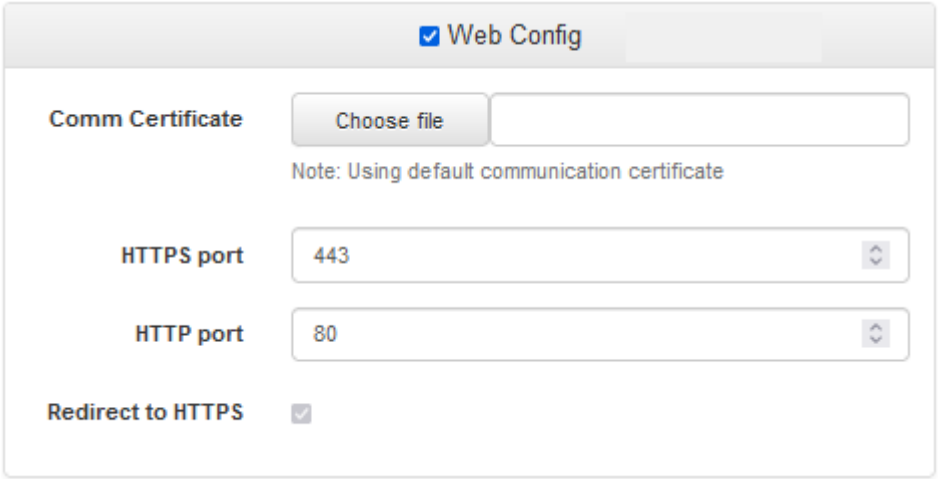
SMTP server password – The password for accessing the SMTP server.

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.

4.3.4 Services



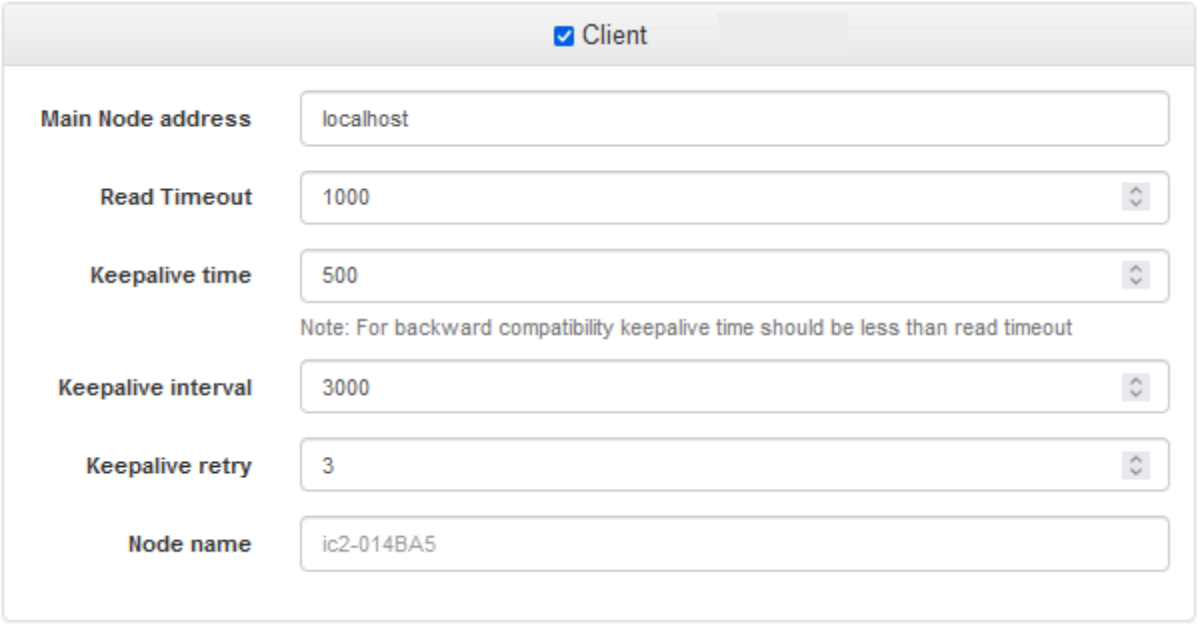
Web Config – Checking this box enables the web server on the controller that can be accessed via web browser.

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 – 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”.

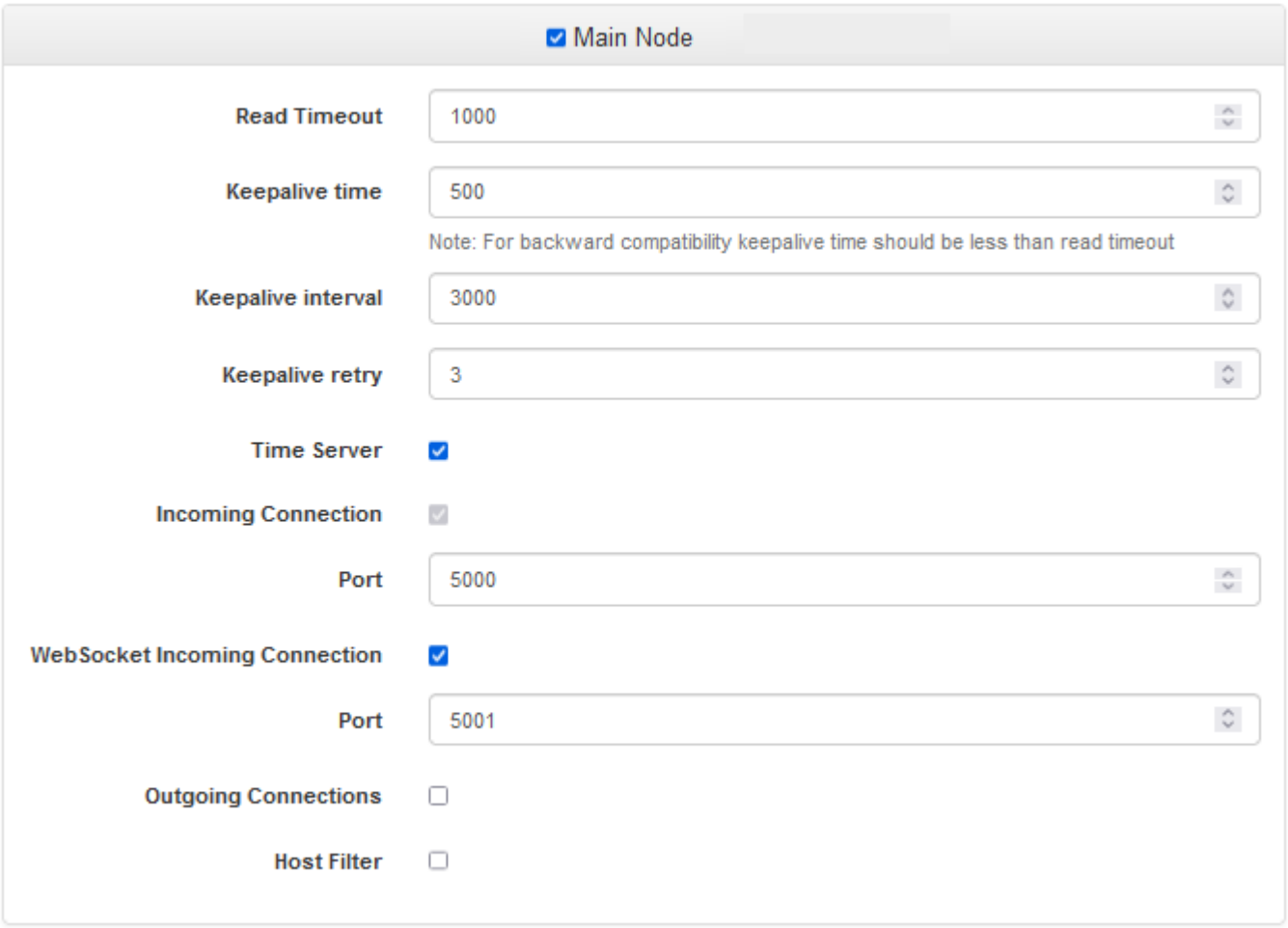
Read Timeout – How long (in milliseconds) the controller should be allowed to process an entire multi-packet message after the first packet is received. This is the Client Node service’s connection to the Main Node service.

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 – 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.

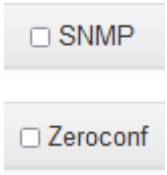
Port – The network port to accept incoming network connections.

WebSocket Incoming Connection – Enable incoming WebSocket connections.

Port – The network port to accept incoming WebSocket connections.

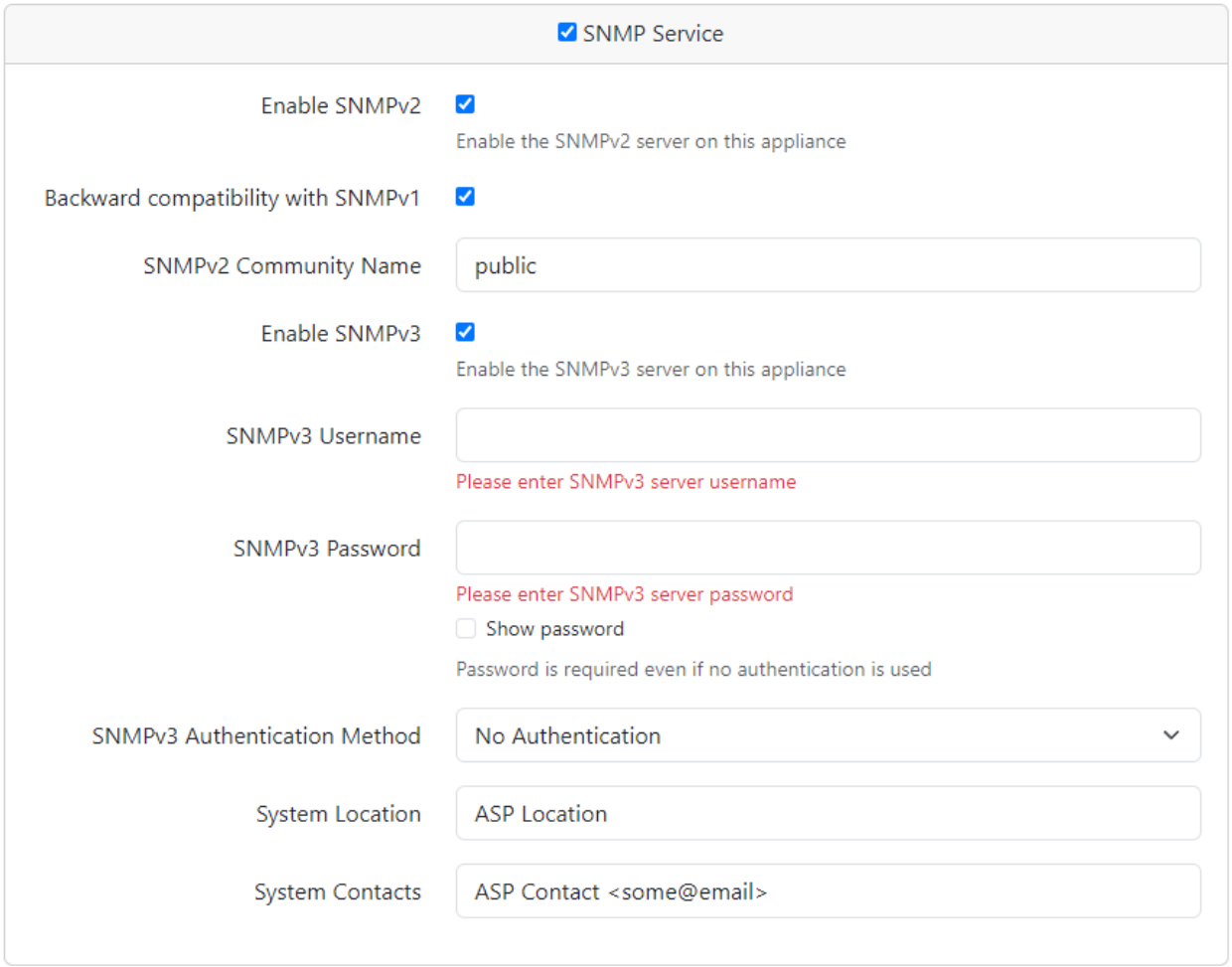
Outgoing Connections – Checking this box will configure the controller to be the initiator of the connection to the Host or a WebSocket endpoint.

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 – 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.

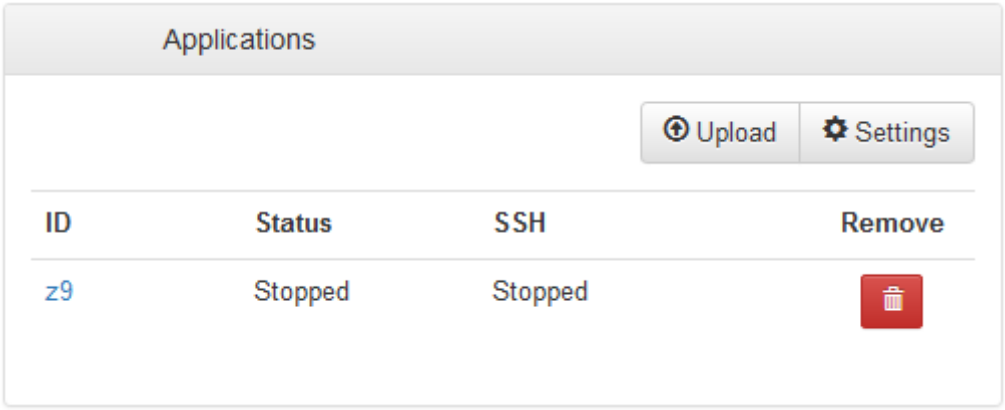


Zeroconf – If enabled, the controller is discoverable on the network by tools such as Bonjour Browser. This is recommended to always be enabled.

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

4.3.5 Applications

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



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. The developer certificate applied here must match the certificate used to build the application.

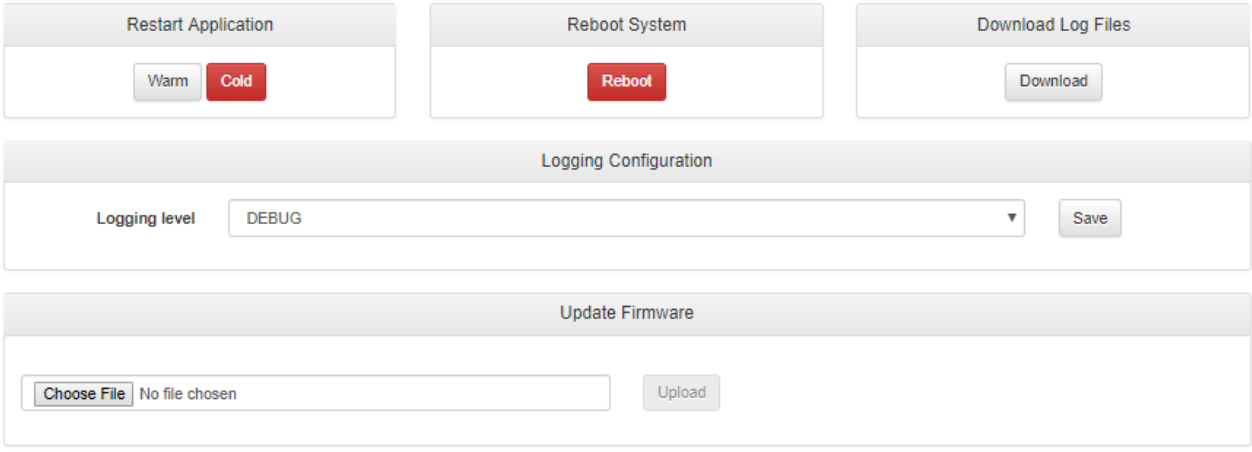
ID – The text string identifying the app. Clicking this ID will open a new window that shows some configuration options and app information. In this window, the user can start up the application, see version information, enable/disable SSH, and see what ports are mapped for the application to use.

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.

4.3.6 Maintenance



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.

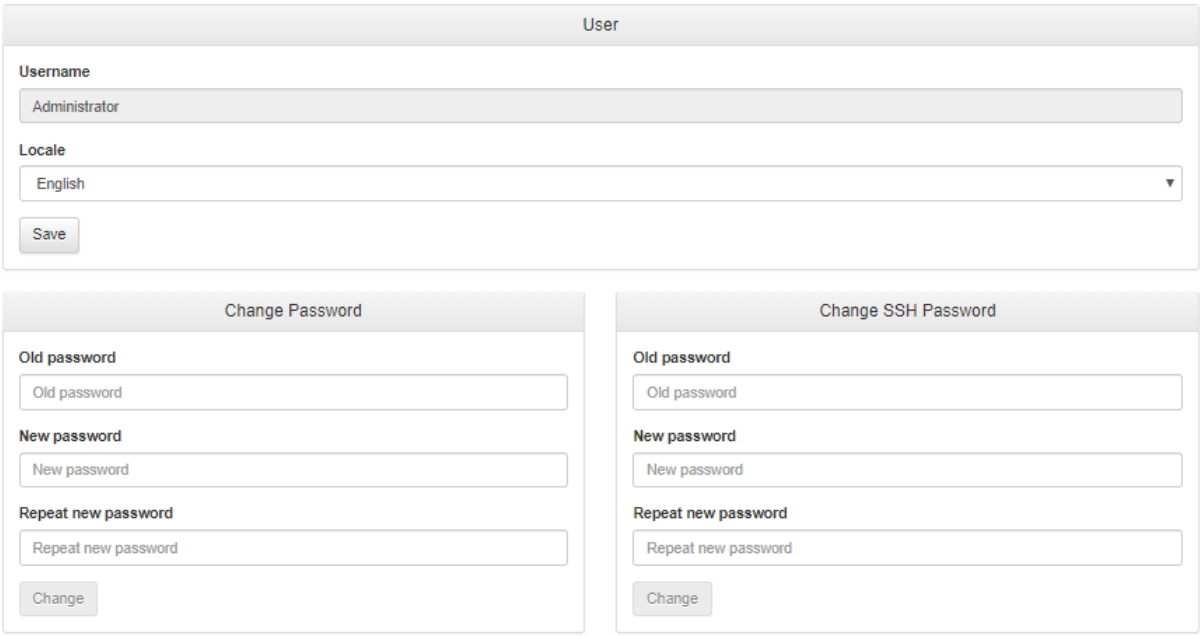
Reboot System - Completely restarts the controller as if power was cycled, while retaining the configuration. This will cause the controller to temporarily drop offline.

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.

4.3.7 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.

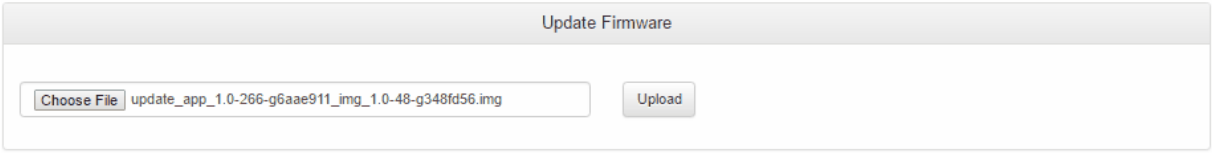
4.4 Firmware & License Updates

Firmware Updates

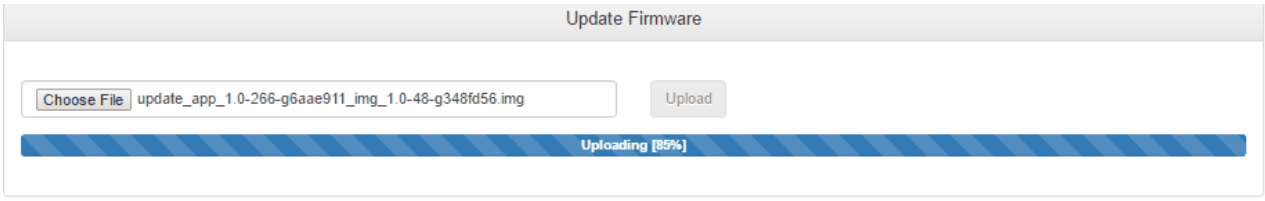
Firmware updates are provided electronically and can be loaded to a controller with no modifications to the hardware. The firmware file is uploaded to the controller using either the controller's web server or SDK/Host connection. Updates should be done as needed to make use of new features, improvements,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

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

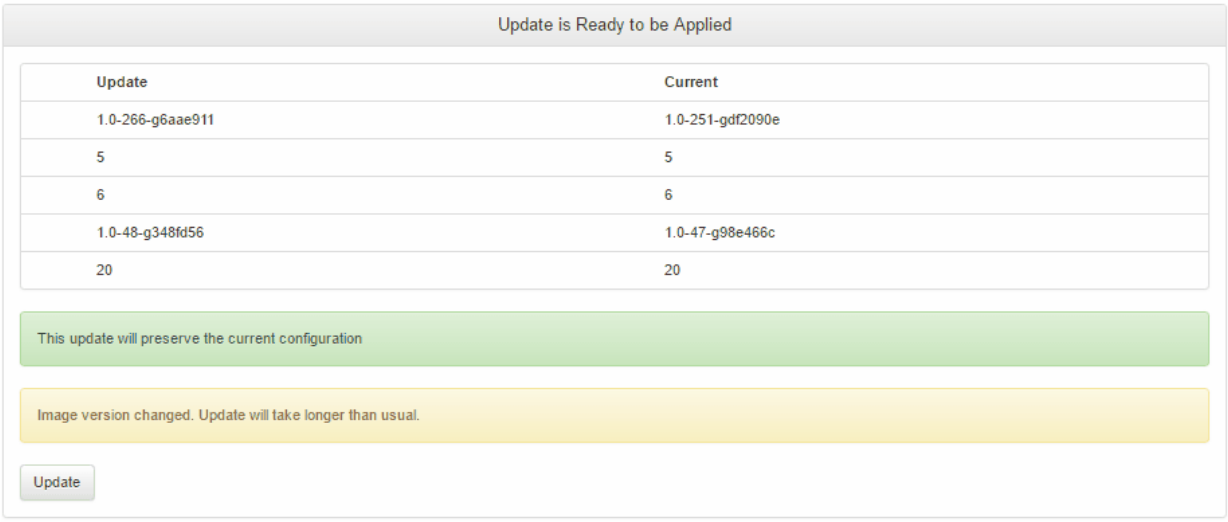
1. Obtain the new firmware package from the Azure Access partner portal or your solution provider and save it to a PC that is visible to the controller on the network.
2. Using the PC's web browser, connect to the controller's web server and go to the "Maintenance" page (see section 4.4.5).
3. Under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



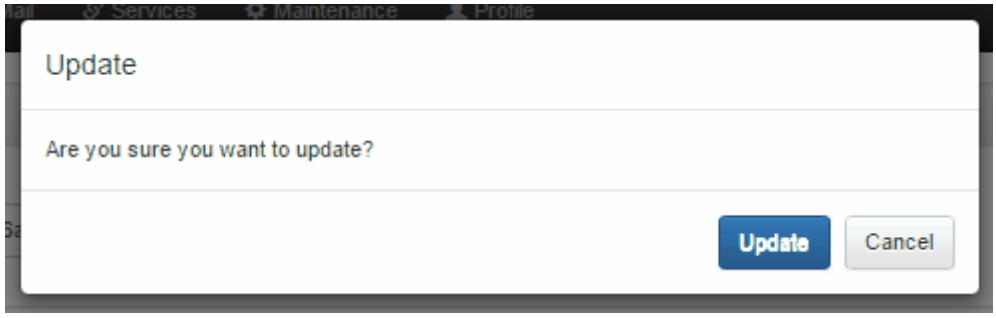
4. Click Upload and the upload of the file will begin. This will only upload the file but not apply it yet.



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 patters. 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

4.5 Embedded Applications

The controller supports running custom 3rd party, embedded-applications in a containerized environment on the board. The provided ADK (Application Development Kit) comes with a tool-chain for building the application, example project templates, and the embedded version the SDK. Embedded applications can utilize the SDK for access control functionality as well as interact with the Linux system itself and other onboard services. For added security, a “developer certificate” is provided by the factory to authenticate the custom applications deployed on the board.

4.5.1 Modes of Operation

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.

To exit and app running in Exclusive Mode, hold the Factory Reset pushbutton for at least 5 seconds and then, while still holding Factory Reset button, press the SSH push button. Release both buttons and the board will exit Exclusive Mode.

Non-Exclusive Mode – In non-exclusive mode, the application runs on the board as a parallel application. The controller’s native web server interface, network ports, and services remain active.

4.5.2 App Management

Apps can be installed and managed through the controller’s web server (see section 4.4.5) or via the Host. To run, applications will also need a copy of the “developer certificate” applied the application manager on the board’s web server. This certificate must match the certificate used to build the application. Embedded applications support SSH connections for root access to the app’s container.

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.

4.6 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.

4.6.1 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.

4.6.2 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.

4.7 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.

4.8 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

For any issues not reference here, contact Azure Access support for assistance.

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.

PART VI
Specifications

6 Specifications

Specifications are subject to change without notice.

Primary Power (VIN)	**DC/DC:** 12 to 24 VDC ± 10% • 12VDC board operating current: 320mA 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 ** "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 normal operating max, which may be below the "peak inrush" current consumption. **PoE+** Source: 42.5 to 57V (converted to 12VDC on the board) • Board Full-Load Power Budget: 2.3A max @ 12VDC • Board operating current: 95mA max @ 42.5V • Full-load (powering VOUT & RVO) current: 660mA max @ 42.5V
Auxiliary Power (VOUT)	VIN Passthrough; 1000mA (1A) max. Add to VIN current
Reader Power (RVO)	VIN Passthrough or Regulated 12VDC (selected with onboard jumper). **Only use Regulated 12VDC setting when VIN > 20VDC** • **VIN Passthrough –** 500mA per port max. Add to VIN current • **Regulated 12VDC –** 500mA per port max and combined 600mA max for both ports. Add up to 360mA @ 24V VIN to current
RTC Coin Cell Battery (BAT1)	CR1225; 3V; 48mAh capacity recommended
Micro USB OTG	5VDC; 500mA max (add 270mA to VIN current)
Micro SD Card	Not supported at this time
Host Communication	Network 10BaseT/100Base-TX
Downstream Serial Comm (x2)	RS-485; 2-wire (half-duplex) plus Signal Ground; 9600 to 115200 baud
Tamper & Power Fault	Unsupervised digital inputs for cabinet tamper & power supply failure
Alarm Inputs (x8)	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 (x4)	Dry, Form-C contacts; 2A @ 30VDC / 0.5A @ 120VAC max **Note:** When connecting an inductive load like a magnetic strike, it is recommended to derate the relay's current rating by 50%

Reader Ports (x2)	**Reader Power:** See “Reader Power (RVO)” above **Data Input:** Supports F/2F, TTL (Wiegand or Clock/Data), and 2-wire RS-485 (9,600 to 115,200 baud) for OSDP readers **Buzzer Output:** Open collector; 18 VDC max; sink 50mA max **LED Output:** Tri-State LED output; Active Low; 20mA source or sink max; TTL logic levels (High > 3V & Low < 0.5V)
Cable Requirements	**DC Power:** 18 AWG minimum; 1 twisted pair **Ethernet/PoE+:** Cat 5 minimum **RS-485:** 24 AWG. 1 shielded twisted pair. 4000 ft. (1,219m) max @ 9600 baud; Belden 9841 or equivalent cable **Reader Data (TTL):** 4 to 6 wires; 500 ft. (152 m) max; 18 to 22 AWG depending on cable length; non-twisted pairs. For 6-conductor wiring, Belden 9536 or equivalent is recommended. **Inputs:** 1 twisted pair; 22 AWG minimum; 1000 ft. (304.8 m); 30 Ω max loop resistance **Relay outputs:** 16 to 18 AWG. Use sufficient gauge to avoid voltage loss.
Environmental	**Temperature:** -40 to 85ºC operating and storage; Indoors **Humidity:** 5 to 95% RHNC.
Mechanical	**Dim:** 8 in. (203.2 mm) W x 6 in. (152.4 mm) L x .75 in. (19.05 mm) H **Weight:** 0.6 lbs. (272.2g)

Part VII
UL Compliance

7 UL Compliance as Recognized Product

- For UL installations using PoE, the following must be observed:
- Compliance with IEEE 802.3 (at or af) specifications was not verified as part of UL
  - 294.
- Locations and wiring methods which shall be in accordance with the National
  - Electrical Code, ANSI/NFPA 70.
- This product is not intended for outside wiring as covered by Article 800 in the
  - National Electrical Code, NFPA 70.
- Category 5e, cabling is the minimum performance category recommended.
- The minimum conductor gauge permitted to connect between the PSE or power
  - injector and the PD shall be 26 AWG (0.13 mm^2) for patch cords; 24 AWG (0.21
  - mm^2) for horizontal or riser cable.
- Connected through standard eight-pin RJ-45 connectors.
- Evaluated for Mode B only.
- PoE power is to be supplied by an Access Control System Unit (ALVY), Class 2 power
  - limited, PoE injector (PSE) providing 42.5-52VDC and 25.5W for maximum output."
- Power to be provided by a Listed UL 294, UL 603, or UL 2610 power limited/class 2, power
- supply or PoE injector with appropriate ratings and standby power.
- Wiegand, OSDP 26-bit card format tested by UL.
- 1K/2K, 300/10K, & 3K/4.5K EOL values verified.
- Supervised Inputs required for burglar applications.
- When used with a Listed system for burglar use, system is to be monitored by a Listed receiver for the standards used.
- 12V regulated reader-power setting is only for use with 24VDC input.
- Using the 12V regulated reader-power setting configures reader outputs for special application use only.
- 4-wire connection for half-duplex not evaluated.
- Battery on NOP-IC2 is assumed to be serviced by qualified technicians only.
- Product evaluated as a recognized component by UL and is not suitable to be used as a Listed subassembly. Products are for user with listed access control or proprietary burglar alarm control units/system.