Hexicurity System Installation

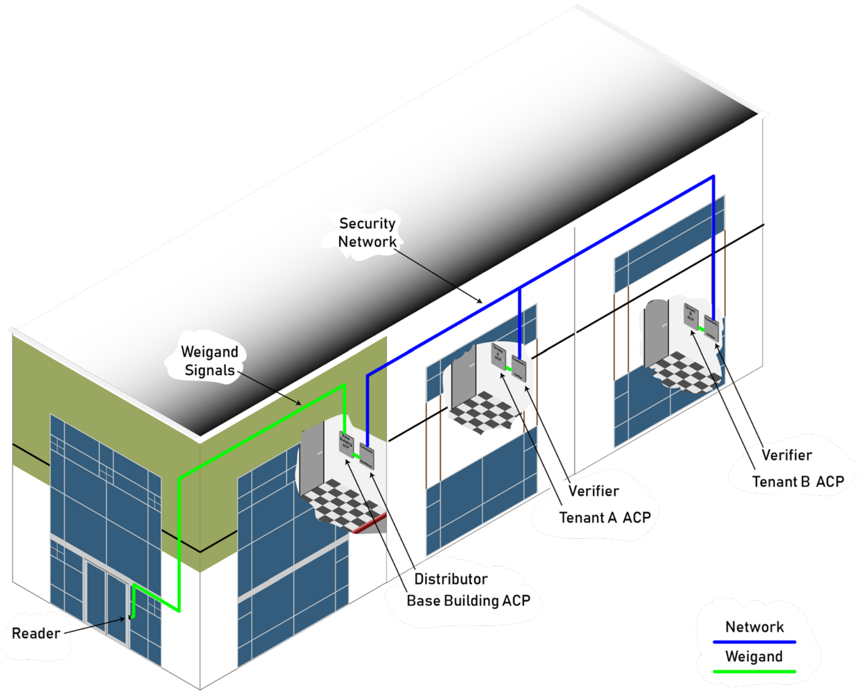
Edition 12, 07/2019

The information contained herein is subject to change without notice.

The only warranties for Hexicurity products and services are set forth in the express warranty statements accompanying such products and services.

Nothing herein should be construed as constituting an additional warranty. Hexicurity shall not be liable for technical or editorial errors or omissions contained herein.

10 9 8 7 6 5 4 3 2 1



Contents

1 Cards and Readers

Cards

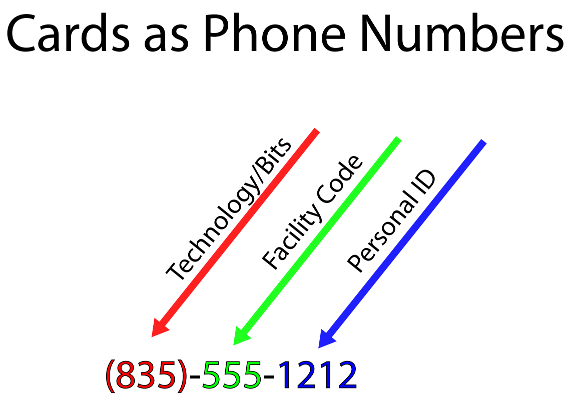
Access cards have three numbers: external, internal, and facility code. The external number is the one visible on the card, allowing identification the card without a card reader. The internal number is the electronic serial number embedded in the card that is read by the card reader and internally tracked by the computer. Both numbers are permanent and determined when the card is manufactured. The third number associated with the card is also an electronic internal number only seen by the card reader, the facility code. This number identifies the card as belonging to your system.

When the card reader (and computer) sees a card being read it first checks the facility code to be sure it is yours, then the internal number is read. The internal number is used to look up the access, name and external number assigned to the card.

Electronically cards have several characteristics. The technology could be Proximity, MiFare, iClass, or Wiegand. The number of bits in the card with 26 being the most common and 35 bits for HID Fortune 1000 cards. The facility code distinguishes one company's cards from another. Finally, the personal identification number makes the card unique within the company.

Cards as Phone Numbers

A method of visualizing the pieces that make a card unique is to look at it as a phone number.



Where the area code is the technology/number of bits, the exchange is the facility code and finally the last four digits or line number is the personal ID number.

For example assume your company uses the HID Fortune 1000 card. We will represent that 35 bit card by area code 835. The company's facility code is 555 and your card is number 1212. Now a company in your same building also uses the Fortune 1000 card uses facility code 212. Your friend who works for that company carries card number 1212. So even though the technology is the same and the personal ID is the same the two cards differ because the facility codes are different.

Using our analogy the two phone numbers 835-555-1212 and 835-212-1212 are similar but they are not the same phone number. That is why your card won't work in your friend's company and his card won't work for your doors.

How the bits are used

The basic card has 26 bits (ones or zeros). The facility code takes eight bits and can range from 0 to 255. The internal number uses sixteen bits and ranges from 0 to 65,535. The remaining two bits are used for error detection. The next most common format is the "Corporate 1000" format which uses thirty five bits.

Multiple Technology Cards

Multiple technology cards have been developed to allow seamless administration of proximity, iClass, MiFare, AVI and Wiegand cards within your system. All card technologies are administered with the same tools and the same methods. Each of the technologies within the card is called a "load". So when the phrase "prox load" or "iClass load" is used we are referring to that specific portion of the overall card.

Multiple Technology Readers

Readers are available which will read several different technologies. For example, a single reader is available to read both iClass and 125 KHz Prox cards. These readers offer the building owner the most flexibility. Since the wiring is the same for standard technology readers, retrofitting a building equipped with a single technology reader can be done at minimal cost.

Multiple meets Multiple

What if a multiple technology card is presented to a multiple technology reader? We posed this question to HID, a major manufacturer of cards and readers. The head of engineering stated that either card load may be read. In planning and implementation for a tenant with a multiple technology card, all card loads should be considered as readable.

Summary

This section covers the internal, external, and facility code numbers. Corporate 1000, multiple technology cards, multiple technology readers and card loads are discussed.

2 System Planning

Network

The TransVerify system is composed of two types of network appliances, the Verifier and the Distributor.

The planning of the network is critical to trouble free operation of your system. This chapter covers the basics of planning a small network and will teach how to configure the three workhorses of networking; the IP address, the Mask, and the Gateway.

Simplest Example

In the early days of civilization towns grew up and needed a method to share information. Thus the town crier was born, and everyone heard every message. Later, messengers would deliver messages only to intended recipients within the village.

A flat network is like that village. Initially we had hubs which like the town crier delivered every message to everyone on the network. Later switches were invented which only delivered messages to the intended recipient. All IP addresses are visible to each other. For a network with less than sixteen devices a flat network will serve. Just purchase a single switch with an adequate number of ports and plug your devices into it. Common technology today is a switch which relays only the messages a device might need to see. This is known as a Layer 2 switch, and a hub is considered a Layer 1 switch.

If your system is its own network this will serve for the short term. The problem is growth. Even a designated purpose network will exhibit surprising growth in a short period of time. Consider the industry trends in IP cameras and intercoms which will produce amazing performance at a lower cost.

Therefore it is our recommendation that your plan for network growth. If you don't plan for growth you will in short order have a "fur ball" network, which are hard to maintain and build on.

Routed Networks

Consider for a moment a small friendly neighborhood. There is a child who will happily run letters between the homes in the neighborhood. The child's mother has laid down some specific rules on how far he can go to deliver a message. If the address on the letter is across town then the child must put the letter in the mailbox.

In the world of networking that child is a router, all the houses in the neighborhood are on the same subnet, and the mailbox is the gateway. The mask is the rules that his mother laid down for how far he can go to deliver a message.

The introduction of routers or Layer 3 switching requires the gateway and mask be configured in addition to the IP address. All the devices plugged into a specific router have identical gateway and mask settings. The gateway is typically the IP address of the router. The mask tells the device if another is a neighbor. If a device is a neighbor then it is typically attached to the same switch. These devices are said to be on the same subnet. If a device is not on the same subnet then it be routed by the switch to another neighborhood.

Masks

Masks are comparable to the rules the child's mother laid down. They describe for the devices who are their neighbors and who's messages must be routed.

Take the simplest and most common mask:

255.255.255.0.

The number series, called octets, or the numbers between the periods define the neighborhood.

This example tells the devices that if the first three octets are the same they are local. So for our mask we have three 255 octets and one 0 octet. For IP 4 networks four octets are used. So an IP address of 10.1.0.7 has four octets; 10, 1, 0 and 7. So if we combine the mask and our example IP address we find that any device with the same first three octets 10.1.0 are in the same neighborhood or as the network geeks call it, on the same subnet.

Masks are sometimes defined by the number of leading one bits in the mask. As each octet is 8 bits, a mask of 255.255.255.0 is sometimes referred to as /24. Similarly if you have a mask of 255.0.0.0 that is referred to as /8. This notation carries the name CIDR, or Classless Inter-Domain Routing. Both notations mean the same thing, the CIDR notation is shorter. We use the CIDR notation on some of our setup screens.

Our masks are entered using the number of bits in the host part. This is simply 32 less the CIDR number. An appendix table lists some of the more common masks in all three notations.

Gateway

The routing switch or router has an IP address, typically at one of the extreme ends of the IP range. For our example: 10.1.0.1 or 10.1.0.254. The IP addresses ending in 0 and 255 have a special purpose so we don't use them. The other IP address we are free to use for our devices so the 252 IP addresses from 10.1.0.2 through 10.1.0.253 are available.

The IP address of the router is the gateway. So returning to our paradigm, the router is the gateway.

Planning

We recommend using the physical layout of your building to logically define your "neighborhoods" or subnets. In a campus setting the buildings themselves will be logical neighborhoods. In a high rise, perhaps the elevator rises will provide those logical subnets. If we use a campus setting with three buildings A, B, and C we can define three subnets all with a mask of 255.255.255.0, The routers IP addresses will be 10.1.0.1, 10.1.1.1, and 10.1.2.1. As an example, the IP address of 10.1.2.7 will be the sixth available IP address in building C.

Reality

In reality most properties have existing networks used for business purposes. These networks have been planned and your security devices will simply attach to their network. You will need to obtain a Static IP address, mask, and gateway for each of your devices. We strongly encourage you to have the network administrators give security their own VLAN or Virtual Local Area Network which logically separates your devices from the other business and desktop devices. Properly implemented a VLAN presents a formidable barrier to someone on the business network or outsiders from hacking the security subnet.

The best method is to employ encription techniques on the network switch. Major network equipement manufacturers offer this as an option.

If the network is congested a valuble technique is to mark the ports used by the Verifiers and Distributors as VOIP or Voice Over IP in the network switch setups. This works best when all of the network switches are the same manufacture and model. What this setting does is mark all traffic in and out of these ports as time sensitive giving them priority routing. The network load from our devices is minimal and will not cause issues.

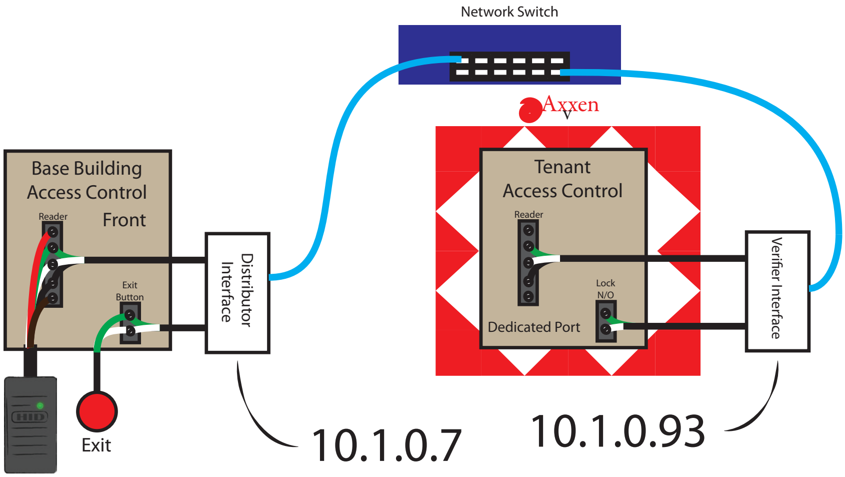
3 System Scenarios

Potential System Layouts

Your project will follow one of the four potential layouts: simple, multiple base building doors, multiple tenants, or multiple doors and tenants.

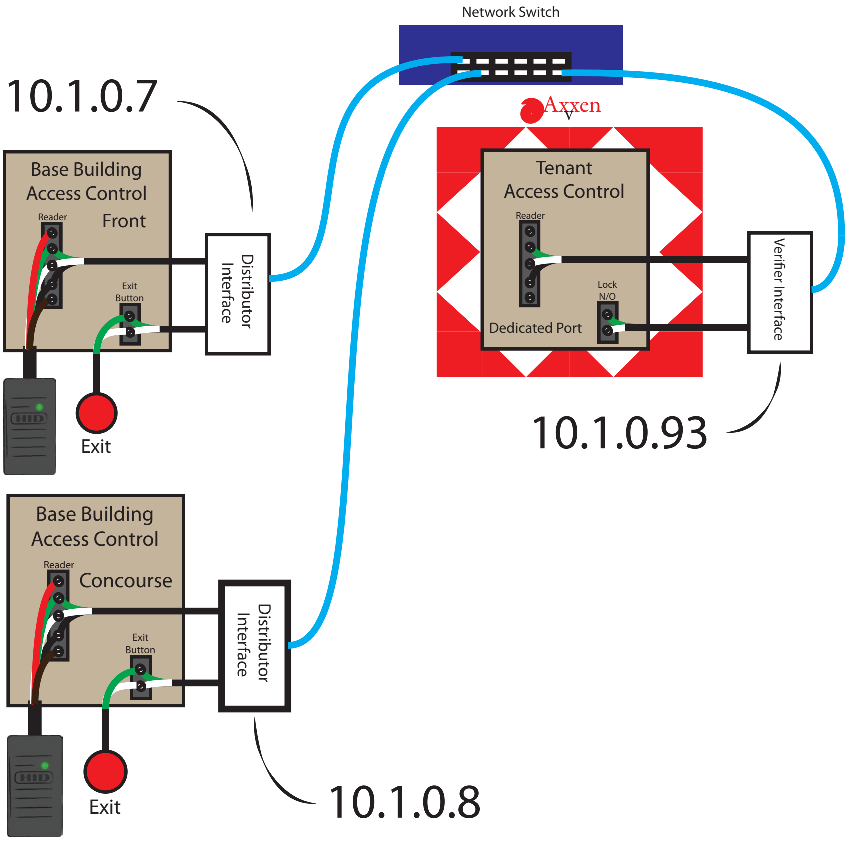
Simple

The simplest layout is one shared door and one tenant. This layout requires one Distributor for the shared door and one Verifier for the tenant system. Each device must have its own IP address, one for the Distributor and one for the Verifier. The Distributor has an address of 10.1.0.7 and the Verifier has an address of 10.1.0.93.



Multiple Doors

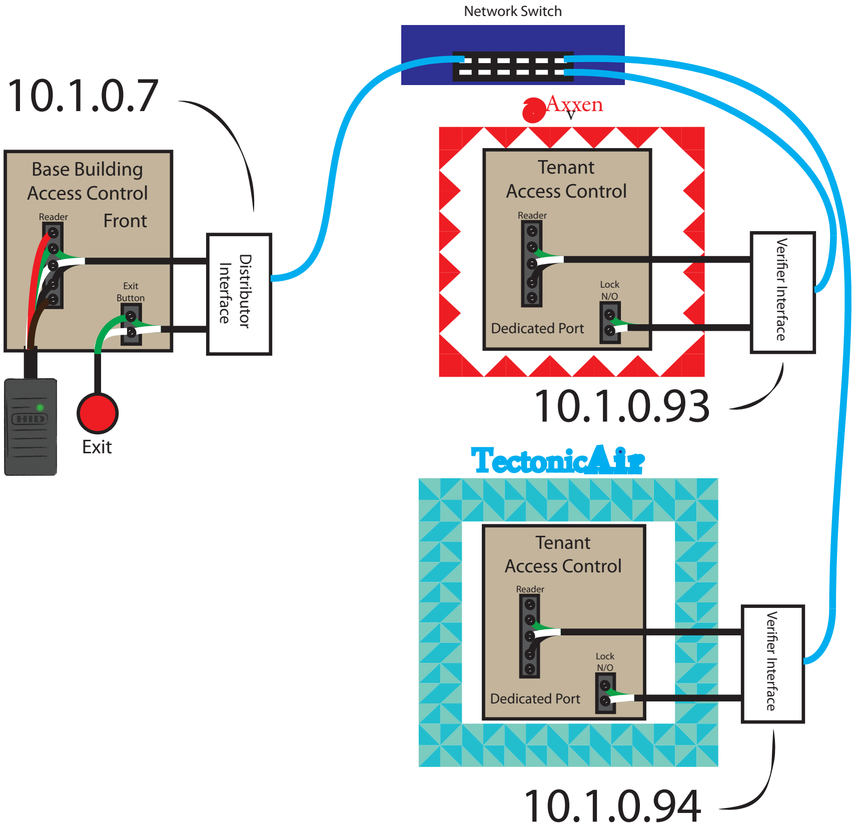
Like the previous example, this layout serves one tenant. Unlike the previous example this layout services multiple base building doors, in our example two. The doors Distributor units have IP addresses of 10.1.0.7 and 10.1.0.8, while the Verifier unit has an IP address of 10.1.0.93. Each Verifier unit will support 1024 Distributor units. The only limitation is lag time while the previous transaction is processed. This is typically not a limitation in after hours access, but could be a potential factor when used with turnstiles or barrier gates.



Multiple Tenants

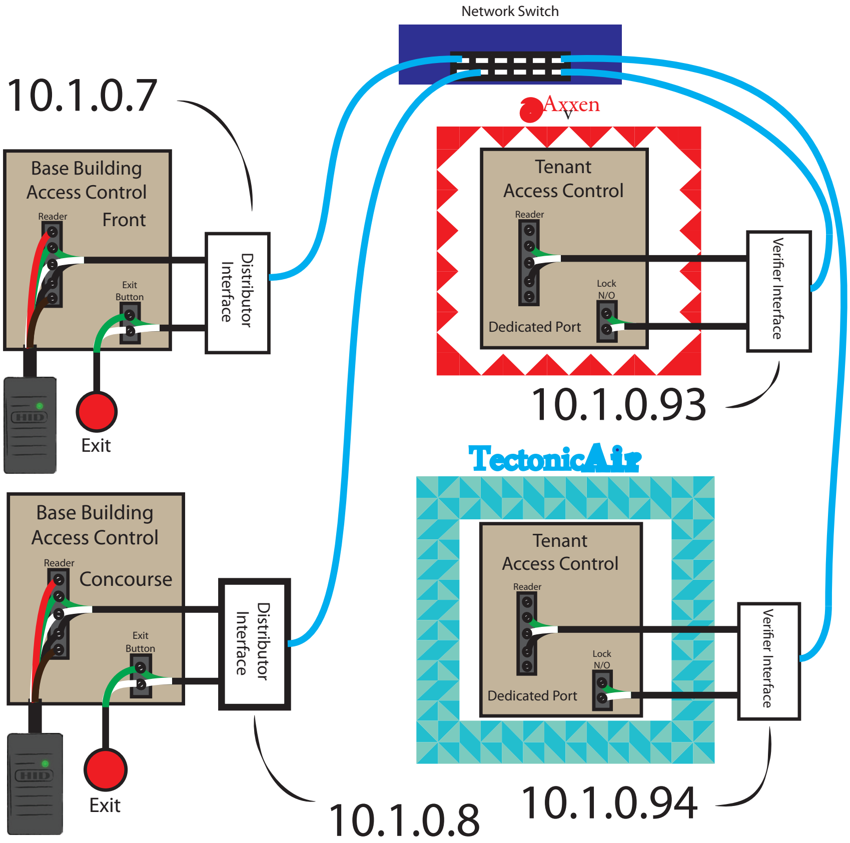
The next example is one door and multiple tenants. It is important to note that the standard Distributor unit will support up to sixteen Verifiers.

The base building door has an IP address of 10.1.0.7 and Axvxen's Verifier unit has an IP address of 10.1.0.93. Tectonic Air's Verifier is assigned an IP of 10.1.0.94.



Multiple Doors and Multiple Tenants

The most general and common scenario is a building with multiple doors and tenants. Shown below is our final example. The base building doors use IP addresses 10.1.0.7 and 10.1.0.8. The tenant Verifiers are assigned the IP addresses of 10.1.0.93 and 10.1.0.94.



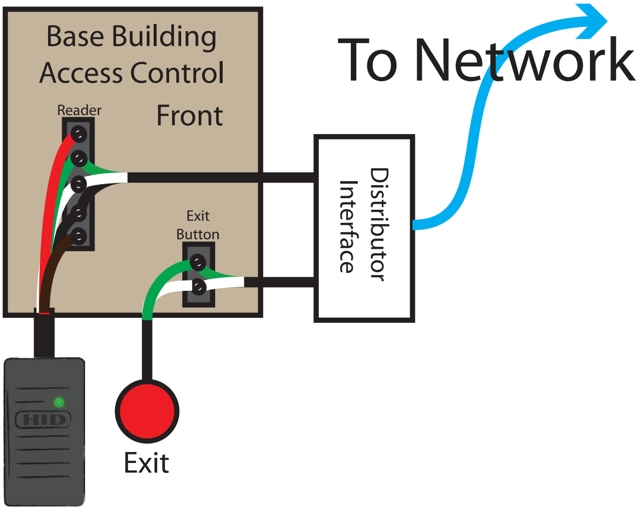
Summary

This chapter reviewed the four base configurations that might be encountered at base buildings. It should be apparent that each network appliance requires its own IP address to distinguish it from the other appliances on the network. Finally, it take two types of appliances to form a working system, Distributor units for the base building and Verifier units for the tenants.

4 Distributor Configuration

Prerequisites

Connect a Distributor in parallel for each the card reader and exit button at the access control panel. Therefore, each door requires its own Distributor. Distributors can share single Verifier, but the base building requires a one to one connection of Distributors to tenant accessable entrances.

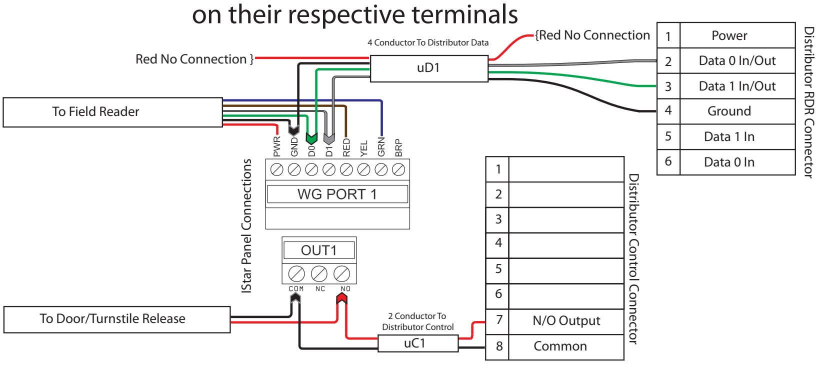


Distributor II Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. Form A normally open release are pins 7 and 8 of the CTRL connection. Ethernet is connected to the RJ-45. Below are show typical whip connections.

Typical Distributor Connections

D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel on their respective terminals

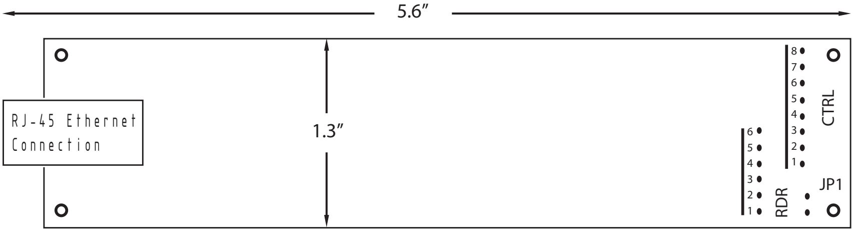


N/O and Com are connected in parallel

Distributor II Physical Layout

We recommend using insulated standoffs and nylon screws,

Board Layout Considerations for Distributor II



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - rfu
5 - rfu
6 - rfu
7 - C - Blue
8 - N/O - Orange

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc)

5 Verifier Configuration

Prerequisites

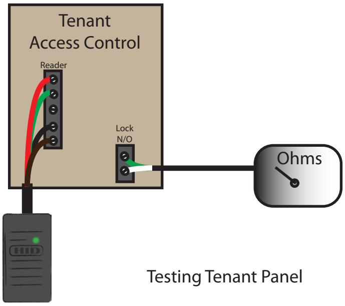
Each tenant will require a Verifier unit connected to a dedicated card reader port and door release output in the tenant access control panel.

Pre Test Tenant Panel

The first step to a successful installation is pretesting the Tenant Panel and settings. Simply connecting a card reader to the card reader input and a meter across the Lock control will verify their system settings.

Present a known good tenant card and observe the meter. When the card is presented the contact closure should be observed on the meter.

DO NOT SKIP THIS STEP as many "problems" are directly traceable to tenant configured panels or software.

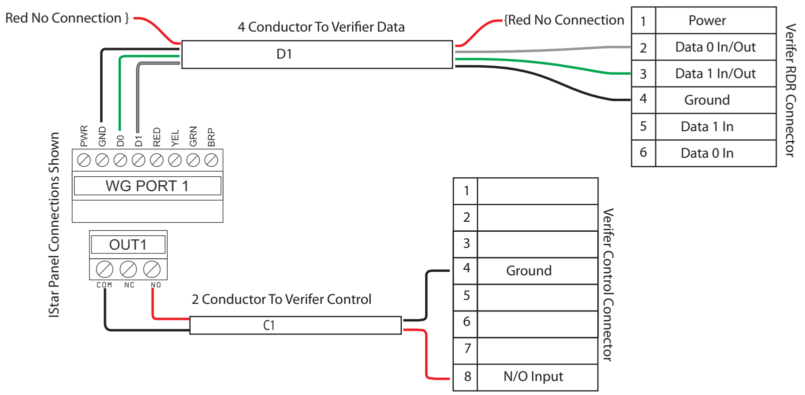


Testing Tenant Panel

Verifier II Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Power may be delivered from the associated tenant panel, just like a reader. Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. The tenant dry contact form A normally open release are connected to pins 4 and 8 of the CTRL connection. Ethernet is connected to the RJ-45. Below is a typical whip connection.

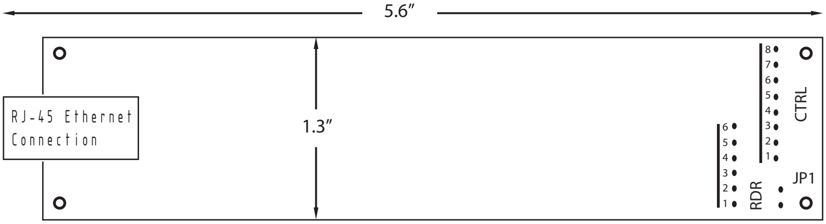
Verifier Connection



Verifier II Physical Layout

We recommend using insulated standoffs and nylon screws,

Board Layout Considerations for Verifier II



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - C - Blue
5 - rfu
6 - rfu
7 - rfu
8 - N/O - Orange

JP1
Pullup Jumper
(4.7K to 5vdc)
typically required

6 MetaDistributor

Prerequisites

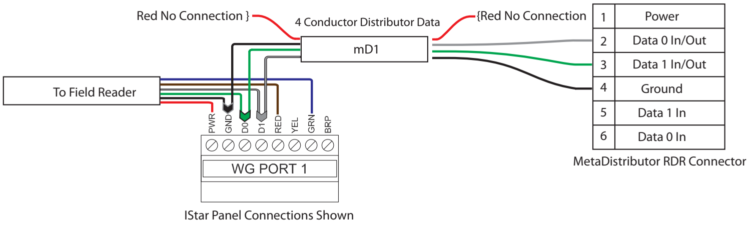
Each building elevator or environmental control card reader device requires a MetaDistributor. Connect MetaDistributors in parallel with the reader data at the base building access panel reader input. The system requires tenant MetaVerifiers that may be shared by MetaDistributors. In other words, one MetaVerifier can service several MetaDistributors. Card traffic analysis will determine sharing potential for MetaVerifiers.

MetaDistributor Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Output Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. Input Data 1 (white) and Data 0 (green) are pins 5 and 6 respectively. Ethernet is connected to the RJ-45.

MetaDistributor Parallel Connection

D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel
on their respective terminals


Red No Connection }
4 Conductor Distributor Data
{Red No Connection
mD1
To Field Reader
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
IStar Panel Connections Shown
MetaDistributor RDR Connector

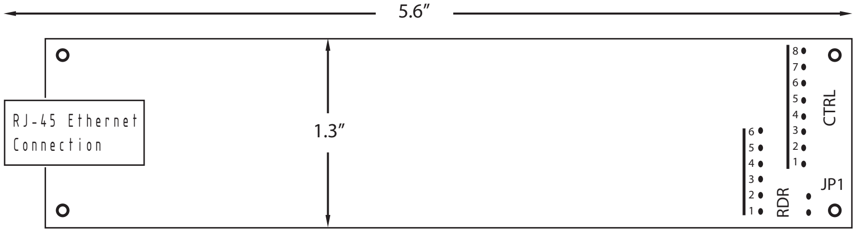
1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

TransVerify®

MetaDistributor Physical Layout

We recommend using insulated standoffs and nylon screws,

Board Layout Considerations for MetaDistributor



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green OUT
3 - Data 1 - White OUT
4 - Gnd - Black
5 - Data 1 - White IN
6 - Data 0 - Green IN

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - rfu
5 - rfu
6 - rfu
7 - rfu
8 - rfu

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc) on Data 0,1 OUT

7 MetaVerifier

Prerequisites

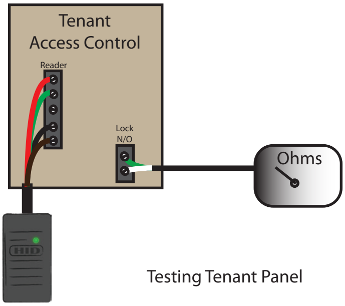
Each tenant will require a MetaVerifier unit connected to a dedicated card reader port and door release output in the tenant access control panel.

Pre Test Tenant Panel

The first step to a successful installation is pretesting the Tenant Panel and settings. Simply connecting a card reader to the card reader input and a meter across the Lock control will verify their system settings.

Present a known good tenant card and observe the meter. When the card is presented the contact closure should be observed on the meter.

DO NOT SKIP THIS STEP as many "problems" are directly traceable to tenant configured panels or software.

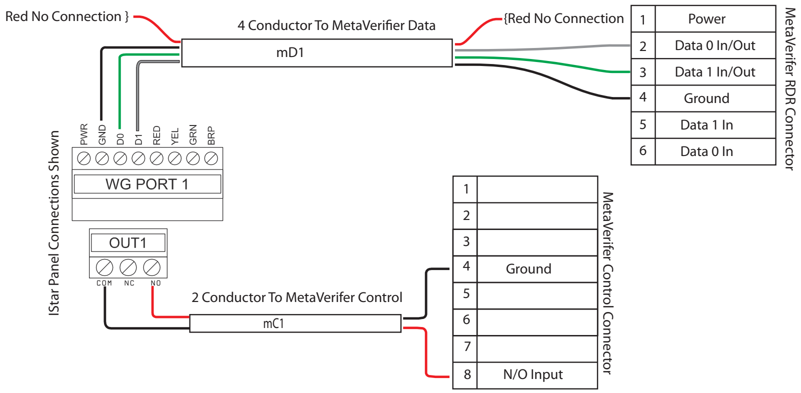


Testing Tenant Panel

MetaVerifier Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Power may be delivered from the associated tenant panel, just like a reader. Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. The tenant dry contact form A normally open release are connected to pins 4 and 8 of the CTRL connection. Ethernet is connected to the RJ-45. Below is a typical whip connection

MetaVerifier Connection


Red No Connection }
4 Conductor To MetaVerifier Data
mD1
{Red No Connection
MetaVerifier RDR Connector
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
IStar Panel Connections Shown
OUT1
COM
NC
NO
2 Conductor To MetaVerifer Control
mC1
MetaVerifer Control Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

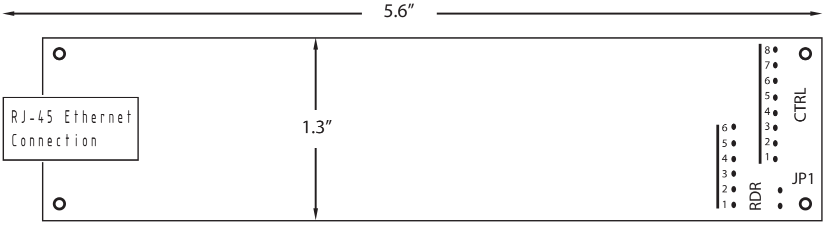
1	
2	
3	
4	Ground
5	
6	
7	
8	N/O Input

.

MetaVerifier Physical Layout

We recommend using insulated standoffs and nylon screws,

Board Layout Considerations for Verifier II



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - C - Blue
5 - rfu
6 - rfu
7 - rfu
8 - N/O - Orange

JP1
Pullup Jumper
(4.7K to 5vdc)
typically required

8 UltraDistributor

Prerequisites

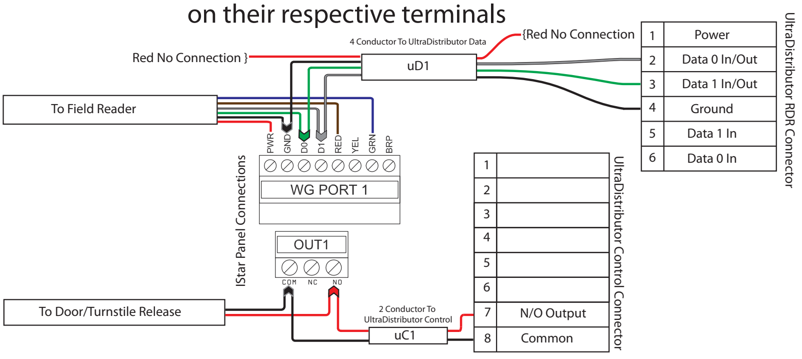
Each building door, gate, or turnstile card reader device requires a UltraDistributor. Connect UltraDistributor in parallel with the reader data at the base building access panel reader input. The system requires tenant UltraVerifiers that may be shared by UltraDistributor. In other words, one UltraVerifier can service several UltraDistributors. Card traffic analysis will determine sharing potential for UltraVerifiers.

UltraDistributor Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. Form A normally open release are pins 7 and 8 of the CTRL connection. Ethernet is connected to the RJ-45. Below are show typical whip connections.

Typical UltraDistributor Connections

D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel
on their respective terminals



UltraDistributor RDR Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

UltraDistributor Control Connector

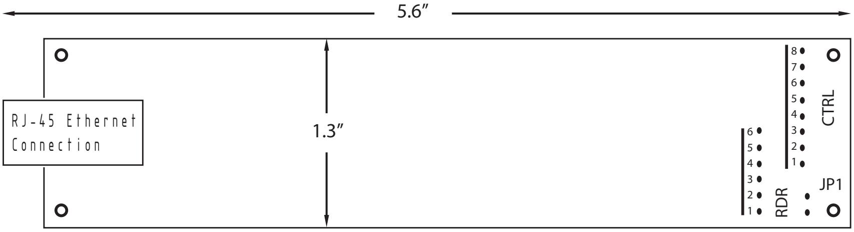
1	
2	
3	
4	
5	
6	
7	N/O Output
8	Common

N/O and Com are connected in parallel

UltraDistributor Physical Layout

We recommend using insulated standoffs and nylon screws.

Board Layout Considerations for UltraDistributor



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - rfu
5 - rfu
6 - rfu
7 - C - Blue
8 - N/O - Orange

JP1
No Jumper if in parallel with panel

Jumper if pullup required (4.7K to 5vdc)

9 UltraVerifier

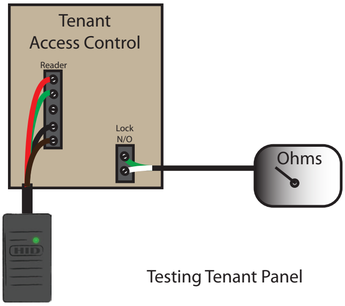
Prerequisites

Pre Test Tenant Panel

The first step to a successful installation is pretesting the Tenant Panel and settings. Simply connecting a card reader to the card reader input and a meter across the Lock control will verify their system settings.

Present a known good tenant card and observe the meter. When the card is presented the contact closure should be observed on the meter.

DO NOT SKIP THIS STEP as many "problems" are directly traceable to tenant configured panels or software.

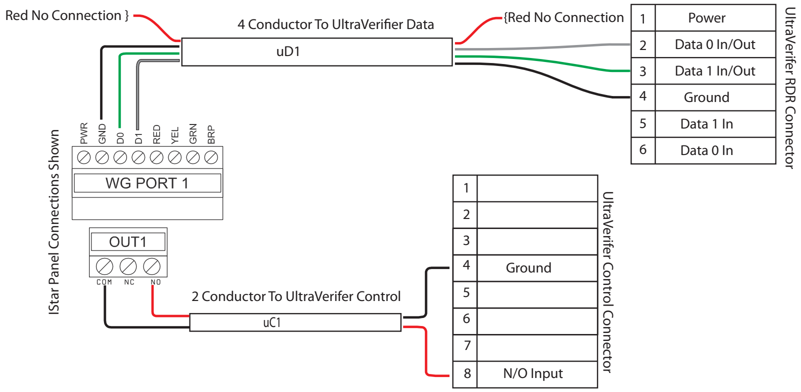


Testing Tenant Panel

UltraVerifer Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Power may be delivered from the associated tenant panel, just like a reader. Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. The tenant dry contact form A normally open release are connected to pins 4 and 8 of the CTRL connection. Ethernet is connected to the RJ-45. Below is a typical whip connection.

UltraVerifier Connection


Red No Connection }
4 Conductor To UltraVerifier Data
uD1
{Red No Connection
UltraVerifer RDR Connector
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
OUT1
COM
NC
NO
IStar Panel Connections Shown
2 Conductor To UltraVerifer Control
uC1
UltraVerifer Control Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

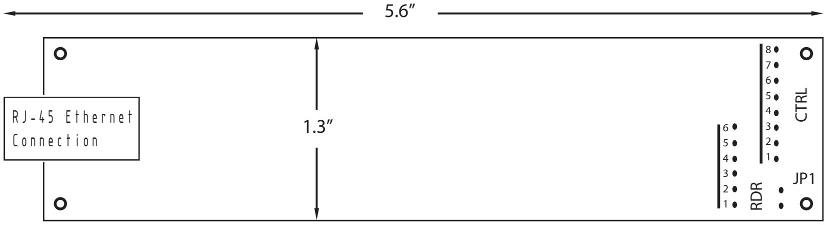
1	
2	
3	
4	Ground
5	
6	
7	
8	N/O Input

TransVerify®

UltraVerifier Physical Layout

We recommend using insulated standoffs and nylon screws,

Board Layout Considerations for UltraVerifier



RDR Connections
1 - Pwr - Red
2 - Data 0 - Green
3 - Data 1 - White
4 - Gnd - Black
5 - rfu
6 - rfu

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - C - Blue
5 - rfu
6 - rfu
7 - rfu
8 - N/O - Orange

JP1
Pullup Jumper
(4.7K to 5vdc)
typically required

10 Facility Code Filter

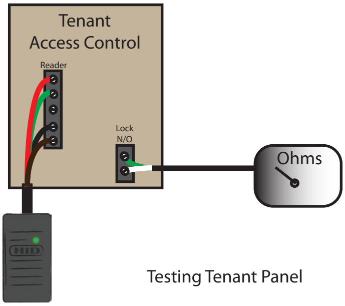
Prerequisites

Pre Test Tenant Panel

The first step to a successful installation is pretesting the Tenant Panel and settings. Simply connecting a card reader to the card reader input and a meter across the Lock control will verify their system settings.

Present a known good tenant card and observe the meter. When the card is presented the contact closure should be observed on the meter.

DO NOT SKIP THIS STEP as many "problems" are directly traceable to tenant configured panels or software.

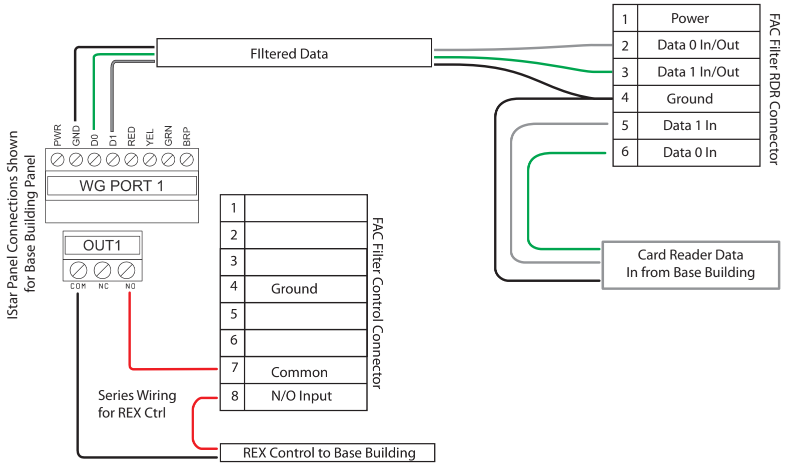


Testing Tenant Panel

Facility Code Filter Electrical Connections

Power is delivered through Pin 1 and Pin 4 of the RDR connection. Positive 7.5 to 12 volts DC are connected to pin 1 with ground connected to pin 4. Power may be delivered from the associated tenant panel, just like a reader. Data 0 (green) and Data 1 (white) are pins 2 and 3 respectively. The tenant dry contact form A normally open release are connected in series with pins 7 and 8 of the CTRL connection. Ethernet is connected to the RJ-45. Below is a typical whip connection.

FAC Filter Connection


FIltered Data
IStar Panel Connections Shown for Base Building Panel
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
OUT1
COM
NC
NO
Series Wiring for REX Ctrl
REX Control to Base Building
Card Reader Data In from Base Building
FAC Filter RDR Connector
FAC Filter Control Connector

FAC Filter RDR Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

FAC Filter Control Connector

1	
2	
3	
4	Ground
5	
6	
7	Common
8	N/O Input

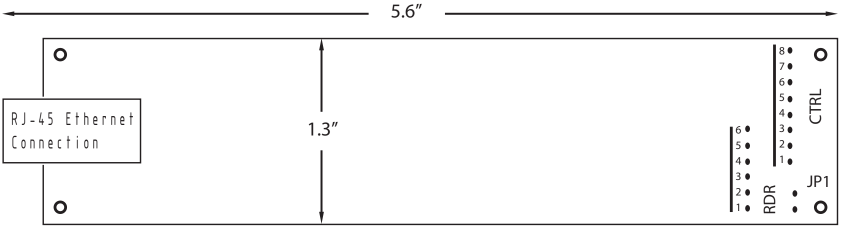
TransVerify®

Are you enterprise ready?

Facility Code Filter Physical Layout

We recommend using insulated standoffs and nylon screws to secure the board.

Board Layout Considerations for Facility Code Filter



RDR Connections
1 - Pwr - Red
2 - Out Data 0 - Green
3 - Out Data 1 - White
4 - Gnd - Black
5 - In Data 1 - White
6 - In Data 0 - Green

CTRL Connections
1 - rfu
2 - rfu
3 - rfu
4 - rfu
5 - rfu
6 - rfu
7 - C - Blue
8 - N/O - Blue

JP1
Pullup Jumper
(4.7K to 5vdc)
typically required

Theory of Operation

Some security conscious tenants would prefer to shield their employee card activity from the base building. The Facility Code Filter acts to block the viewing and recording of specified card activity by the base building.

The filter stands between the base building readers and the building access control system. The filter accepts reader data on the input port and reflects those filtered reads to the output port.

If the credential matches certain criteria, the filter blocks the card reader signals; else, the card reads are passed to the base building. You set the criteria with the card-filtering menu described in the chapter on System Settings.

♦ IMPORTANT: Matching Cards are BLOCKED!

When the FAC Filter reflects a card to the output port, the normally open contacts close. You set the length of the contact closure in the system settings. To prevent sporadic accesses, wire this output in series with the REX or “card valid” output of the base building panel to the door release circuitry.

11 System Settings

Setting Access

Accessing the settings depends upon the encryption mode. If encryption is disabled, use Telnet; enabled you must use our configuration program.

- Telnet

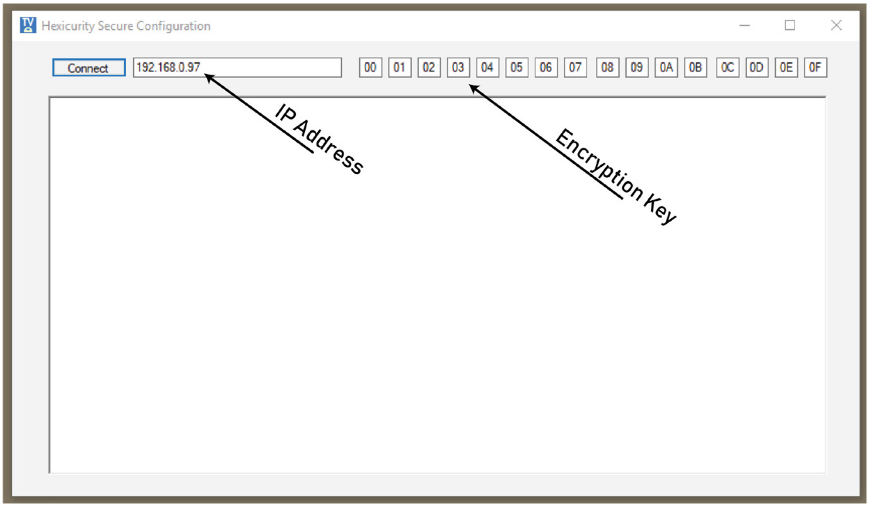
To access the device setting with Telnet, use port 9999. By way of example, if the Device has an IP of 192.168.0.97, use the following command line:

```
C>Telnet 192.168.0.97 9999
```

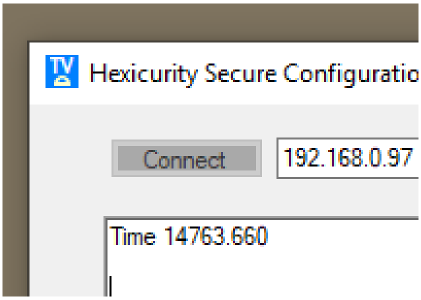
- Encrypted

You must use the Hexicurity Secure Configuration Windows® application when encryption is enabled. Devices with revision 7.6. are supported.

Enter the device's IP address and the 128-bit encryption key in hexadecimal. The installing dealer provides the device IP and the encryption key with the system documentation.



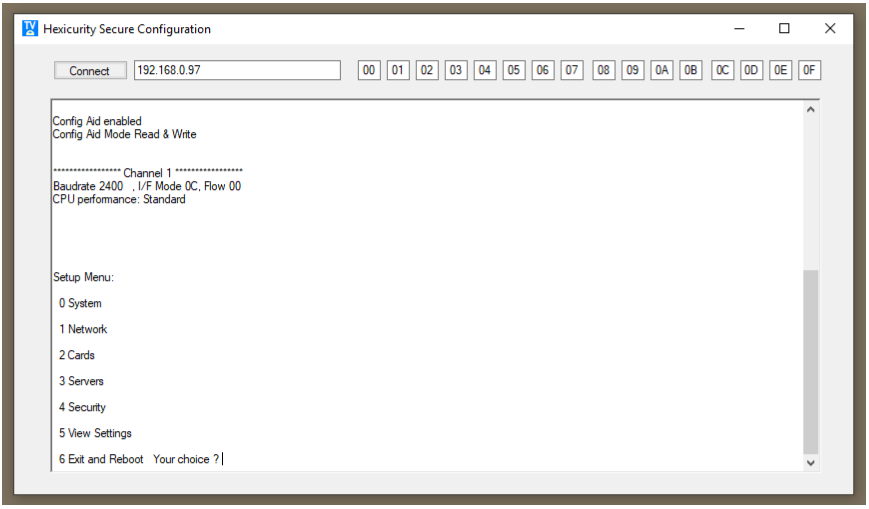
Click on "Connect"; the device responds with "Time" and a number, your challenge. Your cursor should appear on the line below. Enter your challenge number carefully, without backspacing. If you make an error, wait sixty seconds for the device to reset, then start over with "Connect."



192.168.0.97

```
Time 14763.660
|
```

A correct entry that matches the challenge will be first greeted with configuration information, followed by the Setup Menu. Optionally, move the scroll bar on the right side to review the setup information.

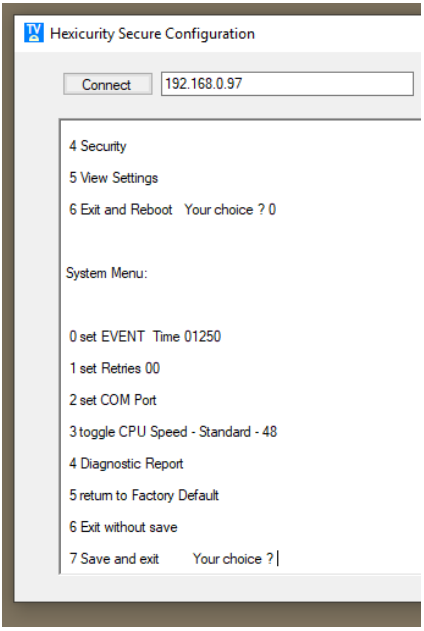


192.168.0.97

```
Config Aid enabled
Config Aid Mode Read & Write


***************** Channel 1 *****************
Baudrate 2400   , I/F Mode 0C, Flow 00
CPU performance: Standard




Setup Menu:

 0 System

 1 Network

 2 Cards

 3 Servers

 4 Security

 5 View Settings

 6 Exit and Reboot   Your choice ?|
```

Some important information is shown at the top on the screen, the Config Aid status. When Config Aid is Enabled, all settings are network visible, including the encryption key. When the setup is complete, the device must be "Locked Down" under "Security" selection 4. "Locked Down" disables the Conf Aid and other vulnerable settings.

System



192.168.0.97

```
4 Security
5 View Settings
6 Exit and Reboot   Your choice ? 0

System Menu:

0 set EVENT  Time 01250
1 set Retries 00
2 set COM Port
3 toggle CPU Speed - Standard - 48
4 Diagnostic Report
5 return to Factory Default
6 Exit without save
7 Save and exit        Your choice ?
```

- Event Time

Enter the Event Time in milliseconds; a thousand milliseconds equal one second. The Event time has different meanings depending upon device type; Distributor or Verifier.

For a Distributor, Event time is the time the Normally Open contact closes when authorized. Additionally, for a Meta or Ultra Distributor, the Event time is the minimal dwell time between a card read, and a Virtual or Chaser card being out-pulsed. Increase this setting if the base building misreads the Chaser card.

The Verifier Event Time defines how long a Verifier will wait for the Tenant system to respond with an authorization.

- Retries

Set Retries to zero.

- COM Port

Typically set the COM Port to 2400 baud.

- CPU Speed

Typically set the CPU Speed to Standard.

- Diagnostic Report

Diagnostics are a future feature.

- Factory Default

Sets the COM port speed to 2400 baud.

- Exit without Save

Make no changes to the settings, exit this menu.

- Save and Exit

Save the settings to persistent memory and exit this menu.

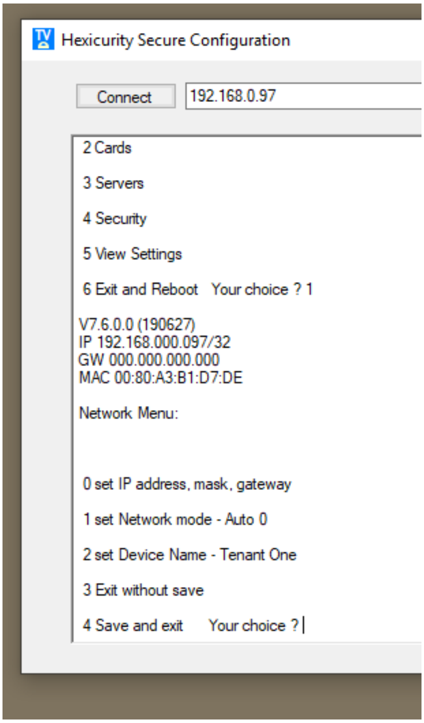
Network

The Network Sub-Menu choice will respond with the current version and network settings, including the IP Address, Gateway, Mask, and MAC address. The MAC address serves as the serial number and is printed on the device network connector.

Setting the IP address

Selection 0 allows you to enter the IP address as four octets. Enter each of the four octets as a three digit decimal number; 0 - 255. It is best to terminate the octet entry with a period or decimal point. Pressing enter works, but the cursor will advance to the next line.

Enter the host part of the mask as a two-digit decimal number 0-31, the CIDR notation. Typically this value is zero eight (08) which is the mask of 255.255.255.0.



```
2 Cards

3 Servers

4 Security

5 View Settings

6 Exit and Reboot   Your choice ? 1

V7.6.0.0 (190627)
IP 192.168.000.097/32
GW 000.000.000.000
MAC 00:80:A3:B1:D7:DE

Network Menu:


0 set IP address, mask, gateway

1 set Network mode - Auto 0

2 set Device Name - Tenant One

3 Exit without save

4 Save and exit     Your choice ?|
```

The gateway is entered just as the devices IP, with preference to ending each octet with a period.

- ♦ Network Mode

The network mode chooses if the network speed and duplex options. Auto is the usual setting.

- ♦ Device Name

Device Name is the device's network name. This name appears in the Distributor's server menu as the Verifier name. We recommend the Device Name incorporate a tenant identifier as a setup aid. It is only available if the device has not been "Locked Down."

- ♦ Exit without Save

Make no changes to the settings, exit this menu.

- ♦ Save and Exit

Save the settings to persistent memory and exit this menu.

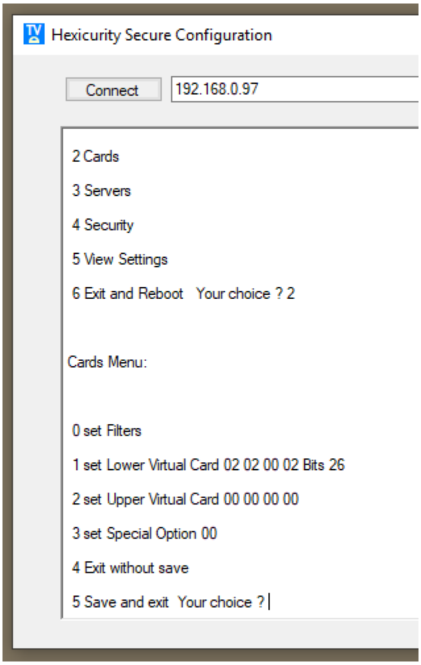
Cards

- Filters

In Normal mode filters will either allow (Verifiers) or deny (Distributors) out-pulsing from the primary Weigand connection, pins 2 and 3. This action can be inverted with a special option bit.

The filtering can be set up for either a single 64 bit mask and match raw option or cooked four facility codes supporting cards up to 35 bits. The number of bits in the card read is also considered. The cook mode removes the lowest parity bit, bit 0, and works with bits 17 through 32.

Mask and match is a technique most often seen in subnetting where the input is first Masked for significant bits then matched to a template.



```
2 Cards
3 Servers
4 Security
5 View Settings
6 Exit and Reboot   Your choice ? 2

Cards Menu:

0 set Filters
1 set Lower Virtual Card 02 02 00 02 Bits 26
2 set Upper Virtual Card 00 00 00 00
3 set Special Option 00
4 Exit without save
5 Save and exit  Your choice ? |
```

An example; a twenty-six bit card has a facility code of 100 (decimal) which is 0x64 (hexadecimal). The facility code of a twenty-six bit card has eight bits, positions seventeen through twenty-four. Thus your mask entries are 00 and FF, the matching entry is 00 64, and the bit count is 1a (hexadecimal) or twenty-six (decimal).

Windows® 10 offers a calculator with programmer mode, allowing conversion between decimal numbers to hexadecimal. To access it, just enter "calculator" into the search bar. Change to programmer mode from the "hamburger" menu, found in the upper right of the calculator window.

- Lower Virtual Card

The lower virtual card is a digitized representation of the "raw" chaser card. This only applies to the Meta or Ultra Verifiers. The entry should include the parity bits, the facility code, the PIN and the bit count. A twenty-six bit card with a facility code of 1 and a pin of 1 is shown. Searching for Weigand card calculator on the web returns several calculators. Use the example above to orient yourself in the various proprietary calculators.

- Upper Virtual Card

The upper virtual card extends the lower virtual card up to sixty-three bits.

- ♦ Special Options

Zero is the Special Options bit field standard setting. The options are: Bit 0 test for known bit counts, Bit 3 (Bit 0 is required) will strip the parity bits for compatibility with some access panels. Bit 1 sets raw mode for card filtering. Bit 2 controls reflection of bits from the auxiliary Wiegand input (pins 5 and 6) to the Wiegand output (pins 2 and 3) on a Distributor. Cards matching the filter option are not reflected when Bit 2 is clear; when set only reflect cards matching the filter option. Add the bit weights to combine options: Bit 0, the weight is 1; Bit 1, the weight is 2; Bit 3, the weight is 4; and Bit 3, the weight is 8. To strip the parity bits requires Bit 0 and Bit 3, adding the weights of 1 for Bit 0 and 8 for Bit 3 totals to 9. Nine entered for the Special Option will strip parity bits.

- ♦ Exit without Save

Make no changes to the settings, exit this menu.

- ♦ Save and Exit

Save the settings to persistent memory and exit this menu.

Server

Apart from the NTP server setting, this is a Distributor menu. This setting ties the Distributors to the Verifiers, routing card reads from the base building to the tenants. In this context, a Verifier is a server.

- ◆ Set Servers

The top section shows this device's name and IP address. Also shown are the server options. Verifiers entries always use option 2 or Raw.

The first sixteen selections, zero (0) through fifteen (15), allow you to choose Verifiers on the network by entering their IP address. If the Verifier is not "Locked Down," the Network Name appears at the end of the entry. As the name comes from the Verifier, this confirms network connectivity.

The seventeenth selection (16) allows you to enter the NTP Time Server IP address. You should choose Option 1 for conventional NTP servers. The server issues the four-letter identifier at the end of the entry, confirming network connectivity.

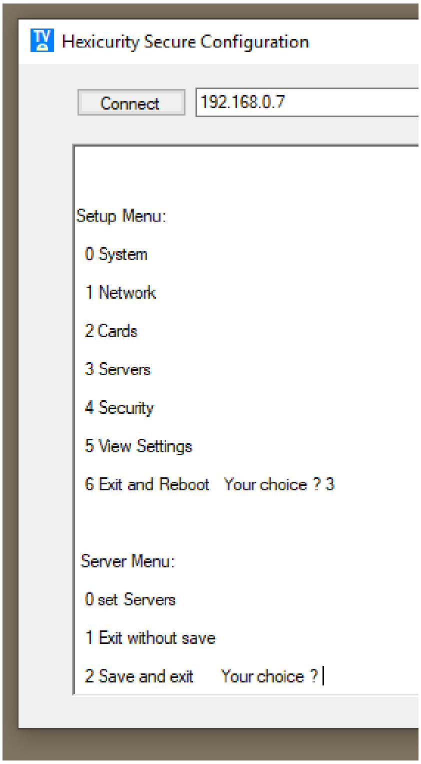
After editing the final selection, 17 will return to the prior menu.

- ◆ Exit without Save

Make no changes to the settings, exit this menu.

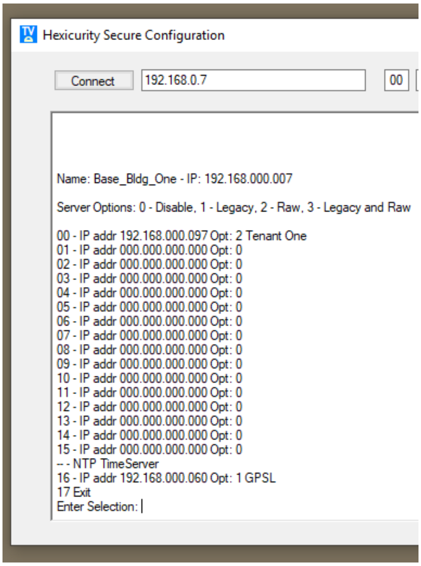
- ◆ Save and Exit

Save the settings to persistent memory and exit this menu.



192.168.0.7

```
Setup Menu:
 0 System
 1 Network
 2 Cards
 3 Servers
 4 Security
 5 View Settings
 6 Exit and Reboot   Your choice ? 3

Server Menu:
 0 set Servers
 1 Exit without save
 2 Save and exit     Your choice ? |
```



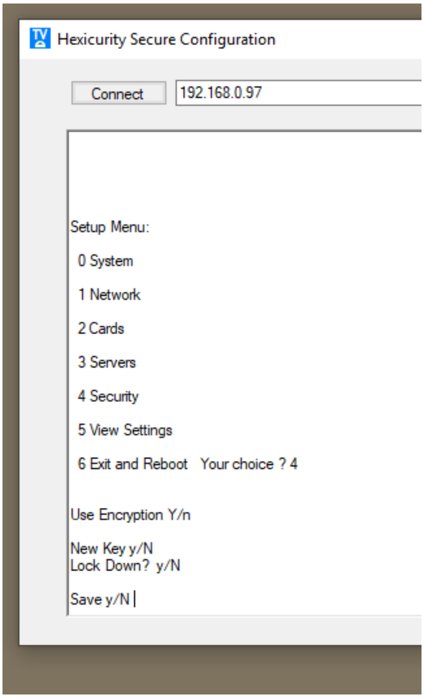
192.168.0.7 00

```
Name: Base_Bldg_One - IP: 192.168.000.007

Server Options: 0 - Disable, 1 - Legacy, 2 - Raw, 3 - Legacy and Raw

00 - IP addr 192.168.000.097 Opt: 2 Tenant One
01 - IP addr 000.000.000.000 Opt: 0
02 - IP addr 000.000.000.000 Opt: 0
03 - IP addr 000.000.000.000 Opt: 0
04 - IP addr 000.000.000.000 Opt: 0
05 - IP addr 000.000.000.000 Opt: 0
06 - IP addr 000.000.000.000 Opt: 0
07 - IP addr 000.000.000.000 Opt: 0
08 - IP addr 000.000.000.000 Opt: 0
09 - IP addr 000.000.000.000 Opt: 0
10 - IP addr 000.000.000.000 Opt: 0
11 - IP addr 000.000.000.000 Opt: 0
12 - IP addr 000.000.000.000 Opt: 0
13 - IP addr 000.000.000.000 Opt: 0
14 - IP addr 000.000.000.000 Opt: 0
15 - IP addr 000.000.000.000 Opt: 0
-- - NTP TimeServer
16 - IP addr 192.168.000.060 Opt: 1 GPSL
17 Exit
Enter Selection: |
```

Security

The Security Selection will step you through four questions. The capitalized selection, Y or N, is the default selection.

- Use Encryption (Y/n) enables encryption on the device. If you are using Telnet, enabling this will become effective when you exit and reboot from the main menu.
- New Key (y/N) allows you to enter the 128-bit key as sixteen hexadecimal numbers. This is the system key and must be identical for all Distributors and Verifiers in the system. This key allows device access after a reboot. If you error entering the key (or forget the key) and "Lock Down" the device, there is no known recovery method.

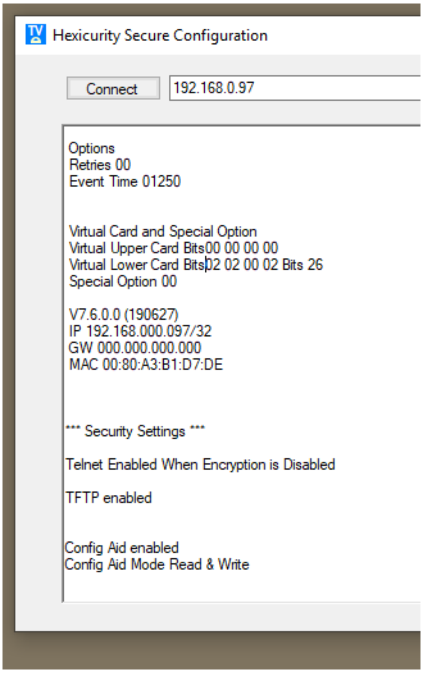


```
Setup Menu:
 0 System
 1 Network
 2 Cards
 3 Servers
 4 Security
 5 View Settings
 6 Exit and Reboot   Your choice ? 4

Use Encryption Y/n
New Key y/N
Lock Down? y/N
Save y/N |
```

- Lock Down (y/N) is a critical setting. Leaving this option deselected exposes all settings to the network. If the Encryption key is wrong or forgotten, recovery is impossible. Therefore, enable Lock Down only after verifying the system operation with test cards.
- Save (y/N) is your last chance to correct any errors you may have made in entering the encryption key etc.

View Settings

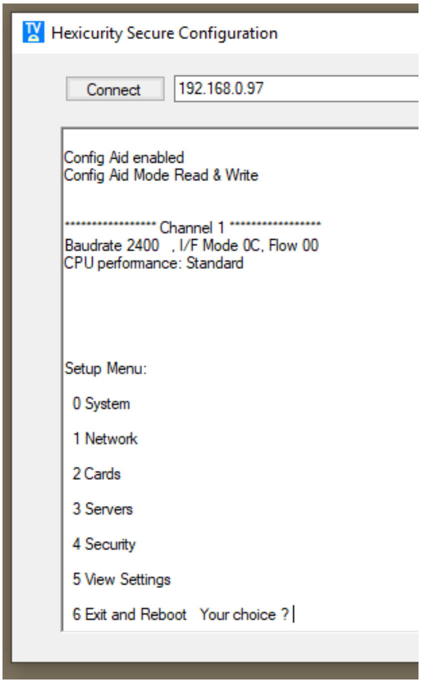
This selection will scroll most settings for your review. Use the scroll bar on the right to see the information that has scrolled off the screen.



```
Options
Retries 00
Event Time 01250


Virtual Card and Special Option
Virtual Upper Card Bits00 00 00 00
Virtual Lower Card Bits02 02 00 02 Bits 26
Special Option 00

V7.6.0.0 (190627)
IP 192.168.000.097/32
GW 000.000.000.000
MAC 00:80:A3:B1:D7:DE


*** Security Settings ***

Telnet Enabled When Encryption is Disabled

TFTP enabled


Config Aid enabled
Config Aid Mode Read & Write
```

Exit and Reboot

Selection 6 exits the menu system and reboots the device.



```
Config Aid enabled
Config Aid Mode Read & Write


***************** Channel 1 *****************
Baudrate 2400   , I/F Mode 0C, Flow 00
CPU performance: Standard




Setup Menu:

 0 System

 1 Network

 2 Cards

 3 Servers

 4 Security

 5 View Settings

 6 Exit and Reboot   Your choice ?
```

12 System Installation

Pre Installation

A profitable and successful installation starts with planning and preparation.

We strongly recommend complete network planning before arriving on site with the equipment.

If your installation involves using an existing network, plan a site visit to verify the IP addresses are available. Use a laptop attached to the network and "Ping" the list of addresses you intend to use.

On a corporate network using the recommended VLAN, verify connectivity with two laptops attached to your assigned ports on the network switches. Temporarily set the laptops to your intended device IP addresses for those ports and ping them. The network professionals are more accustom to setup using computers and any VLAN problems will be resolved more quickly.

Also gather some tenant cards for testing. These will allow you to verify the card bit structures and their Verifier settings before you arrive on site.

Perform the recommended card reader test on the tenant panels with your test cards.

Enclosure site requirements

Temperature Range	0 - 30° C
Maximum Altitude	2000 Meters
Mounting Height	No more than 2 meters above finished floor

At your office

With a network plan setup all the devices and test them. Settings are much easier to verify and change on the test bench than at the customer site.

Setup Order

Set the network parameters for the Verifier and Distributor units, leaving the Verifier card settings blank but setting the Verifier time to 5000 as shown in chapter 10.

Attach a test card reader to a Distributor unit.

Test that the card reads at the Distributor unit are reflected at the Verifier outputs.

Finally, set the Verifier card bit structures and test with tenant card.

Network Setup

If all of your devices are either on a “flat” network or share the same mask and gateway they should be able to communicate.

If your devices need to be “routed”, in other words they do not share the same mask and gateway, you can set the mask /8 if the first octet is the same for bench testing. For example if the assigned IP addresses in your plan are 192.168.0.10 /24 and 192.170.0.88 /24 then setting the mask to /8 will allow them to communicate on a “flat” network. Wait until after you have tested the Verifier units on the tenant panels before adjusting the mask.

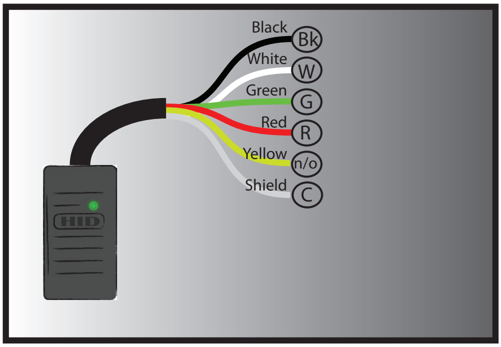
Set a laptop to an unused IP address within the mask range and ping each of the devices as they are set. Label those devices with their IP address and final

location.

Test Card Reader

Attach a test card reader as shown below. The colors shown are for an HID ProxPoint reader.

Connections to the yellow and shield allow the beeper to sound on granted card reads, easing testing.



Verifier Test Setup

Attach the Hexicurity Verifier test harness to the indicated terminal strips. A wiring diagram for the test harness is shown in Appendix B. The green and white LEDs will flash when a card is presented to a Distributor test reader. Pressing the test button within the allocated time, 5 seconds if the time is set to 5000, will cause the test reader to beep. This indicates a successful test.

Tenant Card Bit Structures

The last bench test is to set the tenant bit structure into the Verifier unit. Test with a tenant card and observe the green and white LEDs flash. Press the test button and the reader should beep as before. Leave the device network settings until you have completed testing the Verifier units with the tenant panels. Set the Verifier time to the planned setting.

Tenant Panel

At the tenant panel, test with your test reader and test card to verify tenant panel operation. Next, attach the Verifier unit. Test using the tenant card on test reader and Distributor to verify operation. Finally, set the Verifier network settings.

Base Building Panel

Install the Distributor and adjust the network options to the planned settings. Test with tenant cards.

On Site

Enclosure Mounting

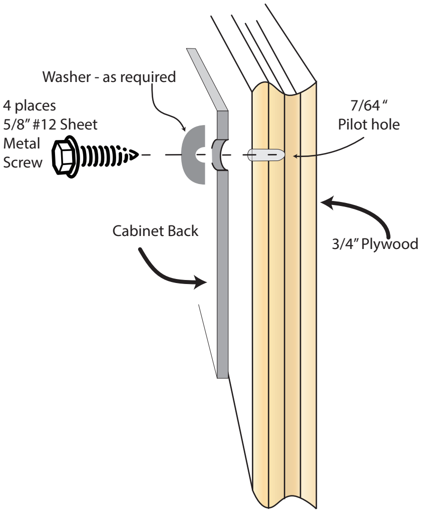
Open the carton and remove everything, setting the contents to one side. The mounting instructions below apply to the base model Hoffman box.

The provided Ethernet cables are sized for the hinge to be on the left as you face the enclosure. You should choose a location that will allow the door to open at least 100°, Preferably 150° for easier access to the network switch. Do not mount the cabinet more than 2 (two) meters above the finished floor.

The preferred method of mounting begins with the wall finished with a sheet of 3/4" plywood. Attach the cabinet to the plywood with 4 (four) each 5/8" #12 sheet metal screws (not included) through the .31" mounting holes provided in the back of the cabinet.[1]

Employing "Strut Channel" secured to the wall is an alternative. Support the cabinet with 4 (four) 1/4-20 bolts engaging spring nuts in the strut channel.

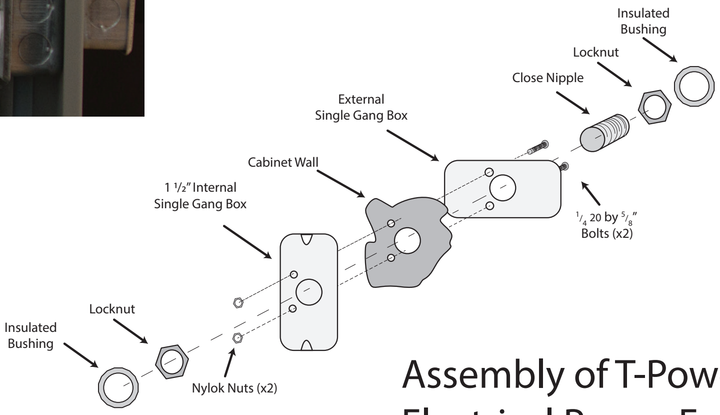
Verify your method of mounting is in accordance with local building codes. Quoting the National Electric Code "installed in a neat and workmanlike manner" and "shall be firmly secured to the surface on which it is mounted".



[1] Fastener specifications provided by the Engineered Wood Association in their 1995 publication "Fastener Loads for Plywood - Screws" Number E830C.

Mounting holes have been provided for an electrical box included with the cabinet power option. Install as shown below to allow clearance for installation of the back panel.

Install the optional convenience outlet.



Assembly of T-Power Electrical Power Feed

TransVerify

The preferred location for the data conduit is the top or bottom cabinet center.

Install the data conduit.

The Ethernet switch is mounted to the enclosure door with the included 10-32 hardware.

Remove the screws from the mounting bracket, position the switch, secure with mounting screws through the door face.

Unpack the back panel and install on the four enclosure studs found on the back wall.

Route the data cables.

Connect the Ethernet jumpers between the network switch and the circuit boards.

Route the switch power cable and secure with hook and loop cable ties attaching to magnetic cable clamps.

Install and attach the power supply.

First, open all the fuse holders disconnecting the power supply circuits from the boards.

Second, if you have the power supply accessory, attach the 2.1 mm barrel connector to the mating connector on the chassis. If you choose to supply your own power, refer to the table at the end of this chapter for specifications. Verify the center is positive relative to the barrel before attaching the connector.

Third, verify the voltage at the supply side of the fuse holder relative to the ground buss.

Fourth, close the first fuse holder and observe the first board. You should see the link lights on the Ethernet connector flash. This indicates all is well with the power.

Finally, close the remaining fuse holders, checking the link lights on the corresponding boards.

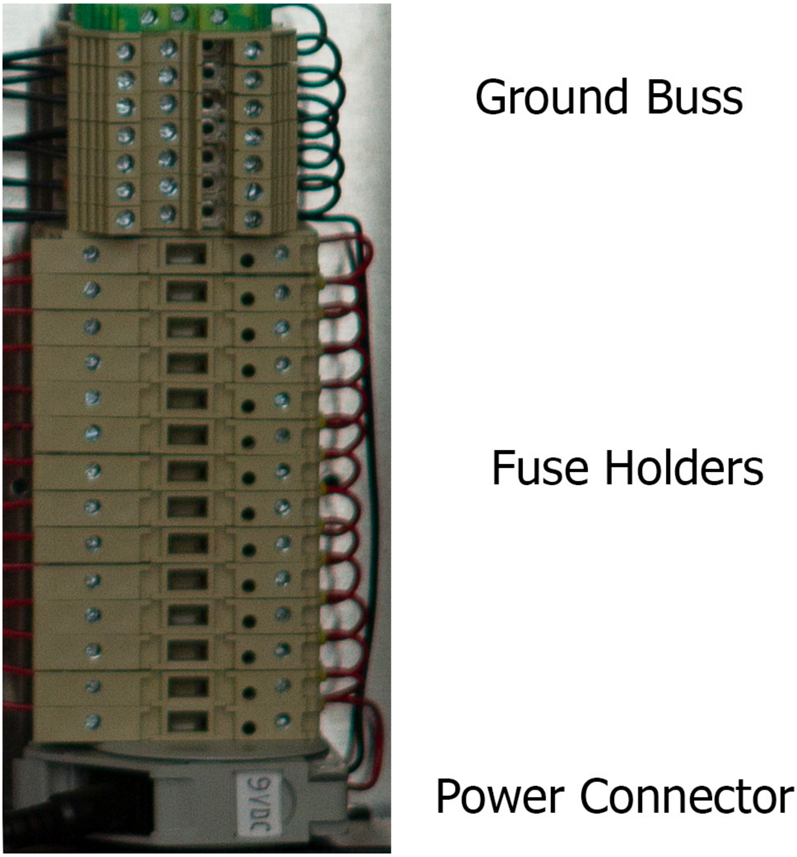
Leave the device network settings until you have completed testing the Verifier units with the tenant panels. Set the Verifier time to the planned setting.

Tenant Panel

At the tenant panel, test with your test reader and test card to verify tenant panel operation. Next, attach the Verifier unit. Test using the tenant card on test reader and Distributor to verify operation. Finally, set the Verifier network settings.

Base Building Panel

Install the Distributor and adjust the network options to the planned settings. Test with tenant cards.



POWER SUPPLY REQUIREMENTS

Voltage / Current / Power	7.5 - 14 VDC / 3 amps / 100W Max
Power Connector	2.1 mm barrel, center positive Adafruit 369 or equivalent
Temperature Range	0 - 45° C
Agency Approvals	Both EMC and Safety appropriate to final installation. Example USA installation; FCC and MET Labs or equivalent.
Maximum Altitude	2000 Meters

13 Dallas Installation

Pre-installation

3/8 " Variable Speed Reversing Drill with Integrated Bubble Level

Extension Cord

PVC Electrical Tape

Measuring Tape

Large Plastic Spring Clamps

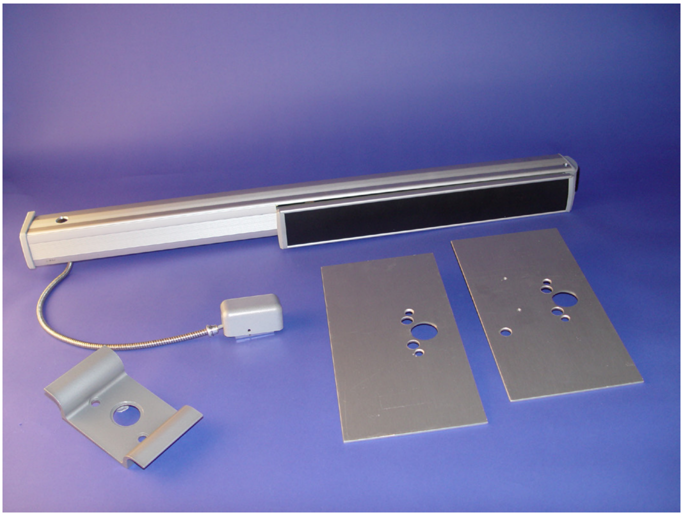
Small Ball Peen Hammer

#1 and #2 Phillips Screwdriver

Small and Medium Flat Blade Screwdriver

Wire Cutters/Strippers with crimping jaws
Needle Nose Pliers
Allen Wrench Set (1/16" to 1/4")
7 Step Drill Bit (1/4"-3/4")
1 1/4" Metal Hole Saw
5/32" Masonry Drill Bit
High-Speed Drill Bit Set (1/8". 5/32", 3/16", 1/4", 3/8", 1/2")
12-24 Tap and Matching Drill
Tap Handle
1/4" High-Speed Bullet Point Drill Bit 24" Long
Measuring Tape
Pencil
Flashlight

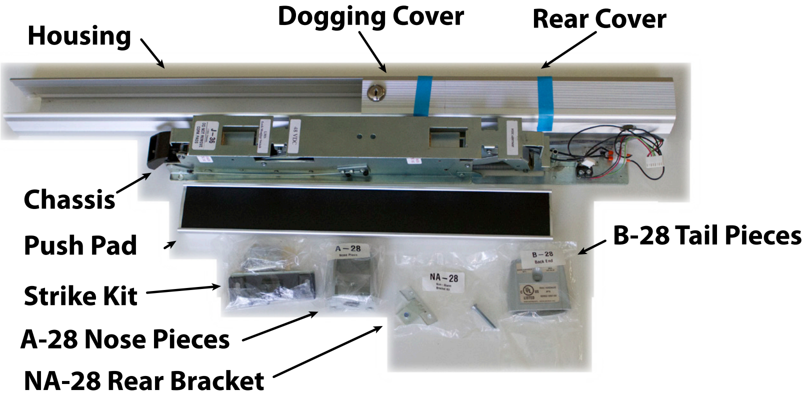
Installation Kit



Shown above are the armored cable, retrofit door pull, and retrofit Swiss Plates. In addition, a reader, flexible CAT-5e cable, and hardware kit are included. Slab door installation uses a different handle.

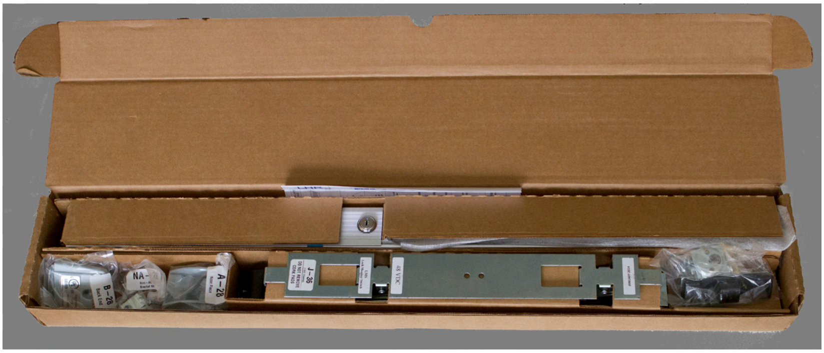
What is in the box

The diagram below calls out the principal panic hardware components as shipped.



Box Contents

This picture shows the components packed in their shipping carton. You should first remove the bagged components, then the housing, and finally the chassis.

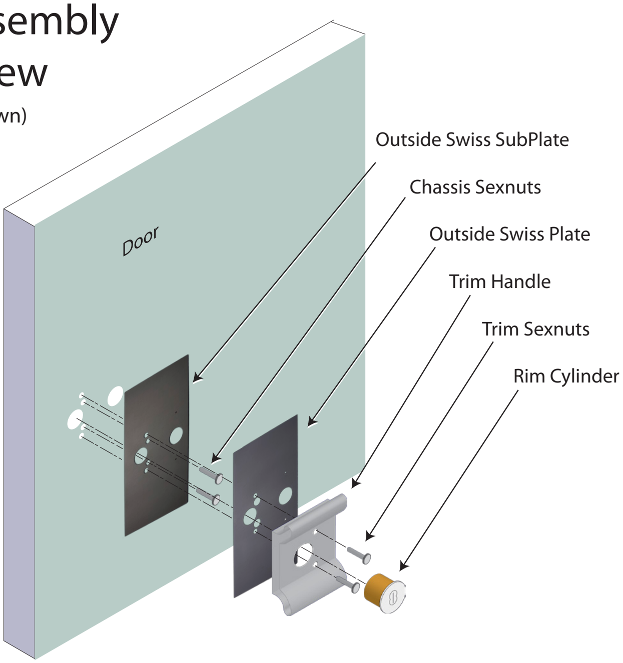


Panic Hardware Carton

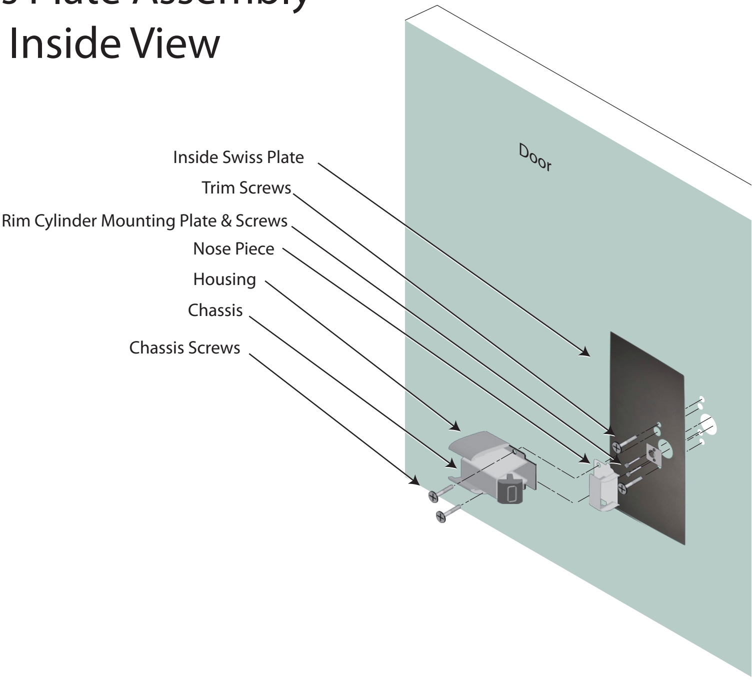
Be careful as the box is a bit of a puzzle designed to support the heavy chassis without suffering shipping damage. In particular, cardboard tongues thread through the push pad support bracket on the chassis.

Swiss Plate Assembly Outside View

(Reader is not shown)

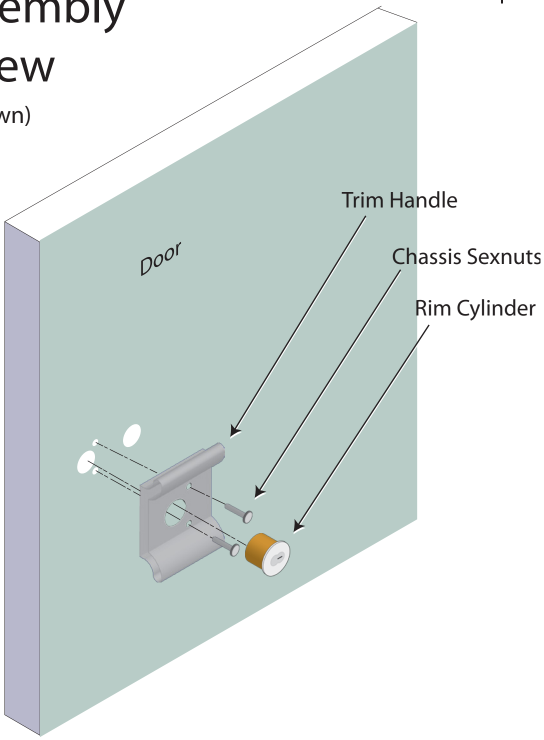


Swiss Plate Assembly Inside View

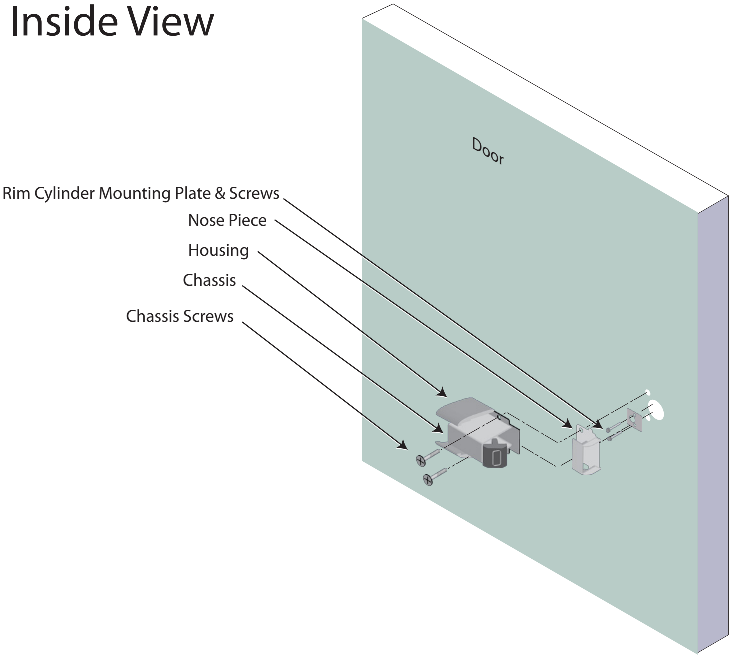


Slab Door Assembly Outside View

(Reader is not shown)



Slab Door Assembly Inside View



Installation of Push Pad

Slide the Push Pad onto the Chassis push pad support bracket, mating the upper slots in the Push Pad with the movable support bracket. The support bracket has the white labels attached. Remove the front push pad end cap and screw from the nose piece A-28 bag. This cap has a "U" shaped cutout to accommodate the nose. Use the included screw to secure the cap to the front of the chassis push pad bracket.

Next, remove the rear pad end cap and screw from the B-28 tail piece bag. Use the screw to secure the rear cap to the rear of the chassis push pad bracket.

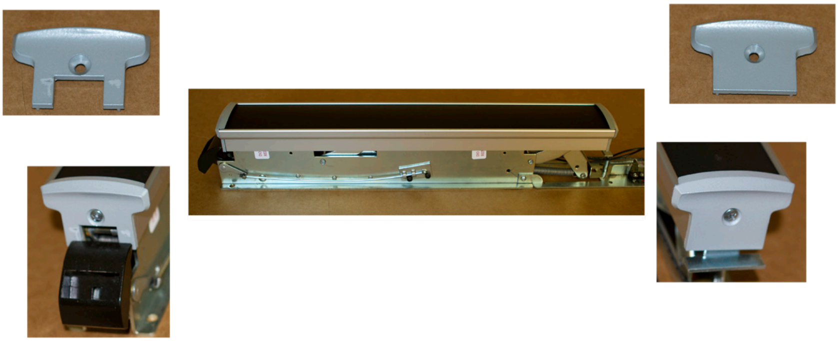


Illustration of Push Pad End Cap Installation

Installation Overview

Your task is to mount the Dallas panic hardware and the reader on the door. This chapter covers both retrofit and slab door installations. The two procedures are similar. The retrofit requires more labor but allows installation on doors that have been previously drilled for other hardware. The retrofit uses swiss plates to cover the holes and provide mechanical support.

Where they differ is noted with a table:

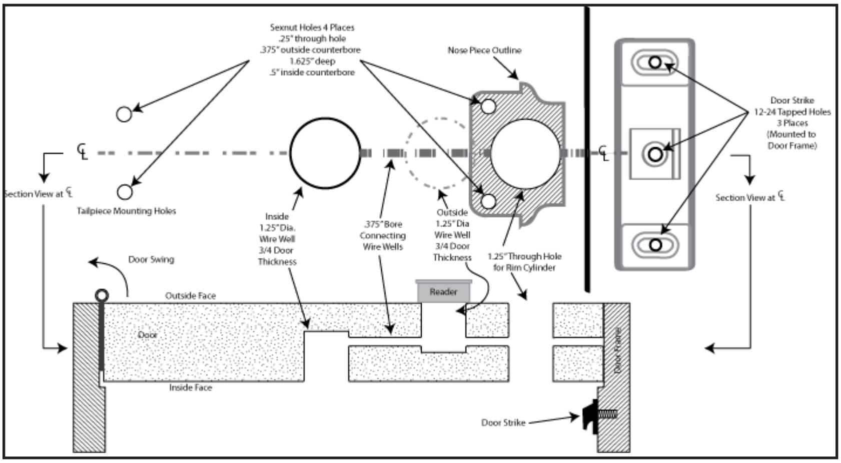
Retrofit	Slab Doors
Use Swiss plates and handles	Swiss plates are not needed

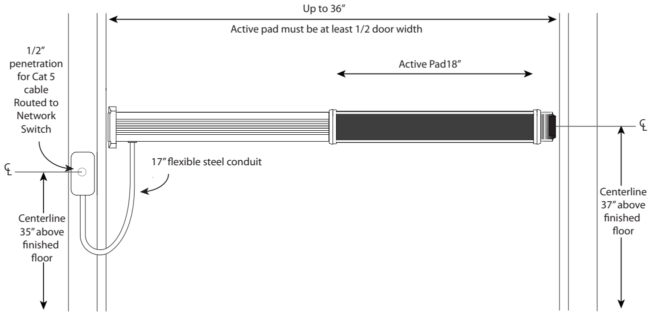
Cable Routing

The reader wiring passes through the door and attaches to the network processor board inside the housing. The network processor board attaches to the network and power by the provided flexible CAT-5e cable. The CAT-5e cable passes through the armored door loop to the hinge side of the door frame. Use the included wire caps to splice the CAT-5e cable to the network drop cable in the armored cable termination. At the network switch (not shown and provided by the IT group) a Midspan device injects power into the network drop cable.

Hole Drilling

It is very important to understand that most holes in the door have the same inside and outside locations but different diameters. Also, note the card reader wiring channel has two “wells” where the holes do not penetrate both faces. They should be deep enough to connect with the center bore drilled from the leading edge of the door. The panic hardware is located relative to the door frame, not the edge of the door. Read carefully.

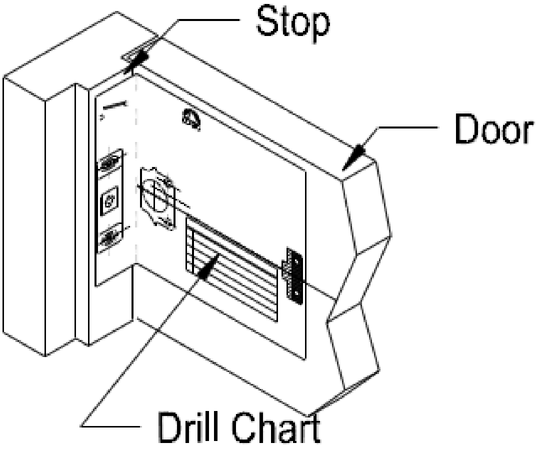



Up to 36"
Active pad must be at least 1/2 door width
1/2" penetration for Cat 5 cable Routed to Network Switch
Active Pad18"
℄
17" flexible steel conduit
℄
Centerline 35" above finished floor
Centerline 37" above finished floor

On Site

Step 1 Marking holes

Measure 37" up from the floor, marking a horizontal line on the door's leading edge. Extend that line on the inside of the door. Locate the paper template drill chart enclosed with the panic hardware. Close the door. On the inside, align the center of the paper template with the 37" line. Follow the template instructions to mark and drill all holes. Some doors have removeable stops that snap off. Mounting the strike directly to the frame is preferred, cutting the stop to fit around the strike. It is important the strike back to be fully supported across its width.
Note: Filler plates may be necessary for some installations.



Strike a mark 24¼" from the leading edge of the door on the panic hardware center line for the card reader 1¼" wire well center.

This well must not penetrate the outside of the door!

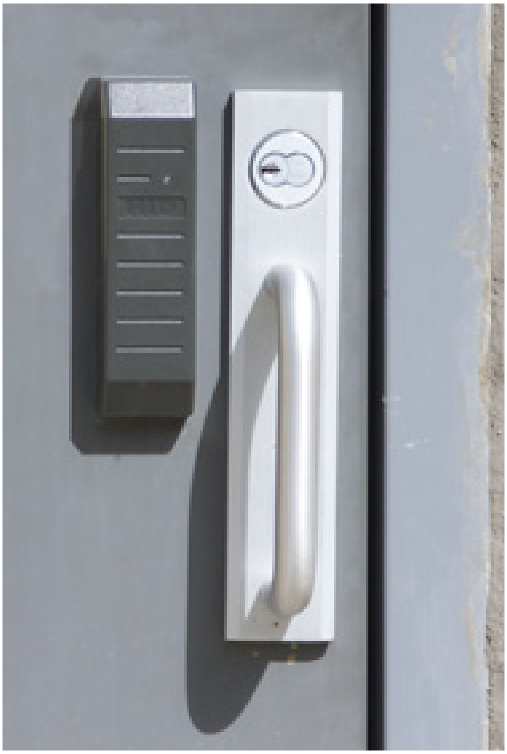
Temporarily mount the nose piece to the housing. Align the holes in nose piece with the holes from the drill chart. Align the housing parallel with the floor. Mark the two rear housing mounting locations.

Marking the Trim (Door Pull) Holes

Retrofit	Slab Doors
Use the Swiss Plates, align the marked holes with the large lock cylinder hole and the two panic hardware holes. Mark the two outer door pull holes. The outer plate has holes for the reader wiring, and two 6/32 tapped holes for mounting	No additional holes should be needed because the door handle uses the same holes as the chassis.

Reader Mounting

Retrofit	Slab Doors
Use the outside Swiss plate to locate the reader wire well.	Follow the instructions in the reader box to mount the support frame adjacent to the door pull. Locate the wire well on the center line of the rim cylinder hole.



Drilling Mounting Holes and Wireway

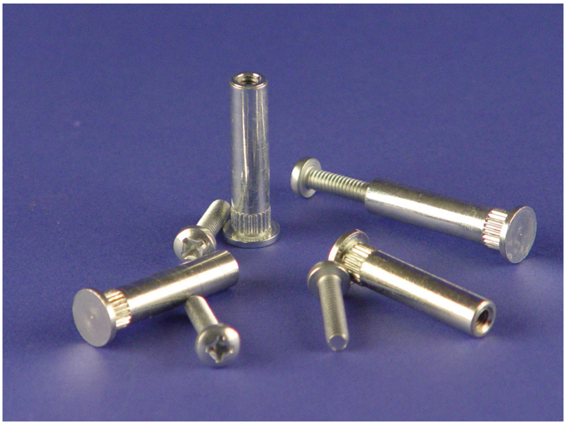
Drill out the center of each hole mark with a ¼" drill. On wood doors use the bullet point bit for a cleaner more accurate hole. The two tailpiece holes must penetrate the door, The drill bubble level helps keep the holes parallel to the floor.

Using the 1¼" hole saw, drill the large hole for the rim cylinder. Next drill the wire well (24¼" from the leading edge) on the inside only.

DO NOT PENETRATE THE OUTSIDE OF THE DOOR!

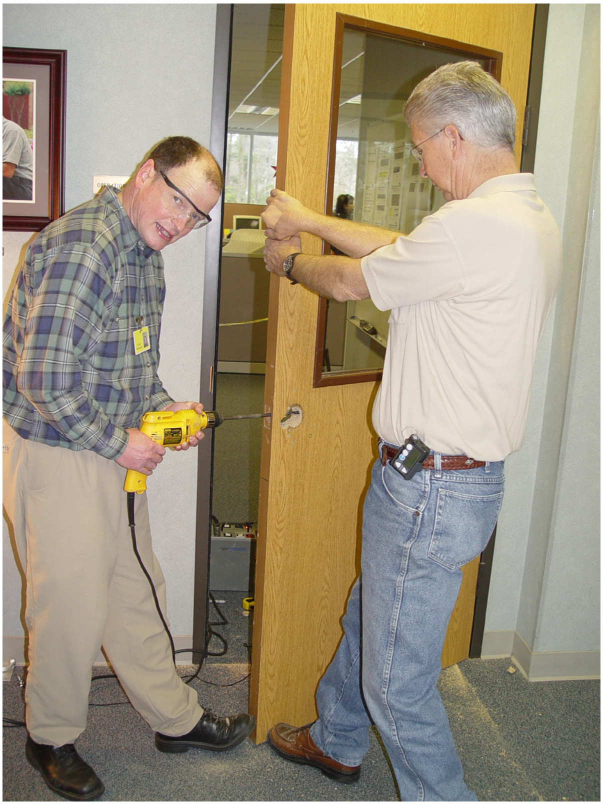
Enlarge all remaining OUTSIDE holes to ⅜" and all INSIDE holes to ½".

Retrofit	Slab Doors
Find four 12-24 sexnuts in the hardware package and insert two into the tailpiece holes and two into the holes closest to the 1¼" hole in the Outside Swiss Subplate at the leading edge of the door. Use the handle and sexnuts found in the door pull box, mate the door pull with the outside swiss plate and clamp both plates to the door using the holes for alignment. Use two 12-24 screws to secure the door pull and plates to the door.	Find two 12-24 sexnuts in the hardware package and insert into the tailpiece holes



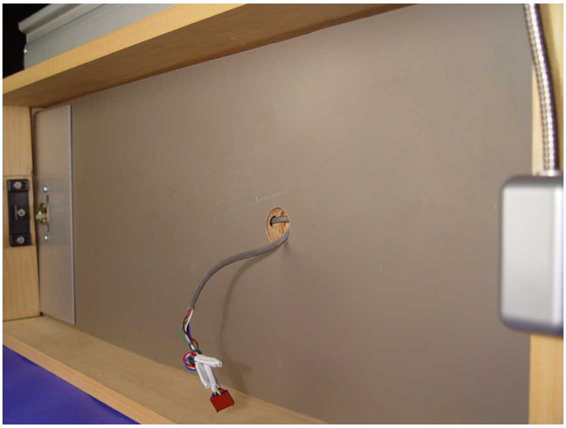
Center bore for reader cable

Use the 36" flexi-bit to drill a hole from the leading edge to the 1¼" wire well at the center of the door. Insert a pull string to connect the wire well and the card reader wire hole on the OUTSIDE.



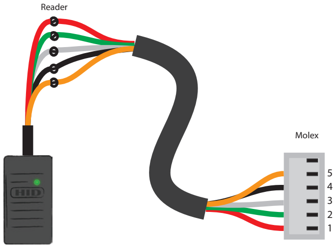
Mount and Connect Card Reader

Now thread a pull string through the horizontal hole to the wire well. Secure the card reader wire to the pull string with electrical tape and pull the card reader wire until the Molex connector is hanging with about 3 inches of slack.



Attach the Reader as shown below using the included "peanuts" in the wire well behind the reader.

Reader to Molex Connection



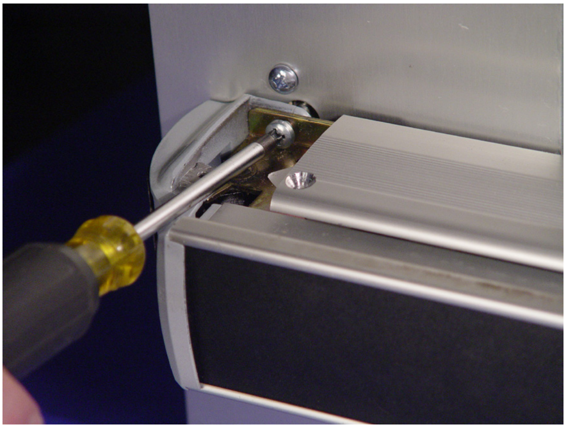
Mount the Rim Cylinder

The customer is to provide a rim cylinder keyed to their master key system. Remove the rim cylinder, trim ring, and mounting screws from the rim cylinder packaging. Trim the rim cylinder tongue to fit. Using the small square rim cylinder back plate in the panic hardware package. You may need to trim the two corners of the plate closest to the tongue hole to 45^0 to clear the sexnut mounting for the panic hardware.

Install the rim cylinder. The tongue hole on the back plate is toward the center of the door, and the two screw holes are toward the leading edge of the door.

Mount the Panic Hardware

Slide the housing back to expose the mounting holes in the chassis. Fish the card reader cable through the back of the housing. Be sure the tongue of the rim cylinder is vertical and mates with the cross hole in the nose piece. Pass two of the included 12-24 screws through the chassis then the nosepiece to tighten into the sexnuts.



Slide the housing until it snugs against the nosepiece. Pass the reader cable through the large hole in the housing. Now secure the tailpiece with two 12-24 screws into the remaining sexnuts near the hinge side of the door. Attach the armored cable housing to the door frame on the hinge side of the door. Drill appropriate holes to bring the network drop cable into the housing.

Thread the included flexible RJ45 cable through the armored cable and attach color for color to the network drop cable. Plug the reader cable into the circuit board, and with the power off, jack the RJ-45 plug into the circuit board.

Close the housing and attach tail plate with included screw.

Rim Latch Plate Installation

Check the swing of the door to make sure it closes completely and does not bounce to a partial open position. Adjust the door closer if necessary.

Line the rim latch plate, marking the top and bottom slots. Using a #16 bit drill holes in the center of the slots.   Next thread the holes with a 12-24 tap. Mount the latch plate with the spacer plate behind it using two 12-24 screws found in the panic hardware package.

Open the door and let it close and latch by itself. Adjust the latch plate to allow a small amount of play when latched. Have a helper wait inside and stand outside repeating the self-closing procedure. The door should secure itself. Using the lock, gently turn the key but do not pull on the door. The door should not "pop" open at all. If it does adjust the rim latch to compensate. Tighten the two mounting screws after each adjustment.

Remove the rim latch to prevent damage to the panic hardware before moving the building.

Final Installation Step

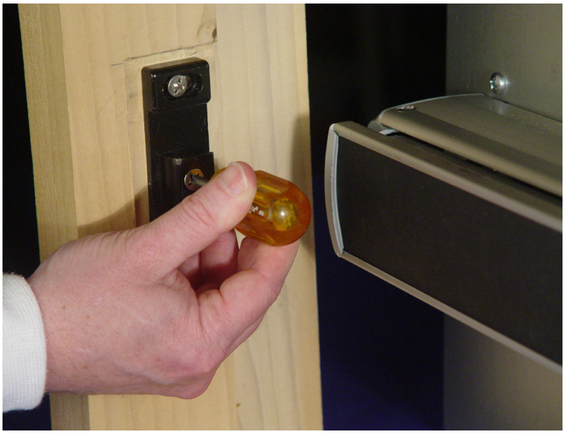
Did you tighten the mounting screws again?

Did you test the door several times for proper operation?

Is the building in its final position?

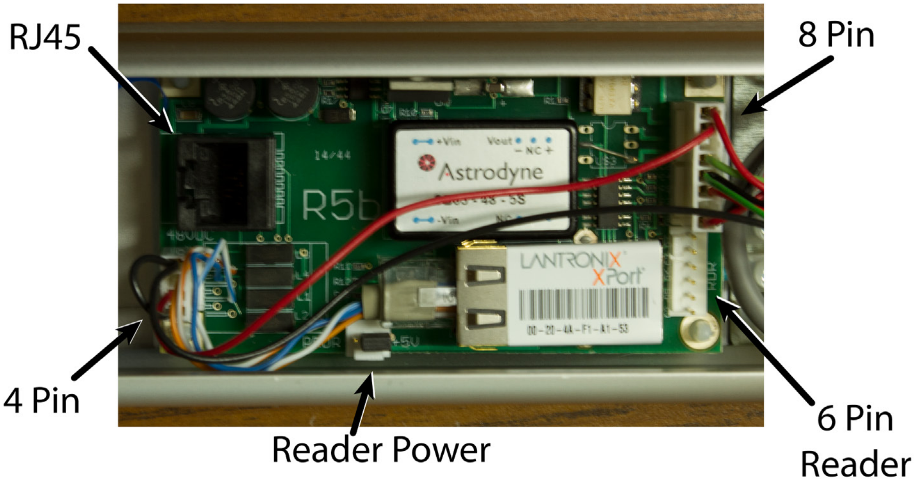
If and only if you can answer these three questions "yes" should you proceed to the final step.

Drill and tap the center hole of the rim latch plate for 12-24.
Install the last 12-24 screw.

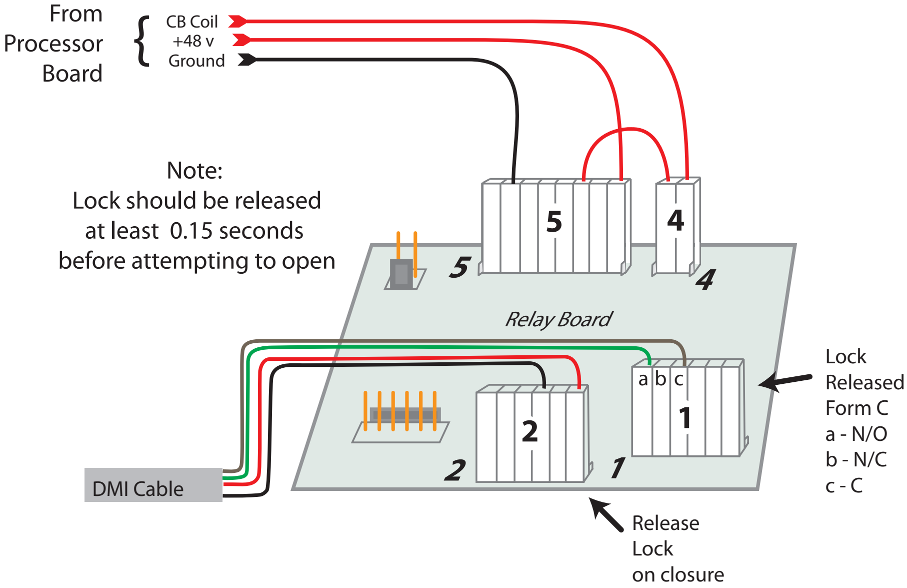


Wiring Hookup

The diagram below shows the processor board connections. The wiring harness from the panic device has an eight-pin and a four-pin connector. The alignment tabs at each end of the connector aids proper seating. The reader cable passes through the large hole in the back of the housing and mates with the six-pin reader connector. The RJ-45 network connection plugs into the indicated jack on the processor board.



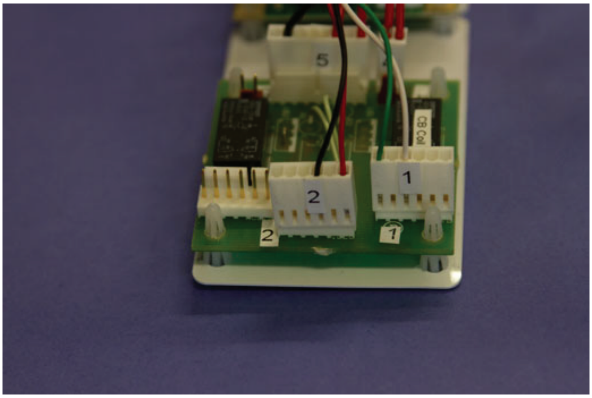
Door Motor Interface



Note:
Lock should be released
at least 0.15 seconds
before attempting to open

Lock
Released
Form C
a - N/O
b - N/C
c - C

Release
Lock
on closure



14 Wiegand Extender

Wiegand Transmitter

The Wiegand transmitter is to be located near the reader. It is installed in series with the reader. Data pulses are amplified (in current and voltage capacity) and stretched to 100 microseconds from the norm of 50 microseconds.

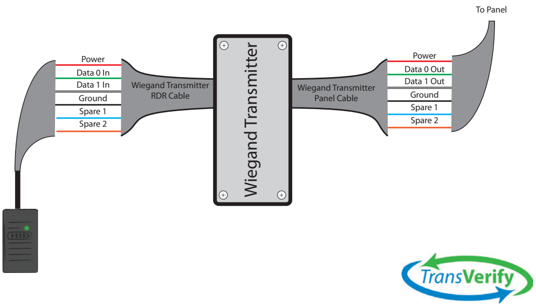
The longer pulses extend the distance a pulse can be sent over a given wire type. You have probably witnessed this effect when driving by a rock concert. You hear the low notes well before the higher ones.

The amplification simply increases the current capacity of the outputs. This allows the companion current mode Wiegand receiver to operate with a higher noise immunity.

Installation

The two cables are marked **To Reader** and **To Panel**. Tie the wires in color for color to their respective cables. The transmitter derives its power from the panel on the Red and Black wires. Data pulses from the reader white and green lines are amplified and stretched. This operation can be observed on the white and green LEDs respectively.

Wiegand Transmitter connections: reader and host panel



Wiegand Receiver

The Wiegand receiver is mounted to the MegaDistributor and provides connections for power, reader, and host panel. The receiver changes the mode of operation for Wiegand data from voltage mode to current mode thus improving noise immunity. This is particularly useful in elevator applications where the Wiegand data must pass through the traveling cable.

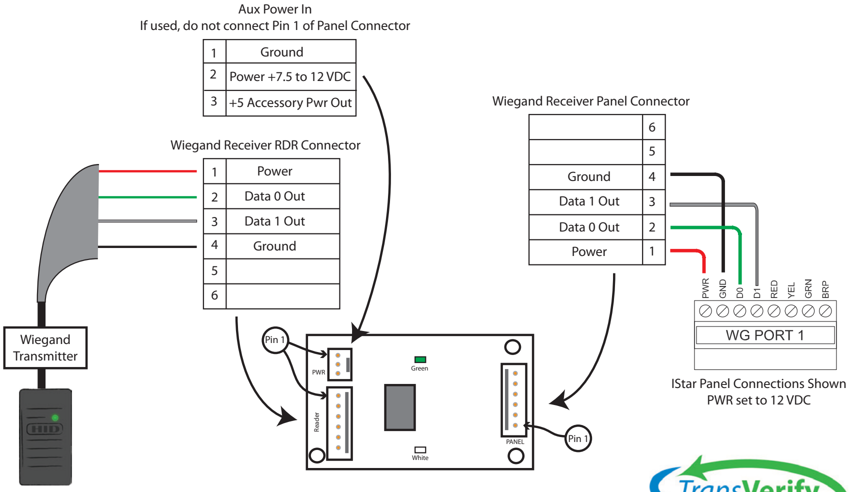
Installation

Data from the reader (Wiegand transmitter), Power, and Data to the host panel are connected as shown below.

IMPORTANT

Use either host Panel Power or Aux Power. Connection of both may cause serious damage to either or both the host panel and the Wiegand Receiver!

Wiegand Receiver connections: power, reader and host panel



Aux Power In
If used, do not connect Pin 1 of Panel Connector

1	Ground
2	Power +7.5 to 12 VDC
3	+5 Accessory Pwr Out

Wiegand Receiver RDR Connector

1	Power
2	Data 0 Out
3	Data 1 Out
4	Ground
5	
6	

Wiegand Receiver Panel Connector

	6
	5
Ground	4
Data 1 Out	3
Data 0 Out	2
Power	1

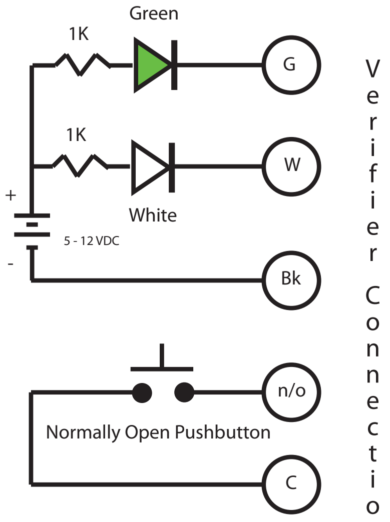
IStar Panel Connections Shown
PWR set to 12 VDC

A Appendix

IP Mask Table

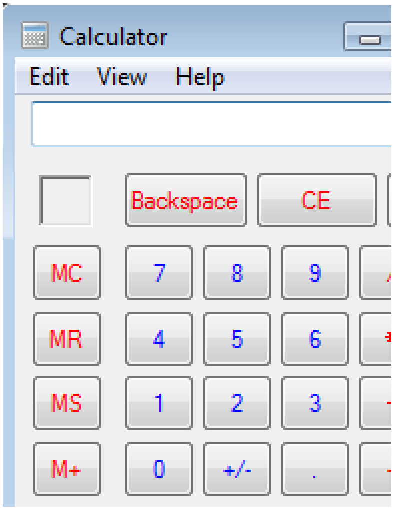
CIDR notation	Network Mask	Host Part
/8	255.0.0.0	24
/16	255.255.0.0	16
/24	255.255.255.0	8
/25	255.255.255.128	7
/26	255.255.255.192	6
/27	255.255.255.224	5
/28	255.255.255.240	4
/29	255.255.255.248	3
/30	255.255.255.252	2
/31	255.255.255.254	1

Verifer Test Harness

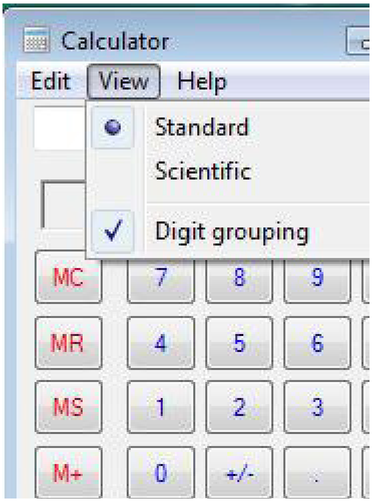


Converting from Decimal to Hexadecimal

Use the Windows calculator to easily change decimal numbers to hexadecimal. The first step is to get the calculator into scientific mode as shown below

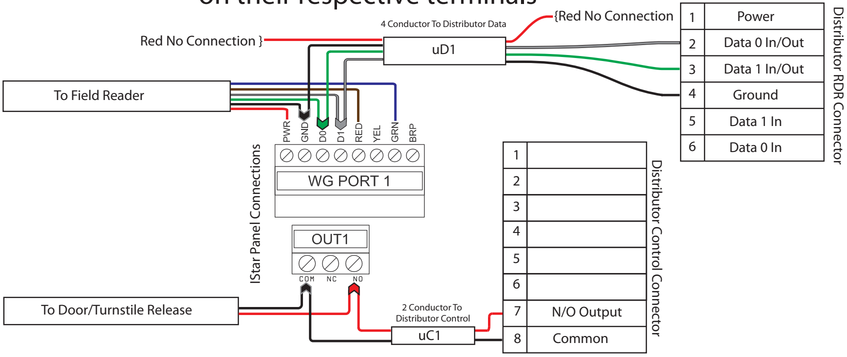


Change the view to scientific.



Typical Distributor Connections

D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel on their respective terminals

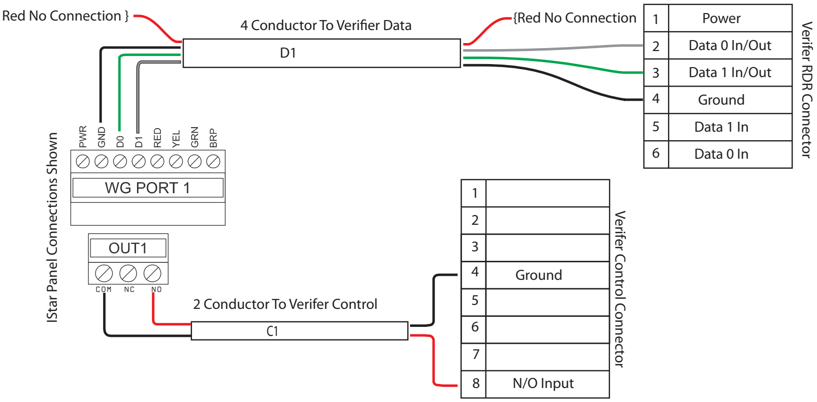

4 Conductor To Distributor Data
Red No Connection }
{Red No Connection
uD1
To Field Reader
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
IStar Panel Connections
OUT1
COM
NC
NO
To Door/Turnstile Release
2 Conductor To Distributor Control
uC1
Distributor RDR Connector
Distributor Control Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

1	
2	
3	
4	
5	
6	
7	N/O Output
8	Common

N/O and Com are connected in parallel

Verifier Connection

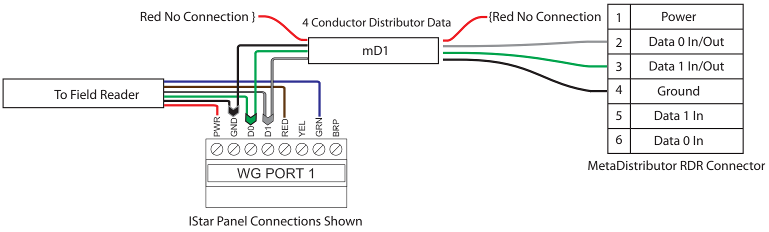

Red No Connection }
4 Conductor To Verifier Data
{Red No Connection
D1
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
IStar Panel Connections Shown
OUT1
COM
NC
NO
2 Conductor To Verifer Control
C1
Verifer RDR Connector
Verifer Control Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

1	
2	
3	
4	Ground
5	
6	
7	
8	N/O Input

MetaDistributor Parallel Connection

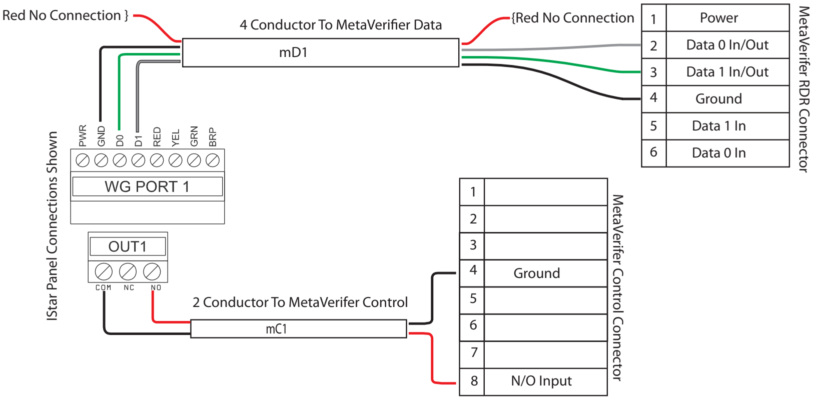
D0 (Grn) , D1(Wht) , and GND (Blk) are connected in parallel on their respective terminals


Red No Connection }
4 Conductor Distributor Data
{Red No Connection
mD1
To Field Reader
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
IStar Panel Connections Shown
MetaDistributor RDR Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

MetaDistributor RDR Connector

MetaVerifier Connection


Red No Connection }
4 Conductor To MetaVerifier Data
{Red No Connection
mD1
PWR
GND
D0
D1
RED
YEL
GRN
BRP
WG PORT 1
IStar Panel Connections Shown
OUT1
COM
NC
NO
2 Conductor To MetaVerifer Control
mC1
MetaVerifer RDR Connector
MetaVerifer Control Connector

1	Power
2	Data 0 In/Out
3	Data 1 In/Out
4	Ground
5	Data 1 In
6	Data 0 In

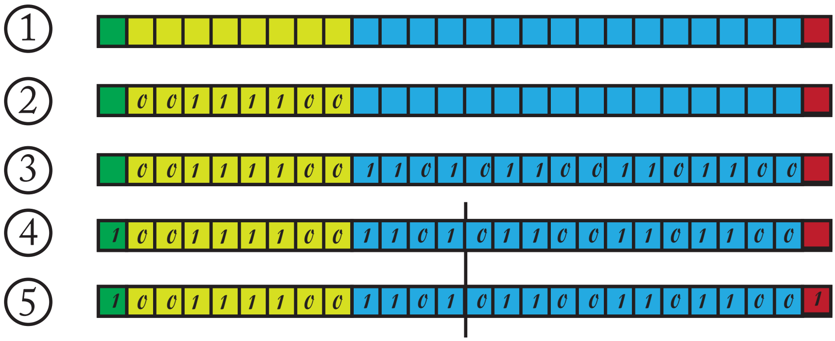
MetaVerifer RDR Connector

1	
2	
3	
4	Ground
5	
6	
7	
8	N/O Input

MetaVerifer Control Connector

Raw Card Calculation

Given a facility code and a PIN number how is the raw card number calculated?



①

② 0 0 1 1 1 1 0 0

③ 0 0 1 1 1 1 0 0 1 1 0 1 0 1 1 0 0 1 1 0 1 1 0 0

④ 1 0 0 1 1 1 1 0 0 1 1 0 1 | 0 1 1 0 0 1 1 0 1 1 0 0

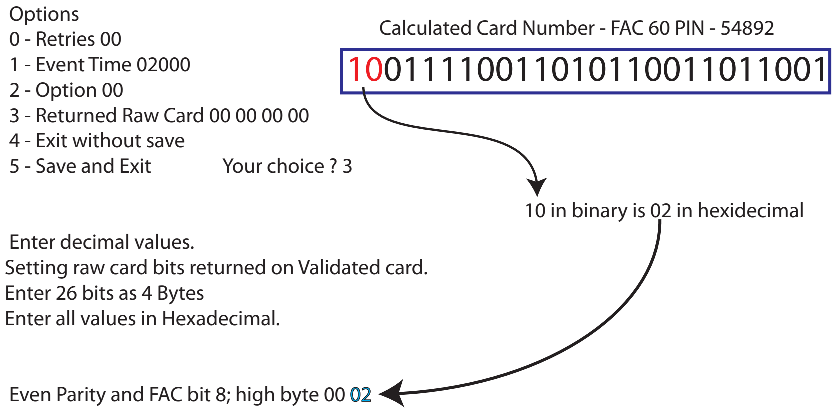
⑤ 1 0 0 1 1 1 1 0 0 1 1 0 1 | 0 1 1 0 0 1 1 0 1 1 0 0 1

Using a 26 bit card as an example, translate the facility code to a binary number, see appendix for instructions, with the Windows calculator. A decimal 60 facility code is binary 00111100. Enter eight ones and zeros in the yellow area into table below ②. Add two zeros to the right, filling all the yellow squares. Next, translate the PIN number, decimal 54892 is binary 1101011001101100. Enter those sixteen ones and zeros in the light blue area ③. The next step is to calculate even parity on the first 12 bits. Count the 1's to the left of the dividing line. If your count is odd, enter a 1 in the dark green square; if even enter a 0. The count is odd, 7, enter a 1 ④. Now we can calculate odd parity on the last 12 bits. Count the 1's to the right of the dividing line. If your count is odd, enter a 0 in the dark red square; if even enter a 1. The count is even, 6, enter a 1 ⑤.

Raw Card Entry

IMPORTANT NOTE

Use a facility code for the return raw card unique to the building.



```
Options
0 - Retries 00
1 - Event Time 02000
2 - Option 00
3 - Returned Raw Card 00 00 00 00
4 - Exit without save
5 - Save and Exit            Your choice ? 3


Enter decimal values.
Setting raw card bits returned on Validated card.
Enter 26 bits as 4 Bytes
Enter all values in Hexadecimal.


Even Parity and FAC bit 8; high byte 00 02
```

Calculated Card Number - FAC 60 PIN - 54892

10011110011010110011011001

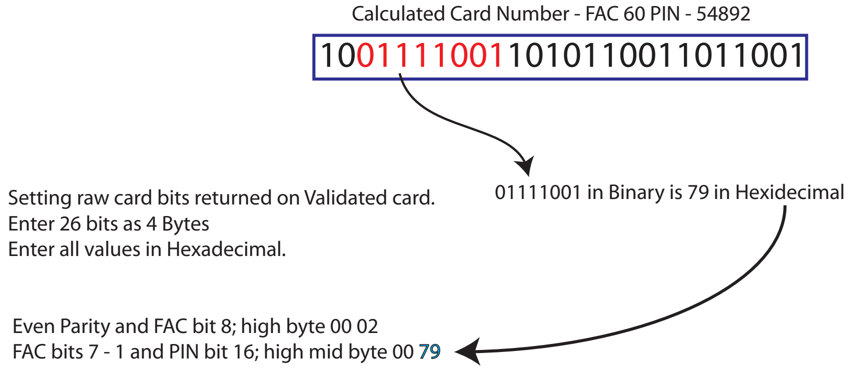
10 in binary is 02 in hexidecimal

This section describes how to take a 26 bit binary raw card number and enter it as 4 hexadecimal bytes. We will illustrate the process using an example card with a Facility code of 60 and an internal or PIN number of 54892. The bits from a card with these numbers is shown in the upper right. The bits of this card that are to be translated to binary are shown in red.

The first byte will only carry the parity for the first 12 bits and the first bit of the Facility Code. In our example the parity is calculated to be a 1 and the first bit of the facility code is a 0. Our entry will be 02 in hexadecimal.

The Windows calculator described in the appendix can translate from binary to hexadecimal

The second entry will be the remaining 7 bits of the Facility code and the first bit of the PIN number.



Calculated Card Number - FAC 60 PIN - 54892

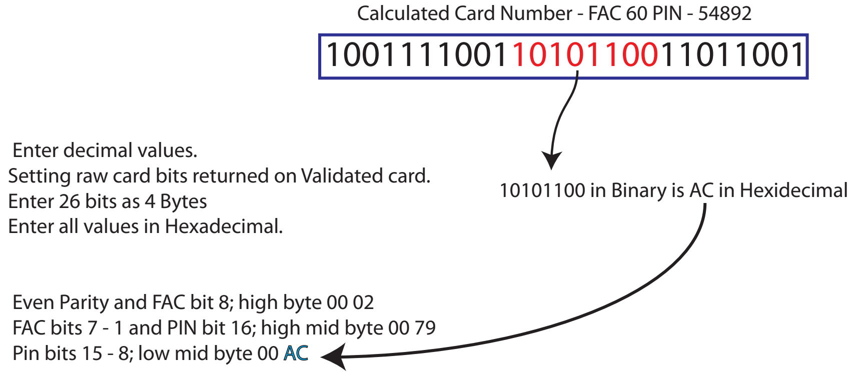
10011110011010110011011001

01111001 in Binary is 79 in Hexidecimal

Setting raw card bits returned on Validated card.
Enter 26 bits as 4 Bytes
Enter all values in Hexadecimal.

Even Parity and FAC bit 8; high byte 00 02
FAC bits 7 - 1 and PIN bit 16; high mid byte 00 79

The third entry will be bits 8 through 15 of the PIN number



Calculated Card Number - FAC 60 PIN - 54892

10011110011010110011011001

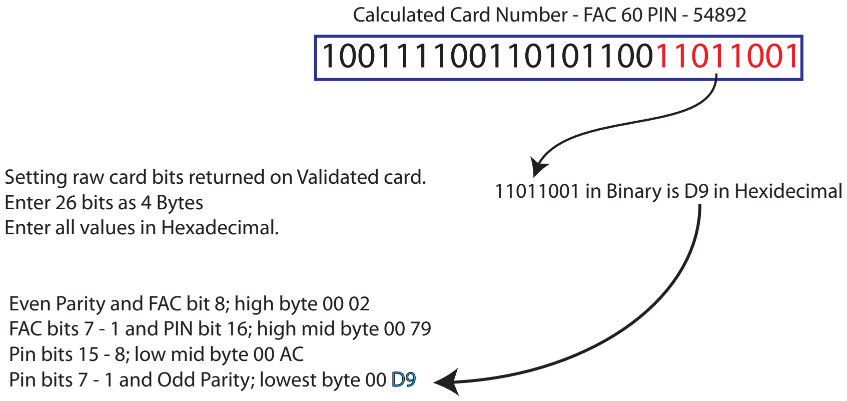
Enter decimal values.
Setting raw card bits returned on Validated card.
Enter 26 bits as 4 Bytes
Enter all values in Hexadecimal.

10101100 in Binary is AC in Hexidecimal

Even Parity and FAC bit 8; high byte 00 02
FAC bits 7 - 1 and PIN bit 16; high mid byte 00 79
Pin bits 15 - 8; low mid byte 00 AC

The last entry will be the remaining PIN bits and the odd parity bit calculated on the last 12 bits of the card number

.



Calculated Card Number - FAC 60 PIN - 54892

10011110011010110011011001

11011001 in Binary is D9 in Hexidecimal

Setting raw card bits returned on Validated card.
Enter 26 bits as 4 Bytes
Enter all values in Hexadecimal.

Even Parity and FAC bit 8; high byte 00 02
FAC bits 7 - 1 and PIN bit 16; high mid byte 00 79
Pin bits 15 - 8; low mid byte 00 AC
Pin bits 7 - 1 and Odd Parity; lowest byte 00 D9

A tutorial is available at www.TransVerify.com which has helped many understand the math behind this process.