ISONAS
SECURITY SYSTEMS

How to Install an IP-Enabled ISONAS Reader-Controller

Table of Contents

Document Version

Date of Revision	Revision	Author	Description
6/29/2007	2.0	Roger Matsumoto	Updated to include installation information for PowerNet reader-controllers

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])

1.Wire the unit to the door for physical access control.

1.Connect the unit to the data network for communication with the server/workstation 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
Standalone Memory Capacity	2048 Cards/ 250 Events/ 32 Time zones
Visual Indicators	2 LEDs for Normal Operations
Operating Temperatures	-36° To 126° Fahrenheit -20° To 70° 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/Wireless
Inputs/Outputs	3 Inputs/2 TTL Outputs/1 Tamper Output
Relay	1.0 amp @ 30V DC
Standalone Memory Capacity	64000 Cards/ 5000 Events/ 32 Time zones
Visual Indicators	2 LEDs for Normal Operations
Operating Temperatures	-36° To 126° Fahrenheit -20° To 70° 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 processes 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 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) 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.

5) 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.

6) The cables extending from the back of the reader-controller are 36 inches long. Plan for terminating the wiring and CAT 5 cable within that distance of the reader-controller.

7) The wall mounting features required for the reader-controller are shown in the next figures. Electronic version of these figures can be found on the ISONAS website, and can be printed out, for use as life-size drill templates.

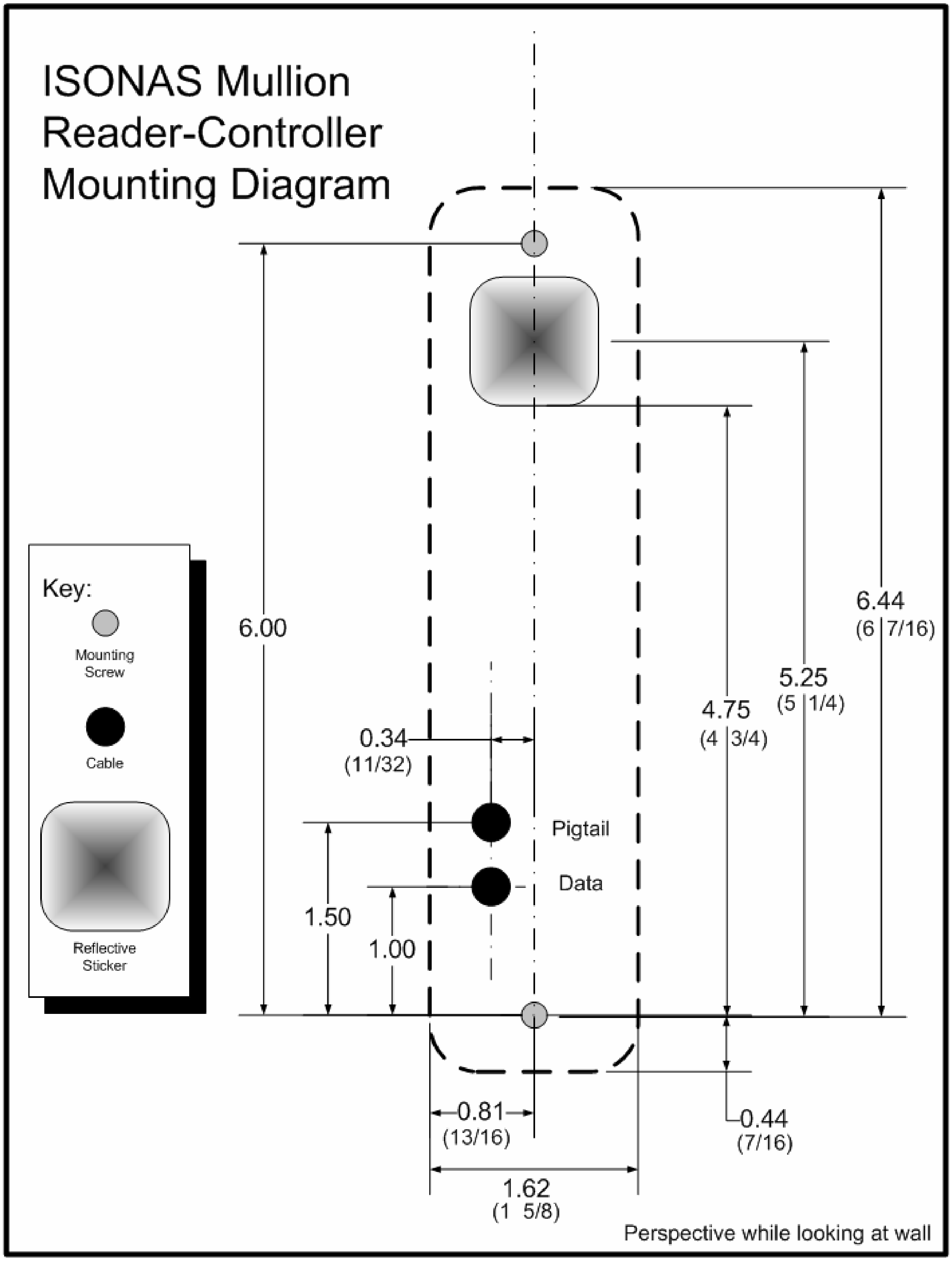


Figure 1 (Mullion Mounting Diagram)

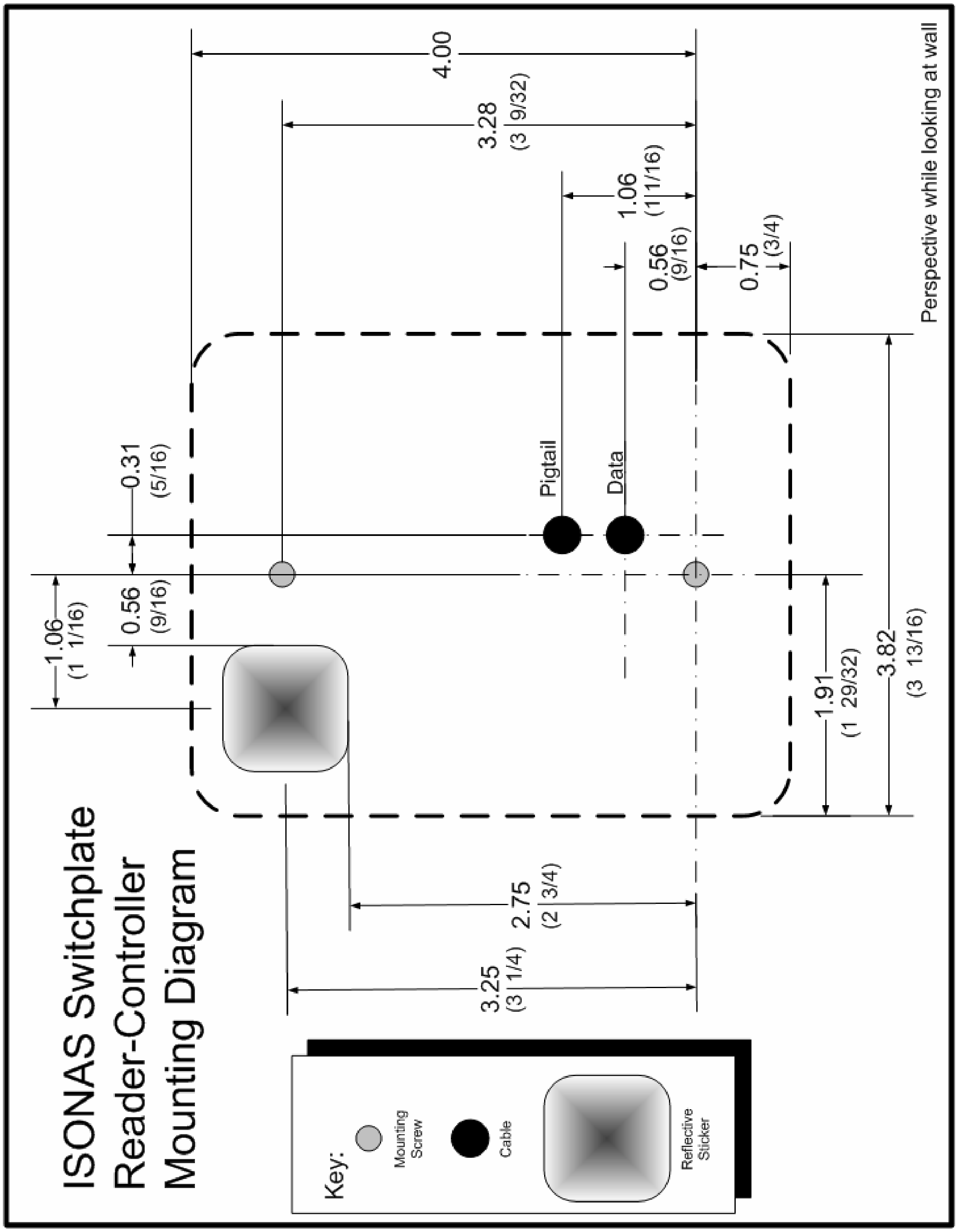


Figure 2 (Switchplate Mounting Diagram)

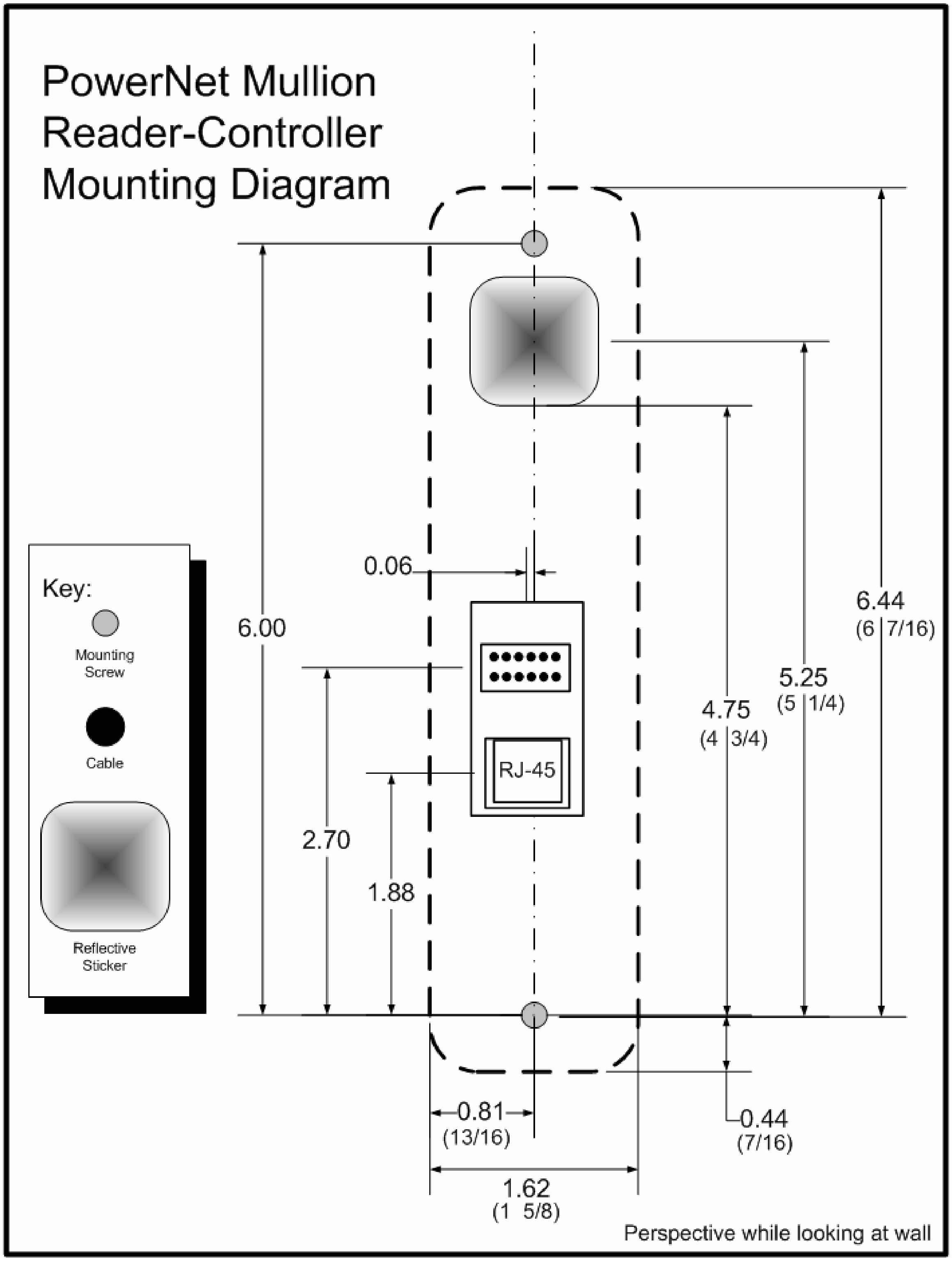


Figure 3 (PowerNet Mullion Mounting Diagram)

1.6 POWERNET READER-CONTROLLER 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 to be used for the lock or other devices at the door location.

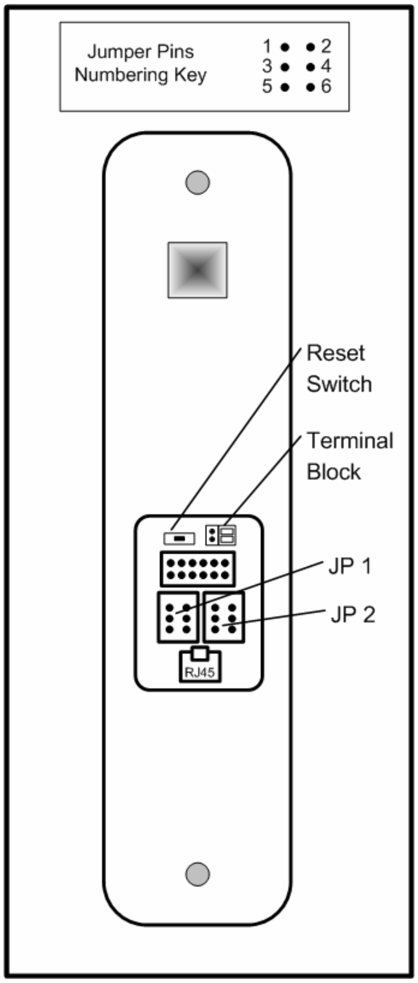


Figure 4
(View of back of PowerNet)

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	
Supply 12VDC to relay common (to power an external lock or other devices). Available only with POE option selected		1 to 3
Connect the "special" serial data signal to the relay common line for use by the lock isolator		4 to 3
Connect GROUND to relay’s common contact.		5 to 3

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

- **Reset CPU:** Press and hold (1 second) the Reset button. Once the Reset Button is released, the Green LAN Status LED should turn off, and then back on.

- **Reset Configuration:** Press and hold the Reset button, until the Green LAN LED turns off (approx 10 seconds). 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 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.

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 12 V 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. Note: PoE can be used with the ClearNet reader, but an external PoE splitter is required.

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.

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 3 shows the typical configuration of equipment at the door.

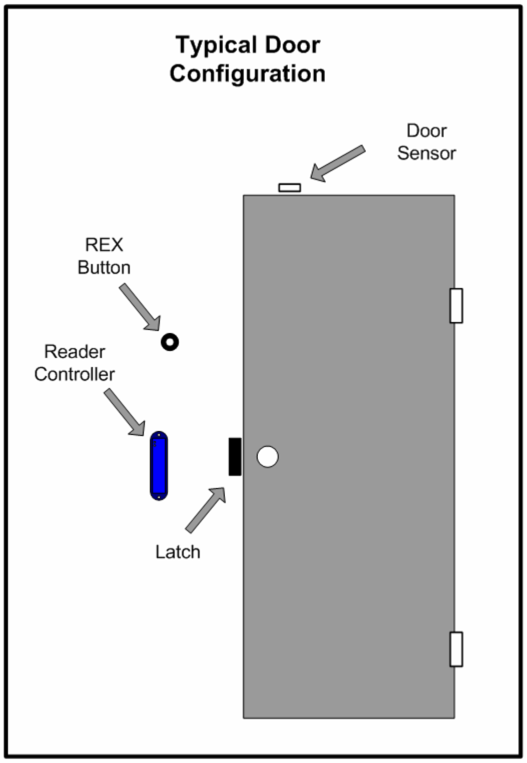


Figure 5

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 mechanism 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 6 (ClearNet) and Figure 7 (PowerNet)**.

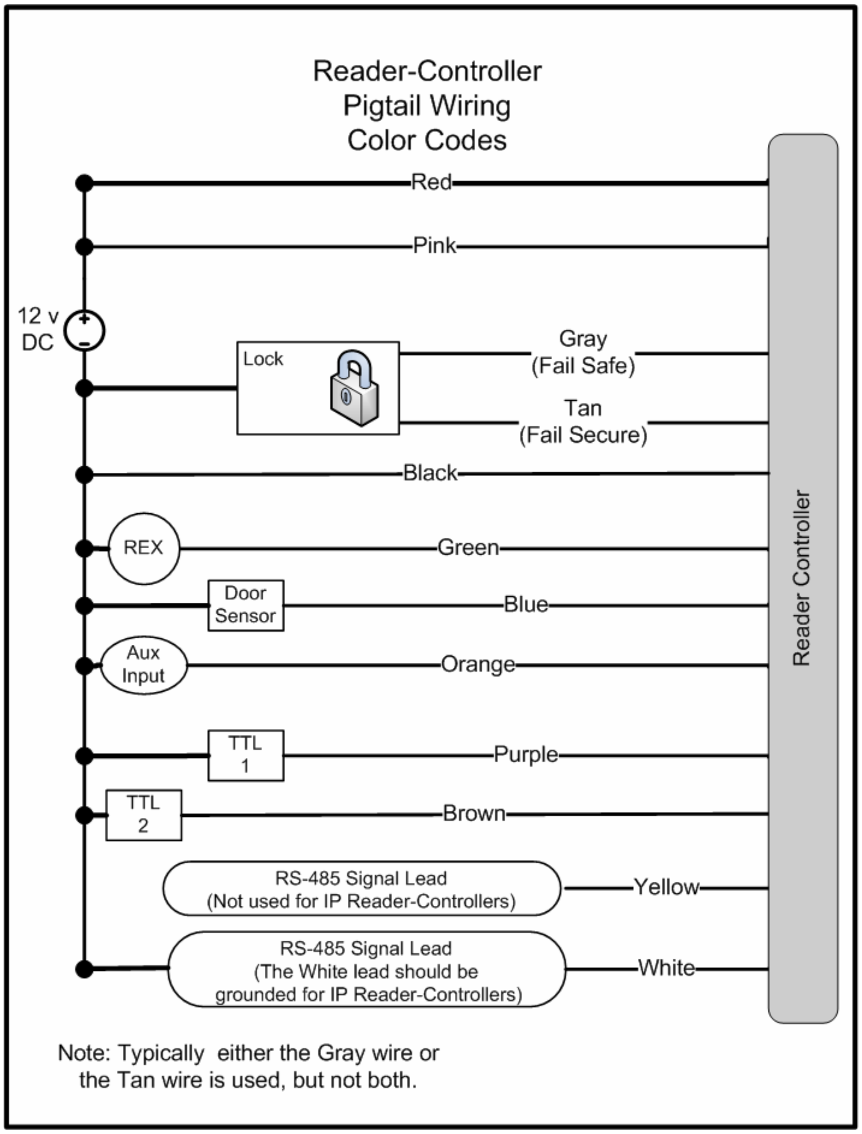


Figure 6

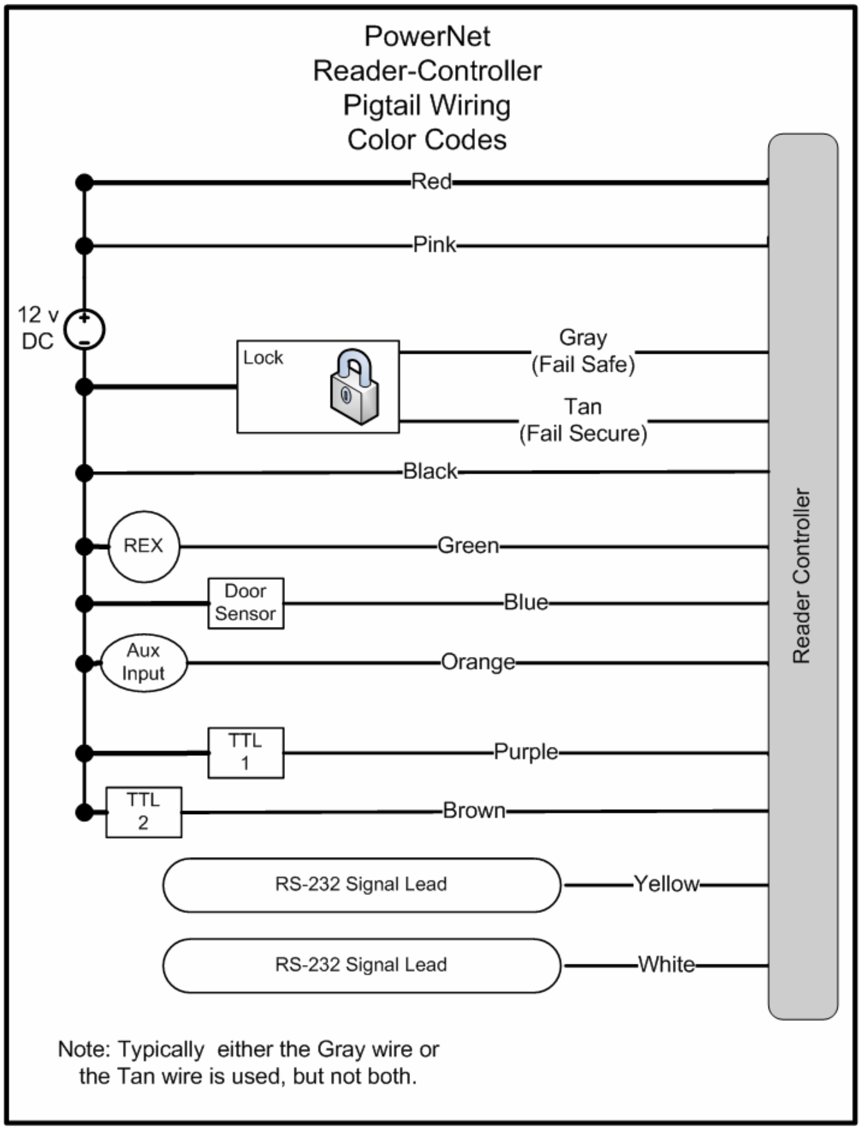


Figure 7

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.

2.2.1: WIRING THE DOOR LOCK

Door Lock wiring steps: See **Figure 8**

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.

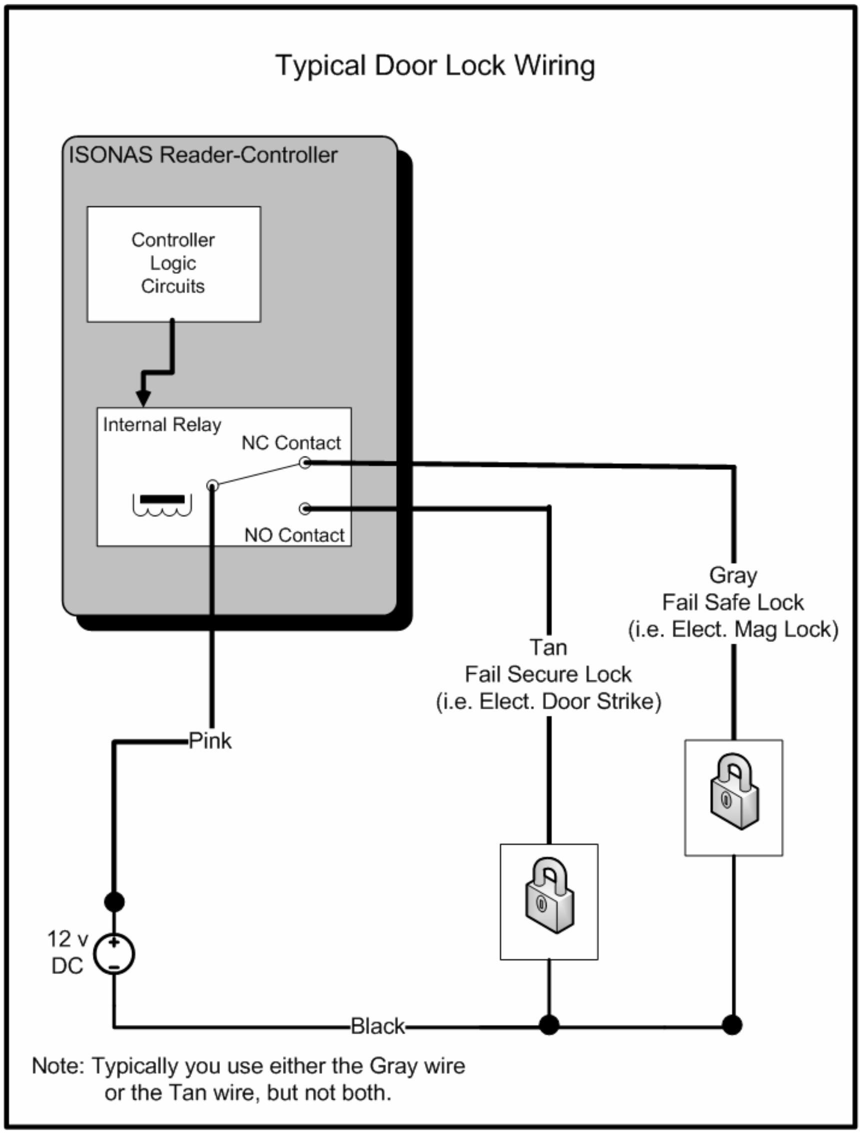


Figure 8

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. 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.

2.2.2: POWER OVER ETHERNET (PoE) OPTION

Figure 9 is an overview of how to use PoE to power both the ISONAS PowerNet Reader-controller and an electronic locking mechanism.

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 supports providing PoE power, then it replaces the PoE Injector.

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.

The PowerNet reader will supply 0.5 amps @12 Volts of power for the lock

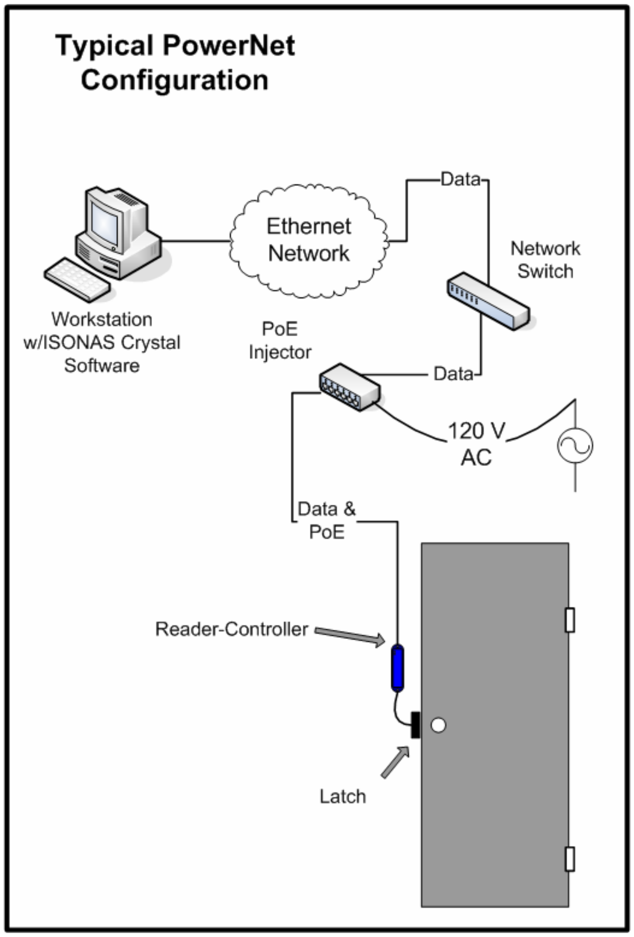


Figure 9

Using Non-PoE Power (PowerNet or ClearNet) Door wiring steps:

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

Lock Voltage:

Typically, the same voltage is used for both the reader-controller and the lock.

If required, the lock can be run at a different voltage. To do this, connect lock's power supply to the Pink lead, the Gray or Tan lead to the lock's 1st lead, and the lock's 2nd lead to the lock's power supply.

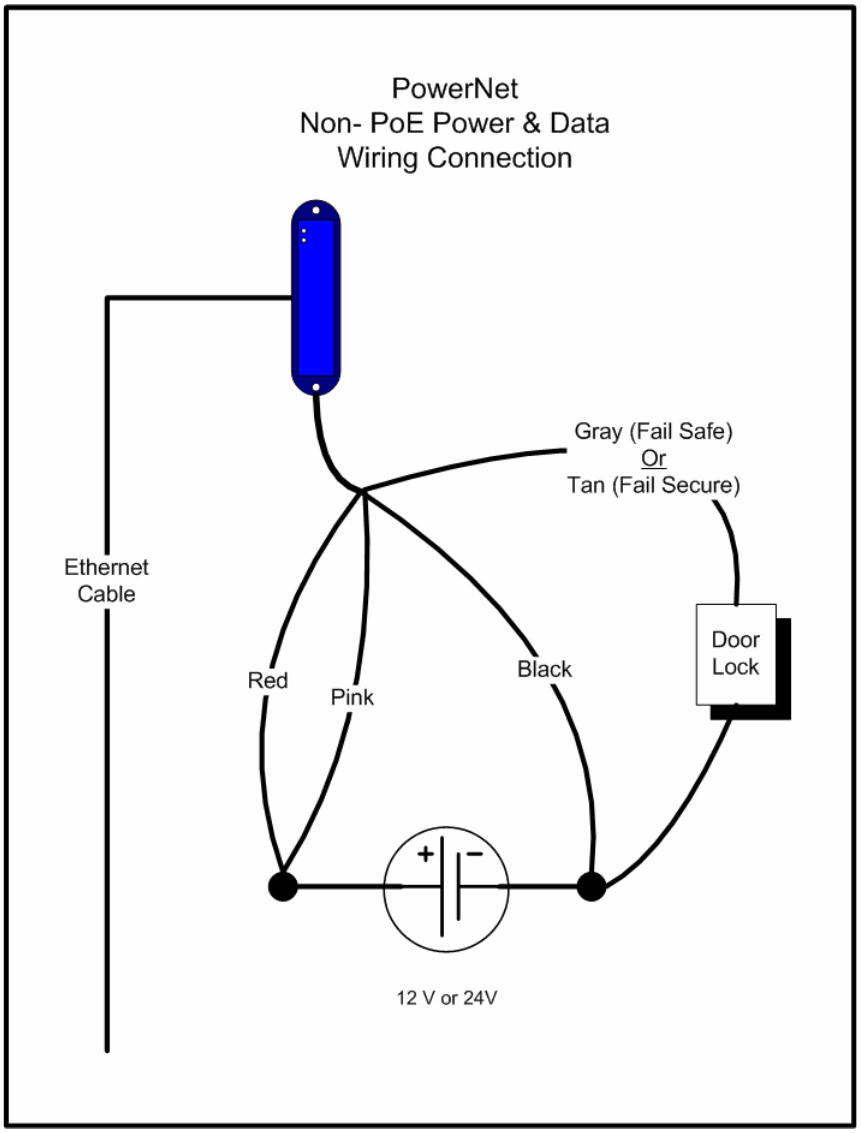


Figure 10

2.2.3: 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**.

Programming

Reader #1 must be programmed to accepted REX inputs

Two Readers & One Lock Wiring Steps: See **Figure 11**

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.

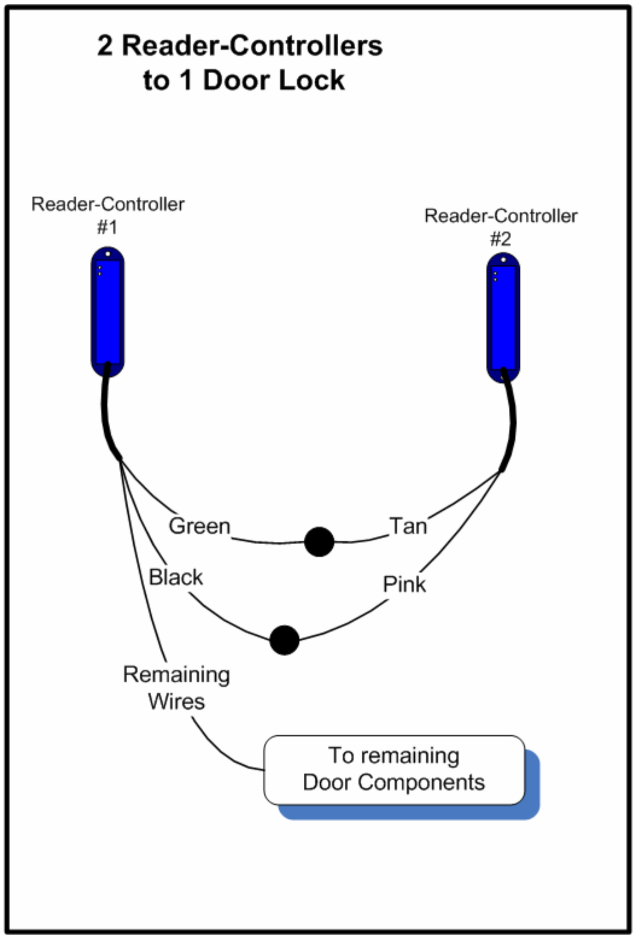


Figure 11

2.2.4: 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 employees 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 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 12**) 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)**.

2.2.5: WIRING THE AUX INPUT

The AUX Input is another momentary switch which functions exactly like the REX button. (See **Figure 12**) 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)**.

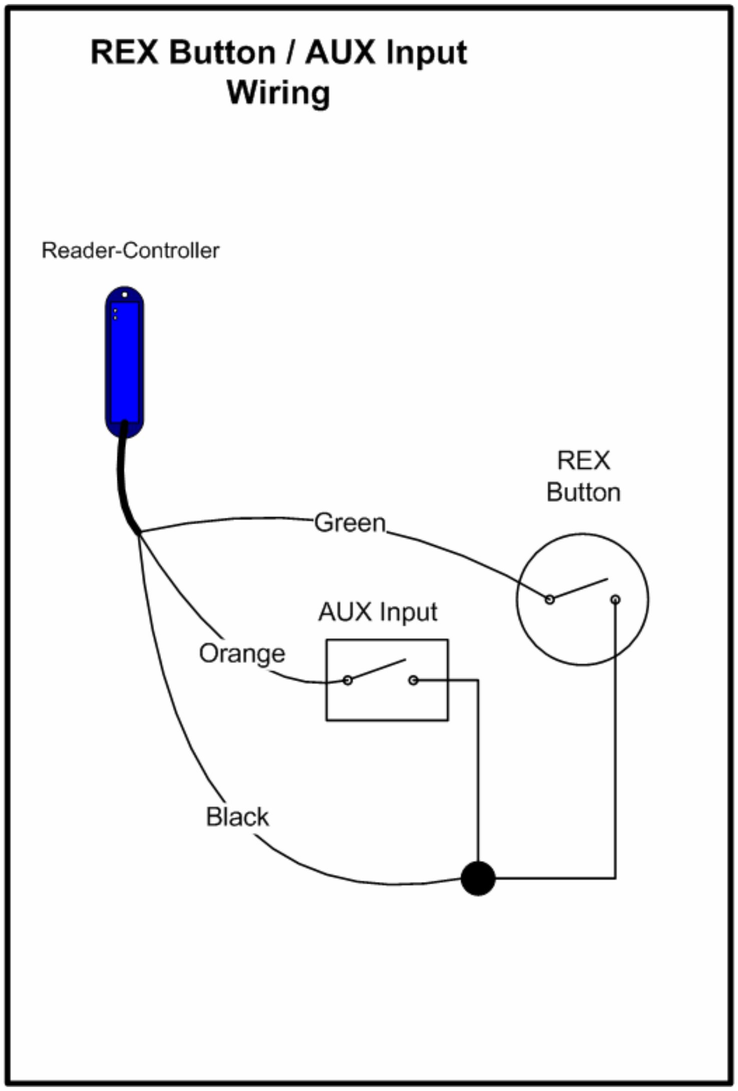


Figure 12

2.2.6: 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 13 shows how to wire the door sensor.

About the Door Sense

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

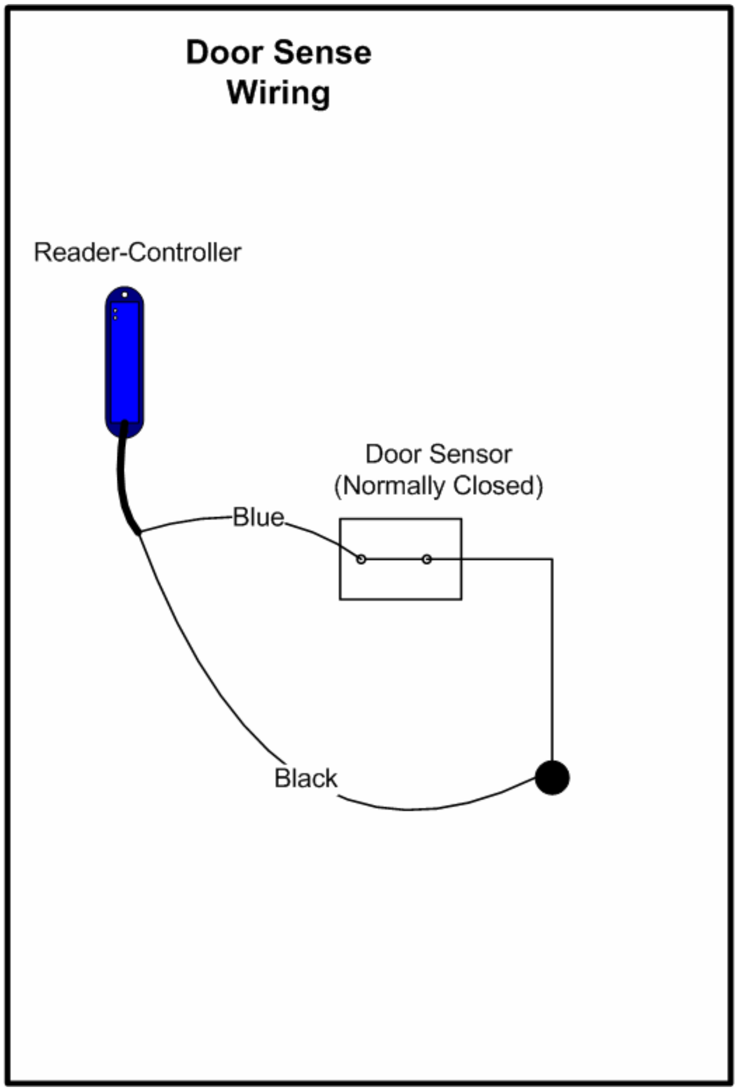


Figure 13

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."

2.2.6: 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.

2.2.7: MANAGING INDUCTIVE LOAD PROBLEMS

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 14 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.

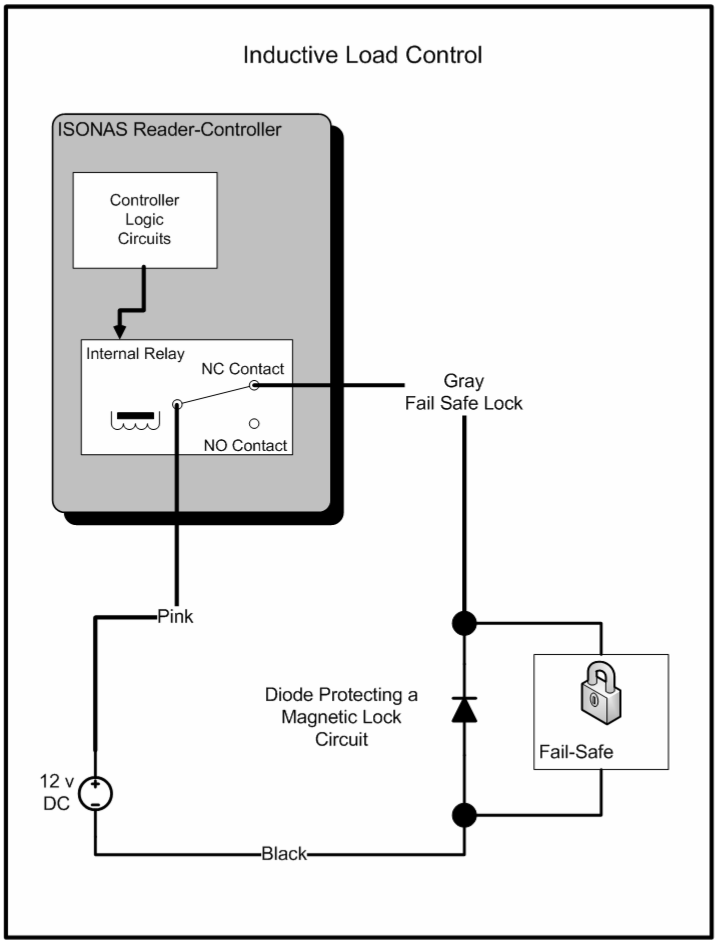


Figure 14

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. lightening), we recommend using a fast-switching transient voltage suppressor, such as a bipolar TranZorb

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 in located in your own Austin Texas office, and 1 is located in the company's Singapore office. Your networking staff gives you three IP address 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.

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

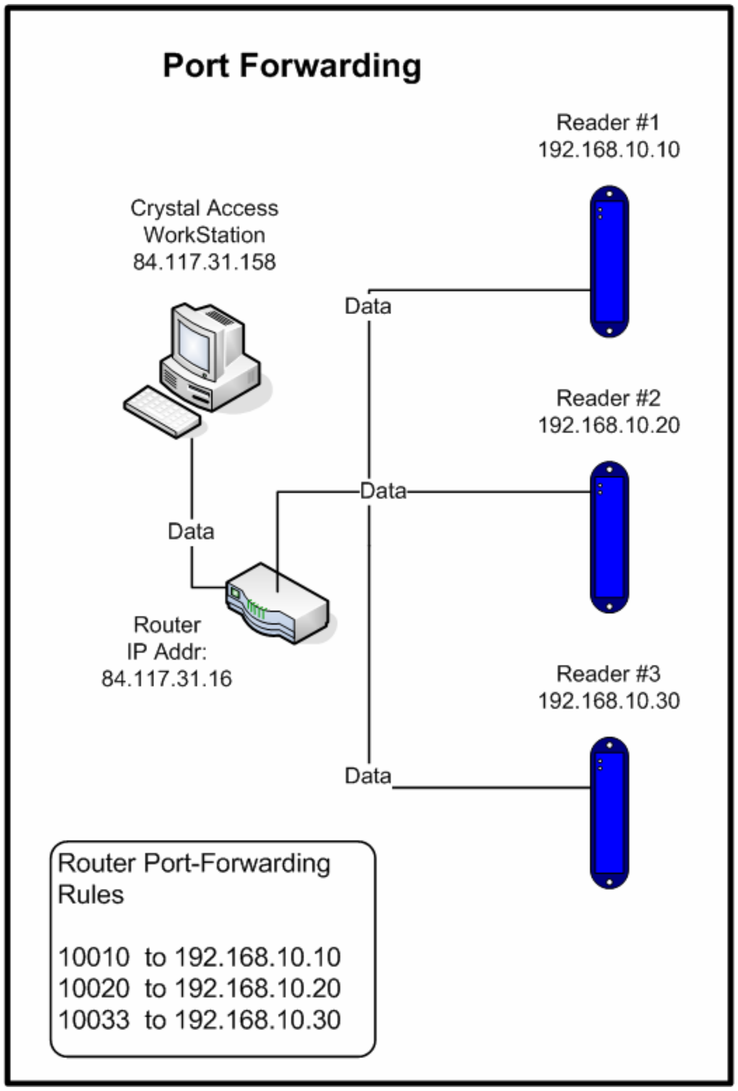
- **Using Port Forwarding to reach the Readers.** This is common on networks where the available number of IP addresses is limited. It can also be used when the ISONAS software must communicate with Reader-controllers on another site that is behind a network firewall.

  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 isolates the access-control traffic to workstation's and router's subnet. It also 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 15**) 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.

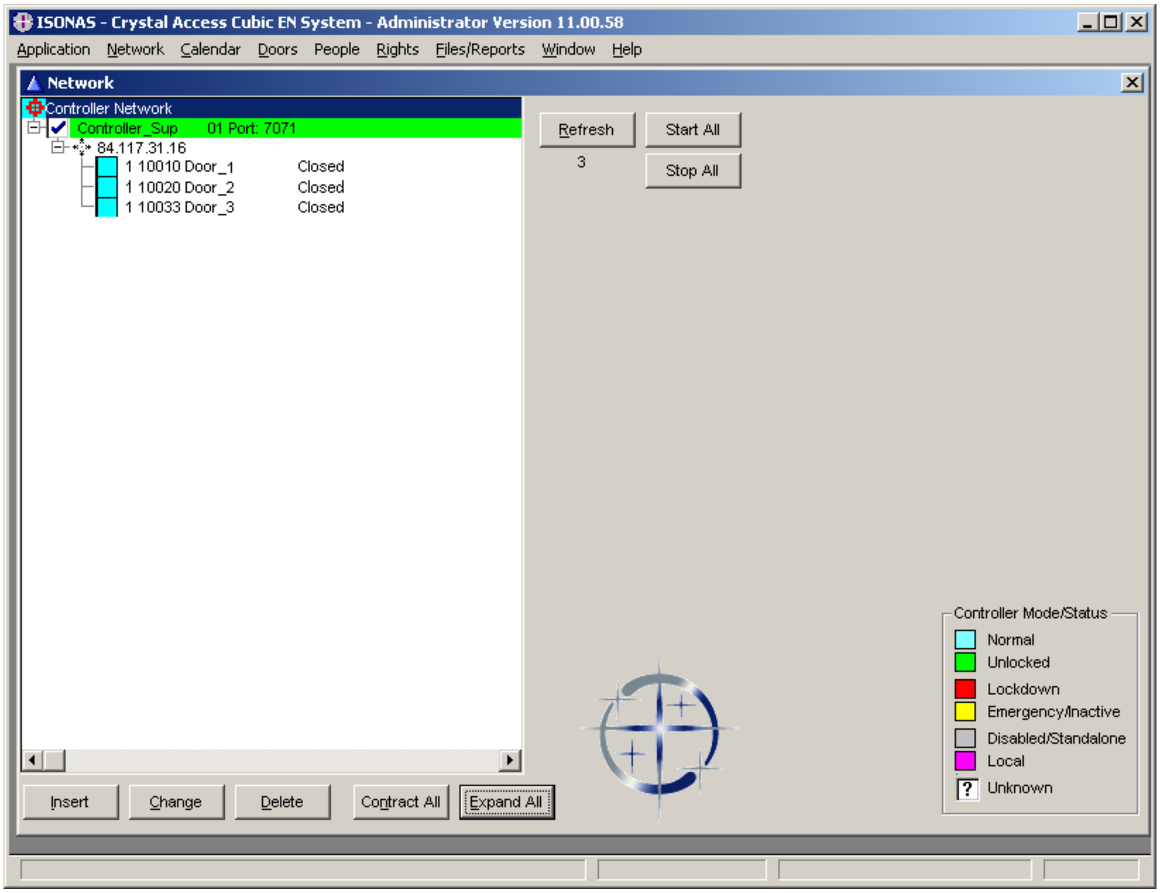


Router Port-Forwarding Rules

10010 to 192.168.10.10
10020 to 192.168.10.20
10033 to 192.168.10.30

Figure 15

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



```
Controller Network
  ✓ Controller_Sup      01 Port: 7071
      84.117.31.16
        1 10010 Door_1          Closed
        1 10020 Door_2          Closed
        1 10033 Door_3          Closed
```

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 Telnet or a WEB based product offered through the Lantronix web site. For additional information please refer to http://www.lantronix.com/support/documentation.html

The ISONAS 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 TCP/IP 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 x106 (toll-free) or 303-567-6516 x106 (CO)

Fax: 303-567-6991

ISONAS Headquarters:

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