UNC100

HARDWARE MANUAL

Revision 1.4

new generation
building security

RBH ACCESS

WWW. RBH-ACCESS.COM

Copyright Notice

Trademark

Disclaimer

RBH ACCESS TECHNOLOGIES INC.

2 Automatic Road, Suite 108
Brampton, Ontario
CANADA
L6S 6K8
Tel: (905) 790-1515
Fax: (905) 790-3680
Email: info@rbh-access.com
WWW: www.rbh-access.com

Contents

Revision History

Editor	Revision	Comment	Date mm/dd/yyyy
DM	1.0	First Release	08/13/2013
RB	1.1	Removed reference to fire input Removed partial firmware upgrade (formats) Added dip-switch 5 Added Revision History Updated copyright Eliminated reference to rack mount type Clarified the use of the Power Input/ Output Moved all cable specs to one location. Moved all input specs to one location. Moved all output specs to one location. Reduced the number of pages.	03/19/2014
DM	1.1	Minor editing of text.	03/24/2014
RB	1.2	Changing output voltage from 12V to 12v – 14v Changing battery charger spec	07/21/2014
DM	1.2	Minor editing.	07/31/2014
DM	1.2	ULC text added.	08/06/2014
RM	1.3	Added OSDP /OSDP-S Reader options Added E-NET communication Added AES option for Encrypted communication between PC and master UNC-500 and between slave UNC-500s	08/10/2020
RM	1.4	Updated copyright year Rearranged text and Images	01/14/2021
RM	1.4	Added UL 294 Declaration Table	02/03/2021

Introduction

The RBH-UNC100 series is a welcome addition to the new generation of powerful and reliable Axiom hardware. The two door native TCP/IP controllers come equipped with onboard battery backup chargers and accommodate up to 16 individual IOC-16 input/output controllers or 254-SafeSuite keypads. The units are expandable to 8 doors, using 3 additional RC-2 or NIRC/NURC controllers.

The UNC-100 also features a 32-bit processor with encryption and expanded memory.

The UNC100-132 models come equipped with IEEE 802.3at compliant PoE capability, further increasing this UNC series' award-winning efficiency.

POE Features are:

- IEEE 802.3at Compliant
- 30 Watt power rating
- Built-in battery backup with charger
- Operates with non-compliant PoE+PSEs
- Available auxiliary power output

UNC-100 unit fits into existing enclosures and if ordered with metal protective shell can be mounted directly on back boards or inside of 3rd party cabinets.

UNC-100 uses AES-256 bit encryption for secure communication over Ethernet. This communication can be either between the host computer & master panel or amongst the master & slave panels. Both panel & the host computer needs to be provided with a Customer Key and need to enable AES option both in Axiom and UNC-100.

C e r t i f i c a t i o n s

FCC, CE, UL-1076, ULC-S319-05 III, UL-294, UL-294B compliance, all wiring into the chassis mount panel's cabinet must enter through metal conduit. Also be sure to mount the panel in a protected area.

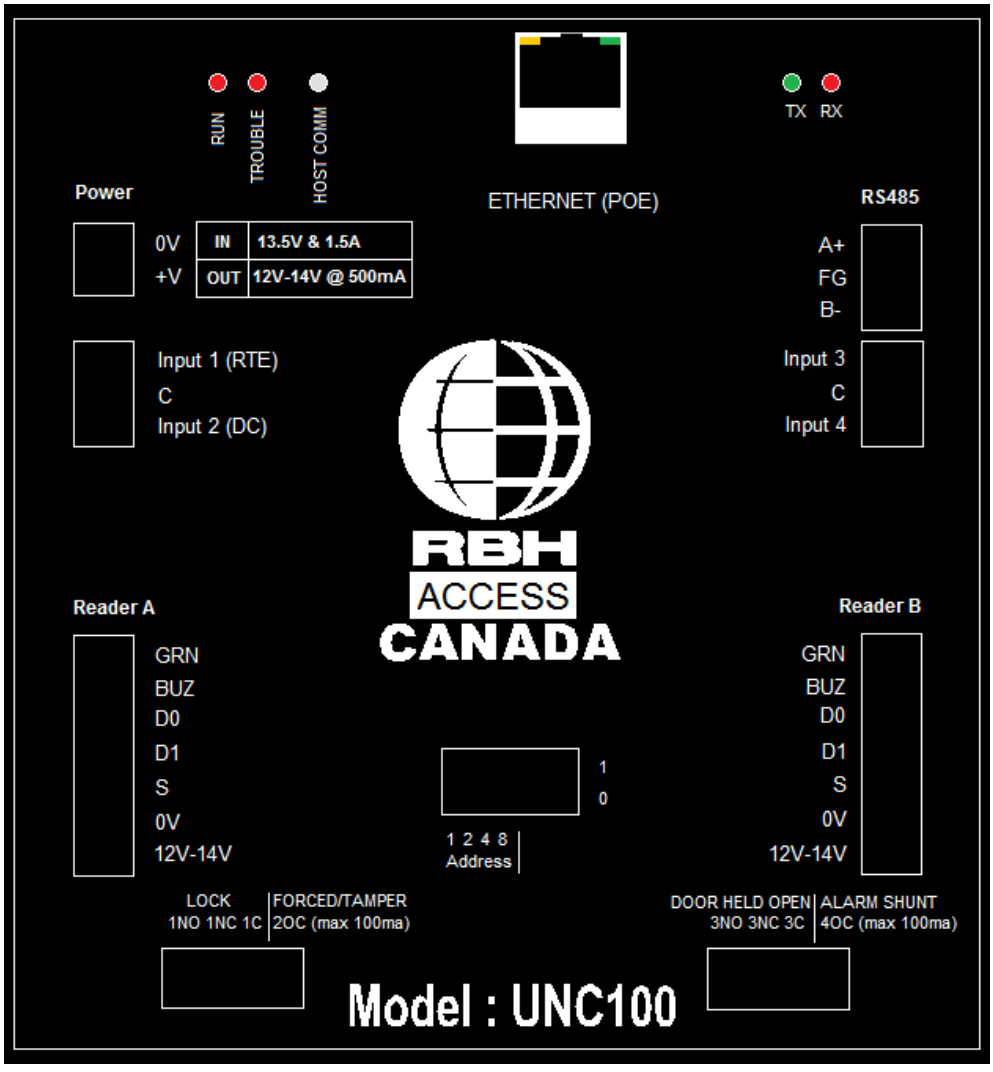
Declaration Performance level Definitions of UNC-100 under evaluations in the table below according to UL 294 Ed7 section 8 Performance level Definitions for Access Control in table 8.

Declaration Levels for UNC-100

Feature	Levels
Destruction Attack Level	Level III
Line Security	Level II
Endurance Level	Level IV
Standby Power	Level IV
Single Point Locking device with key Locks	Level I

UNC100 Controller Description

The Axiom™ access control system consists of one or more network controllers (**UNC100**). All information required by the controller is downloaded from the PC and stored locally non-volatile flash memory. This information includes configuration data, cardholder records, access levels, schedules, and all other records necessary for the operation of the system. The controller operates independent of the PC and all decision-making is performed locally, even in the event of total power loss.



Battery Protection

To protect the battery from being drained during shipping/storage of the UNC100, there is a small paper between the battery and the panel. This must be removed before powering up the panel.

PC Connection

The Master UNC-100 is connected through the local Ethernet via a static IP address. The means of communication is configured in the Axiom™ software under *Network Configuration/Port Type*.

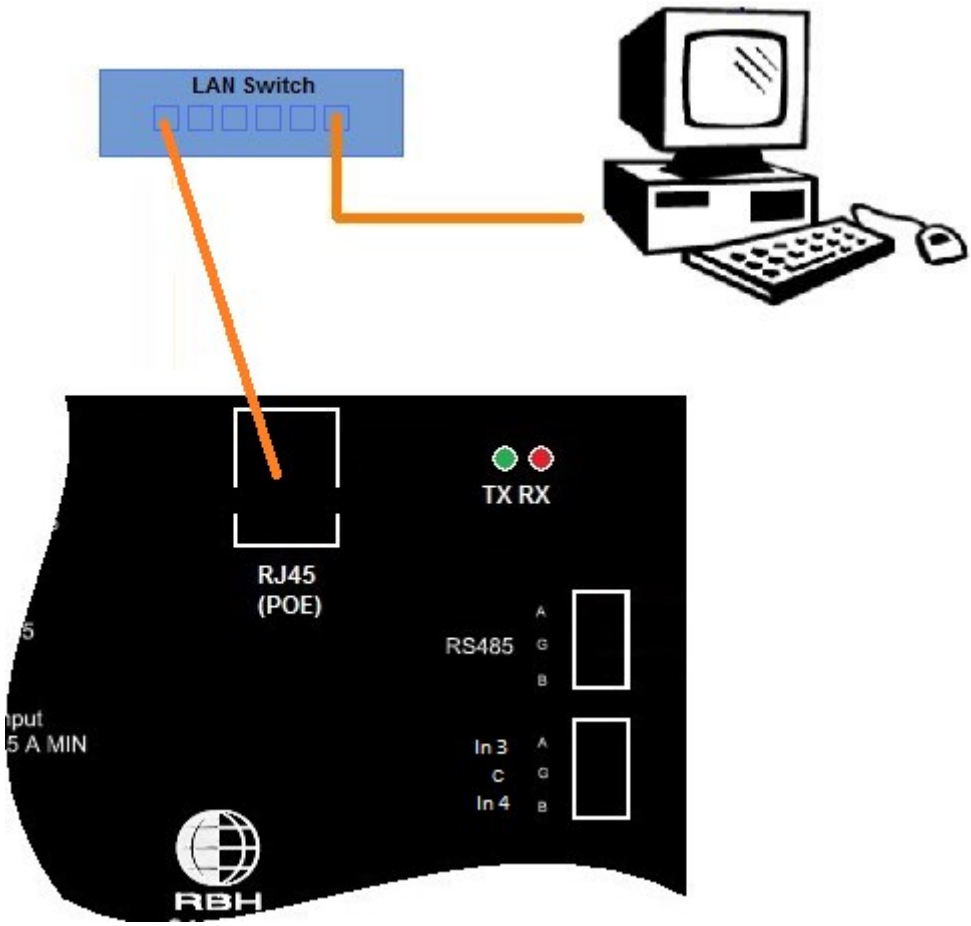
UNC100 TCP/IP Connection

The master controller in installations is linked by the local Ethernet. The system supports a static IP address only [*default address is 192.168.168.125*] and Port 3002.

UNC-100 uses AES-256 bit encryption for secure communication over Ethernet. This encrypted communication can be either between the host computer & master panel or amongst the master & slave panels. Both UNC-100 & the host computer needs to be provided with a Customer Key and need to enable AES option both in Axiom and UNC-100.

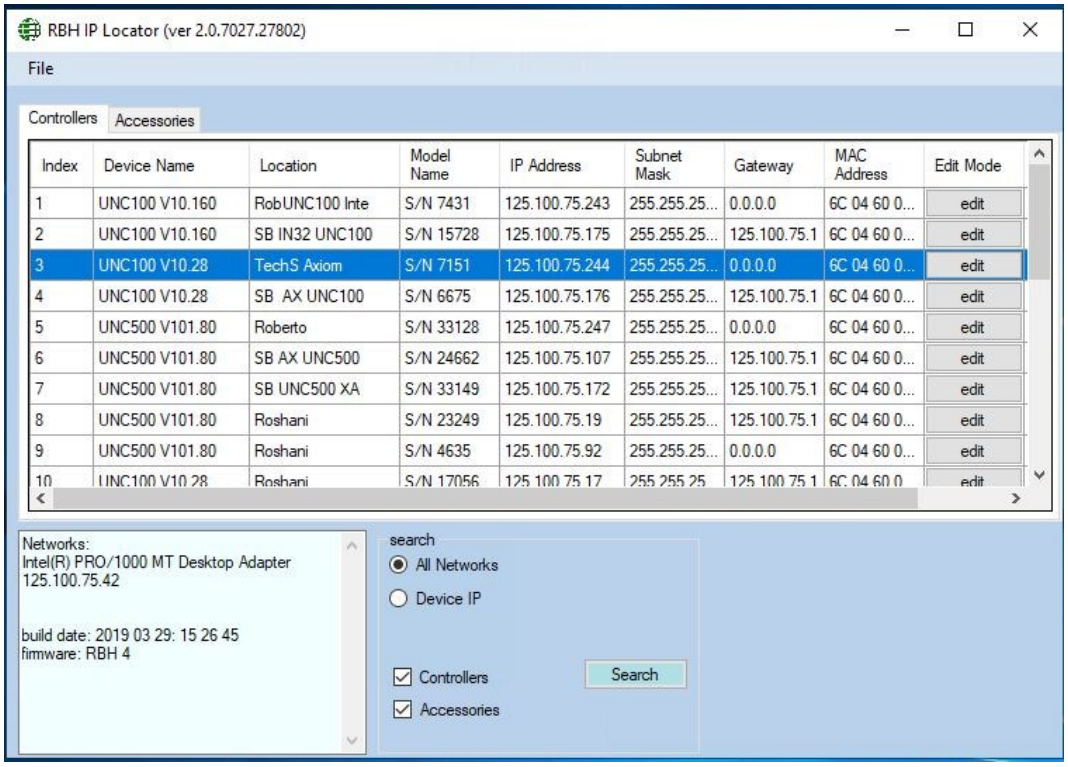
To change the IP address of the unit or enable/disable AES option, users can use ***IP Device Discovery*** [*a utility program provided by RBH*]

PC to UNC100 Connection - LAN

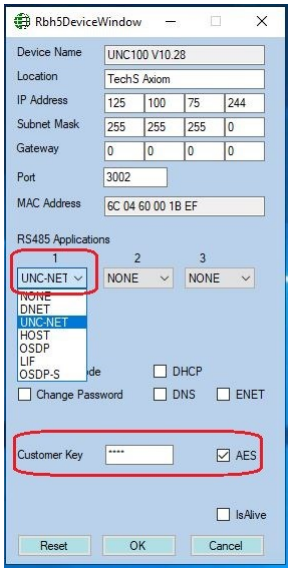


IP Device Discovery

When the IP Device Discovery program finds an Ethernet connected panel with the correct requirements it will display under “Edit Mode” an *edit* button.
When pressed, the software will allow the editing of the following items; Location Text, IP data, LIF/LAN application parameters, Channel Application and Encryption (AES) and other options.



Make changes to the various items displayed. After entering the data and clicking on “OK” the unit will re-boot. Please note that only Channel 1 is available for UNC100 RS485 Applications..



Battery Charger

The battery charger routes input power from the 13.8v input source or POE module and constantly monitors the battery voltage.

Reverse Battery Protection

A combination of a three ampere diode and a 1.6 amp thermal fuse protects against accidental connection of a battery in the reverse direction.

Battery Test

A battery test cycle is operator initiated or scheduled. When initiated the charger is turned off and a 24Ω resistor provides a load to the battery for about ten seconds. If during this period the voltage drops below 10 volts a battery alarm message is sent to the host, otherwise a battery normal message is sent.

Fuse Monitoring

Besides monitoring the battery voltage the UNC100 also monitors the input voltage (DC), auxiliary voltage (aux) and the reader voltage (reader) and reports to the host whenever the state changes.

Diagnostic LED's

The RS485 circuit has a red and green LED to indicate when a signal is received or transmitted.

Host Comms LED is a bicolour LED when red indicates receiving data from the host and when green indicates transmission of data.

Run LED will flash slowly when connected to the host and quickly when not connected.

Trouble LED will flash when a power problem such as a low battery or low auxiliary power is detected.

Tamper Detection

A tamper wire may be connected to JP1 located close to the center of the board. A short to this input is normal and an open is alarm.

RAM Memory

The static ram memory holds the database from the host (capable of handling 50k cards) that is downloaded using Axiom software. The coin cell provides power to the memory as well as the real time clock.

Power Input / Output

Located on the top right corner of the board is a jumper that selects if the power terminals are to be used to supply power or provide power. Select "OUT" when using a POE supply and require 13.8V @ 500ma for other equipment.
When not using POE, the jumper should be set to "IN".
The UNC100 controller requires 13.8VDC to be supplied from an external source. (Note: Although the unit can run on 12VDC, you will need 13.8VDC to be able to charge backup batteries.

UNC-100 Communication

The UNC100 has one RS485 port and an Ethernet 10/100 interface. Communications from the host computer running Axiom software can be achieved in the following ways; either via the Ethernet interface or via RS485 through a direct connection to a designated channel. The UNC100's RS485 channel may be programmed as HOST, DNET, UNC-NET, LAN, and OSDP/OSDP-S. Use the DIP switch to select baud rate for Host communications as 9600, 38400, 57600, or 115200.

Networks

There are three networks supported by the UNC100 these are:

1) **Host Communications** through the Ethernet. **Host communication between PC and UNC-100 can be encrypted by using AES-256 bit encryption.**
2) **Device Communications** for devices such as additional RC-2s starting at address 2, Alarm Keypads, IOC-16 controllers, and PC100.
3) **Controller Communications** for controllers such as additional UNC500s or for UNC100s via **:**
    a. **UNC-NET,** a protocol designed for RS485 communications between UNC100's and UNC500s.
    b. **E-NET**, a method designed using Ethernet port rather than physical RS-485 connections between UNC100's, and a mix of UNC100s and UNC500s

RS485 Applications

Application name	Description
HOST	The Host port connects the UNC100 to a PC through an RS485 interface.
D-NET	The D-NET (Device Network) connects local device controllers (RC-2, IOC-16, SafeSuite™ Panels, NRC2000, or NURC2000) to the UNC100 controller on a high-speed bi-directional RS485 network.
UNC-NET	The UNC-NET (Controller Network) connects the UNC100 controller to other on a high-speed bi-directional RS485 network.
OSDP/OSDP-S	**O**pen **S**upervised **D**evice **P**rotocol (OSDP) communication protocol is for interfacing one or more Peripheral Devices (PD) to a UNC100 controller. The communication over OSDP can be encrypted/unencrypted. When encrypted, OSPD-S option need to be selected *(Available in Firmware 10.28 and up.)*

DIP Switch Settings

The UNC100 DIP switch controls the device's address and serial port baud rate.

☞ **To Clear Panel memory – All DIP switches must be off and the unit powered off and on.**

DIP Switch	
DIP Switch	Function
1 - 4	Controller Address
5	Ethernet Secure Mode[1]
6,7	Controller Baud Rate
8	Not used

Controller Addressing

Use DIP switches 1, 2, 3, and 4 to select the controller address. The address is binary coded and the switch settings for all fifteen possible addresses are given below.

Controller Addressing				
Switch 1	Switch 2	Switch 3	Switch 4	Address
On	Off	Off	Off	1 (Master)
Off	**On**	Off	Off	2 (Slave)
On	**On**	Off	Off	3 (Slave)
Off	Off	**On**	Off	4 (Slave)
On	Off	**On**	Off	5 (Slave)
Off	**On**	**On**	Off	6 (Slave)
On	**On**	**On**	Off	7 (Slave)
Off	Off	Off	**On**	8 (Slave)
On	Off	Off	**On**	9 (Slave)
Off	**On**	Off	**On**	10 (Slave)
On	**On**	Off	**On**	11 (Slave)
Off	Off	**On**	**On**	12 (Slave)
On	Off	**On**	**On**	13 (Slave)
Off	**On**	**On**	**On**	14 (Slave)
On	**On**	**On**	**On**	15 (Slave)

[1] DIP switch 5 up will enables Ethernet Secure Mode. This will prevent access to the panel's programming through the Ethernet.

Master Controller

Each network must have a single unit designated as the master controller. The master controller connects to the PC. Setting the DIP switch address to 1 will automatically designate a unit as the master controller.

Slave Controller

All controllers addressed 2 through 15 are referred to as slave controllers.

Ethernet Secure Mode

When dip-switch 5 is ON the IP locator program cannot locate the unit on the Ethernet and therefore cannot make any changes or reset the unit.

RS485 (HOST) Port Baud Rate Selection (Master Only)

The controller's serial port baud rate is set with controller DIP switches 6 and 7. This setting determines the speed used to communicate with the PC; the controller baud rate must be the same as the baud rate set for the port within the Axiom™ software. The default baud rate is 9600.

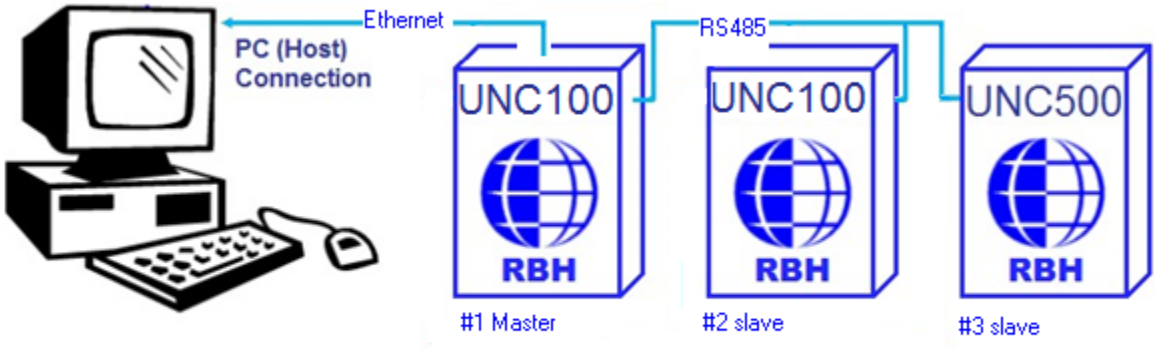
Controller Baud Rate Selection

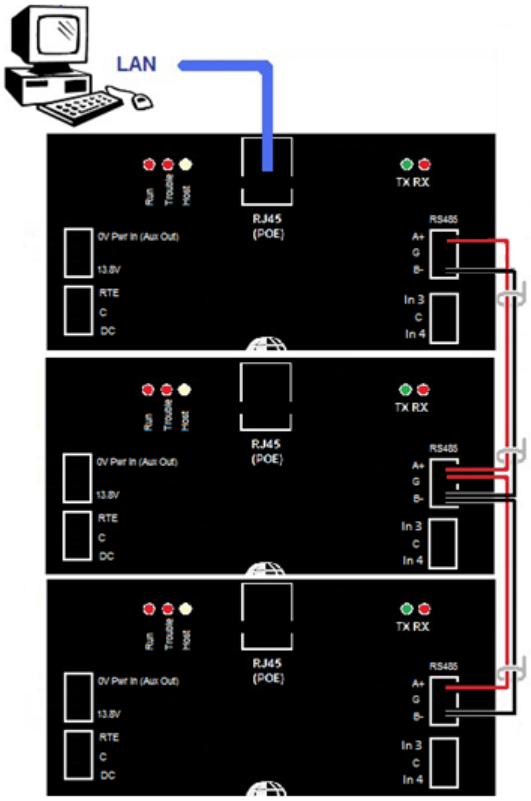
DIP Switch 6	DIP Switch 7	Baud Rate
OFF	OFF	9600
ON	OFF	38400
OFF	ON	57600
ON	ON	115200

UNC-NET (Controller Network)

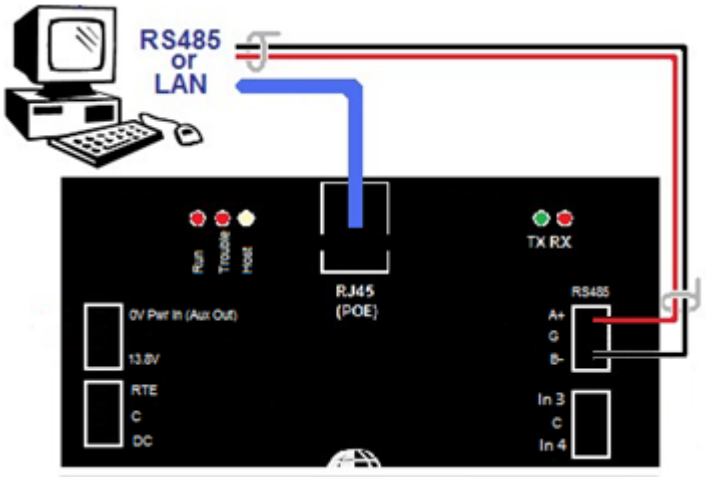
Up to fifteen network controllers (UNC-100) can be linked together and feed into a single communication port on the PC. Controller number 1 is designated the master controller and connected to the PC using TCP/IP communications. The remaining controllers are referred to as slaves and can only communicate to the PC through the master UNC-100.

UNC-NET (Controller Network)





When combining UNC500s and UNC100s; connect the RS485 of the previous UNC100 to CH3 (Configured as UNC-NET) of the UNC500.



If host connection is made through the RS485 port, then only one panel can be connected.

UNC-NET Cable

Use 20 to 22 AWG shielded stranded twisted pair cable for all UNC-NET connections.

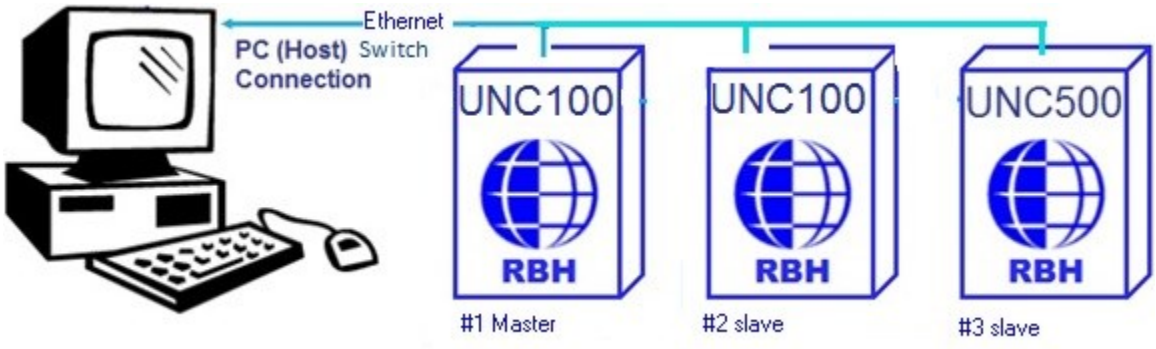
UNC-NET Maximum Cable Length

The maximum distance for any link in the UNC-NET is 2500 feet (760 meters) and the total length cannot exceed 10000 feet (3000 meters).

E-NET (Ethernet Network)

To avoid the use of an RS485 port a method has been developed that uses the Ethernet port as a C-NET port.

The basic principle of the E-NET is to allow a group of controllers to be virtually wired together by sharing a membership list. Only units belonging to the list will be able to talk to each other.



The master controller is the controller that has an E-Net socket connection to Axiom software (available in AxiomXA™ software in *Advance* tab of *Network Configuration*).

ENET option needs to be enabled in device locator as well.

Once checked only E-NET communications will be used.

The IP address has to fall in the range of the subnet mask in order for UNC-500s to talk to each other and duplicate addresses are not allowed.

E-NET communication can be encrypted or unencrypted.

E-Net Encryption

RBH system uses AES-256 bit encryption, for secure communication over Ethernet. This communication can be either between the host computer & master panel or amongst the master & slave controllers.

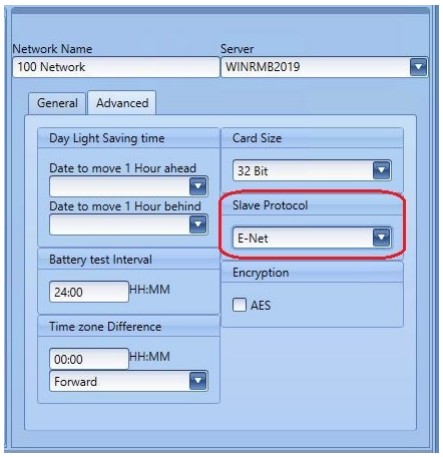
Both Master panel & the host computer needs to be provide with the AES key. Also for communication amongst the slave panels ENET feature has to be enabled.

Before E-net configuration, all the UNC-100s need to be upgraded to Firmware 10.28.

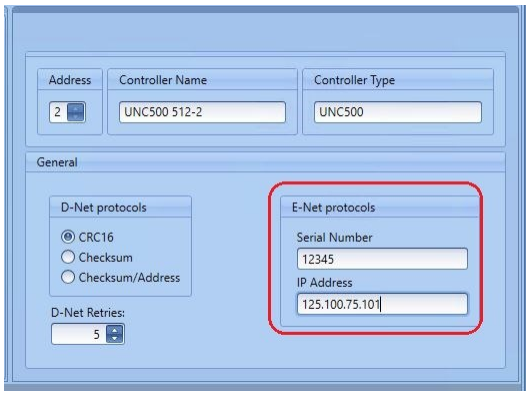
Steps to enable E-net Encryption

To achieve encryption the following steps have to be followed:

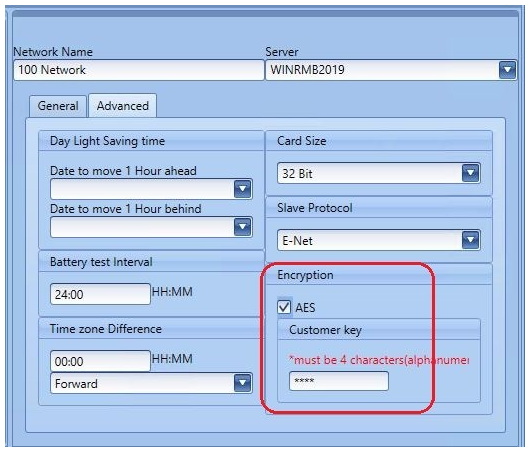
In the advanced tab of Network Configurations of AxiomXA software, select *E-Net* as Slave Protocol.



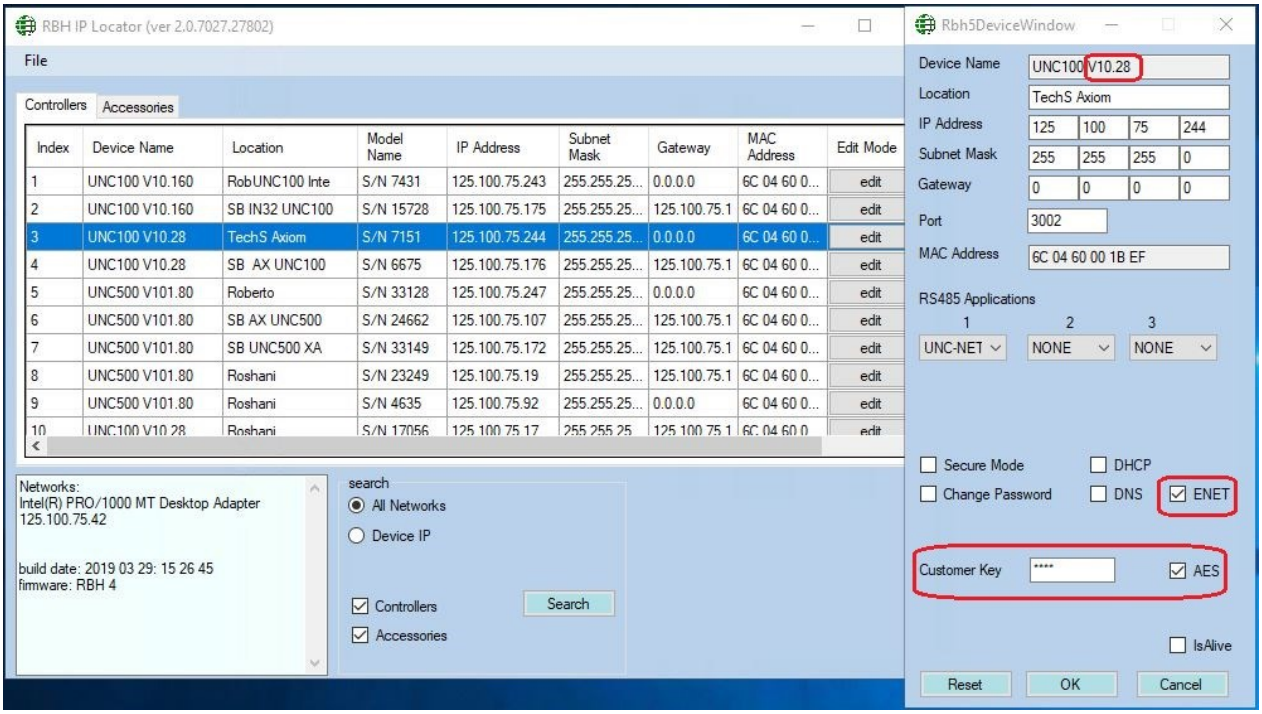
In Master and Slave UNC-100s configuration enter serial number and IP address of panels.



In the advanced tab of Network Configurations, check *AES* option and enter a four character customer key.



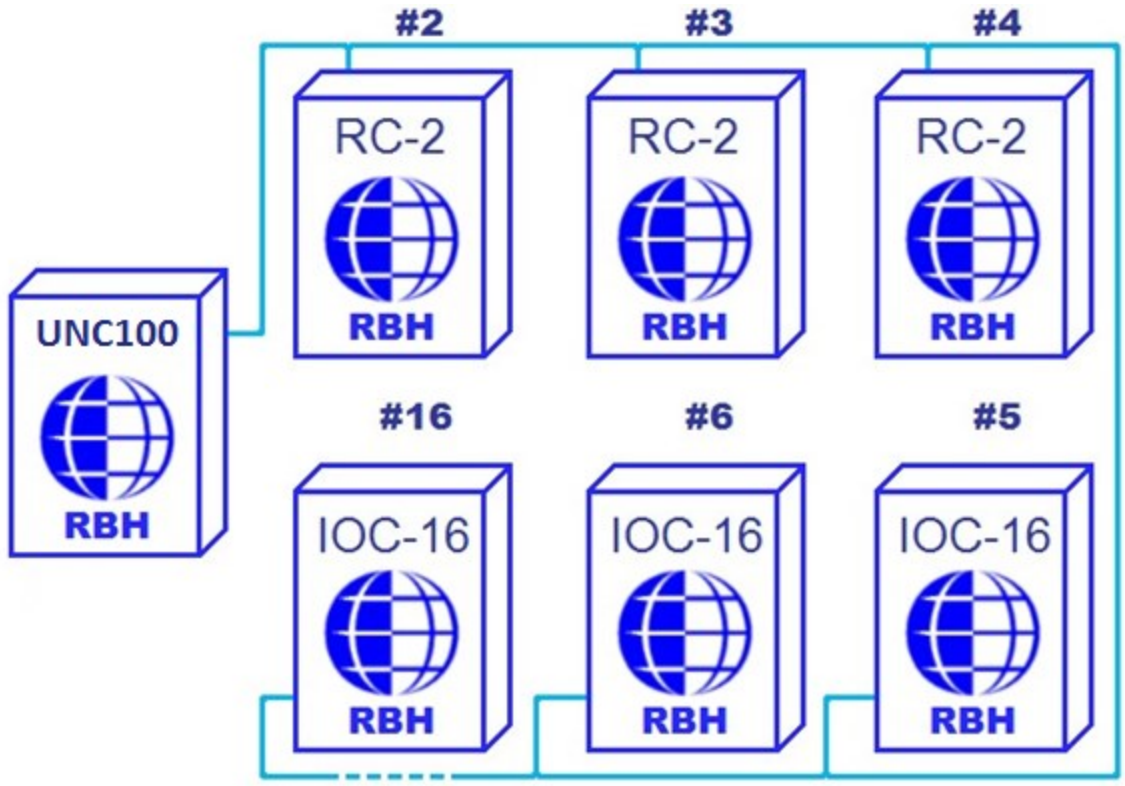
Using the IP Device Discovery Program, check the *AES* box and enter the same four character customer key matching the one added in software.



D-NET Device Network

Up to four RC-2 reader controllers (The UNC100 is configured for 1, then you can connect 3 physical RC2s), and up to sixteen IOC-16 input/output controllers, may be connected to each network controller in the UNC-NET using high speed RS485 communications.

D-NET (Device Network)



NRC2000 panels may be used in place of RC-2 panels.

NURC2000 may also be used in place of RC-2 panels.

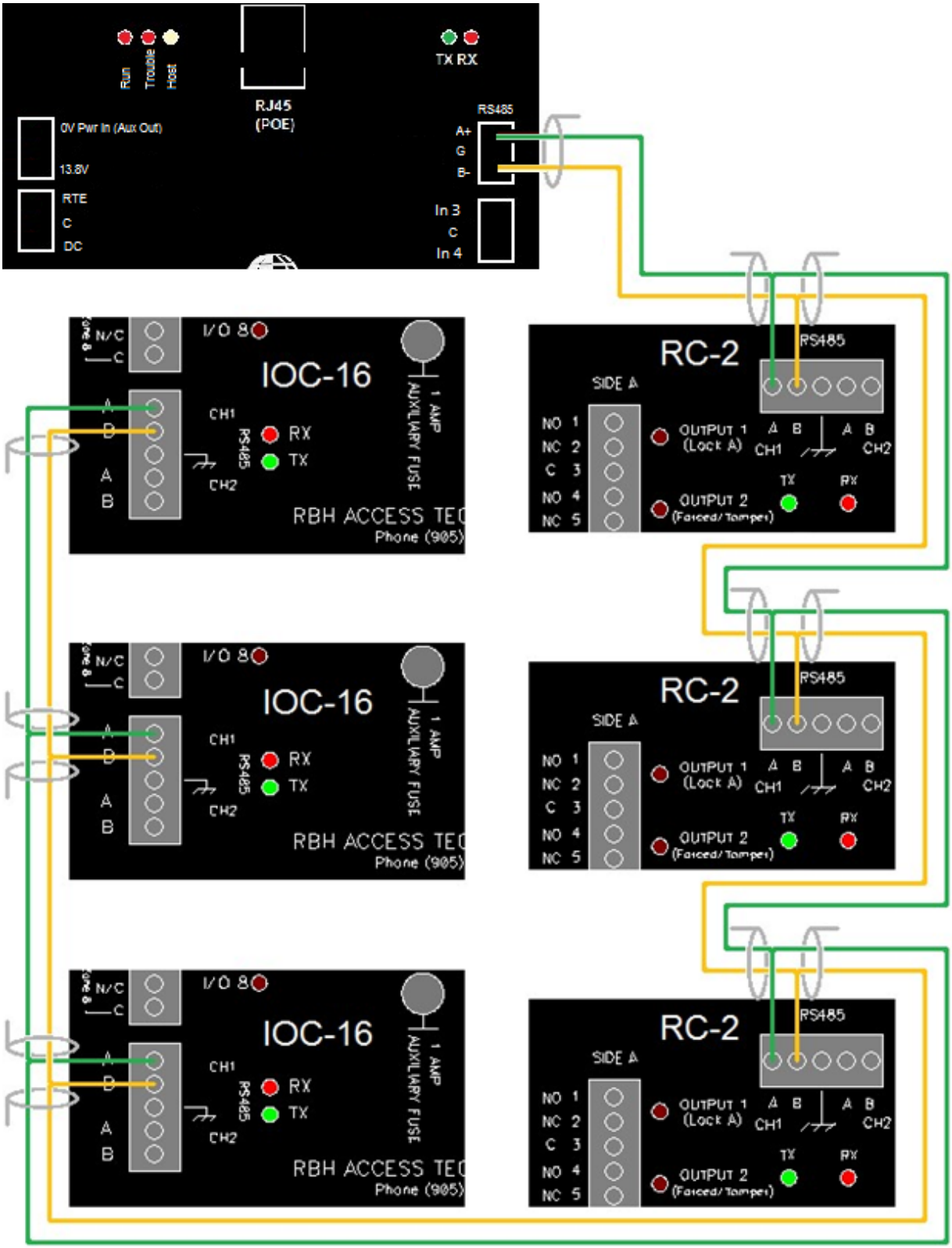
The D-NET connects IOC-16, RC-2, SafeSuite™ panels, PC-100, NRC2000, and NURC2000 devices in a daisy chain fashion (parallel connection) to the network controller. Device controllers do not have to be addressed sequentially. However, using sequential device controller addressing is recommended as this makes your cabling diagrams easier to follow and simplifies troubleshooting as the devices are in the correct numerical sequence.

UNC100 D-NETs comprising SafeSuite™ panels, PC-100, NIRC2000, and NURC2000 devices must have the last unit in the line terminated.

Device Controller Address Assignment	
Address	Device Controller
1 – 4 *	RC-2, NRC2000, NURC2000
5 – 20	IOC-16, PC-100
1-255	SafeSuite™ panel

*** The first NURC is on the UNC100 – Therefore, the first physical RC2 to be connected will start at address 2.**

D-NET (Device Network) Connection Example



D-NET Maximum Cable Length

The maximum distance for any link is 3000 feet (*900 meters*) and the total length cannot exceed 15,000 feet (*4600 meters*).

D-NET Cable

Use 20 to 22 AWG shielded twisted pair cable for all D-NET connections. Shielded cable is recommended to minimize problems that can arise in electrically noisy environments. In addition, shielded cable may be necessary to prevent the network from interfering with signals on other cables in the same trunk.

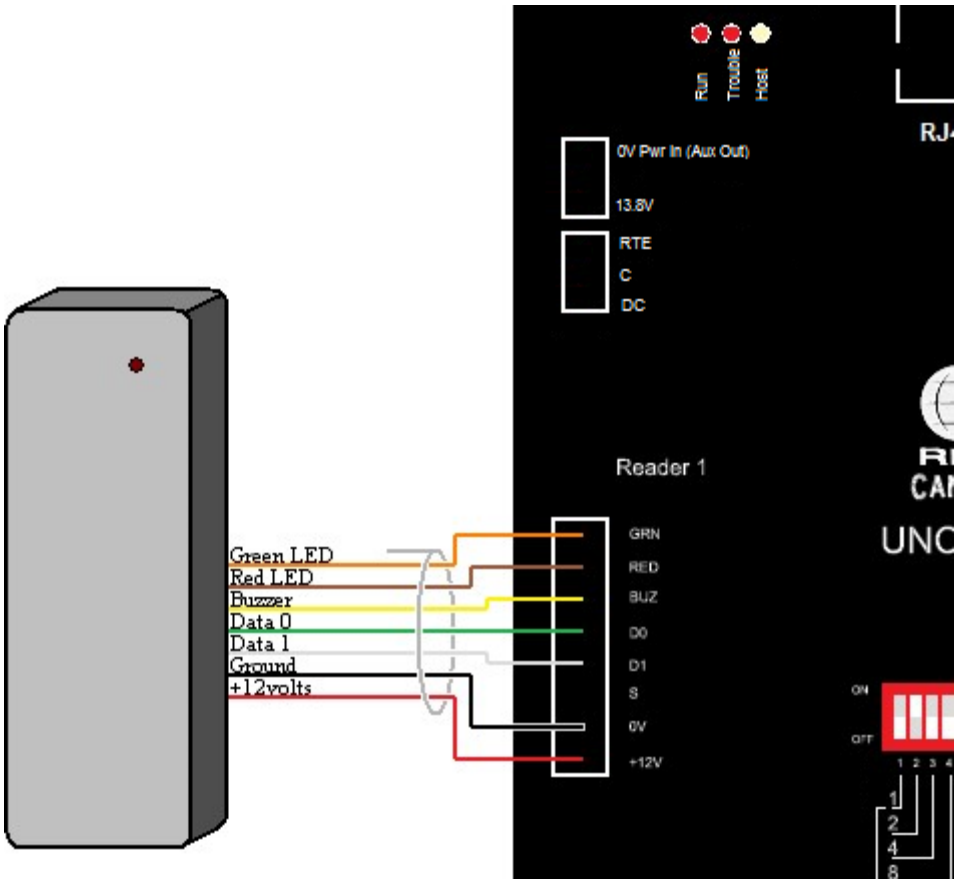
Reader Interface

Two standard Wiegand interfaces provide the following connections for typical proximity readers:

1) Thermal fuse protected power (500ma @13vdc).
2) Reader tamper input(s). Initially if open it will be ignored but once a short is connected it will report a reader tamper alarm whenever the input is opened.
3) LED and beeper outputs are open collector current limited to 100ma.

Reader Connection

RC-2 to 12-Volt Reader Connection Diagram[1]



Cable Specification

7-conductor[2], stranded, shielded cable (*not twisted*), 20 to 22 AWG

Maximum Cable Length

20 to 22 AWG Cable: 500 feet (*150 meters*)

[1] Reader wire colours may vary for different reader manufactures. Please verify your wiring.
[2] Some readers only require 6-conductors since they only have one LED wire (wired to GRN).

Access Point/Reader Operating Modes

Two Person

The Red LED flashes slowly.

In Two Person Mode, two valid cards are required for access. The reader Buzzer beeps rapidly after the first card is presented. A second valid card must be presented within ten seconds for access to be granted.

High Security

The Red LED flashes quickly.

In High Security Mode, only cardholders with *High Security Privilege* are allowed access.

Unlocked

The green LED turns on to indicate the door is unlocked.

Tamper

The Buzzer sounds continuously.

Lockout Alarm

The Buzzer beeps rapidly.

A lockout alarm occurs when a user-defined number of 'Access Denied' messages occur. These messages can include 'Invalid Card Number', 'No Access at this Time', 'No Access at this Reader', or 'Invalid PIN Code'.

Door Held Open Warning

The Buzzer beeps slowly.

Door Held Open Alarm

The Buzzer sounds continuously.

Keypad / Reader Combination

The Buzzer emits a short beep every second after a card is presented, until a PIN is entered.

Access Granted

The Buzzer emits one long beep and the green LED turns on for the duration of the unlock time.

Access Denied

The Buzzer emits two short beeps and the red LED flashes twice.

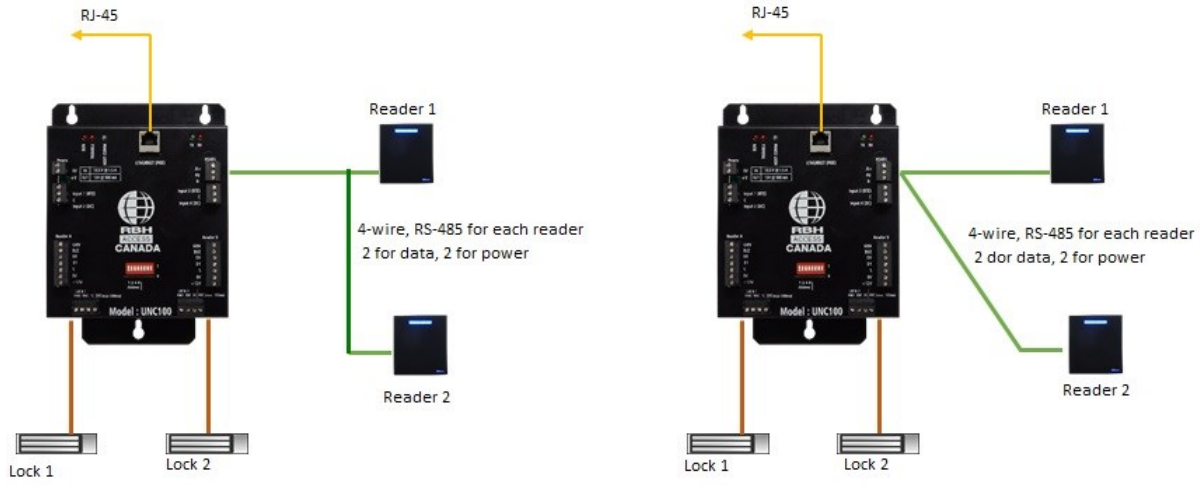
OSDP

Open Supervised Device Protocol (OSDP) is an access control communications standard developed by the Security Industry Association (SIA) to improve interoperability among access control and security products.

RBH is using this protocol for interfacing one or more Peripheral Devices (PD) to a UNC-100.

The protocol implementation is over a two-wire, multi-dropped, serial communication channel, such as RS-485. The physical interface is Half-duplex RS-485- One twisted pair, shield/signal ground. Signaling uses 8 data bits, 1 stop bit & no parity bits

OSDP Reader connection



OSDP Readers (*RBH Blue-Line*) can be connected in daisy chain or in star configuration. Star configuration will reduce the communication distance over RS-485.

Locks should be powered from separate power supply.

The communication over OSDP can be encrypted/unencrypted based on the UNC-100 settings & the capabilities of the PD (OSDP Readers).

The secure communication uses AES-128 bit encryption. Key for secure communication setup is pre-set in UNC100 & PD. In case these keys do not match, secure channel is not set up, in that case the PD has to be updated for the key.

UNC-100 addresses up to eight OSDP readers with address 1 to 8. For secure communications, every PD has unique key. This key is generated using Master Key & ID of the PD. The master key is known only to the UNC-100 controller. If PD is being used with the panel for the first time, Key has to be written to the PD.

Following is the Default Key:

16 Byte long key															
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
0x30	0x31	0x32	0x33	0x34	0x35	0x36	0x37	0x38	0x39	0x3A	0x3B	0x3C	0x3D	0x3E	0x3F

☞ **It is assumed that the Readers from the manufacturer have already been integrated with RBH firmware, if not, it is not possible to connect with this reader in secure mode. At present Readers from manufacturers that have been integrated with RBH Firmware are HID & RBH blue LINE™**

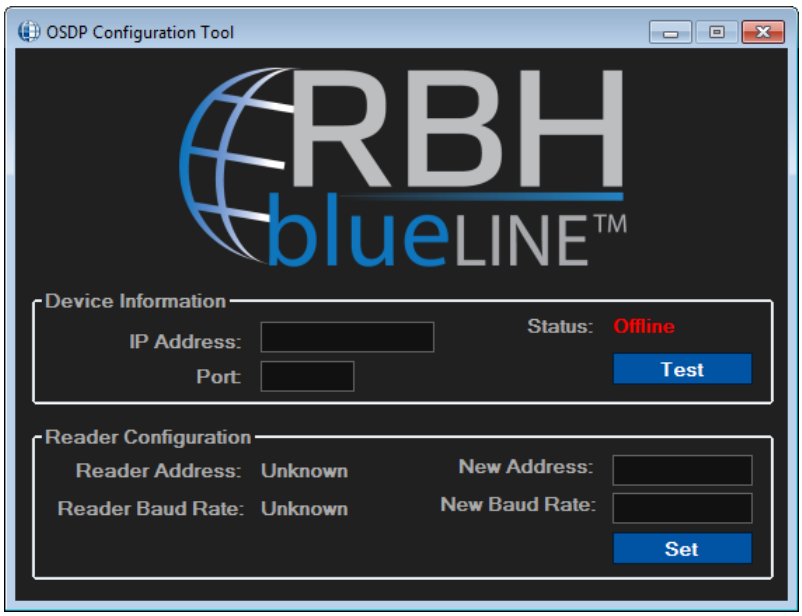
UNC-100 can be set to installation mode using DIP Switch setting ↓↓↓↓↑↑↑↑& then power on.

For reader installation mode refer to manufacturer specifications.

The key writing process takes around 10 seconds (Check for the regular blinking on the TX/RX LED's on channel).

Power off the panel, set the Dip switches to regular state & power on the panel & reader.

RBH OSDP Configuration Tool is used to write the key in OSDP Readers:

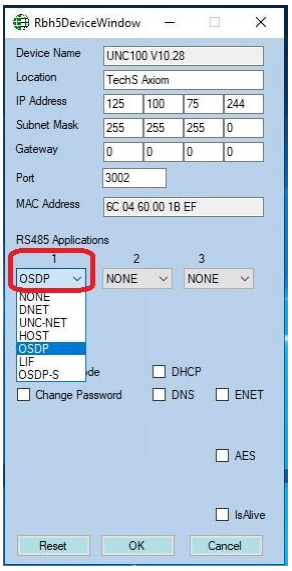


Enabling the OSDP Feature in UNC-100

It is possible to set up the unencrypted/encrypted OSDP communication mode of the UNC-100 using APP setting feature of utility program IP Device Discovery.

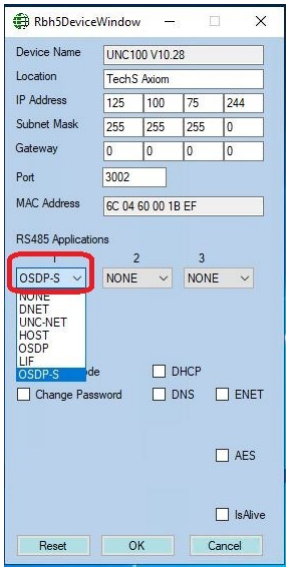
Unencrypted OSDP settings

In order to make UNC-100 communicate to PD in unencrypted mode, from The IP Device Discovery select ‘OSDP’ APP on RS-485 channel.



Encrypted OSDP settings

In order to make UNC-100 communicate to PD in OSDP encrypted mode, from The IP Device Discovery select ‘OSDP-S’ APP on RS-485 channel.



Extended use of OSDP Channel

At present, the reader is connected to the respective controller viz RC-2, NURC2000, NIRC2000 etc.

With the OSDP extension, it is possible to use the OSDP readers to

- Read cards
- Buzzer & Led indications as per the access control decisions made

Controllers in this case will only use their respective input & output infrastructure for access control, all the indications & raw card data read are done at OSDP readers. OSDP can control up to 8 readers (Assuming max 4-RC DNET).

Since only UNC-500 platform as multi-channel RS-485, Extended OSDP can be used on this platform only.

Configuration

Two readers are associated with every reader controller. The OSDP index is based on the readers DNET address. See the table below

DNET Address	Access point	OSDP Address
1	A	1
	B	2
2	A	3
	B	4
3	A	5
	B	6
4	A	7
	B	8

Inputs

The UNC100 has four fully supervised inputs, two on side A and two on side B. All Four inputs are added as defaulted application by default, and can be programmed as General purpose from the PC

Number	Default Application
1	Request to Exit
2	Door contact
3	Request to Exit
4	Door contact

Each input has four states: Restore, Alarm, Trouble, and Illegal. Trouble is reported if a short or break is detected on a supervised circuit and illegal is reported if the measured loop resistance lies between valid states. For example, if the circuit type is programmed as "2 resistor normally closed", 1k represents a restored state and 2k represents an alarm state. If the loop resistance changes by more than 15% but not enough to enter the next state, an illegal state is reported.

Request to Exit (RTE)

The Request to Exit [RTE] input is connected to a push button mounted on the door or to a motion detector mounted near the door. A normally open or normally closed button can be used and the circuit type can be programmed from the PC. Activating the RTE input will unlock the door. The RTE can be disabled by time zone. This input can be used as a general purpose input if RTE operation is not required. If not used, leave the default RTE settings in the Axiom™ software configuration.

Door Contact (DC)

The Door Contact [DC] input monitors the state of the door. Forced entry, door held open alarm, and door held open warning require monitoring of the door state. This input can be used as a general-purpose input if the door contact is not required. If not used, leave the default DC settings in the Axiom™ software configuration.

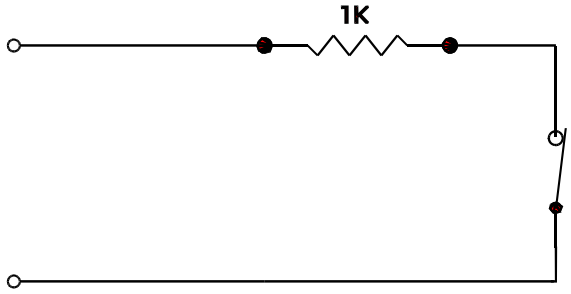
Input Circuit Types

The device controllers supports seven different input circuit types ranging from no resistor for low security applications to two resistor normally closed circuits where the highest security is required.

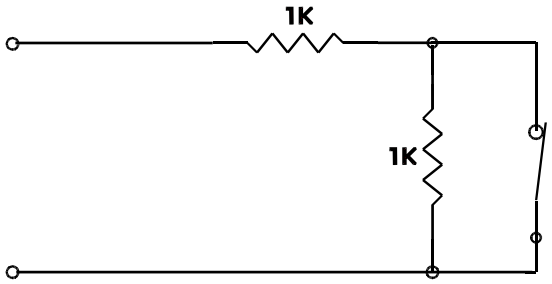
Normally Closed, No Resistor	
Loop Resistance	State
Short	Restore
Open Circuit	Alarm

Normally Open, No Resistor	
Loop Resistance	State
Short	Alarm
Open Circuit	Restore

Normally Closed, One Resistor	
Loop Resistance	State
Short	Trouble
1k	Restore
Open Circuit	Alarm

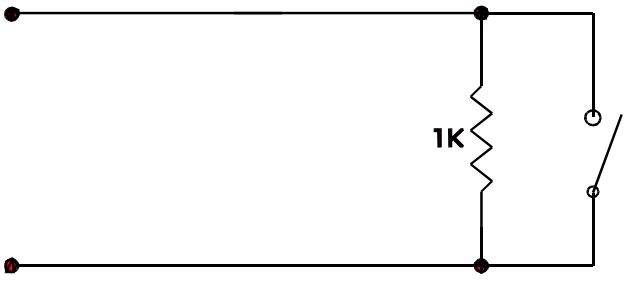


Normally Closed, Two Resistor	
Loop Resistance	State
Short	Trouble
1k	Restore
2k	Alarm
Open Circuit	Trouble

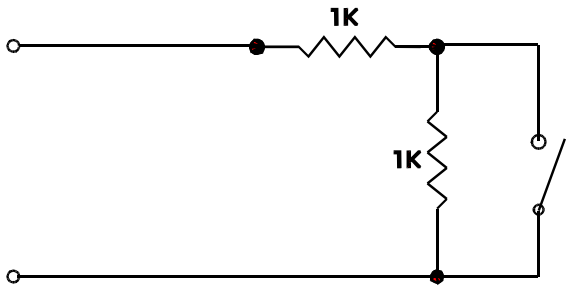


This circuit provides a high degree of supervision and detects both short and open circuit fault conditions. Use this circuit in high security applications.

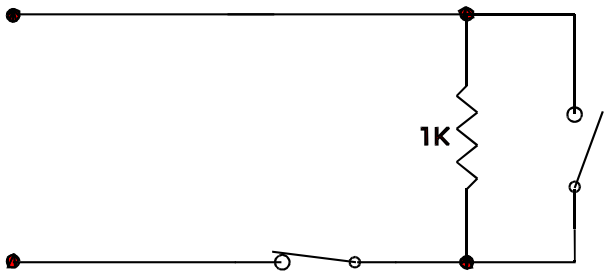
Normally Open, One Resistor	
Loop Resistance	State
Short	Alarm
1k	Restore
Open Circuit	Trouble



Normally Open, Two Resistor	
Loop Resistance	State
Short	Trouble
1k	Alarm
2k	Restore
Open Circuit	Trouble



Normally Open And Normally Closed, One Resistor	
Loop Resistance	State
Short	Alarm
1k	Restore
Open Circuit	Alarm



This circuit type is used where normally open and normally closed contacts are used in the same loop.

Outputs

There are two form C relays and two open collector outputs that can be programmed as general purpose or default applications. Although the contacts are rated at 12 amperes at 125vac the surge protectors prevent voltages greater then 40vac or 56vdc from being applied. The recommended use of the relays is to provide isolated outputs for driving electric strikes or magnetic locks at a maximum voltage of 24v. The open collector outputs are current limited to 100 milli-amperes direct current only.

Number	Default Application	Type
1	Lock	Relay form C
2	Forced Entry Alarm	Open Collector (100ma)
3	Lock	Relay form C
4	Forced Entry Alarm	Open Collector (100ma)

Default Output Operation

Lock Output

For magnetic locks, the relay should be configured from the PC as On State de-energized for fail-safe operation. If power fails (*AC and battery*) the power to the magnetic lock is removed and the door is opened.

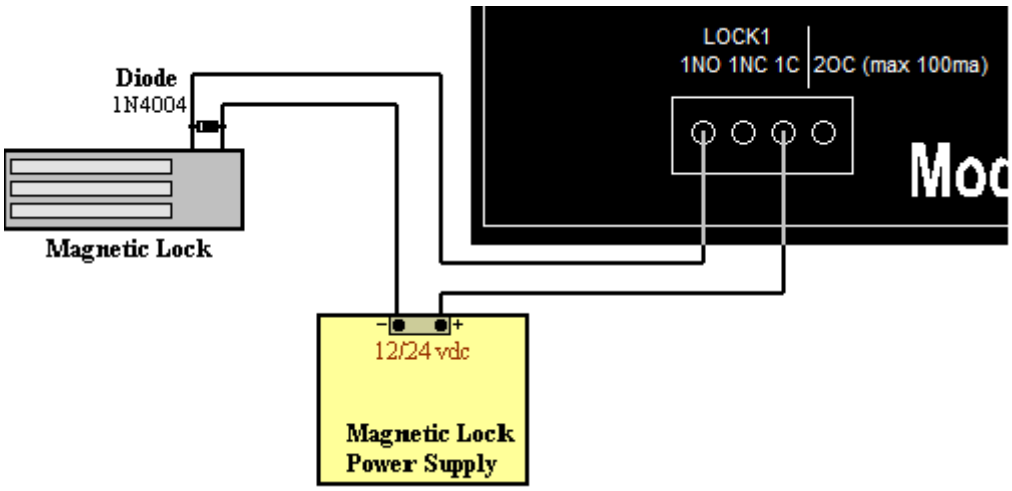
Forced / Tamper

The Forced/Tamper output turns on if the door is forced open or if a reader tamper is detected. This output remains on for as long as the alarm condition exists.

Switching Inductive Devices (Locks, Bells)

Exercise caution when switching an inductive load. Inductive devices include external relay, solenoids, bells, and door locks. All of these devices generate extremely high voltage spikes (several thousand volts) when applied power is removed. Possible disruption of operation could occur if this interference gets on to the electronic circuit board.

This interference can be suppressed by placing a diode (*1N4001 or similar*) across the lock or other inductive device being switched. Connect the diode cathode (*end with band*) to the positive terminal and the other end to the negative terminal. The diode must be placed at the device being switched and not at the controller.


LOCK1
1NO 1NC 1C
2OC (max 100ma)
Diode
1N4004
Magnetic Lock
12/24 vdc
Magnetic Lock
Power Supply

UNC100 Specification

Controller Power Requirements	12 – 14vdc
Current Consumption	250mA
Processor	32 bit micro controller
Memory	2MB
UNC-NET Connections	15
RC-2 Connections	4 (3 + 1 internal)
IOC-16 connections	16
UNC-NET Communication speed	156250 baud
DNET Communication speed	38400 baud
HOST Ethernet speed	10/100 TCP/IP Ethernet, RS485 4 wire
HOST RS485 Speed	9600, 38400, 57600, 115200 baud
Clock/RAM backup battery	3v Lithium battery CR1632
Real Time Clock	Built-in as standard
Watch Dog Circuit	Built-in as standard
Board Dimensions	H 5 ½ in x W 5 in (14 x 12 ½ cm)
Operating Temperature	0 to 70C (35 - 150F)
Operating Humidity	20 to 85% RH (non-condensing)

Cable Specification

Circuit Function	Cable type	Length
PC To Controller (Ethernet)	CAT5 communications cable	323 feet (100 meters)
PC To Controller (RS485)	Twisted pair, shielded, stranded 18 to 22 AWG	4000 feet (1200 meters)
UNC-NET	Twisted pair, shielded, stranded 20 to 22 AWG	2500 feet (*750 meters*)
D-NET	1 twisted pair, shielded, 20 to 22 AWG	3000 feet (*900 meters*)
Reader	20 to 22 AWG, 6 or 8-conductor, stranded, shielded (*not twisted*)	500 feet (1*50 meters*)
Input / Output Port Circuit Loop	2-conductor, 20 to 22 AWG	1000 feet (*300 meters*)