



How to Install an IP-Enabled ISONAS Reader-Controller

*Copyright © 2006-2009, ISONAS Security Systems
All rights reserved*

ISONAS Inc.

FCC ID: 0CZRC-01

This device can be expected to comply with Part 15 of the FCC Rules provided it is assembled in exact accordance with the instructions provided with this kit. Operation is subject to the following 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.

Table of Contents

1: BEFORE YOU BEGIN	5
1.1: GENERAL REQUIREMENTS:	5
1.2: CLEARNET READER-CONTROLLER SPECIFICATIONS:	6
1.3: POWERNET READER-CONTROLLER SPECIFICATIONS:	6
1.4: ISONAS IP READER-CONTROLLERS COMMUNICATIONS OPTIONS	7
1.5: INSTALLATION LOCATION GUIDELINES	8
2: WIRING AT THE DOOR AND READER-CONTROLLER	14
2.1: POWERING THE READER-CONTROLLERS	14
2.1.1: POWER OVER ETHERNET (PoE) OPTION	14
2.1.2: LOW-VOLTAGE DC POWER OPTION	17
2.2: WIRING THE DOORS	18
2.2.1: READER-CONTROLLER CONTROL-LEADS DESCRIPTION	20
2.2.2: WIRING THE DOOR LOCK	22
2.2.3: WIRING THE EXTERIOR DOOR KIT (PowerNet Only)	24
2.2.4: WIRING 2 READERS TO 1 LOCK	26
2.2.5: WIRING THE REX BUTTON	27
2.2.6: WIRING THE AUX INPUT	27
2.2.7: WIRING THE DOOR SENSE	28
2.2.8: USING THE TTL LEADS	29
2.2.9: MANAGING INDUCTIVE LOAD CHALLENGES	30
2.2.10: MANAGING IN-RUSH CURRENT LOADS	31
3: CONFIGURING THE READER-CONTROLLER'S COMMUNICATIONS	32
3.1: ETHERNET-BASED TCP/IP READER-CONTROLLERS	32
3.2: WIRELESS CLEARNET READERS AND NETWORKS	36
3.2.1: SECURITY FOR WIRELESS READERS	36
3.2.2: INSTALLING A WIRELESS READER	37
3.3: SECURING MESSAGES ON YOUR NETWORK	38

Document Version

Date of Revision	Revision	Author	Description
6/29/2007	2.0	Roger Matsumoto	Updated to include installation information for PowerNet reader-controllers
7/10/2007	2.1	Shirl Jones	Updated to cover the Exterior Door Kit
8/11/2007	2.2	Shirl Jones	Clarified differences between ClearNet and PowerNet configurations
10/14/2007	2.3	Shirl Jones	Improved External Door Kit instructions
4/15/2008	2.4	Shirl Jones	Typical lock wiring diagram for PowerNet w/PoE added
4/24/2008	2.5	Shirl Jones	Clarified jumper configuration for lock relay
6/20/2008	2.6	Shirl Jones	Added In-Rush Current Suppressor section
5/12/2009	2.7	Shirl Jones	Removed 12V Terminal Block references. Power supplied by the PowerNet is now routed thru Pigtail
6/16/09	2.8	Michael Radicella	Added the FCC compliance ID and notice

1: BEFORE YOU BEGIN

To install an ISONAS Reader-controller unit, you must complete three key wiring tasks:

1. Supply power to the Reader-controller unit. This may be accomplished with a power feed on the Ethernet Data cable (Power over Ethernet [PoE])
2. Wire the unit to the door's locks and other components for physical access control.
3. Connect the unit to the data network for communication with the server/workstation host PC.

This guide discusses each wiring process separately. Understanding all of these processes makes this project much simpler and guarantees success.

1.1: GENERAL REQUIREMENTS:

- If PoE is not being used, then use only UL-listed, access control, power-limited power supplies with an 'AC on' indicator light clearly visible on the enclosure. Power supplies should provide at least four hours of standby power.
- Never connect power supplies to a switch-controlled receptacle.
- Install the ISONAS system in accordance with the National Electrical Code NFPA 70. (Local authority has jurisdiction.)
- Use only suitable recognized wire or UL-listed cabling for ISONAS power supply and data communications, in accordance with the National Electrical Code.
- Where possible, separate ISONAS equipment and cabling from sources of electromagnetic interference (EMI). Where this is not possible, take other steps to reduce the effect of EMI on cabling or equipment.
- Protect input and output terminals adequately from transient signals. Also, connect these terminals to power-limited circuitry.

1.2: CLEARNET READER-CONTROLLER SPECIFICATIONS:

Input Voltage	12V DC
Current Draw	0.20 AMPS
Read Range	1 TO 3 inches typically
Read Speed	<250msec
Exciter Field Frequency	125khz
Modulation Schemes	FSK/ASK
Communication Interface	TCP/IP Over Ethernet/Wireless
Inputs/Outputs	3 Inputs/2 TTL Outputs/1 Tamper Output
Relay	1.0 amp @ 30V DC (Resistive load)
Standalone Memory Capacity	2048 Cards/ 250 Events/ 32 Time zones
Visual Indicators	2 LEDs for Normal Operations
Operating Temperatures	-4° To 122° Fahrenheit -20° To 50° Celsius
Weight	Mullion Approximately 7 Ounces Switchplate Approximately 9 Ounces
Size	Mullion 6 ¾"H BY 1 5/8"W Switchplate 4 ¾"H BY 3 7/8"W

1.3: POWERNET READER-CONTROLLER SPECIFICATIONS:

Input Voltage	12V DC, 24V DC, or PoE per IEEE 802.3af
Current Draw	0.25 AMPS
Read Range	3 TO 5 inches typically
Read Speed	<250msec
Exciter Field Frequency	125khz
Modulation Schemes	FSK/ASK
Communication Interface	TCP/IP Over Ethernet
Inputs/Outputs	3 Inputs/2 TTL Outputs/1 Tamper Output
Relay	1.0 amp @ 30V DC (Resistive load)
Standalone Memory Capacity	64000 Cards/ 5000 Events/ 32 Time zones
Visual Indicators	2 LEDs for Normal Operations
Operating Temperatures	-40° To 122° Fahrenheit -40° To 50° Celsius
Weight	Mullion Approximately 8 Ounces
Size	Mullion 6 ¾"H BY 1 5/8"W

1.4: ISONAS IP READER-CONTROLLERS COMMUNICATIONS OPTIONS

ISONAS offers two types of IP Reader-controllers:

●**Ethernet:** Uses TCP/IP communication over a wired data network (Ethernet). The Ethernet version connects to a standard CAT5 cable via an RJ45 connector.

●**Wireless:** Uses TCP/IP communication over a wireless (WiFi) data network. The wireless version requires no network cable.

The process of connecting the reader to the door is the same for any ISONAS Reader-controller.

How you connect the Reader to the network depends on the style of Reader selected. The style of Reader must correspond to the type of communication network used in the building.

Double-Check Your Product Order!

It's crucial to order the correct Reader for the type of network used in the building (Ethernet or Wireless).

1.5: INSTALLATION LOCATION GUIDELINES

When selecting the location where you are going to mount the ISONAS reader-controller, a few guidelines should be observed.

- 1) The reader-controller should be kept at least 2 feet from another ISONAS reader-controller, and 6 feet from any other RF emitting device.
- 2) Assure that the window on the back of the reader-controller's is mounted against a reflective surface. A self-adhesive reflective sticker is provided with each reader-controller, in case the wall's mounting surface is non-reflective. Please note that this reflective surface is required for successful operation of the ISONAS reader-controller
- 3) In an exterior location, the reader-controller's mounting should be sealed to prevent water from running down between the mounting surface and the back of the reader-controller.
- 4) For the PowerNet reader, a dielectric insulating compound (Dow Corning DC-4 or equivalent) can be used to obtain extra water protection of the reader-controller's cable connections.
- 5) The reader-controller should be protected from extreme heat and sunlight. It is rated for conditions up to 120 F. A direct southern exposure, in the Southwest area of the United States may exceed these ratings.
- 6) Mounting against a large metal object may affect the read range of the reader. Steel, iron, and copper will have more of an affect on the read range than aluminum. A conservative guideline is to have a 4 inch separation between the reader-controller and the metal surface.
- 7) The cables extending from the back of the ClearNet reader-controller are 36 inches long. Plan for terminating the wiring and CAT 5 cable within that distance of the reader-controller. PowerNet's Pigtail cable comes in 4 ft, 10 ft and 25 ft lengths.
- 8) The wall mounting features required for the reader-controller are shown in the next figures. Electronic versions of these figures can be found on the ISONAS website, and can be printed out, for use as life-size drill templates.

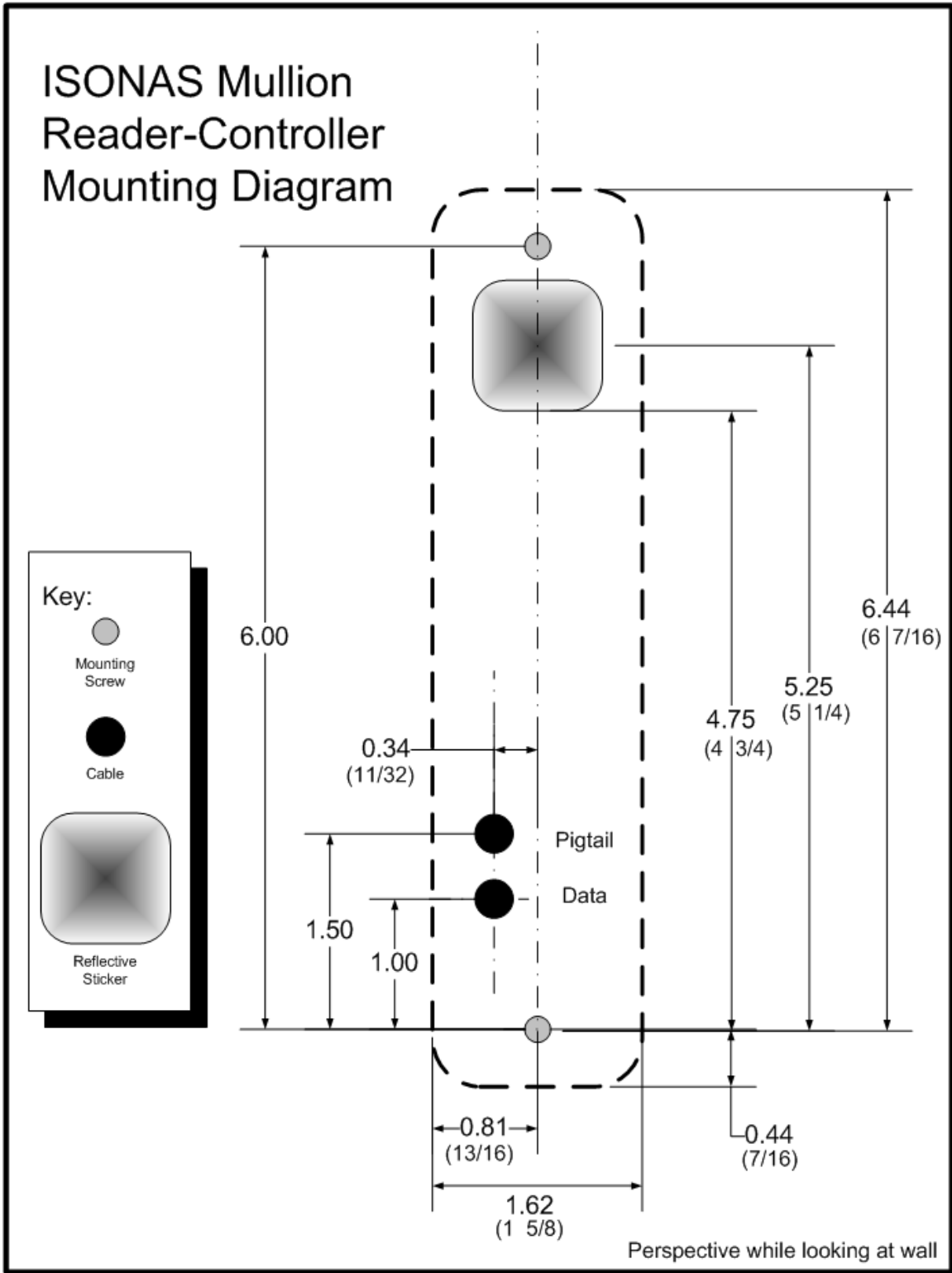


Figure 1 (Mullion Mounting Diagram)

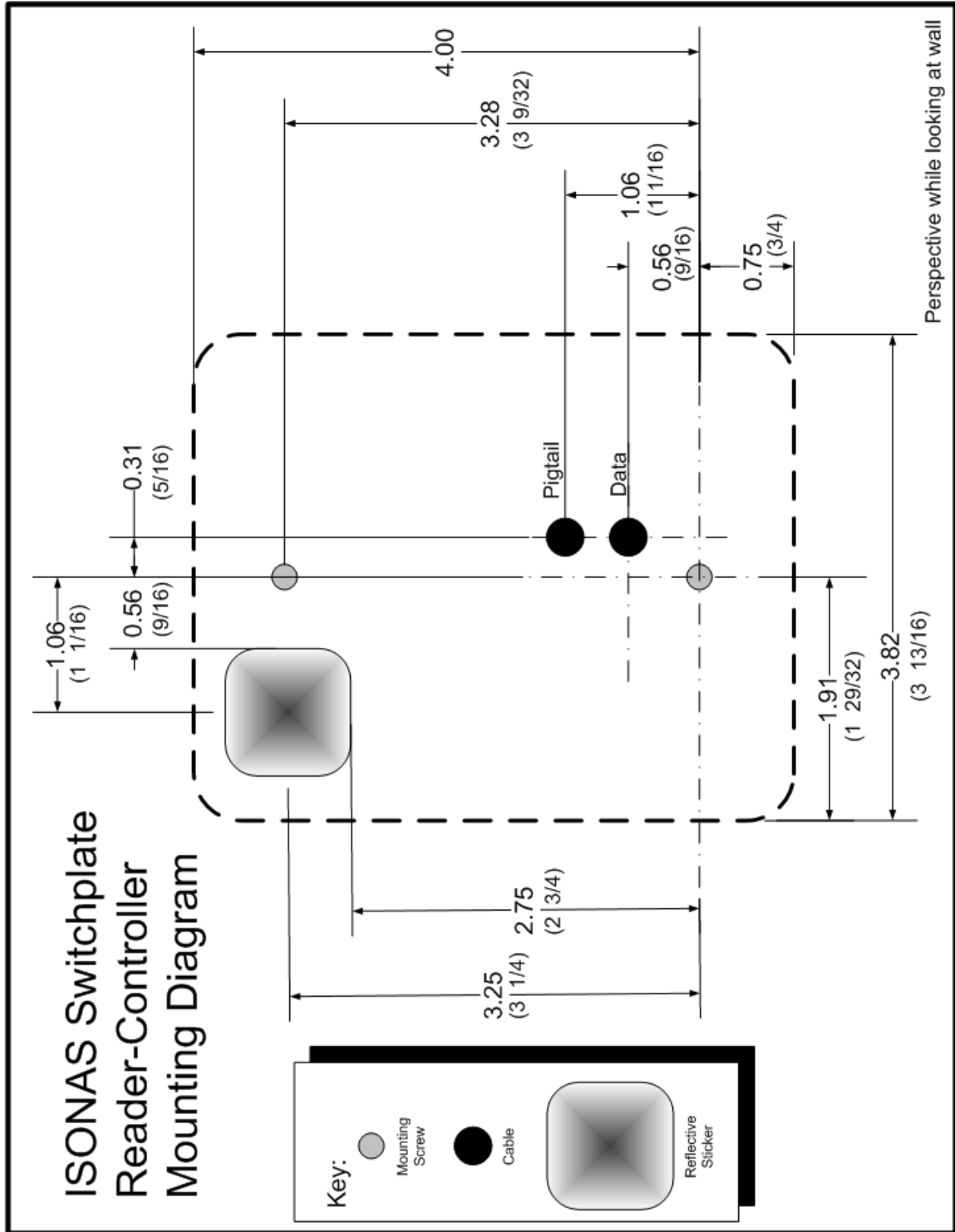


Figure 2 (Switchplate Mounting Diagram)

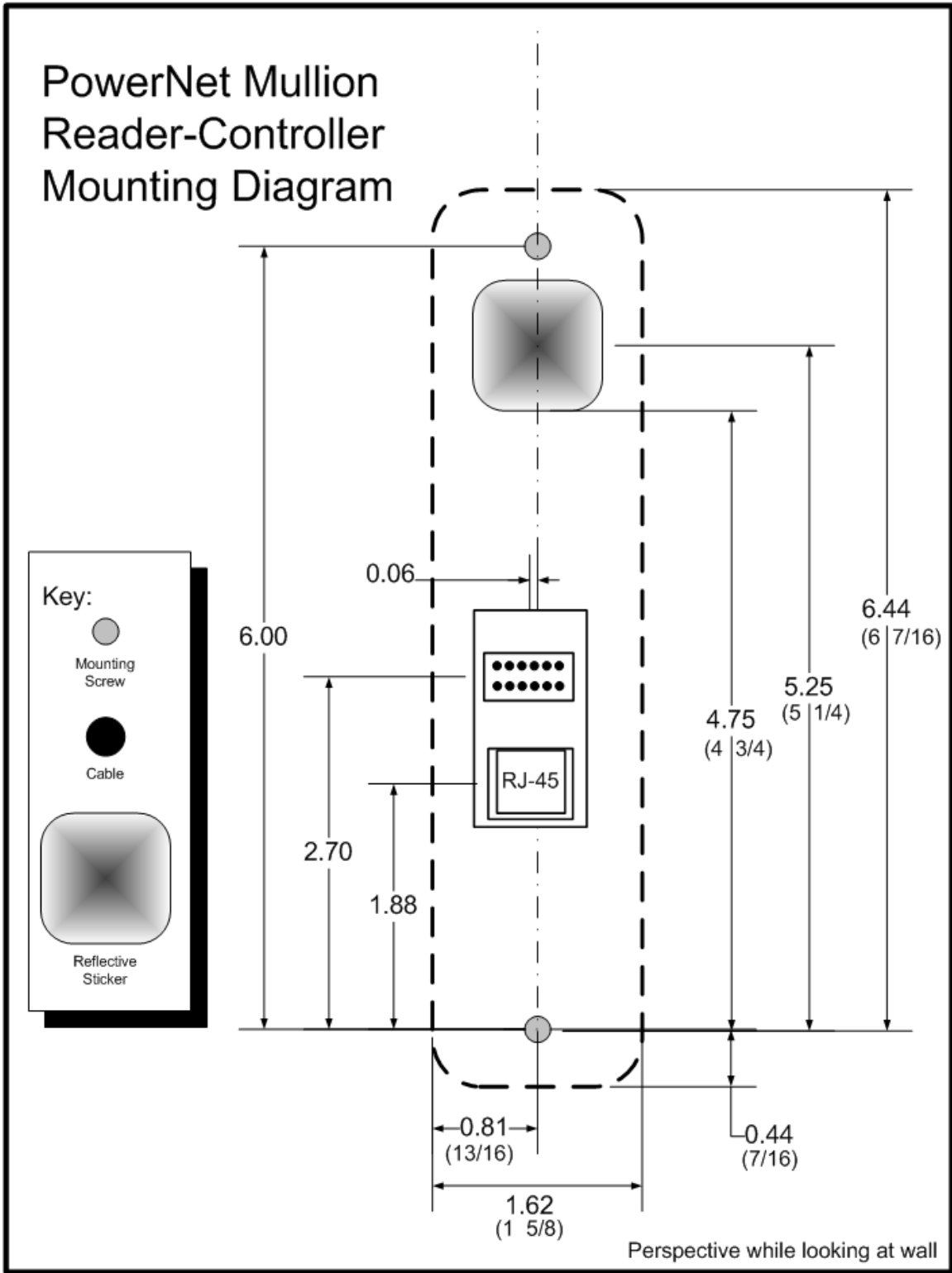


Figure 3 (PowerNet Mullion Mounting Diagram)

1.6 POWERNET CONFIGURATION

The PowerNet reader-controller has a set of jumper pins that configure both its input power source, and its lock control circuit.

The PowerNet reader-controller can be configured for power to be supplied to the reader-controller through the 12 conductor pigtail (either 12VDC or 24VDC) or through the RJ45 connector (Power Over Ethernet).

If POE is used, the reader-controller can supply 12VDC thru its pigtail, which may be used to power the lock or other devices at the door location.

Figure 4 shows the components on the back of the ISONAS PowerNet Reader-controller.

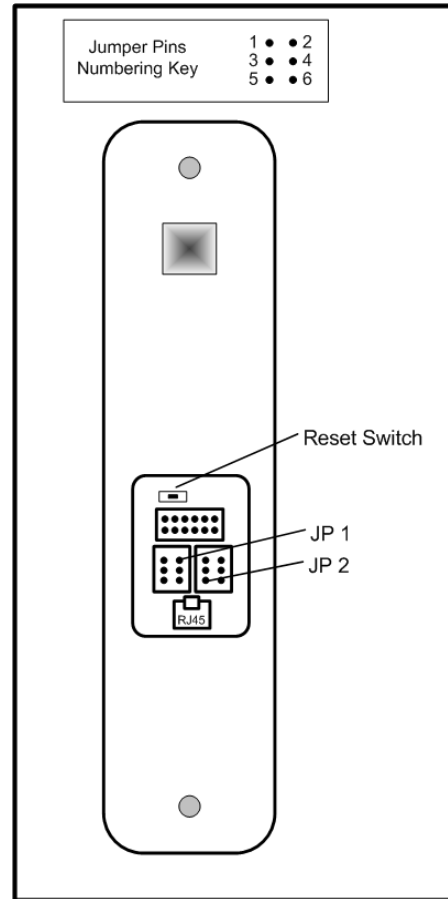


Figure 4

Feature	JP 1 Jumpers	JP 2 Jumpers
Input Power – 12VDC, thru Pigtail	1 to 3	
Input Power -- 24VDC, thru Pigtail	3 to 5 & 4 to 6	
Input Power – PoE, thru RJ45 connector	None	
Input Power – PoE, thru RJ45 connector (See Note 1)	1 to 3	
Lock's power/signal is externally supplied on the pigtail's pink wire		None
Supply internal 12VDC to relay common (See Note 2)		1 to 3
ISONAS External Door Kit being used.		4 to 3
Connect GROUND to relay's common contact.		5 to 3

Note 1. Special case: The unit is PoE powered AND you want 12v output power supplied on the pigtail's red conductor.

Note 2. Used when powering an external lock device. This option only available if JP 1 configured for PoE.

1.6 POWERNET READER-CONTROLLER RESET BUTTON

The PowerNet reader-controller has a Reset Button located on the back. It can be used for two different types of resets.

It is helpful if the PowerNet's Ethernet cable is connected, and functioning (the green LED is lit). Monitoring the green LAN status LED allows you to determine the status of the reset operation.

- **Reset CPU:** Press, hold (approx. 2 seconds) and release the Reset button. Once the Reset Button is released, the Green LAN Status LED should turn off (approx. 6 seconds), and then turn back on. If the Green LED does not turn off, then the reset did not occur.

- **Reset Configuration:** Press and hold the Reset button (approx. 10 seconds), until the Green LAN LED turns off. The reader-controller's communications configuration is reset to factory defaults. Setting that are changed include:
 - IP Address
 - IP Port
 - AES Encryption Configuration
 - Serial Line Configuration

2: WIRING AT THE DOOR AND READER-CONTROLLER

2.1: POWERING THE READER-CONTROLLERS

All ISONAS Reader-controller models require a direct connection to a power source.

The ClearNet reader-controllers require **12 volts DC power**, and the supply must be regulated. Many brands of power sources work well with ISONAS equipment.

The PowerNet reader-controllers can be powered with **12 volts DC, 24 volts DC, or PoE (IEEE 802.3af) power** and the supply must be regulated. Many brands of power sources work well with ISONAS equipment. For the PowerNet reader-controller, the desired input power selection is made thru the use of the jumper pins. See previous section (1.6) for the description of the usage of these jumper pins.

2.1.1: POWER OVER ETHERNET (PoE) OPTION

If you are installing ISONAS Ethernet IP readers, then you can use the Power Over Ethernet (PoE) option. PoE allows one cable to supply data and power to both the Reader-controller and an Electronic lock. The obvious savings here is that you only need to run a single CAT5 cable to the door which will provide enough power to run both the ISONAS Reader-controller and an electronic lock. If you are not familiar with PoE, please take a moment to read the PoE document located on the ISONAS web site.

The PoE Injector is normally located right next to your existing network hub/switch, and the Injector itself is plugged directly into a standard AC outlet, or for extra security, a UPS battery backup. If your network switch is equipped to support providing PoE power, then it replaces the PoE Injector.

Figure 5 is an overview of how to use PoE to power both the ISONAS PowerNet Reader-controller and an electronic locking mechanism.

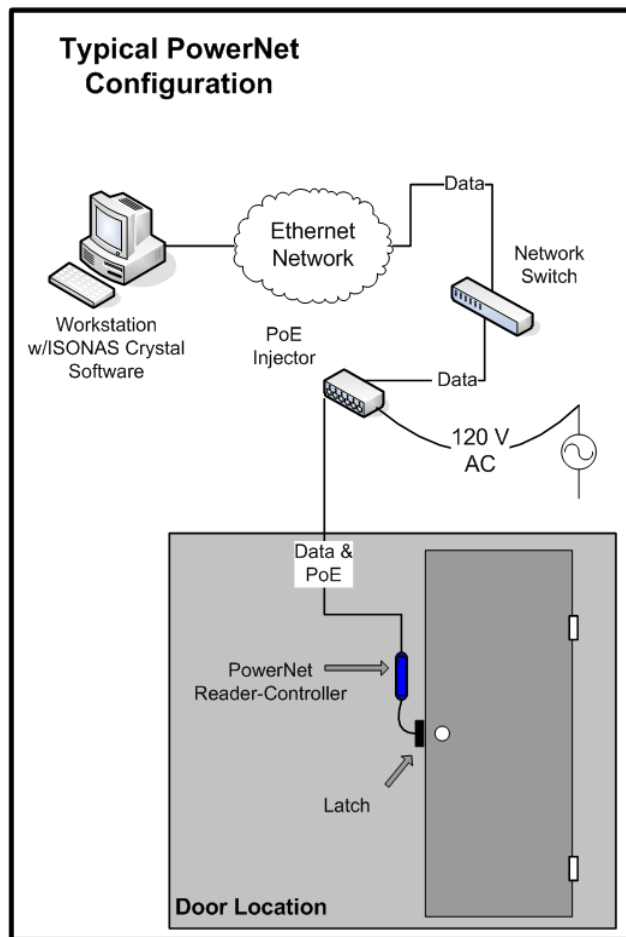


Figure 5

A standard CAT5 cable is then run between the PoE Injector and the PowerNet Reader-Controller which will be located right next to the door. The CAT5 cable can be 100 Meters (328 feet) long. This 100 meter limit is the standard Ethernet CAT5 limitation.

With one cable, you provided the required network connection and all the power that will be needed at the door site.

PoE can also be used with the ClearNet reader-controller, but an external PoE splitter is required at the door location.

Figure 6 is an overview of how to use PoE to power both the ISONAS ClearNet Reader-controller and an electronic locking mechanism.

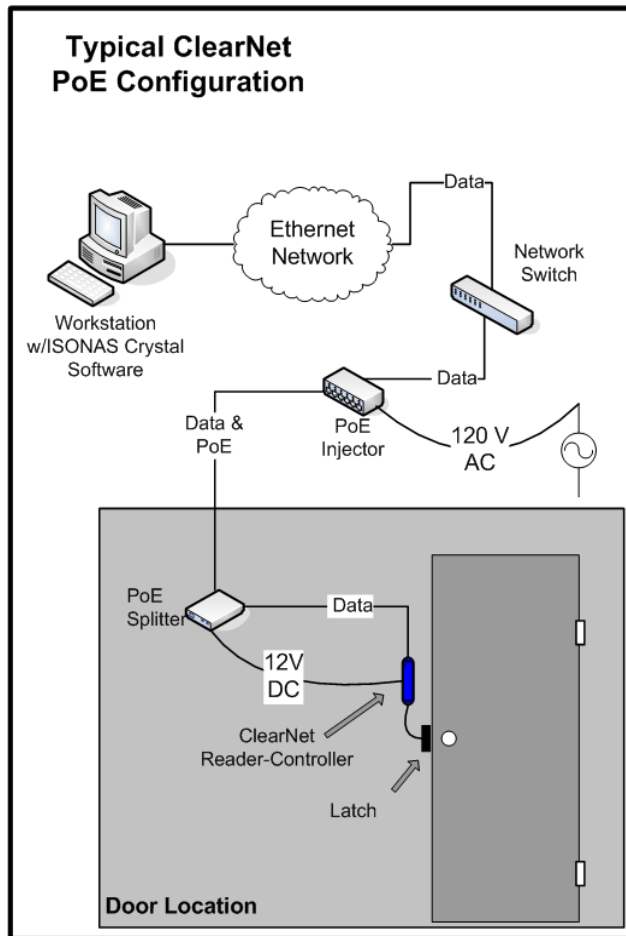


Figure 6

PowerNet Supplying 12 V External Power

When using PoE, the PowerNet reader can supply 0.5 amps@12 Volts of power for the external door components. This power can be routed to the lock control circuit using the jumper pins. The supplied 12V power can also be accessed thru the reader-controller's Pigtail, when the reader's jumper-pins are properly configured (on Jumper block JP1, jumper pin 1 to pin 3). The power will be continuously available on the Pigtail's Red and Black conductors. You might use this 12VDC source to power a Motion Detector located at the door location.

PoE Power Budget Calculations

When planning an installation using PoE, you need to assure that the PoE source (PoE Injector or PoE equipped Network Switch) supplying the PoE power is sized properly for the power draw of all the doors. To do this, you total up the power draw (in watts) of the PoE connections, and compare that total power draw to the rated capacity of the PoE source.

Below is a chart of expected PoE power draws of the ISONAS Reader-controllers.

Door Location Configuration	PoE Power Requirement ** (Watts)
PowerNet Reader-Controller	3.0 Watts
PowerNet Reader-Controller with Electronic Lock (0.5 amp @ 12V)	10.0 Watts
ClearNet Reader-Controller (External PoE Splitter used)	3.0 Watts
ClearNet Reader-Controller with Electronic Lock (0.6 amp @ 12V) (External PoE Splitter used)	13.0 Watts

*** Ethernet cabling power losses not included. Losses range from being negligible for short Cat5 cables up to about 16% for 100 meter Cat5 cables.

2.1.2: LOW-VOLTAGE DC POWER OPTION

Powering the reader-controller using low-voltage DC:

Wiring DC power to a Reader-controller: Simply run the positive and negative wires from the power source to the positive and negative wires on each Reader. The example below shows the typical power connection for a reader-controller and a lock.

1. Connect the positive power from the power supply to the relay's common (pink lead) and to the positive power connection (red lead) of the reader-controller.
2. Connect one side of the electric lock to EITHER the Tan (Fail Secure) or Gray (Fail Safe) connection on the reader-controller
3. Connect the negative power from the power supply to the negative power connection (black lead) of the reader-controller and the remaining side of the electric lock.

Figure 7 shows how to take the power from the External Power supply and drive both the PowerNet Reader-Controller and an Electronic lock.

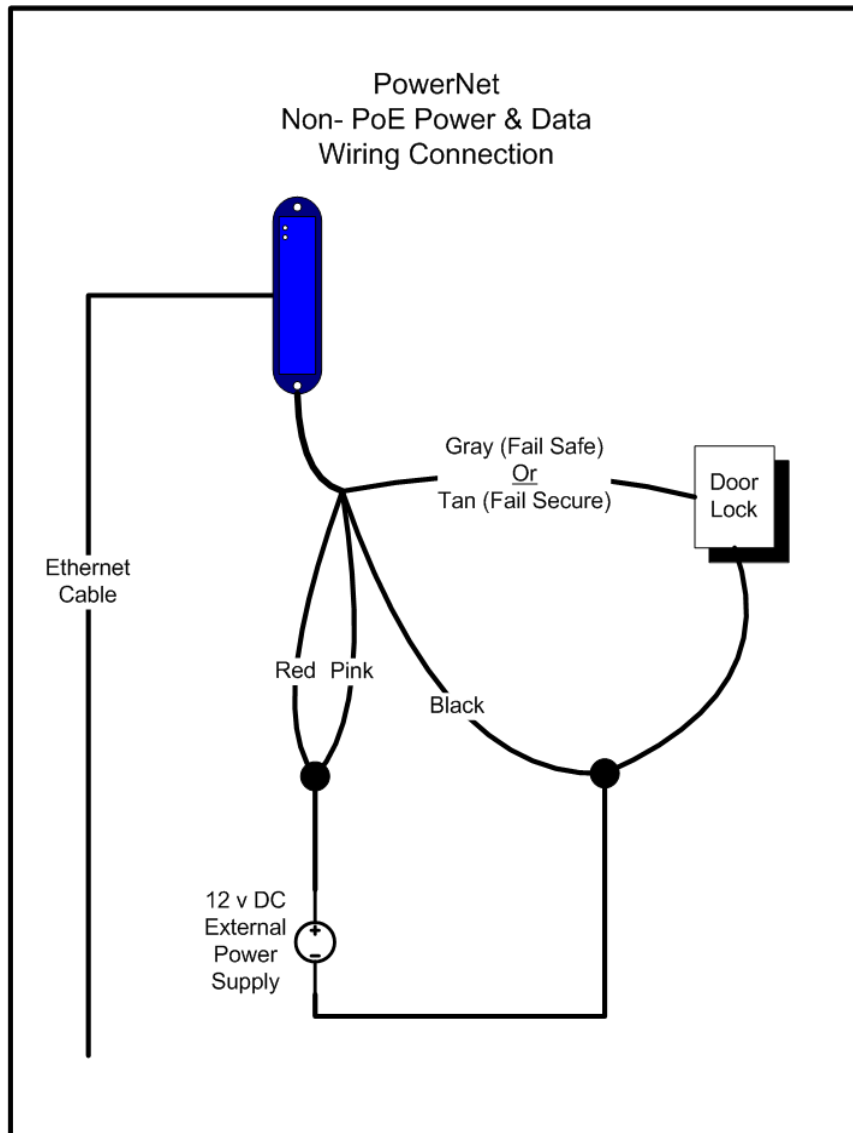


Figure 7

2.2: WIRING THE DOORS

After you connect power to every Reader-controller, the next step is to connect the wiring at each door.

Wiring a door may involve connecting:

- An electronic door latch
- A request to exit (REX) button
- An auxiliary (AUX) button
- Door sensors
- TTL lines (TTL1 and TTL2)

Figure 87 shows the typical configuration of equipment at the door.

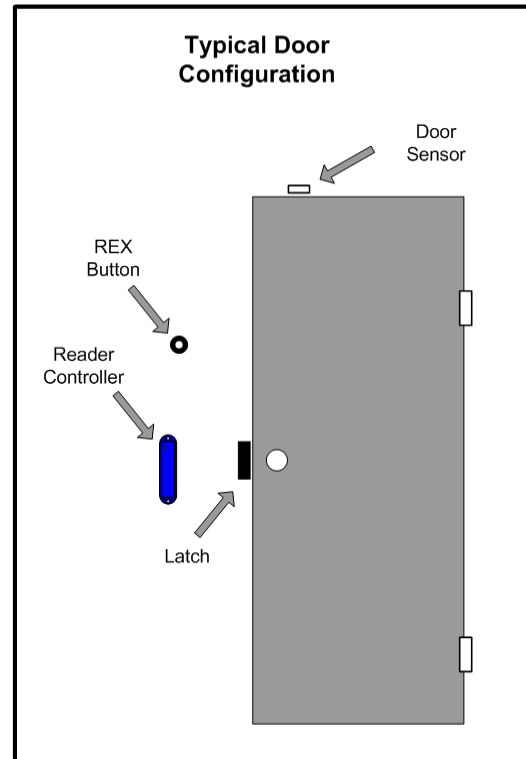


Figure 8

Electronic door locks come in two basic styles:

- **Fail Safe:** A door lock that will unlock when the power fails. Magnetic locks use power to keep the door *locked* and are typically “Fail Safe”. When power is applied, the magnets activate and the door locks.

- **Fail Secure:** A door lock that will lock when the power fails. Many electric strike locks are Fail Secure locks. These locks usually use power to *unlock* the door. This means that the strike (latch) physically holds the door closed during a power failure.

If the door does not already have an electronic lock, first install the electronic door lock according to the manufacturer's instructions. Examine the lock to determine whether applying power will lock or unlock the door.

- **Fail Safe:** If applying power *locks* the door (usually magnetic locks), use the gray wire labeled (NC).

- **Fail Secure:** If applying power *unlocks* the door (usually electric strike locks), use the tan wire labeled (NO).

Most locking mechanisms have **two leads for the power coil**. On an electric strike, the leads power a solenoid. On a Mag Lock, the leads power an electromagnet.

The door lock control relay inside the ISONAS Reader-Controller has a set of Form “C” contacts that are rated at 1.0 amp @ 30V DC. This means it can handle most locking mechanisms. If your application requires more voltage or amperage than this, an external relay that is controlled by the reader/controller can be used.

Installation Tip

For non-PoE installations:

Before you start wiring an electronic door lock, check that its power source is separate from the power source for the Reader-controller at that door.

Voltage fluctuations caused by using the same power source for both devices may cause the Reader to malfunction.

2.2.1: READER-CONTROLLER CONTROL-LEADS DESCRIPTION

The reader-controller has a 3-foot cable extending from its back plate that is nicknamed "the pigtail". The pigtail consists of 12 wire leads (24 awg) which are used to connect to the various components at the door location. Most installations do not require the use all the leads. The typical usage of each available lead is shown in **Figure 9 (ClearNet)** and **Figure 10 (PowerNet)**.

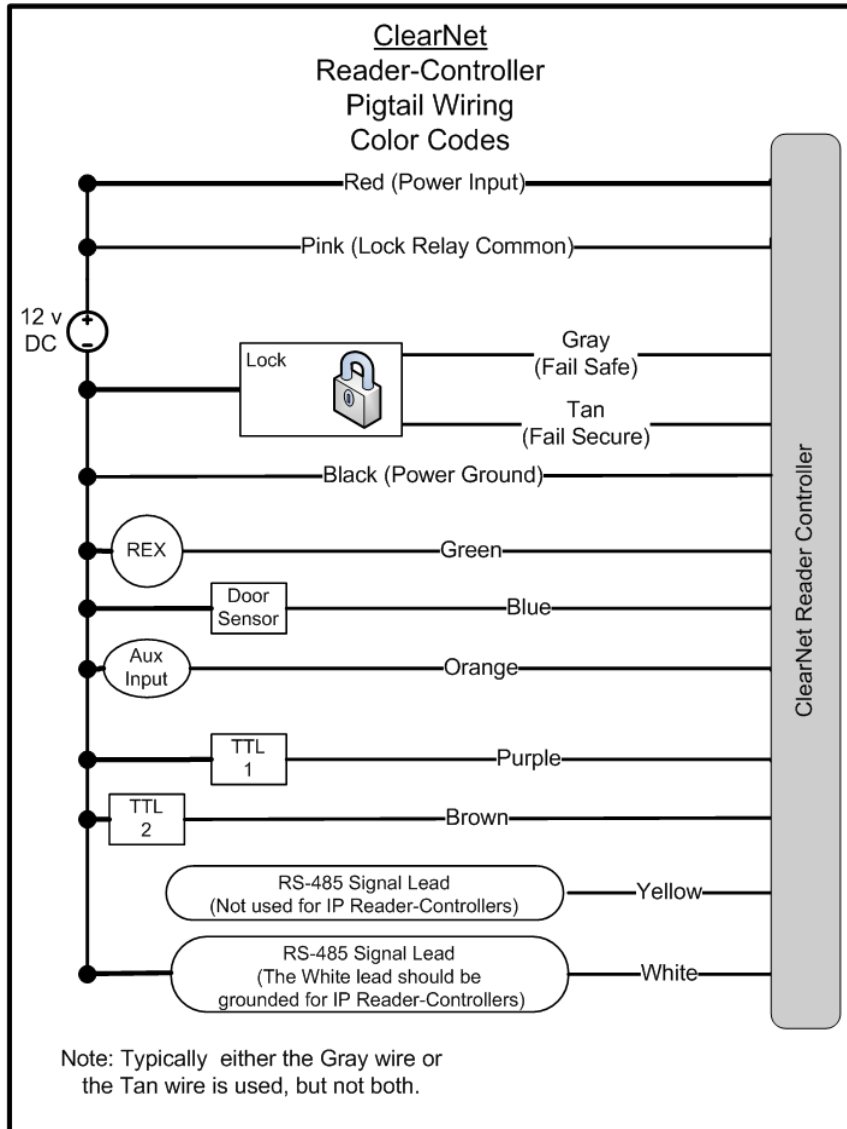


Figure 9

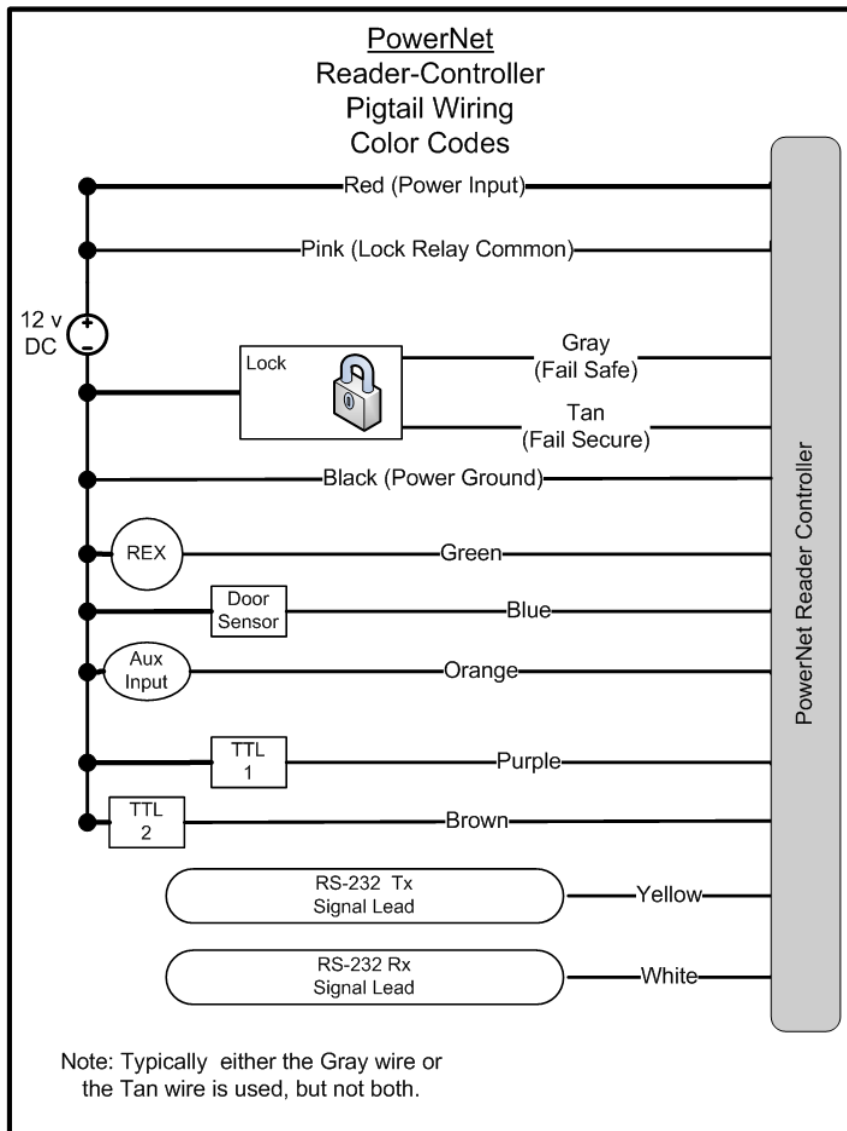


Figure 10

One of the wires is for a door sense switch. Another is for a REX (Request for Exit) signal coming from a switch, infrared sensor or other REX device. A third input signal, called AUX (auxiliary), can be programmed to act in a variety of ways.

The controllers have a lock-control circuit. This circuit consists of a form-C relay, with its “normally open”, “normally closed” and “common” contacts connected to three leads of the pigtail. These pigtail leads can be directly connected to an electronic or magnetic lock to unlock the door when a valid credential is presented.

There are two additional output signals called TTL1 and TTL2 that can be programmed to behave in a variety of ways.

The usage of each lead will be detailed in the next few pages.

2.2.2: WIRING THE DOOR LOCK

Door Lock wiring steps: See **Figure 11**

1. Connect the positive side of the power supply to the **pink (common)** wire on the ISONAS Reader.
2. For a Fail Safe lock, connect the **gray (Normally Closed (NC))** wire on the ISONAS Reader-controller to one lead of the electric lock. For a Fail Secure lock use the Reader's **tan (Normally Open (NO))** wire instead.
3. Wire the other lead of the lock to the **Black** wire on the ISONAS Reader.

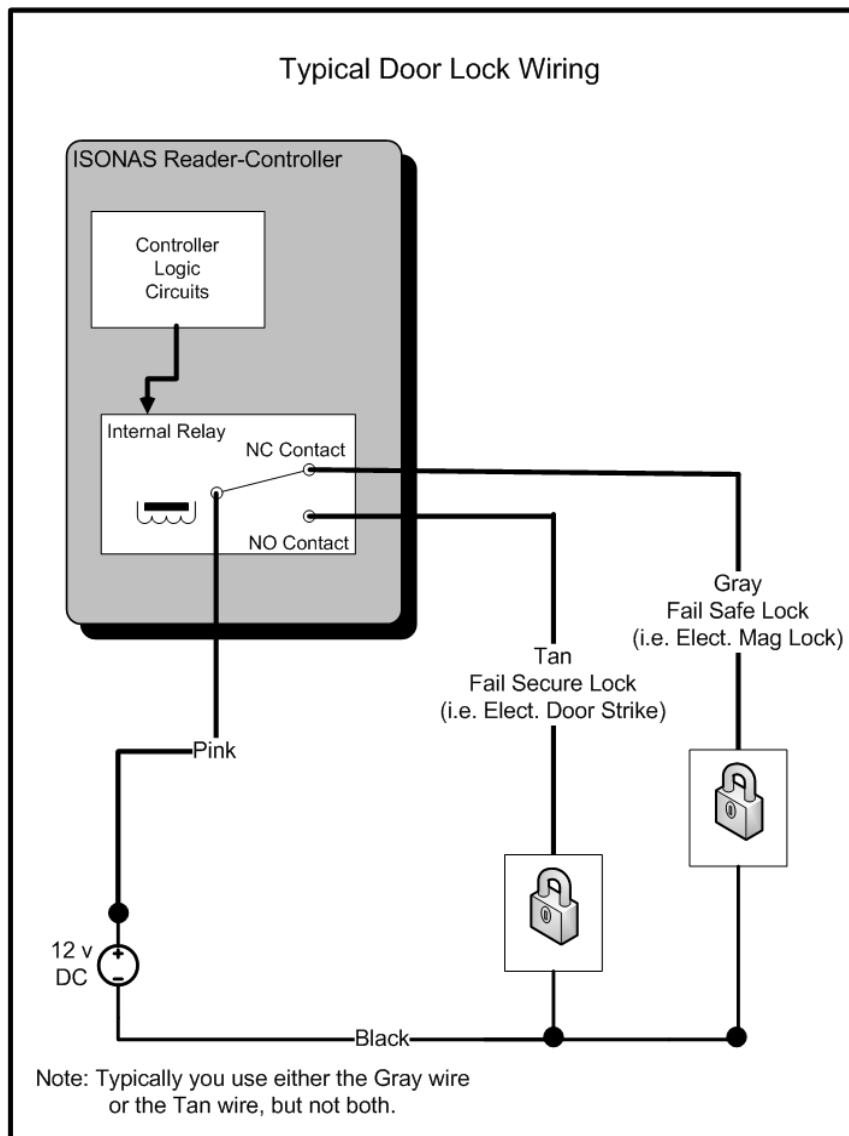


Figure 11

Door Lock wiring steps (PowerNet w/PoE): See **Figure 12**

The PowerNet supports a simplified configuration when PoE is being used to supply the lock's power.

1. Assure that the jumpers are configured as shown:
JP1: No jumpers JP2: Pins 1 to 3.
2. For a Fail Safe lock, connect the **gray (Normally Closed (NC))** wire on the ISONAS Reader-controller to one lead of the electric lock. For a Fail Secure lock use the Reader's **tan (Normally Open (NO))** wire instead.
3. Connect the other lead of the lock to the **black** wire on the ISONAS reader-controller.

Note:
EDK Installation Instructions are listed in the next section

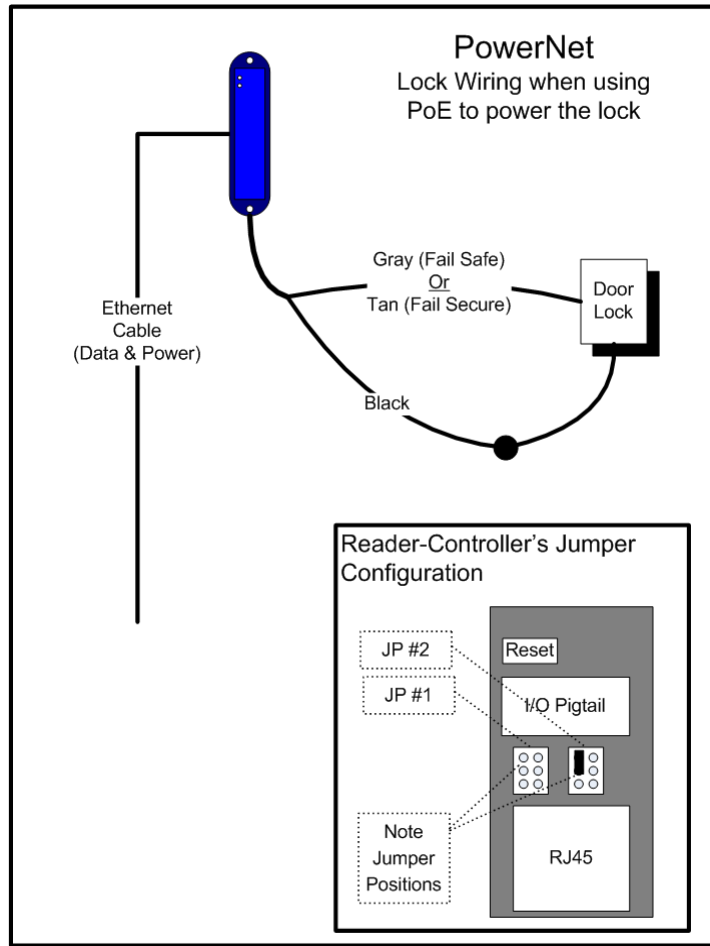


Figure 12

Additional Lock Circuit wiring Notes:

There are many additional ways that the lock-control circuit can be used. Examples include: Gate Controllers, Intelligent locking mechanisms, and Fuel pumps.

The general guidelines for using the Lock-Control Circuit are:

1. Always keep the voltage under 30 volts, and the current under 1 amp.
2. Use the Tan lead, if electrical current flow will unlock the door.
3. Use the Gray lead, if electrical current flow will lock the door.
4. Always use the Pink Lead
 - a. As shown above, if you are using a PowerNet reader-controller and PoE, you may supply 12V power to the lock thru the jumper pins, instead of using the Pink lead.

2.2.3: WIRING THE EXTERIOR DOOR KIT (PowerNet Only)

The PowerNet reader-controller has an optional Exterior Door Kit (EDK), which allows you to isolate the door's lock control circuitry on the secure side of the building. Also, since the EDK is rated for 3 amps of current @ 12 Volts, it can be used in cases where the locking mechanism requires more current than the reader-controller's control circuit is rated for.

Two methods of connecting the EDK are shown

The 1st example shows powering both the lock and the EDK with the Reader-controller's PoE power

See **Figure 13**

Installation Tip:

Jumper Block #1 and #2 should be configured as shown.

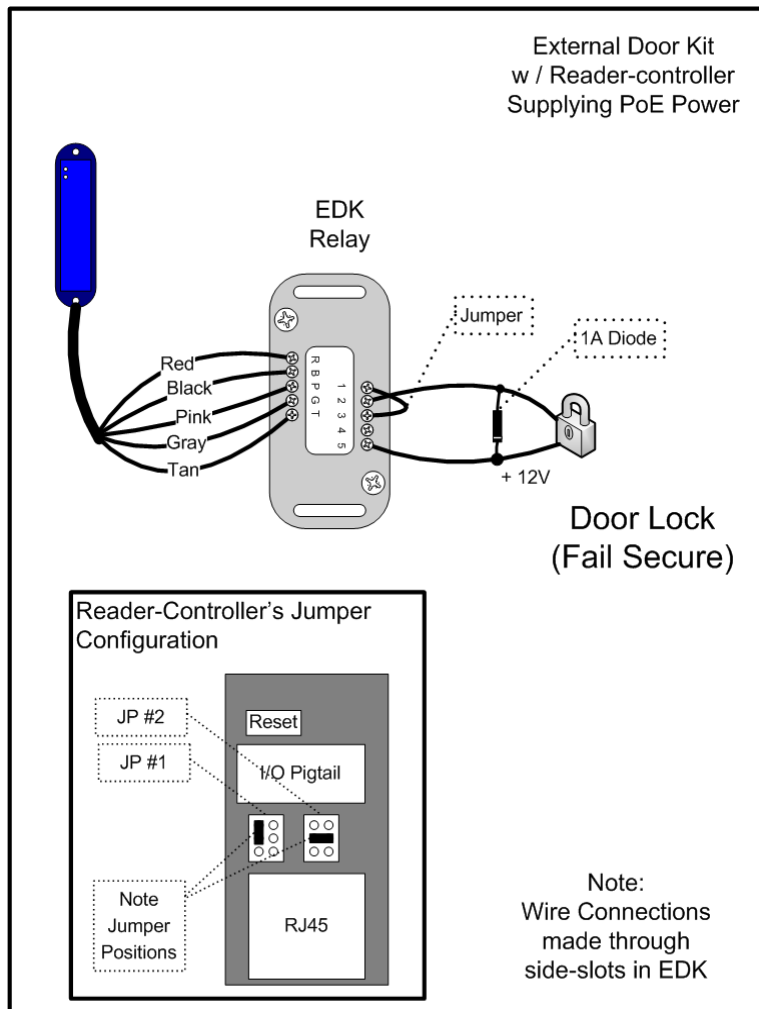


Figure 13

Label	Reader Side Connection	Label	Lock Side Connection
R	Pigtail's Red wire (12 V Input Power)	1	12V Output Power
B	Pigtail's Black wire (Ground)	2	Power Ground
P	Pigtail's Pink wire	3	EDK Relay's Common Contact
G	Pigtail's Gray wire	4	EDK Relay's Normally Closed (NC) contact (Fail-Safe Lock)
T	Pigtail's Tan wire	5	EDK Relay's Normally Open (NO) contact (Fail-Secure Lock)

The 2nd example shows powering the EDK with the Reader-controller's PoE power output, and the lock with an external 24 volt power supply.

See **Figure 14**

Understanding the EDK's LEDs:

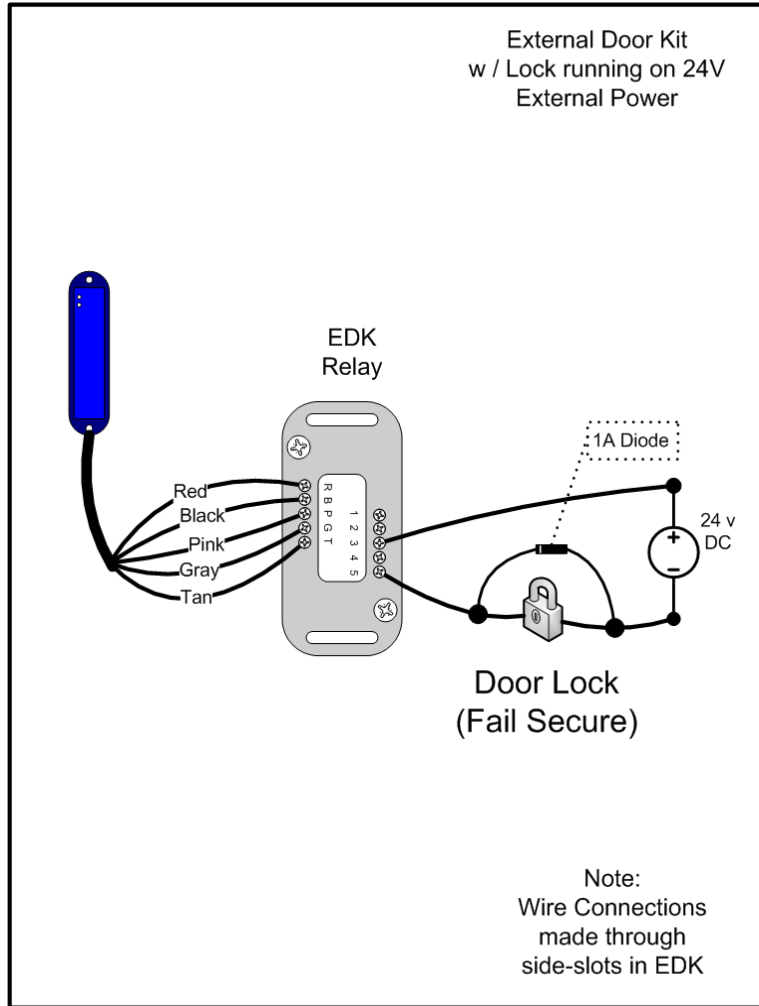
When the EDK Power LED is lite, it indicates that power is available to the EDK.

The EDK communication's LED has three states:

Off: No signal received from the reader-controller.

Red: Signal received from the reader-controller, but no encryption key is available.

Green: Signal received from the reader-controller, and valid encryption key is available.



Installation Tip:
Configure the Jumper Blocks as shown in previous example

Figure 14

Label	Reader Side Connection	Label	Lock Side Connection
R	Pigtail's Red wire (12 V Input Power)	1	Not Used
B	Pigtail's Black wire (Ground)	2	Not Used
P	Pigtail's Pink wire	3	EDK Relay's Common Contact
G	Pigtail's Gray wire	4	EDK Relay's Normally Closed (NC) contact (Fail-Safe Lock)
T	Pigtail's Tan wire	5	EDK Relay's Normally Open (NO) contact (Fail-Secure Lock)

2.2.4: WIRING 2 READERS TO 1 LOCK

If you are wiring both sides of the door to control IN and OUT access, then you will have the special condition of wiring 2 Reader-Controllers to a single locking mechanism.

If there is not a door sensor switch connected to the door, then typically you connect both reader-controllers to the door's lock circuit. For Fail-Secure locks, wire the two reader-controller's lock circuits in-parallel (Lock is connected to both reader-controller's **Tan** leads) For Fail-Safe locks, wire the two reader-controller's lock-circuits in-series (**Gray** lead of Reader #1 connects to **Pink** lead of Reader #2, **Gray** lead of Reader #2 connects to lock).

If there is a door sensor switch connected to the door, then Reader #1 controls the door, and is wired to the door's Door-sense switch. Use the following steps to cause Reader #2 to activate the REX button on Reader #1.

Two Readers & One Lock Wiring Steps: See **Figure 15**

1. Wire reader #1 normally
2. Connect the **tan** (NO) lead from reader #2 to the **Green** (REX) lead on reader #1.
3. Connect the **pink** (common) lead from reader #2 to the **black** (ground) lead on reader #1.

Programming

Reader #1 must be programmed to accepted REX inputs

Installation Tip:

For Figure 15 -- Verify that there are no jumpers installed on Controller #2 's JP 2 jumper block.

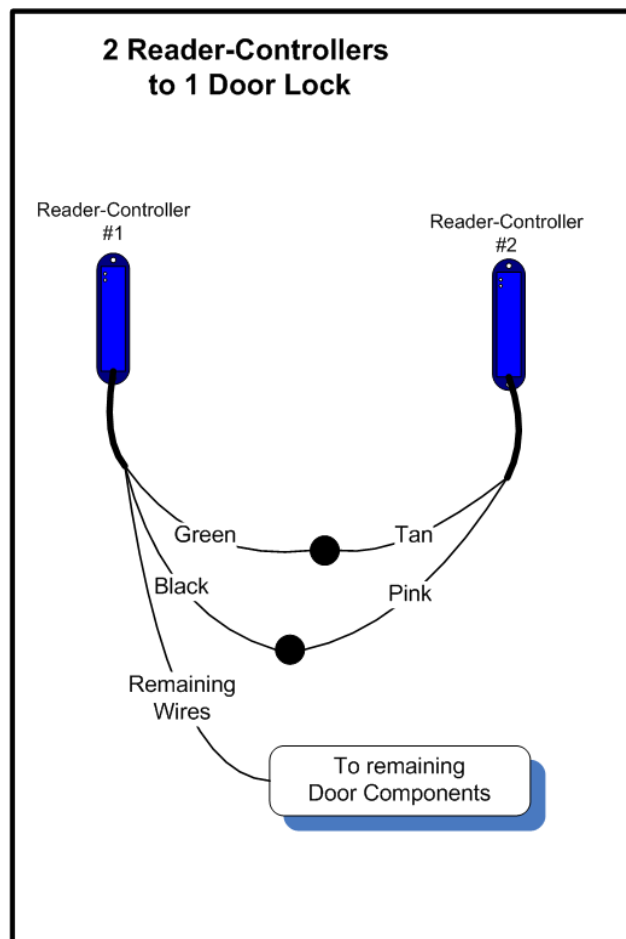


Figure 15

2.2.5: WIRING THE REX BUTTON

The REX (Request for Exit) signal expected by ISONAS Reader-controllers is a **momentary closure**. You can generate this signal with a pushbutton, infrared motion detector, or other simple device. Typically the REX is placed adjacent to the door so that people can press the button and let themselves out the door without setting off the alarm. When pressed, this button tells the ISONAS Reader-controller that someone wishes to pass through the door, and the latch releases. In the ISONAS Crystal software you can configure how the door responds to the REX button.

About REX and AUX

REX and AUX are both normally open inputs. No action is taken until the input is closed.

You must wire this switch through the ISONAS Reader-controller. (See **Figure 16**) First, connect one terminal of the momentary switch to the Reader's **green wire**. Then, connect the switch's other terminal to the Reader's common **ground wire (black)**.

2.2.6: WIRING THE AUX INPUT

The AUX Input is another momentary switch which functions exactly like the REX button. (See **Figure 16**) The AUX Input might be controlled by a relay on an intercom at the door. This would allow the receptionist to unlock the door using the intercom system's functionality.

In the ISONAS Crystal software you can configure how the door responds to the AUX button.

Wiring for the AUX button is similar to that of the REX button. First, connect one terminal of the momentary switch to the Reader's **orange wire**. Then, connect the switch's other terminal to the Reader's common **ground wire (black)**.

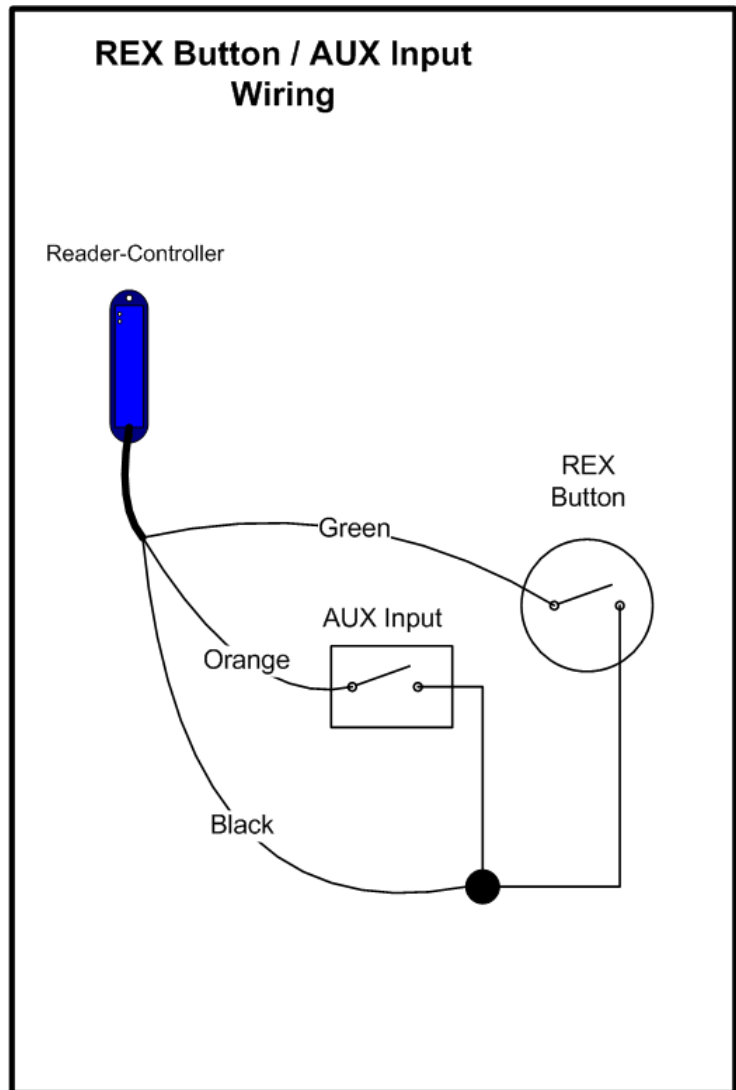


Figure 16

2.2.7: WIRING THE DOOR SENSE

Connecting the ISONAS Reader-controller to a sensor on the door allows our Crystal software to determine whether that door is physically open. This wiring task is similar to wiring the REX or AUX buttons.

First, connect one terminal of the door sensor to the Reader's **blue wire**. Then connect the switch's other terminal to the Reader's common **ground wire (black)**.

Figure 17 shows how to wire the door sensor.

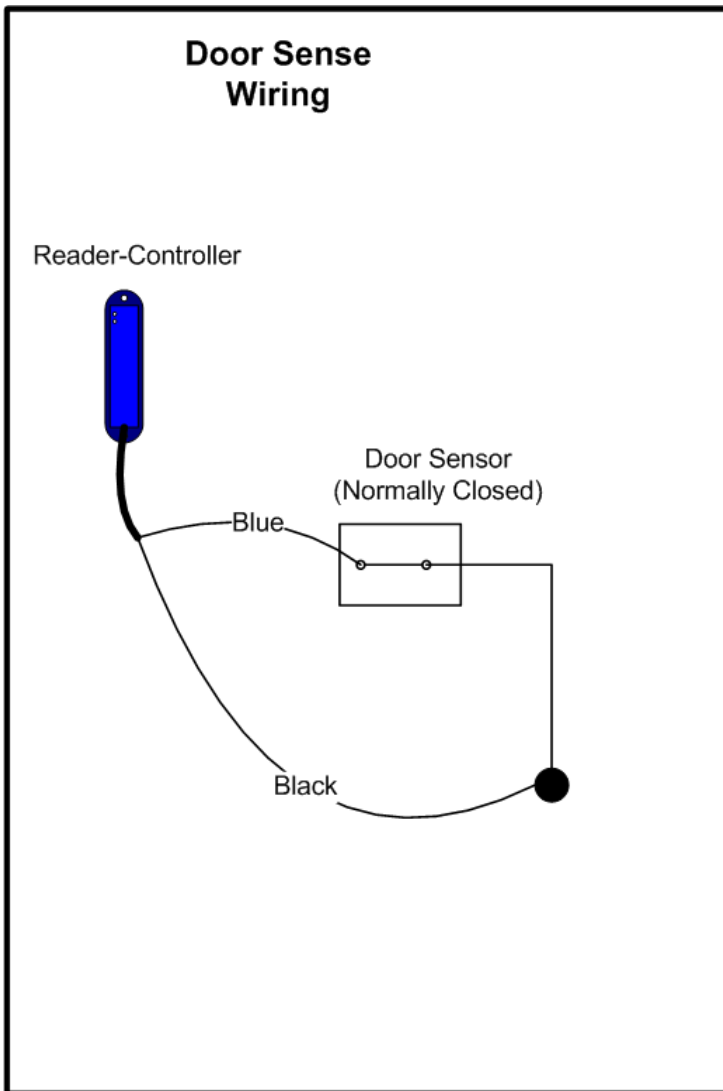


Figure 17

About the Door Sense

The door sense is a normally closed input. No action is taken until the input is opened.

IMPORTANT: If There's No Door Sense Switch

If you choose NOT to install a door sense switch, then you **must permanently ground** the door sense input (blue wire) to the reader's Black wire, so the system will not see the door as "open."

2.2.8: USING THE TTL LEADS

The **TTL1** and **TTL2** leads are logical output leads. In their “normal” state, there is a 5V potential on the leads. When the leads “activate”, this voltage potential is removed.

These leads are typically used to connect to an alarm system. Certain abnormal conditions of the reader-controller can be configured to activate these leads. An example would be having **TTL2** activate when the door is held open too long.

See the Crystal Access Software manual for more information on the usage of these leads.

2.2.9: MANAGING INDUCTIVE LOAD CHALLENGES

Most door latches use a **relay coil** that powers up and down to open and close the door. When this happens, electricity enters the connected circuit. This problem, known as **back EMF**, produces network interference that usually becomes more pronounced when the device is switched off.

Switching off a typical 12 VDC relay coil can produce a back EMF of 300 volts or more. If this relay is switched via an output, that voltage appears across the terminals of the output. The problem gets worse as switching voltage/current rises.

Figure 18 shows a solution. You can virtually eliminate back EMF by installing a **transient suppression device**. Always check that the transient suppressor is correctly rated for the circuit voltage. For optimum performance, the transient suppression device should be installed at the lock or close to the lock. Standard diodes have a stripe-band marking on one side. That side of the diode should be connected to the "+" wire of the lock circuit.

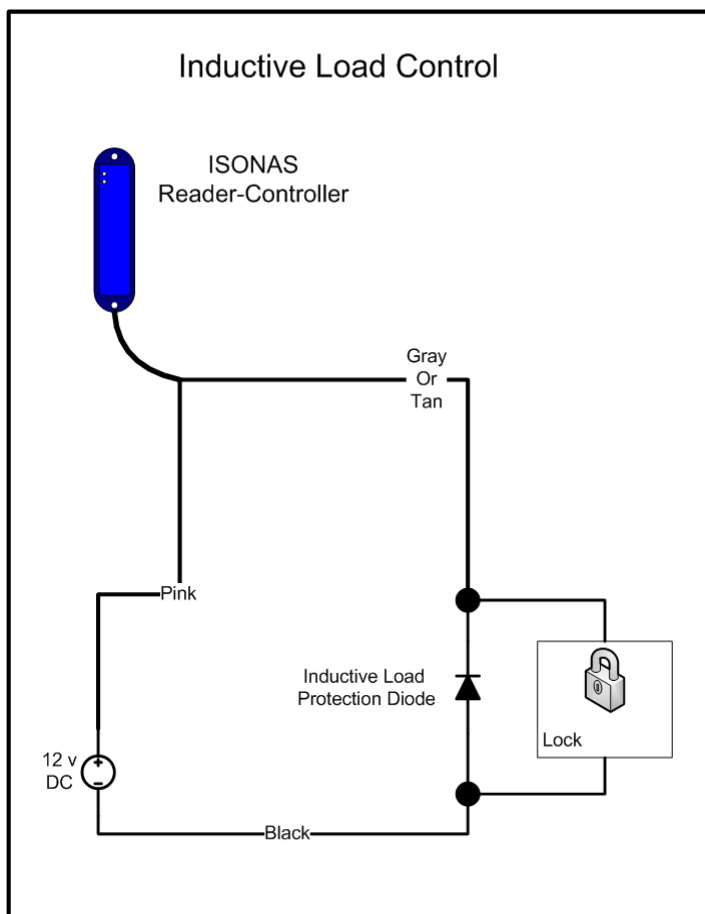


Figure 18

Protect the Digital Output

Which type of transient suppressor should you install? This depends mainly on the type of inductive load being switched. Some locks have Back EMF protection built into the lock itself.

For Back EMF in low-voltage DC applications, a 1N4007 diode will suffice.

However, for protection against other transient voltages (i.e. lightning), we recommend using a fast-switching transient voltage suppressor, such as a bipolar TranZorb.

2.2.10: MANAGING IN-RUSH CURRENT LOADS

Some Magnetic Locks with advanced quick-release circuitry will generate an initial surge of current when the lock is turned on. This surge of current can be 20 times greater than the lock's steady state current requirements. The lock control circuit is rated for 1 amp of current. This in-rush current can greatly exceed that rating, and shorten the useful life of the reader-controller.

Figure 19 shows the solution to this. Installing an in-rush suppressor in the lock circuit will prevent any detrimental affects on the reader-controller.

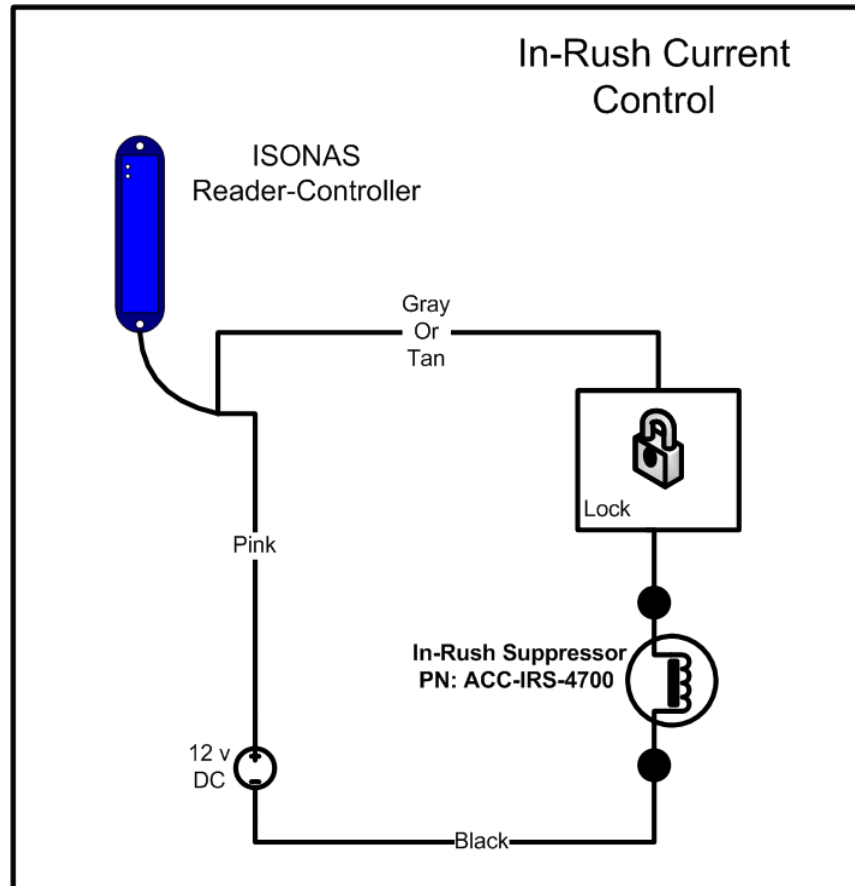


Figure 19

Any installation that is using Magnetic Locks that are equipped with a "quick-release feature" should have this in-rush protection installed.

Other devices who also create this in-rush current include incandescent light bulbs and "capacitive loads". A light bulb's cold resistance is close to 0 ohms, and a discharged capacitor is also a short-circuit when power is initially applied. Any installation which is controlling these types of devices should have the in-rush suppressor installed.

3: CONFIGURING THE READER-CONTROLLER'S COMMUNICATIONS

ISONAS Crystal software communicates to the Reader-controller units over the organization's data network.

3.1: ETHERNET-BASED TCP/IP READER-CONTROLLERS

There are many Ethernet network topology permutations, too many topologies to cover in this guide. Here are two common Ethernet configurations used by ISONAS customers:

- **Direct Server-to-Readers:** This is the simplest type of network connection. ISONAS Crystal software runs on a server/workstation that is connected to a hardwired or wireless Ethernet network. All the Reader-controllers are also directly connected to this network.

Addressing: Each reader's assigned IP address is reachable from the server/workstation. For example, assume that you are installing three Reader-controllers. Two are located in your own Austin Texas office, and 1 is located in the company's Singapore office. Your networking staff gives you three IP addresses to use. 205.155.45.130 and 205.155.45.131 for the Readers that are located in your office. 205.172.37.130 for the reader located in the Singapore office. As long as the network is configured so your workstation can reach all three reader-controllers, there is no difference in configuring or using the three readers.

Here are a couple guidelines to follow to assure that your network's configuration will support the ISONAS access system.

1. The ISONAS reader-controller is a standard "network appliance". Standard TCP/IP rules apply.
2. Each reader-controller requires a static IP address. Typically, the network administrator will define what IP address to use.
3. The reader-controller's IP Address should be a valid IP address for the network-subnet that the reader-controller is physically connected to.
4. If the reader-controller's IP Address must be changed, then the ISONAS tool "Plug and Play" can be used to reset the IP Address. See the Crystal Matrix Software Users Guide for more details on using this tool. Note: Plug and Play requires that the workstation running the Plug and Play application and the reader-controller be physically connected to the same network subnet.
5. The host's IP Address should be a valid IP address for the network-subnet that the host is physically connected to.
6. If the host and reader-controller are on different subnets, then network routers must be in-place to enable TCP/IP communications between the two subnets.
7. One definition of a "Network subnet" is:
 - The set of network connections that can communicate with each other without having to go thru a network router.

Product Options: This network topology supports ISONAS Reader-controller models RC-01-xxx, PRC-001B-IP and PRC-001B-WP.

- **Using Port Forwarding to reach the Readers.** This is common on networks where the available number of IP addresses is limited. It can also be used when the ISONAS software must communicate with Reader-controllers on another site that is behind a network firewall.

As in the first topology, ISONAS Crystal software runs on a server/workstation that is connected to a hardwired or wireless Ethernet network. The readers are connected to a network, but because of the design of the network, the readers can not be directly reached from the workstation/server. A router is between the server/workstation and the readers. The router is configured to implement Port Forwarding. The router will intercept and redirect the IP communications to enable the server/workstation to communicate with the Readers. This configuration allows you to connect many Readers without consuming the primary network's IP address allotment.

Addressing: Each Reader-controller unit is assigned an IP address compatible with its local network (not the server/workstation network). For example, assume the reader's local network uses IP addresses in the range of 192.168.10.2 thru 192.168.10.254. In this example, assume that the Server/workstation has an IP address of 84.117.31.158.

Port Addressing: (please refer to **Figure 20**) Port forwarding is a function of Routers, when using this configuration the ISONAS software does not need the IP address of each reader-controller, it just needs the Port number associated with each reader; however, the software does need the IP address of the *Router*.

Configuring the ISONAS software is easy, you simply define an 'IP address' with the address of the Router (in this example it is 84.117.31.16), then each reader is given a unique Port number assignment under that server.

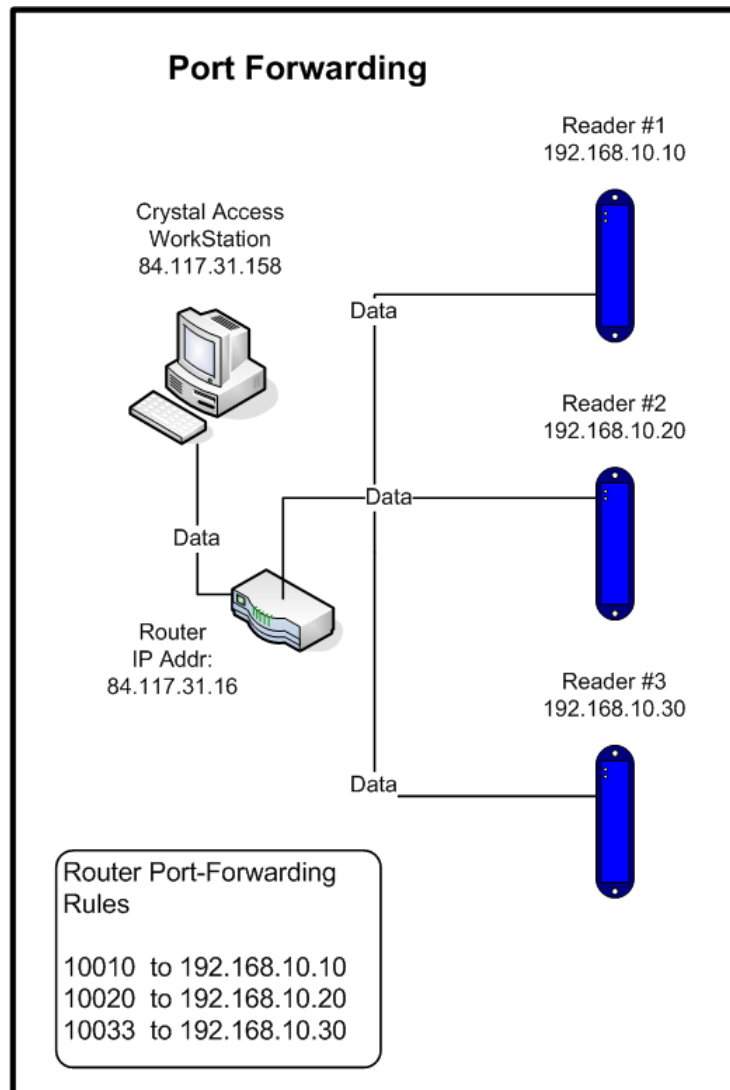
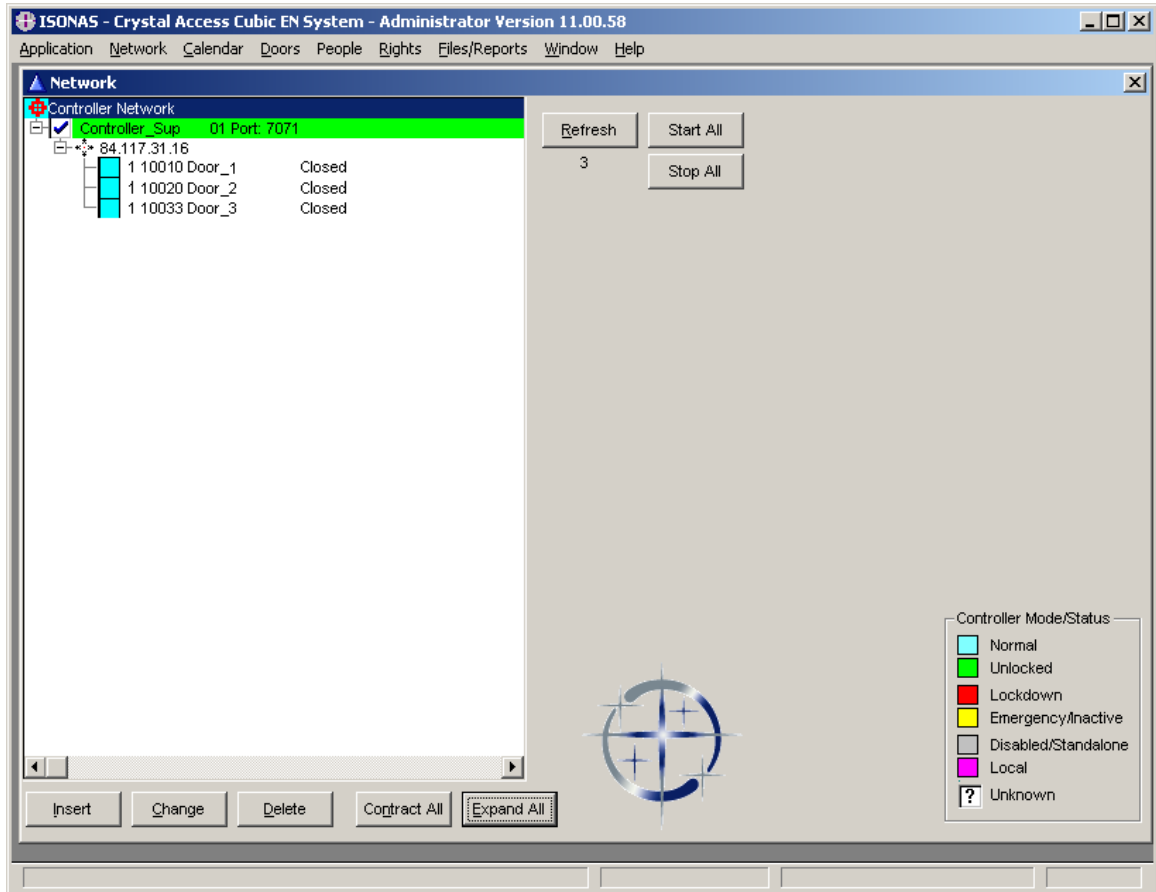


Figure 20

Here is an example of the ISONAS Network screen for the above configuration:



Port Forwarding requires steps outside of the ISONAS software; you must configure your Router to “forward” each port number to exactly one reader. This configuration is specific to the Router that you purchase and will be defined in the vendor’s documentation. Typically the configuration is labeled “port forwarding”; however it is sometimes referred to as “gaming options.”

When using Port Addressing, it will also be necessary to configure each of the Reader-controllers to have the proper IP address and to use the correct Port number. Changing the IP addresses and port number for the reader-controller is easily accomplished using the ISONAS Plug and Play application

The ISONAS Cleartnet reader-controllers incorporate the Lantronix XPort or WiPort internally.

Product Options: This network topology supports ISONAS Reader-controller models PRC-001B-IP and PRC-001B-WP.

3.2: WIRELESS CLEARNET READERS AND NETWORKS

Installing wireless ISONAS TCP/IP Reader-controllers is relatively simple and quick because these devices only require wiring at the door location.

As with any wireless device, you must connect ISONAS wireless Readers to the network via a wireless access point (WAP). Any off-the-shelf WAP will suffice.

Assign a unique (32-character max.) **service set identifier** (SSID, or *network name*) to each WAP. Then, assign that same SSID to all Readers and other wireless devices connected to that particular WAP.

ISONAS wireless Reader-controllers support two **modes of LAN operation**

- **Infrastructure Mode:** In this 802.11 networking framework, devices communicate with each other by first going through an **Access Point**. Wireless devices can communicate with each other or with a wired network. Most corporate wireless LANs operate this way because they must access a wired LAN in order to use services such as file servers or printers.

- **Ad Hoc Mode:** In this 802.11 networking framework, devices or stations communicate directly with each other and they don't need an access point. Ad hoc mode is useful for establishing a network where wireless infrastructure previously did not exist, or where services are not required. This mode is also called *peer-to-peer* or *independent basic service set (IBSS)*.

Most installations of the ISONAS wireless Reader-controllers use the Infrastructure Mode.

3.2.1: SECURITY FOR WIRELESS READERS

You can configure each WAP to use a security **encryption method** which controls whether and how devices connect to that WAP. If you secure a WAP, then all devices connecting to that WAP (including ISONAS wireless Readers) must employ exactly the same encryption method.

ISONAS wireless Readers supports the two most common **types of security encryption:**

- **Wired Equivalent Privacy (WEP):** Designed to offer comparable security to a wired LAN. WEP encrypts data over radio waves so that it is protected as it is transmitted and received. It regulates access to a wireless network based on a computer's hardware-specific MAC. This wireless LAN security protocol is defined in the 802.11b standard.

- **WiFi Protected Access (WPA):** This WiFi standard is more secure than WEP, so if possible, you should purchase and install WAPs which support WPA. This method also works with existing WEP-enabled WiFi products.

Default wireless configuration: When shipped, ISONAS wireless Readers are configured to connect to an SSID named *ISONAS*. Also, security is disabled, so there is no WPA or WEP running. The devices will operate in infrastructure mode unless reconfigured.

Important Security Setup Tip

If you enable WPA or WEP security in your WAP, then you must:

- Enable the same type of encryption in your ISONAS wireless Reader(s).
- Use the exact same encryption keys. Type the information in exactly the same format.

Otherwise you might lose communication to the ISONAS wireless Reader and will not be able to regain it. (In this case, you must return the Reader to ISONAS so we can reset it for you.)

3.2.2: INSTALLING A WIRELESS READER

In the simplest ISONAS wireless installation, you will:

1. Purchase and install a WAP.
2. Configure that WAP with this SSID: *ISONAS*
3. Turn off encryption and run the WAP in infrastructure mode.
4. Configure the WAP and establish a connection to it from your PC.
5. Power on the ISONAS wireless Readers. They will connect to the WAP and become available on the network at the IP address printed on the back of each Reader.

Activate Security: Once you can access the ISONAS Readers over the wireless network, you can activate one of the supported security methods. Security is optional, but we strongly recommend it.

If your WAP supports WPA encryption, then choose that option. It is more secure than WEP. However, if your WAP only supports WEP, all is not lost.

3.3: SECURING MESSAGES ON YOUR NETWORK

You can configure ISONAS Readers and software to *secure each and every message* to and from the Reader using **Advanced Encryption Standard (AES)**.

When you enable AES in both an ISONAS Reader-controller and the Crystal software, every message to and from that Reader-controller is encrypted. Therefore, anyone who manages to hack into your data network would still face a daunting task to decrypt the actual messages to the Reader-controllers. This is a significant ISONAS advantage in protecting Reader-controllers from hackers.

For wireless networks, this is a significant advantage over using just normal WAP security.

Always use AES together with WPA or WEP security. AES secures messages to and from the Reader, but it will not prevent people from hacking into your wireless network. Hackers who penetrate your network would not be able to decrypt ISONAS messages. However, they could access other sensitive areas and information on your network.

For more information:

Web: www.isonas.com **E-mail:** sales@isonas.com

Tel: 800-581-0083 (toll-free) or 303-567-6516 (CO)

Fax: 303-567-6991

ISONAS Headquarters:

6325 Gunpark Drive, Suite 101, Boulder, Colorado 80301 USA