Honeywell | THE FUTURE IS WHAT WE MAKE IT

Pro-Watch 7000

Intelligent Controller and System

PW7K1IC

Install Guide

Ordering Information

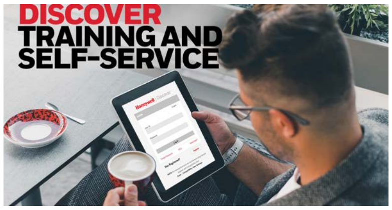
Please contact your local Honeywell representative or visit us on the web at www.honeywellintegrated.com for information about ordering.

Feedback

Honeywell appreciates your comments about this manual. Please visit us on the web at www.honey- wellintegrated.com to post your comments.

Technical Support Self-Service | Customer Portal

https://myhoneywellbuildingsuniversity.com/training/support/

YouTube | Honeywell Help and Support

https://www.youtube.com/channel/UCBEL6ouNV_LN5lEpYRujMTg/featured

TABLE OF CONTENTS

Notices

Wiring methods shall be in accordance with the National Electrical Code (ANSI/NFPA70), Canadian Electrical Code, Part I (CSA C22.1) Safety Standard for Electrical Installations, local codes, and the authorities having jurisdiction.

Caution: Disconnect power before servicing.

Caution: ATTENTION: Débranchez l'alimentation électrique avant l'entretien.

Warnings and Cautions

Note: *See the Remote Enclosure Installation Manuals PW5K2ENC1/PW5K2ENC2 or PW5K1ENC3 (not evaluated by UL) for installation instructions.*

Before Installation

Warning: Before installation, TURN OFF the external circuit breaker which supplies power to the system.

Warning: AVERTISSEMENT: Avant de procéder à l'installation, DESENCLENCHER le disjoncteur via lequel le système est alimenté.

Before connecting the device to the power supply, verify that the output voltage is within specifications of the power supply (see Technical Specifications beginning on page 20).

Do not apply power to the system until after the installation has been completed. Personal injury or death can occur, and the equipment can be damaged beyond repair, if this precaution is not observed.

Fire Safety and Liability Notice (Not Evaluated by UL for fire, life safety, or burglary application)

Warning: Never connect card readers to any critical entry, exit door, barrier, elevator or gate without providing an alternative exit in accordance with all the fire and life safety codes pertinent to the installation.

Warning: AVERTISSEMENT: Ne jamais connecter de lecteur de carte en un point critique (porte de sortie, barrière, ascenseur ou portillon) sans proposer une autre sortie, ce afin de respecter la règlementation en vigueur en matière d'incendie et de protection des vies humaines, afférente à l'installation.

These fire and safety codes vary from city to city and you must get approval from local fire officials whenever using an electronic product to control a door or other barrier. Use of egress buttons, for example, may be illegal in some cities. In most applications, single action exit without prior knowledge of what to do is a life safety requirement. Always make certain that any required approvals are obtained in writing. DO NOT ACCEPT VERBAL APPROVALS SINCE THEY ARE NOT VALID.

Honeywell Integrated Security never recommends using the PW-7000 or related products for use as a primary warning or monitoring system. Primary warning or monitoring systems should always meet the local fire and safety code requirements.

Failure to test a system regularly could make the installer liable for damages to the end user if a problem occurs.

Earth Grounding

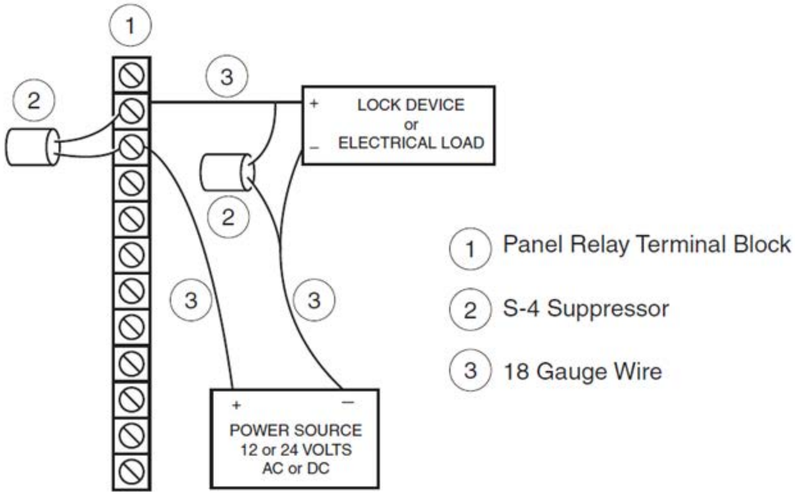
⚠ **Warning: The earth ground is connected at the factory and should not be removed.**

⚠ **Warning: AVERTISSEMENT: La prise de terre est reliée à l'usine et ne doit pas être retirée**

Use Suppressors

⚠ **Warning: The S-4 Suppressor Kit must be installed with every electrical switching device connected through a relay contact, without regard to polarity. One S-4 is installed across the relay at the panel and the other is installed within 18 inches of the electrical switching device.**

⚠ **Warning: AVERTISSEMENT: Employer des suppresseurs de surtensions transitoires (S-4) sur toutes les gâches de porte. Honeywell Integrated Security recommande l'utilisation exclusive de gâches électriques à courant continu.**



UL/ULC Warnings

The following applies to installations that require UL or ULC compliance:

Only UL/ULC Listed readers with standard Wiegand data output communication format (protocol) and OSDP reader have been evaluated to use with this system.

This product is intended to be installed indoors, within the protected premises.

Access Control System, Model PW7000, and Controller, Model PW7K1IC meet the requirements for CAN/ULC-S319-05 Equipment Class 1. This product's compliance to ULC-S319, Electronic Access Control Systems, will be considered invalidated through the use of any add-on, expansion, memory or other module manufactured or supplied by the manufacturer or manufacturer's representative, unless specifically evaluated by ULC.

All unused conduit holes must be properly plated or incorporate a Listed plug to fill any voids.

All interconnecting devices must be UL/ULC Listed.

Shielded cable shall be employed for all Input/Output wiring.

Refer to the following Installation manuals for installation, connection, programming, and operation instructions of the following sub-assemblies:

Assembly Number	Installation Manual Part Number
PW7K1IC	800-25673
PW7K1R2	800-25676
PW7K1IN	800-25674
PW7KOUT	800-25675
PW6K1IC	800-00005V3
PW6K1R2	800-01951V4
PW6K1IN	800-01952V1
PW6K1OUT	800-01953V1
PW5K2ENC1 and PW5K2ENC2	800-06952
PW5K1ENC3	800-06955V1
PW5K2ENC5	800-08421
PW6K2E2PS	800-08279V3

Note: *Not Evaluated by UL for fire, life safety, or burglary applications.*

Note: *The earth ground is connected at the factory and should not be removed.*

Do Not Connect To A Receptacle Controlled By A Switch.

Replacement of 3 volt lithium coin cell with:

Rayovac: BR2325 or Panasonic CR2330

All interconnecting wire must be UL/ULC Listed, rated and suitable for the use.

The battery leads and primary AC main power wiring is non-power limited. This wiring must be separated from all other wiring by at least 0.25" and cannot be installed in the same conduit as any other power limited wiring.

The system must be configured to activate an alarm or trouble signal. Failure to do so will not allow the access function to operate in the event of a tamper.

Note: *The following applies to installations that require UL or ULC compliance:*

- Only UL/ULC Listed readers with standard Wiegand data output communication format (protocol) have been evaluated for use with this system.
- This product is intended to be installed indoors, within the protected premises.
- Access Control System, Model PW-7000, and Controller, Model PW-7000IC meet the requirements for CAN/ULC-S319-05 Equipment Class 1.
- This product's compliance to ULC-S319, Electronic Access Control Systems, will be considered invalidated through the use of any add-on, expansion, memory or other module manufactured or supplied by the manufacturer or manufacturer's representative, unless specifically evaluated by ULC.
- All unused conduit holes must be properly plated or incorporate a Listed plug to fill any voids.

Note: *Total current draw for all included assemblies shall not exceed 4A, including input rating and output load current.*

- Suitable for S319, Class I
- Suitable for the following UL293/UL294 Performance Levels:
- Endurance: IV
- Standby: I
- Line Security: I
- Attack: I
- Suitable panic or exit hardware shall be employed for fail secure applications. For UL293 applications, the Sys Fault contacts of the power supply and the door held, door forced shall be monitored by suitable audible device.

CE + WEEE Marking

Description of the used symbol.

CE -Standard -Logo. This product complies with the harmonized Regulation of the EU

WEEE symbol.It indicates this product is to be recycling and not been thrown in the dustbin

Damage During Shipment

Caution: IF ANY DAMAGE TO THE SHIPMENT IS NOTICED, A CLAIM MUST BE FILED WITH THE COMMERCIAL CARRIER RESPONSIBLE FOR THE DAMAGE.

Caution: ATTENTION: SI L'EQUIPEMENT A SUBI DES DOMMAGES LORS DE SON TRANSPORT, ADRESSER UNE RECLAMATION AU TRANSPORTEUR RESPONSABLE.

Electro Static Discharge

Caution: Electro-static discharge (ESD) can damage CMOS integrated circuits and modules. To prevent damage always follow these procedures:

- Use static shield packaging and containers to transport all electronic components, including completed reader assemblies.
- Handle all ESD sensitive components at an approved static-controlled workstation. These workstations consist of a desk mat, floor mat and an ESD wrist strap. Workstations are available from various vendors.

Caution: ATTENTION: Des décharges électrostatiques peuvent endommager les modules et circuits intégrés CMOS.

Note: *This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation and user guides, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.*

Note: *This document and the data in it shall not be duplicated, used or disclosed to others for procurement or manufacturing, except as authorized by and with the written permission of Honeywell Integrated Security, Inc. The information contained in this document or in the product itself is the exclusive property and trade secrets of Honeywell Integrated Security, Inc. Copyright laws of the United States protect all information in this document or in the software product itself.*

Note: *Any use of this product is subject to the terms and acceptance of the Honeywell Integrated Security, Inc. Software Agreement. Please request a copy from Honeywell Integrated Security, Inc. (http://www.honeywellintegrated.com/index.html), and review the agreement carefully.*

Disclaimer – Product Liability; Mutual Indemnification

If a Customer receives a claim that a Product or any component thereof has caused personal injury or damage to the property of others, Customer shall immediately notify Honeywell Integrated Security in writing of all such claims. Honeywell Integrated Security shall defend or settle such claims and shall indemnify and hold Customer harmless for any costs or damages including reasonable attorneys' fees which Customer may be required to pay as a result of the defective Product or the negligence of Honeywell Integrated Security, its agents, or its employees.

Customer shall hold harmless and indemnify Honeywell Integrated Security from and against all claims, demands, losses and liability arising out of damage to property or injury to persons occasioned by or in connection with the acts or omissions of Customer and its agents and employees, and from and against all claims, demands, losses and liability for costs of fees, including reasonable attorneys' fees, in connection therewith.

Unpacking Procedure

⚠ **Caution: If any damage to the shipment is noticed before unpacking, a claim must be filed with the commercial carrier.**

⚠ **Caution: ATTENTION: SI L'EQUIPEMENT A SUBI DES DOMMAGES LORS DE SON TRANSPORT, ADRESSER UNE RECLAMATION AU TRANSPORTEUR RESPONSABLE.**

All containers should be opened and unpacked carefully in order to prevent damage to the contents.

Follow these steps to unpack equipment in preparation for installation:

1. Open the container and remove the unit(s) and all packing material. Retain the container and all the packing materials. They may be used again for reshipment of the equipment, if needed.
2. Inspect the contents to see if anything is missing. If you notice any missing items, contact the order entry department at 1-800-323-4576 Option-1.
3. Visually check the contents. If you see any damage, do the following:
   a. If shipping has caused damage to the unit, a claim must be filed with the commercial carrier.
   b. If any other defect is apparent, call for a return authorization.

Shipping Instructions

To ship equipment back to Honeywell Integrated Security, contact the customer service department at 1-800-323-4576 before returning the equipment. When you call, please have available:

- A description of the problem or the reason you are returning the equipment.
- Your original purchase order number, invoice number and if the unit is still under warranty.
- A new purchase order number if the unit is not under warranty

From the customer service department, obtain the **Return Authorization Number (RMA)**.

Show the RMA number on all packages shipped. Packages, which are not marked with an RMA number will be refused at the factory and returned to you **COD**.

Carefully pack the equipment for shipment. Use the original packing material whenever possible.

Limited Warranty

All Products sold or licensed by Honeywell Integrated Security include a warranty registration card which must be completed and returned to Honeywell Integrated Security by or on behalf of the end user for Honeywell Integrated Security to provide warranty service, repair, credit or exchange. All warranty work shall be handled through Customer which shall notify Honeywell Integrated Security and apply for a Return Merchandise Authorization (RMA) number prior to returning any Product for service, repair, credit or exchange. Honeywell Integrated Security warrants that its Products shall be free from defects in materials and workmanship for a period of one year from the date of shipment of the Product to Customer. The warranty on Terminals, Printers, Communications Products and Upgrade kits is 90 days from the date of shipment. Satisfaction of this warranty shall be limited to repair or replacement of Products which are defective or defective under normal use. Honeywell Integrated Security's warranty shall not extend to any Product which, upon examination, is determined to be defective as a result of misuse, improper storage, incorrect installation, operation or maintenance, alteration, modification, accident or unusual deterioration of the Product due to physical environments in excess of the limits set forth in Product manuals. THERE ARE NO WARRANTIES WHICH EXTEND BEYOND THIS PROVISION. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. NO REPRESENTATION OR WARRANTY OF THE DISTRIBUTOR SHALL EXTEND THE LIABILITY OR RESPONSIBILITY OF THE MANUFACTURER BEYOND THE TERMS OF THIS PROVISION. IN NO EVENT SHALL HONEYWELL INTEGRATED SECURITY BE LIABLE FOR ANY RE-PROCUREMENT COSTS, LOSS OF PROFITS, LOSS OF USE, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES TO ANY PERSON RESULTING FROM THE USE OF HONEYWELL INTEGRATED SECURITY'S PRODUCTS.

Confidentiality

All software, drawings, diagrams, specifications, catalogs, literature, manuals and other materials furnished by Honeywell Integrated Security relating to the design, use and service of the Products shall remain confidential and shall constitute the proprietary rights of Honeywell Integrated Security and Customer agrees to treat such information as confidential. Customer shall acquire no rights in the design of the Products or the related materials except to use such information solely for the purpose of and only during the time it sells the Products.

Customer shall not copy the design of any of the Products or use or cause to be used any Product design or related materials for its own benefit or for the benefit of any other party. The covenants contained in this section shall remain effective throughout the term of this Agreement and thereafter unless specifically waived by Honeywell Integrated Security in writing.

Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB- 003 du Canada.

To obtain applicable EU compliance Declaration of Conformities for this product, please refer to our website, https://www.security.honeywell.com/All-Categories/access-control-systems/control-panels-hardware.

For any additional information regarding the compliance of this product to any EU-specific requirements, please contact:

Honeywell Security & Communications

Honeywell Security - Quality Assurance Dept., Newhouse Industrial Estate Motherwell

Lanarkshire ML1 5SB Scotland

United Kingdom

Tel: +44(0) 1698 738200

Email: UK64Sales@Honeywell.com

Recommended testing and maintenance

Perform the following on a semi-annual basis. Disconnect power from the enclosure, open the enclosure door and inspect the system including the DC battery. Replace the DC battery if it shows any sign of corrosion or leakage or if the battery is 2 years old or older. Oil the lock cylinder. Close the panel and re-apply power.

CHAPTER

1

PRODUCT OVERVIEW

The Intelligent Controller is the heart of the PW-7000 and provides the real time processing for the connected I/O interfaces.

The PW-7000 is designed to operate without the need for a PC. It can be connected to a Pro-Watch host computer using TCP/IP network connection. The PW-7000 holds the database for the subsystem configuration and card holders, and the event log buffer, which is in battery-backed memory.

Note: *Please refer to the Pro-Watch Software Suite Guide for details on using the Pro-Watch interface.*

PW-7000 and PW-6000

The PW-7000 controller configuration and operation is similar to the PW-6000 controller and has additional R2 functions on board; both use the Pro-Watch front end.

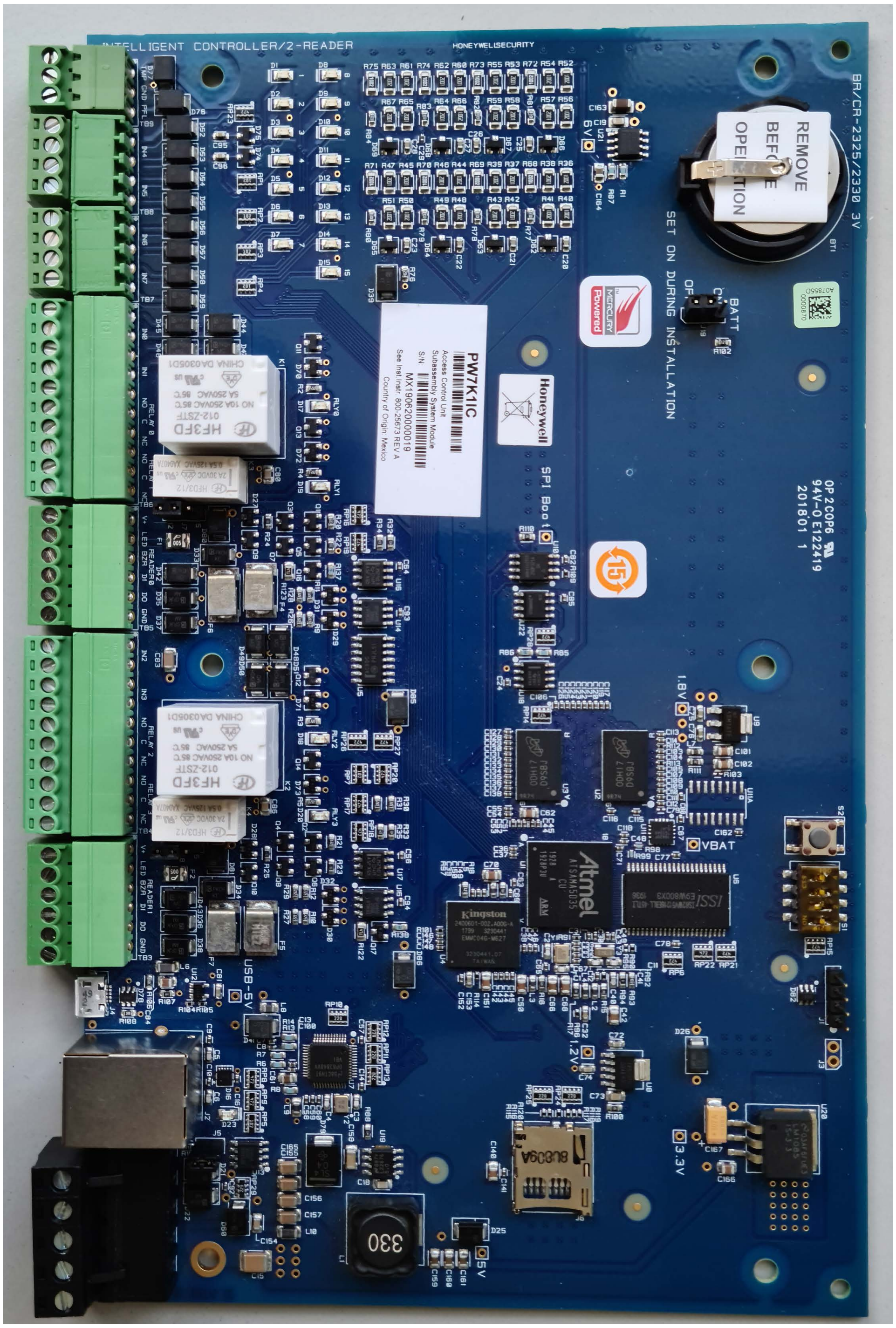
The PW-7000 controller is compatible with the following Honeywell modules; PW7K1R2, PW7K1IN, PW7K1OUT, PW6K1R2, PW6K1IN, and PW6K1OUT. For more details see Pro-Watch Intelligent Compatibility Matrix (page 25).

Port Settings

- Port 0 provides the host-embedded Ethernet interface.
- Ports 1 for RS-485 2-wire downstream support for connecting 32 I/O devices. Note that the I/O communications must be mapped differently in Pro-Watch, according to the following table:

PW-7000 Port	Pro-Watch Port
1	*1*

Figure 1: PW7K1IC Board



Other

- An on-board real time clock maintains the date and time, taking into account leap year and accounting for global time zones and daylight savings time changes.
- The database for the system configuration and card holders are stored in FLASH memory.
- The event log buffer is stored in battery-backed memory.
- Configuration data and event/status reports are communicated to the host via on-board 10-BaseT/100Base-TX Ethernet port, NIC1 and NIC2 as a backup.
- Transactions are stored in 1 MB of battery-backed SRAM. The maximum number of transactions stored while the host is offline is 50,000.
- Cards are stored in Flash memory and read into DRAM when the board is powered up. The amount of storage available for cards and biometric records is 15 MB. The maximum number of cards depends on the card record database configuration, but the number is approximately 240,000. This maximum is dependent on how the card is configured with more space per card used with longer card number, more clearance codes, and so on.

This page is intentionally left blank.

CHAPTER

2

SETTING UP PW-7000 HARDWARE

The PW-7000 processor is configured with 4 jumpers and a set of 4 DIP switches. These jumpers/switches set up the port interface, end of line termination, and operating mode configuration. Refer to the tables below to set the jumpers as required.

Setting the Jumpers

Table 1 PW-7000 Jumper Settings

Jumpers	Set At	Description
J5	OFF	RS-485 EOL Terminator is without termination
	ON	RS-485 EOL Terminator is terminated
J7 J8	Reader Power Select	
	Reader 0	5V-12V, 2-3 12V (default), 1-2 5V
	Reader 1	5V-12V, 2-3 12V (default), 1-2 5V
J19	Battery	
	OFF= Battery OFF	ON = Battery ON

Setting the DIP Switches

Dual In-line Package (DIP) switches are read when the system powers up, except where noted otherwise. The following table shows the setting options.

Table 2 PW-7000 DIP Switch Settings

S1	S2	S3	S4	Selection
OFF	OFF	OFF	OFF	Normal Operating Mode.
ON	OFF	OFF	OFF	Enables the default user name (admin) and (password). The user name and password are read dynamically; you do not need to reboot the panel.
OFF	ON	OFF	OFF	Use the factory default communication parameters.
ON	ON	OFF	OFF	Unless the network administrator reserves an IP address for the panel (based on the controller board's Media Access Control (MAC) address), the PW-7000 uses Dynamic Host Configuration Protocol (DHCP) to obtain an IP address from the network DHCP server. When power is applied with the switches in this position, there is a ten second window (when LEDs 1and 2 flash alternately with LEDs 3 and 4), during which memory is cleared if switch 1 or switch 2 is changed to OFF. When switch 1 or 2 is changed to OFF, only LED 2 flashes and memory begins to be cleared. This period of clearing lasts several minutes. When the memory has been cleared, the LED pattern changes to the flashing of LEDs 1 and 4. The panel then reboots by itself. All data in memory is erased except the serial number, MAC address, hardware revision, and OEM code.
OFF	OFF	OFF	ON	DIP4 = ON -> Legacy Mode, PW7K1IC works as PW6K1IC. DIP4 = OFF -> Native Mode, PW7K1IC Supported Functions and Capabilities, Readers and IN/OUTPUTs on PW7K1IC can be used .For more details see Pro-Watch Intelligent Compatibility Matrix (page 25).

The PW-7000 DIP switches need to be set twice:

1. Configure the **S4-S3-S2-S1** DIP switches to **off-off-on-off** to set the default TCP/IP address to 192.168.0.251.
2. Apply power to the panel to set the IP address.
3. Change the **S4-S3-S2-S1** combination to **off-off-off-on**. (DIP switch 1 is "read on the fly"). This sets the login to the default user ID ("admin") and password ("password") for Ethernet communications.
4. Create users. See User Configuration for instructions.
5. Set the **S4-S3-S2-S1** combination to **off-off-off-off**.
6. Configure the host port(s) for IP Server and/or IP Client communications. See Host Communication for instructions. This will enable both TCP/IP and serial hardware networking when you log in again.

Factory Default Communication Parameters: Interface 1 (Port 0)

Network: static IP address	192.168.0.251
Subnet Mask: Default Gateway	255.255.0.0
Default Gateway	192.168.0.1
DNS Server	192.168.0.1
Primary Host port: IP server, Data Security: TLS if Available, port 3001, communication address	0
Alternate Host Port	**Disable**

Bulk Erase Configuration Memory

The bulk erase function can be used for the following purpose:

- Erase all configuration and cardholder database (sanitize boards, less third party applications)
- Update the OEM default parameters after OEM code is changed.
- To recover from the database corruption and to avoid PW7000 board to reboot continuously.

Note: *If clearing the memory does not correct the initializing problem, contact technical support.*

Bulk Erase

Note: *Do not remove power during steps 1-8.*

Step 1. Set S1 DIP switches to 1 & 2 “ON” and, 3 & 4 “OFF”.

Step 2. Apply power to the PW7K1IC board. LED 1 ON for about 15 seconds while PW7K1IC boots up.

Step 3. After the PW7K1IC boots up, watch for LEDs 1& 2 and 3 & 4 to alternately flash at a 0.5 second rate.

Step 4. Within 10 seconds after the above patterns starts, change switches 1 or 2 to “OFF”. If these switches are not changed, then PW7K1IC board will power up using the OEM default communication parameters.

Step 5. LED 2 will flash indicating that the configuration memory is being erased.

Step 6. Full memory erase will take up to 60 seconds, usually a lot less.

Step 7. Once complete. only LED’s 1 & 4 will flash for 3 seconds.

Step 8. The PW7K1IC board will complete its initialization in 2 seconds after LEDs 1 & 4 stop flashing.

Technical Specifications

Caution: PW-7000 is manufactured for use in low-voltage, Class 2 power-limited circuits only.

Table 3 PW-7000 Technical Specifications

Category	*Description*
Primary Power	12 VDC ± 10%, 500 mA maximum (reader ports not included)
Reader Ports	600 mA maximum for 12V readers (add 600 mA to primary power current) 300 mA for 5V readers.
Memory and Clock Backup	3Volts Lithium, type BR2325 or Panasonic CR2330.
Ports	**Port 0 - Host Communication:** Ethernet: 10-Base T/100Base-TX **Port 1 - Serial I/O Device:** 2-wire RS-485, 2,400 to 115,200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit **Reader Interface:** Data Inputs: TTL compatible, F/2F or 2-wire RS-485. RS-485 Mode: 9,600 to 115,200 bps, asynchronous, half-duplex, 1 start bit, 8 data bits, and 1 stop bit. Maximum cable length: 2000 ft. (609.6 m)
Inputs	8 unsupervised/supervised, standard EOL: 1k/1k ohm, 1%, ¼ watt 2 non-supervised, dedicated for cabinet tamper and power fault monitoring.
Cable requirements	**Power:**1 twisted pair, 18 AWG. **RS-485:** I/O Device Port: 1 twisted pair, shielded, 120 ohm impedance, 24 AWG, 4,000 ft. (1,219 m) max. Reader Port: 1 twisted pair, shielded, 120 ohm impedance, 24 AWG, 2,000 ft. (610 m) max. Alarm Input: 1 twisted pair, 30 ohms maximum **Ethernet:** Cat 5. **Input: 1** twisted pair, 30 ohms maximum.
Environmental	**Temperature:** 0 to 49°C, operating -55 to +85°C, storage **Humidity:** 0 to 85% RHNC
Mechanical	**Dimensions:** 5.5 in. (137.7mm) W x 9 in. (228.6.4mm) L x.75 in. (19.05mm) H **Weight:** 7.1 oz. (201 gm) nominal

Note: *Specifications subject to change without notice.*

Caution: Locate the power source as close to this board as possible. Connect power with minimum of 18AWG wires.

Note: *POLARITY for 12 VDC power is important. Make sure the +12 VDC is connected to the terminal labeled +12V and the return is connected to the terminal labeled GND.*

Status LEDs

Power-up: All LED's OFF.

Initialization

1. Initialization: After power is applied or reset switch pushed, LED 1 is ON for about 15 seconds, then LED's 2, 3, 4, 5, 6, R1, R2, IN0, IN1, IN2, IN3, IN4, IN5, IN6, and IN7 are flashed once at the beginning of initialization.
2. LEDs 3 and 4 is turned ON for approximately 1 second after the hardware initialization has completed, then the application code is initialized.
3. The amount of time the application takes to initialize depends on the size of the database, about 1 second without a card database.
4. Each 10,000 cards will add about 2 seconds to the application initialization.
5. When LED's 1, 2, 3 and 4 flash at the same time, data is being read from or written to flash memory.

Note: *Do not cycle power when in this state.*

6. If the sequence stops or repeats, perform the bulk erase procedure, see Bulk Erase.

Run Time Supplying Power to the PW-7000 Interface

Table 5 PW-7000 Status LED Combinations During Run Time

LED	Description
D1	Off-Line / On-Line and Battery Status
	Off-Line = 20% On, ON-Line = 80% On
	Double Flash means the Battery is Low
D2	Host Communication Activity (Ethernet port)
D3	Internal SIO Communication Activity
D4	External SIO Communication Activity
D5	Unassigned
D6	Reader 0: Clock / Data or D1 / Do mode: Flashes when Data is Received, Either Input F/2F Mode: Flashes when Transmitting Data / Acknowledgment is Received RS-485 Mode (OSDP): Flashes when Transmitting Data
D7	Reader 1: Clock / Data or D1 / D0 Mode: Flashes when Data is Received, Either Input F/2F Mode: Flashes when Transmitting Data /Acknowledgment is Received RS-485 Mode (OSDP): Flashes when Transmitting Data
D8	Input IN 0 Status: OFF = Inactive, ON = Active, Flash = Fault*
D9	Input IN1 Status: OFF = Inactive, ON = Active, Flash = Fault*
D10	Input IN2 Status: OFF = Inactive, ON = Active, Flash = Fault*
D11	Input IN3 Status: OFF = Inactive, ON = Active, Flash = Fault*
D12	Input IN4 Status: OFF = Inactive, ON = Active, Flash = Fault*
D13	Input IN5 Status: OFF = Inactive, ON = Active, Flash = Fault*
D14	Input IN6 Status: OFF = Inactive, ON = Active, Flash = Fault*
D15	Input IN7 Status: OFF = Inactive, ON = Active, Flash = Fault*
D17	Relay K0: ON = Energizes, Door Relay
D18	Relay K1: ON = Energized, Door Relay
D19	Relay K2: ON = Energized
D20	Relay K3: ON = Energized
D23	Flashes with Ethernet Traffic

Wiring

This section presents information on reader wiring, input wiring, and control output wiring. The following figure shows the PW-7000 board and identifies its terminal block pin assignments.

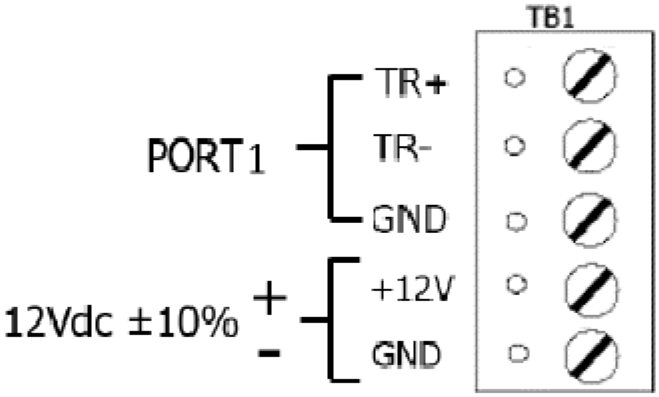
Supplying Power to the PW-7000 Interface

The processor accepts 12 VDC for power. Locate power source as close to the unit as possible and connect it with minimum of 18AWG wires.

Caution: Observe POLARITY on 12 VDC.

Caution: ATTENTION: Observez la polarité du 12 VCC

Figure 2: PW-7000 Power Terminals

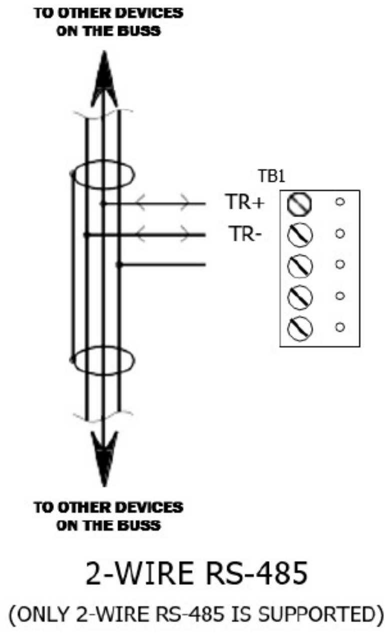


Communications Wiring

The PW-7000 processor communicates to the host via on-board Ethernet 10Base-T/100Base-TX Ethernet port, NIC1 and NIC2 as backup.

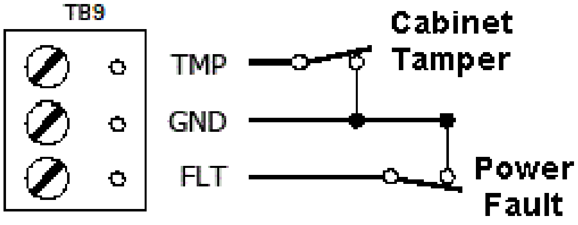
The serial I/O device communication port (TB1) is a 2-wire RS-485 interface which can be used to connect additional I/O panels. The interface allows multi-drop communication on a single bus of up to 4,000 feet (1,219 m). Use 1-twisted pair with drain wire and shield, 120-ohm impedance, 24 AWG, 4,000 ft. (1,219 m) maximum for communication.

Figure 3: PW-7000 Port Wiring


TO OTHER DEVICES ON THE BUSS
TB1
TR+
TR-
TO OTHER DEVICES ON THE BUSS
2-WIRE RS-485
(ONLY 2-WIRE RS-485 IS SUPPORTED)

Cabinet Tamper and Power Failure Input Wiring

Figure 4: PW-7000 TMP and FLT Terminals



Inputs TMP and FLT are used for monitoring cabinet tamper and power failure with normally closed contacts. These two inputs are for contact closure monitoring only; do not use end-of-line (EOL) resistor(s). If these inputs are not used, install a short piece of wire at the input to indicate a safe condition.

Memory and Real Time Clock Backup Battery

The event log buffer and the real time clock are backed up by a 3V lithium battery. This BR2325 or CR2330 battery should be replaced annually. A replacement battery may be obtained from Honeywell or a local battery retailer. However, the replacement battery must be UL recognized.

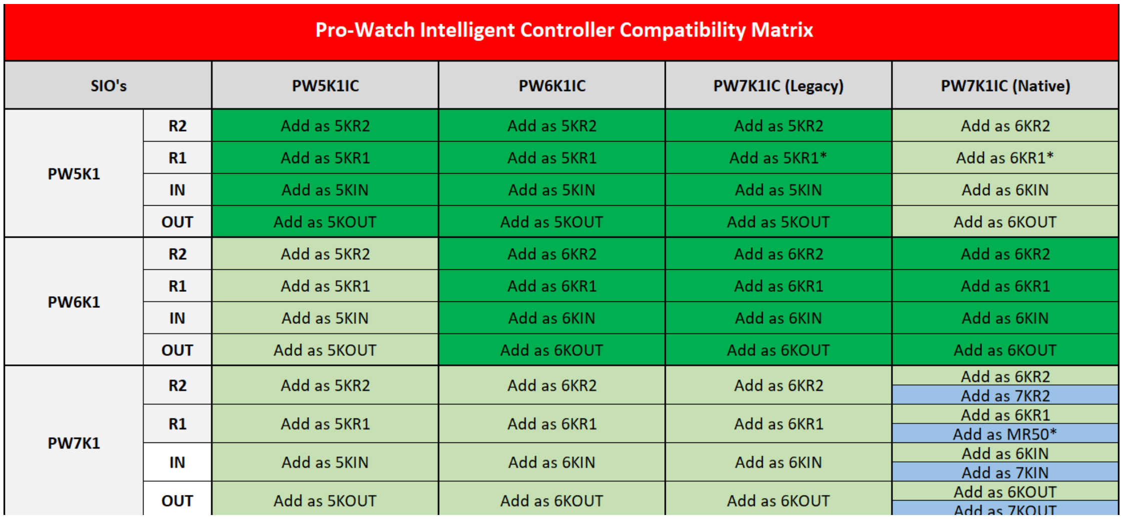
Warning: Battery may explode if mistreated. DO NOT RECHARGE, DISASSEMBLE or DISPOSE OF IN FIRE!

Warning: AVERTISSEMENT: La batterie peut éclater si elle est maltraitée. NE PAS RECHARGER, DEMONTER OU JETER AU FEU!

Pro-Watch Intelligent Compatibility Matrix

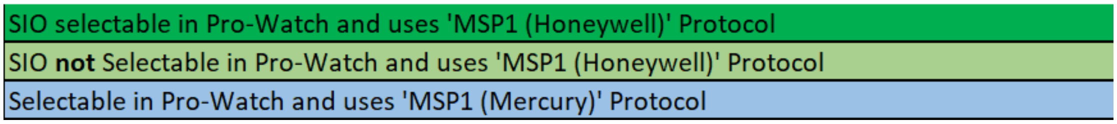
Note:

- PW7KIC available in PW 4.5 SP3 & PW 5.0 SP1 and higher
- PW7K1IC (Legacy) option requires dipswitch 4=ON, configured in Pro-Watch as PW-6000 'Panel Type' and Honeywell channel protocol
- PW7K1IC supports 1 downstream protocol only
- * Not tested



Pro-Watch Intelligent Controller Compatibility Matrix

SIO's		PW5K1IC	PW6K1IC	PW7K1IC (Legacy)	PW7K1IC (Native)
PW5K1	R2	Add as 5KR2	Add as 5KR2	Add as 5KR2	Add as 6KR2
	R1	Add as 5KR1	Add as 5KR1	Add as 5KR1*	Add as 6KR1*
	IN	Add as 5KIN	Add as 5KIN	Add as 5KIN	Add as 6KIN
	OUT	Add as 5KOUT	Add as 5KOUT	Add as 5KOUT	Add as 6KOUT
PW6K1	R2	Add as 5KR2	Add as 6KR2	Add as 6KR2	Add as 6KR2
	R1	Add as 5KR1	Add as 6KR1	Add as 6KR1	Add as 6KR1
	IN	Add as 5KIN	Add as 6KIN	Add as 6KIN	Add as 6KIN
	OUT	Add as 5KOUT	Add as 6KOUT	Add as 6KOUT	Add as 6KOUT
PW7K1	R2	Add as 5KR2	Add as 6KR2	Add as 6KR2	Add as 6KR2 Add as 7KR2
	R1	Add as 5KR1	Add as 6KR1	Add as 6KR1	Add as 6KR1 Add as MR50*
	IN	Add as 5KIN	Add as 6KIN	Add as 6KIN	Add as 6KIN Add as 7KIN
	OUT	Add as 5KOUT	Add as 6KOUT	Add as 6KOUT	Add as 6KOUT Add as 7KOUT



SIO selectable in Pro-Watch and uses 'MSP1 (Honeywell)' Protocol

SIO **not** Selectable in Pro-Watch and uses 'MSP1 (Honeywell)' Protocol

Selectable in Pro-Watch and uses 'MSP1 (Mercury)' Protocol

This page is intentionally left blank

CHAPTER

3 SYSTEM CONFIGURATION

The PW-7000 comes with Access Control Device Server Manager (ACDSM). The ACDSM is a built-in web server, through which you can configure network and other system settings.

Note: *If you are using Internet Explorer Enhanced Security Configuration, you cannot access the ACDSM web server. All pages will display “Bad Request!” You must uninstall the Enhanced Security option before you can access the ACDSM.*

Note: *The default factory-set TCP/IP address for the built-in system configuration web server is **192.168.0.251***

Connecting to ACDSM for the First Time

Step 1. Use the factory default controller IP address **192.168.0.251**.

Step 2. Set the DIP switches to **S4=OFF, S3=OFF, S2=ON, S1=OFF**.

Note: *S1 must be set to OFF for the factory default. After the panel powers up, change S1 to ON to enable the use of the default user name and password.*

Step 3. Connect the computer to host the web server via Ethernet **Port 0**. Connection should be via crossover Ethernet cable or by the regular Ethernet cables connected via the hub.

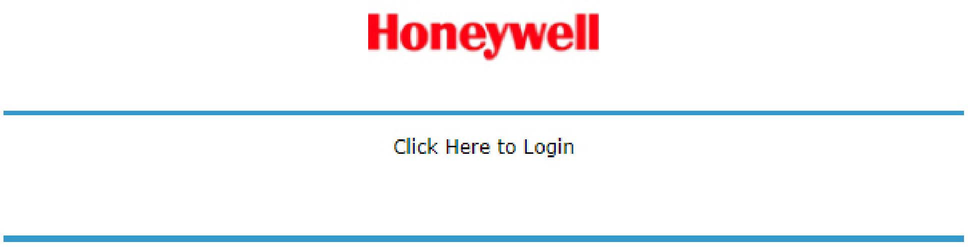
Step 4. Set the host computer to the static IP address **192.168.0.250** to be able to connect to the factory-default PW-7000 controller at address **192.168.0.251**.

Step 5. Power up the PW-7000 controller.

Login Page

Step 1. Click the “**Click Here to Login**” link to display the **User Name** and **Password** fields.

Figure 5: PW-7000 Web Server Login Screen



Click Here to Login

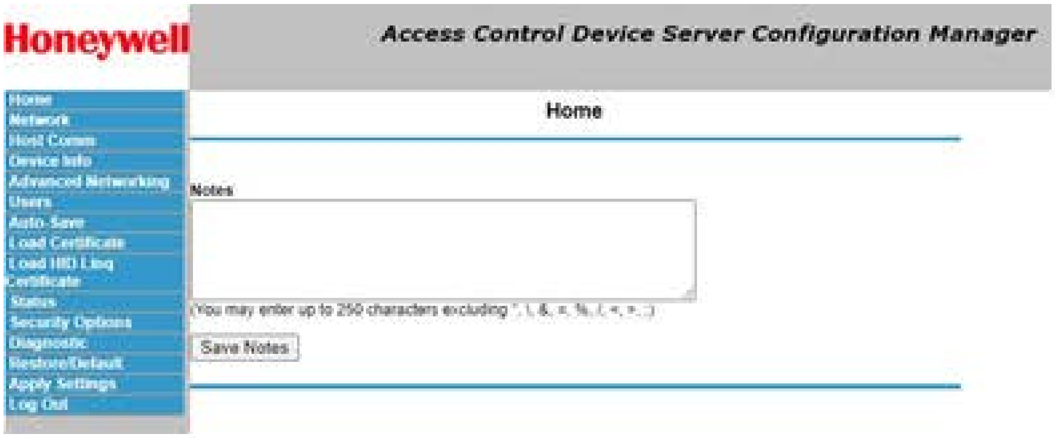
Step 2. Enter your **User Name** and **Password**.

Note: *Default User ID is* ***admin*** *and the default Password is* ***password****.*

Home Page

The first screen after the login is the home page which displays all the available configuration links on the left navigation bar.

Figure 6: PW-7000 Web Server Home Page



Access Control Device Server Configuration Manager

Home

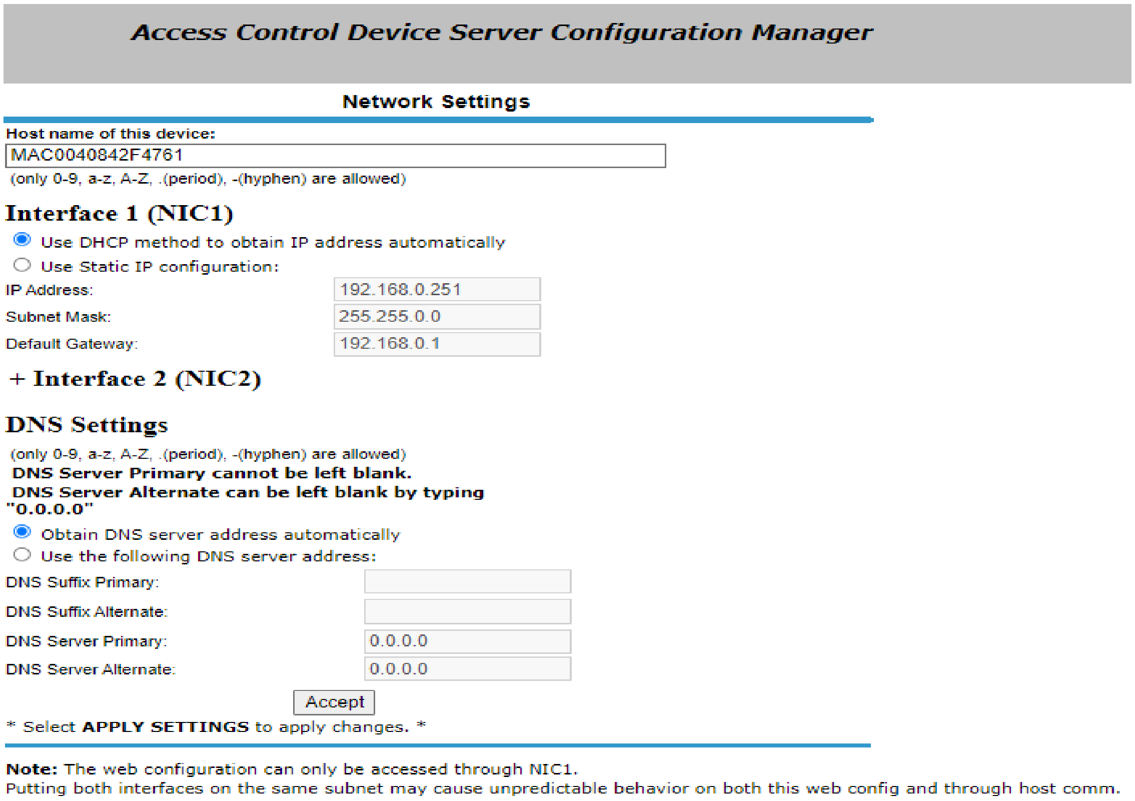
Notes

(You may enter up to 250 characters excluding ", \, &, =, %, /, <, >, :)

Network Settings

Click the Network link on the navigation bar to display the Network Settings screen where you can select the appropriate option button for dynamic or static IP address configuration:

Figure 7: PW-7000 Web Server Network Settings Screen



Access Control Device Server Configuration Manager

Network Settings

Host name of this device: MAC0040842F4761

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

Interface 1 (NIC1)

● Use DHCP method to obtain IP address automatically

○ Use Static IP configuration:

IP Address:	192.168.0.251
Subnet Mask:	255.255.0.0
Default Gateway:	192.168.0.1

+ **Interface 2 (NIC2)**

DNS Settings

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)
DNS Server Primary cannot be left blank.
DNS Server Alternate can be left blank by typing "0.0.0.0"

● Obtain DNS server address automatically

○ Use the following DNS server address:

DNS Suffix Primary:	
DNS Suffix Alternate:	
DNS Server Primary:	0.0.0.0
DNS Server Alternate:	0.0.0.0

* Select **APPLY SETTINGS** to apply changes. *

Note: The web configuration can only be accessed through NIC1.
Putting both interfaces on the same subnet may cause unpredictable behavior on both this web config and through host comm.

Note: *The Host Name of This Device field contains the Media Access Control (MAC) address of the PW-7000 controller board.*

Note: *The users can select the **Dynamic IP** option button and reserve an IP address for the MAC address, or they can select the other option button and assign a **Static IP** address as well.*

Dynamic IP Configuration Method

Step 1. Click the **Dynamic IP** option button to select the Dynamic Host Configuration Protocol (DHCP) method to obtain IP address automatically.

Step 2. Click **OK**.

Note: *Pro-Watch communicates with the PW-7000 panel using an IP address. If you must use the Dynamic IP option because of your network policies or configuration, it is recommended to reserve an IP address at the DHCP server for the MAC (Media Access Control) address in the PW-7000 panel. The MAC address is a unique identifier attached to network adapters. Each time the PW-7000 panel requests an IP address, the DHCP server will assign the address that was reserved for it.*

Static IP Configuration Method

Step 1. Click the **Static IP** option button to assign a static IP address, and enter the following information in the appropriate fields:

- IP Address
- Subnet Mask
- Default Gateway

Step 2. Click **OK**.

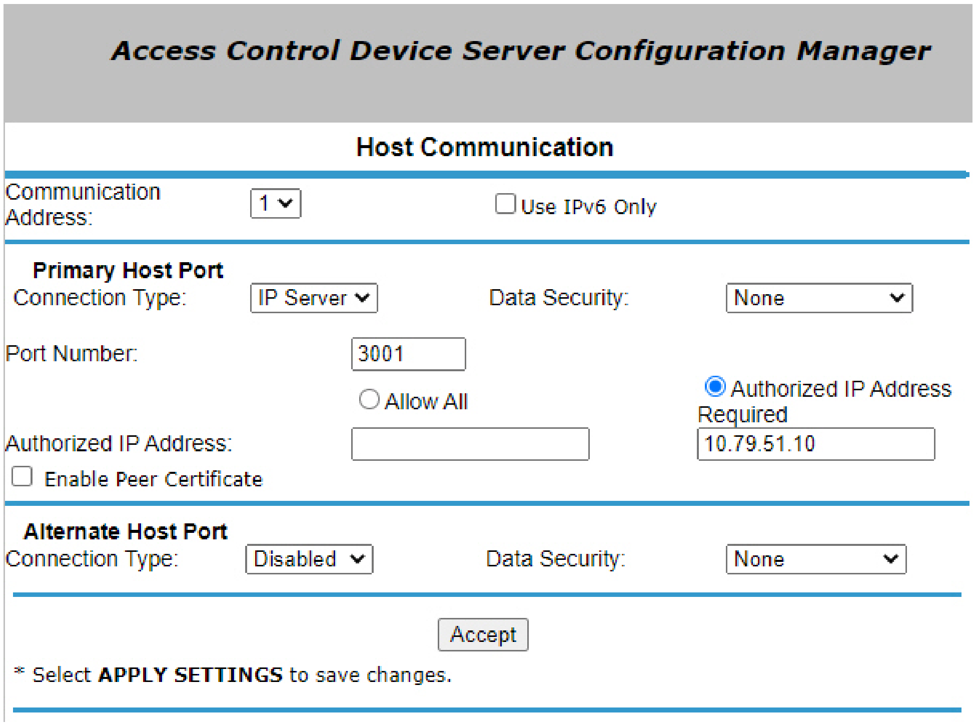
Host Communication

Click the **Host Communication** link on the navigation bar to display the Host Communication Configuration screen where you can select the appropriate settings for the Primary Host Port and Alternate Host Port:

Note: *Some of the fields change dynamically depending on the Connection Type selected.*

IP Server Connection Type

Figure 8: PW-7000 Host Port Configuration Screen with IP Server Connection



Access Control Device Server Configuration Manager

Host Communication

Communication Address: 1 ☐ Use IPv6 Only

Primary Host Port

Connection Type: IP Server Data Security: None

Port Number: 3001

○ Allow All ● Authorized IP Address Required

Authorized IP Address: 10.79.51.10

☐ Enable Peer Certificate

Alternate Host Port

Connection Type: Disabled Data Security: None

Accept

* Select **APPLY SETTINGS** to save changes.

Step 1. From PW7000 Communication Address drop-down list, select one of the eight (0 to 7) available **communication addresses** for the PW-7000 board.

Note: *In the previous panels, this selection was made manually by setting the DIP switches.*

Step 2. For the **Primary Host Port**, make the following selections:

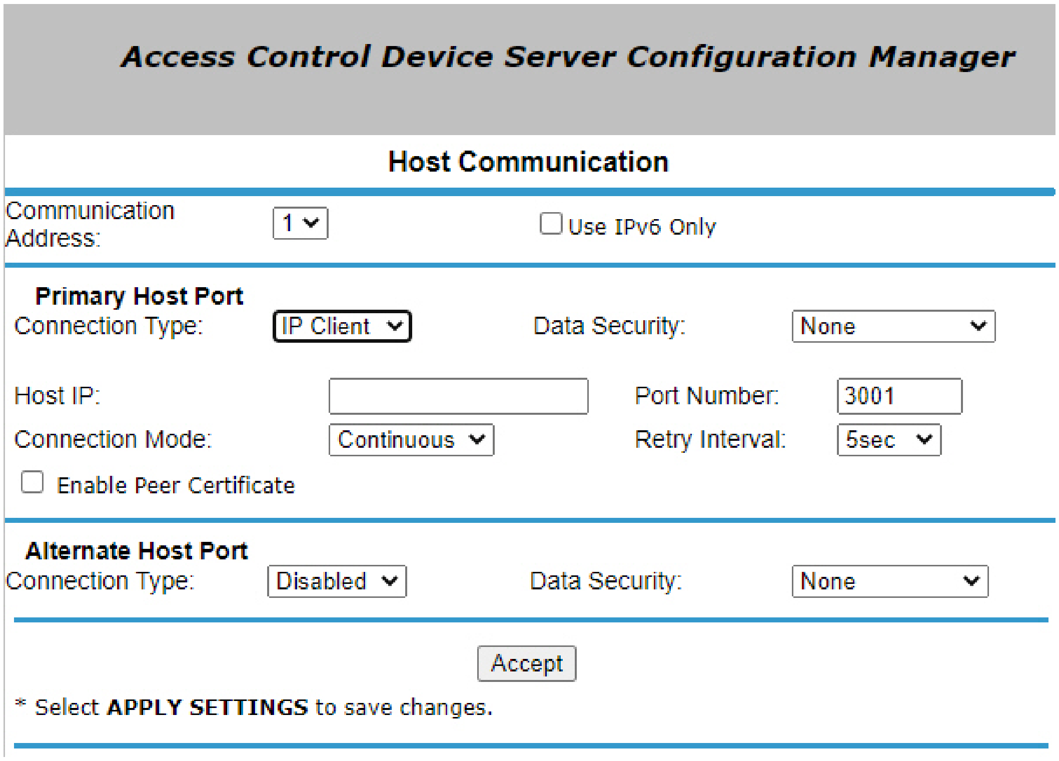
- **Connection Type**. Select **IP Server** (the standard connection type), so that the Pro-Watch Host will poll the PW-7000 panel. The panel does not currently support the **IP Client** option, which would cause the PW-7000 panel to poll the Pro-Watch Host and the Host to reply to the panel.
- **Data Security**. Select one of the following:
  - **None**
  - **Password/AES** from the drop-down list. If you select **Password/AES**, communications between the Pro-Watch Host and the PW-7000 panel are encrypted. Note that encryption must be enabled in Pro-Watch for the appropriate Pro-Watch channel. See Chapter 7, “Hardware Configuration,” in the Pro-Watch Guide for channel encryption instructions.
  - **TLS Required**
  - **TLS if Available**
- **Port Number**. Enter the port number through which the host computer can communicate with the PW-7000 board.

- Select either **Allow All** or the **Authorized IP Address Required** option button.
  - **Allow All,** as the label suggests, allows all IP addresses to communicate with the PW-7000. Select this option for web page browser access.
  - If you select the **Authorized IP Address Required** option, also enter in the **Authorized IP Addresses** fields all the IP addresses that would be allowed to communicate with the PW-7000. Use this option only for Host communication.

Step 3. Click **OK**.

IP Client Connection Type

Figure 9: PW-7000 Host Port Configuration Screen with IP Client Connection



Access Control Device Server Configuration Manager

Host Communication

Communication Address: 1 ▾ □ Use IPv6 Only

Primary Host Port

Connection Type: IP Client ▾ Data Security: None ▾

Host IP: Port Number: 3001

Connection Mode: Continuous ▾ Retry Interval: 5sec ▾

□ Enable Peer Certificate

Alternate Host Port

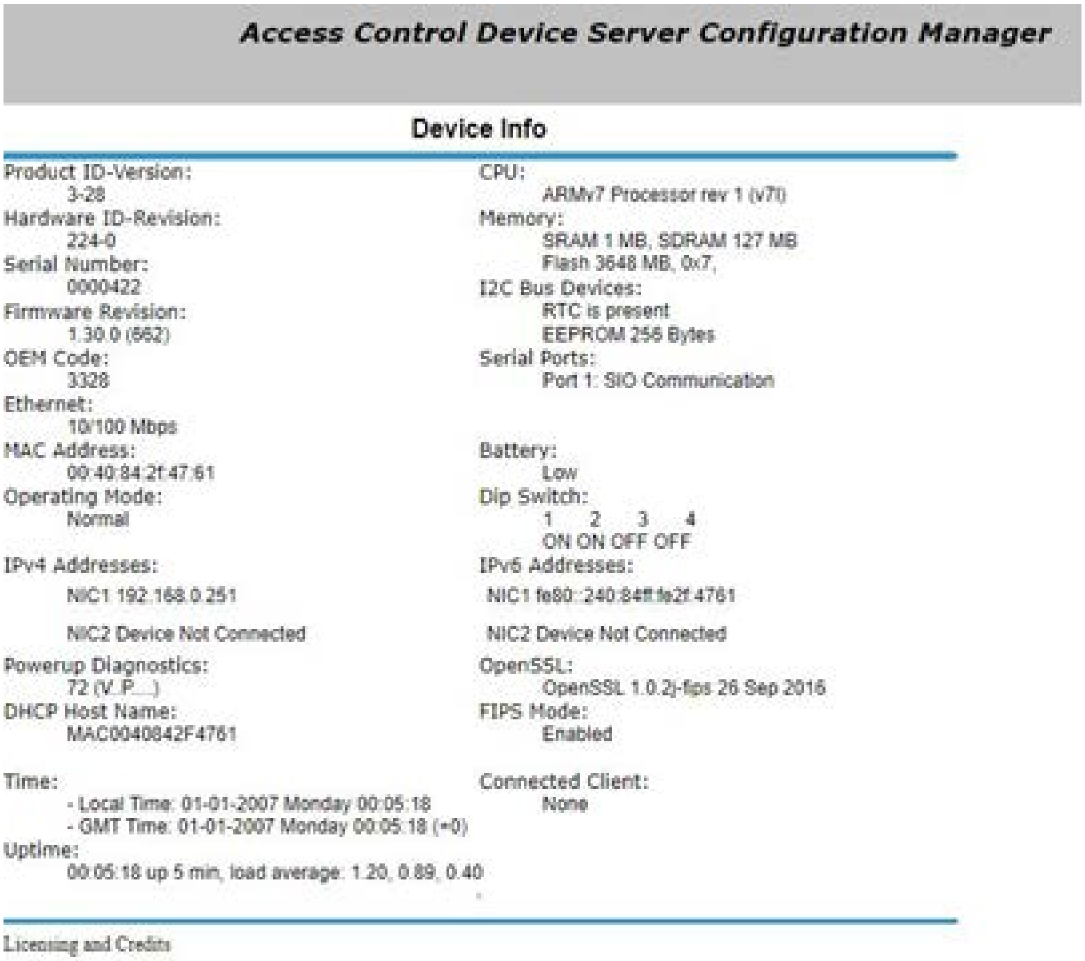
Connection Type: Disabled ▾ Data Security: None ▾

* Select **APPLY SETTINGS** to save changes.

Device Information

- Click the Device Info link on the navigation bar to display the read-only Access Control Device Hardware Information screen:

Figure 11: PW-7000 Web Server Device HW Info Screen



Access Control Device Server Configuration Manager

Device Info

Product ID-Version:
3-28
Hardware ID-Revision:
224-0
Serial Number:
0000422
Firmware Revision:
1.30.0 (862)
OEM Code:
3328
Ethernet:
10/100 Mbps
MAC Address:
00:40:84:2f:47:61
Operating Mode:
Normal
IPv4 Addresses:
NIC1 192.168.0.251
NIC2 Device Not Connected
Powerup Diagnostics:
72 (V..P....)
DHCP Host Name:
MAC0040842F4761
Time:
- Local Time: 01-01-2007 Monday 00:05:18
- GMT Time: 01-01-2007 Monday 00:05:18 (+0)
Uptime:
00:05:18 up 5 min, load average: 1.20, 0.89, 0.40

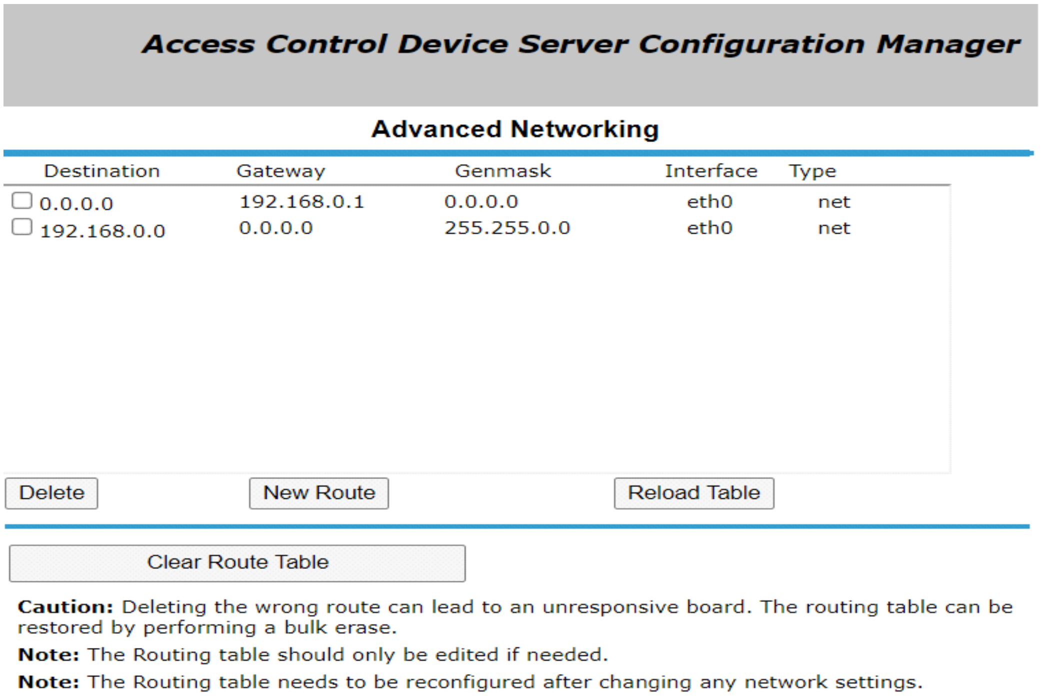
CPU:
ARMv7 Processor rev 1 (v7l)
Memory:
SRAM 1 MB, SDRAM 127 MB
Flash 3648 MB, 0x7,
I2C Bus Devices:
RTC is present
EEPROM 256 Bytes
Serial Ports:
Port 1: SIO Communication
Battery:
Low
Dip Switch:
1 2 3 4
ON ON OFF OFF
IPv6 Addresses:
NIC1 fe80::240:84ff:fe2f:4761
NIC2 Device Not Connected
OpenSSL:
OpenSSL 1.0.2j-fips 26 Sep 2016
FIPS Mode:
Enabled
Connected Client:
None

Licensing and Credits

Advanced Networking

Step 1. Click the Advanced Networking link on the navigation bar to display the Access Control Device Server Configuration Manager.

Figure 10: PW7000 Access Control Device Server Configuration Manager



Access Control Device Server Configuration Manager

Advanced Networking

Destination	Gateway	Genmask	Interface	Type
□ 0.0.0.0	192.168.0.1	0.0.0.0	eth0	net
□ 192.168.0.0	0.0.0.0	255.255.0.0	eth0	net

Caution: Deleting the wrong route can lead to an unresponsive board. The routing table can be restored by performing a bulk erase.

Note: The Routing table should only be edited if needed.

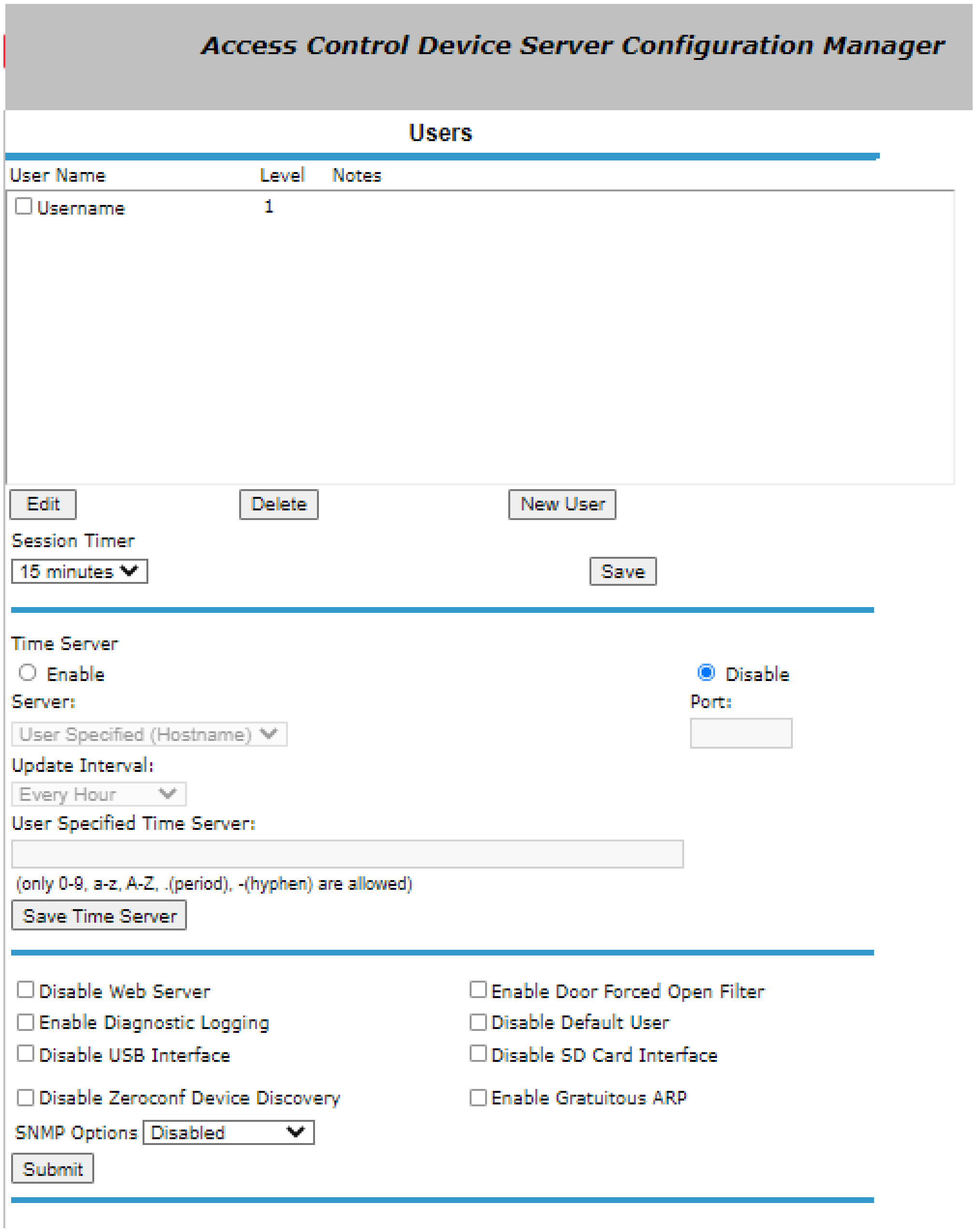
Note: The Routing table needs to be reconfigured after changing any network settings.

The **Advanced Networking** is displayed, and allows new routing information to be added. This Advanced Networking is typically not used as it is only for advanced configurations.

User Configuration

- Click the Users link on the navigation bar to display the User screen where you can add, edit, and delete user records:

Figure 12: PW-7000 Web Server User Info Screen



Access Control Device Server Configuration Manager

Users

User Name	Level	Notes
□ Username	1	

Session Timer
15 minutes

Time Server
○ Enable ● Disable
Server: User Specified (Hostname)
Port:
Update Interval: Every Hour
User Specified Time Server:
(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

□ Disable Web Server
□ Enable Diagnostic Logging
□ Disable USB Interface
□ Disable Zeroconf Device Discovery
□ Enable Door Forced Open Filter
□ Disable Default User
□ Disable SD Card Interface
□ Enable Gratuitous ARP
SNMP Options Disabled

Adding a User

Follow these steps:

Step 1. Click **New Account** to display the new user account screen.

Step 2. Enter the following:

User name – a unique character string that identifies the user.

- Level – level of privileges the user will have. Level 1 grants the user read/write privileges to all panel features; level 2 grants the user
- read-only privileges to the Notes, Network, Host Port, and Device Info features; level 3 grants the user read-only privileges to just the Notes and Device Info features.

Step 3. Specify the maximum period of time a session will remain open without user activity. If the period expires without user activity, the user is logged out. After specifying the time period, click **Save Session Timer** to save the setting.

Step 4. Configure the auto-save timer. This feature, if enabled, automatically saves the hardware configuration in non-volatile Random Access Memory (RAM) at the specified time interval. If you select Enable Auto-Save, then select a time interval from the drop-down list, and click **Save Auto-Save Timer** to save the setting.

Editing a User

To edit a user record, click to select the user from the Username column and then click **Edit**. Use the information provided in the previous section, “Adding a User,” to edit the record.

Deleting a User

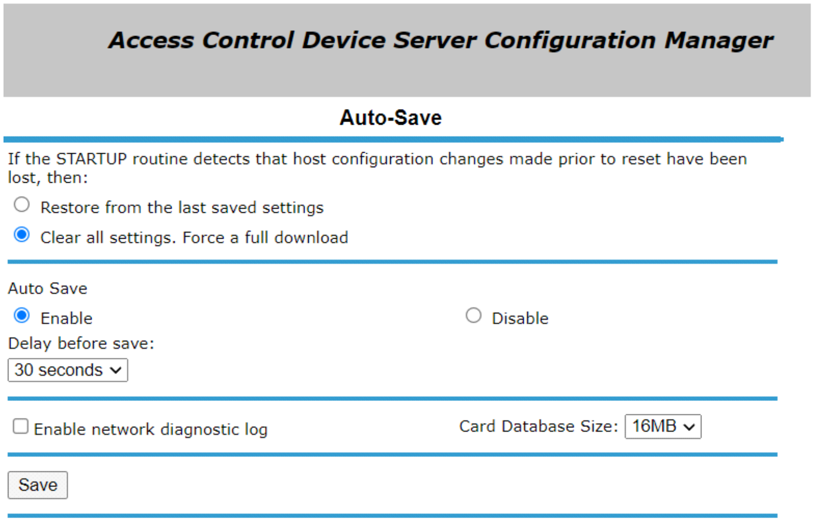
- To delete a user record, click to select the user from the Username column and then click **Delete**.

Auto-Save

Step 1. Click the Auto-Save link on the navigation bar.

Step 2. The Auto Save configuration automatically saves the behavior and determines how the controller reacts on start up, if host configuration changes have been lost.

Figure 13: PW-7000 Access Control Device Server Configuration Manager



Access Control Device Server Configuration Manager

Auto-Save

If the STARTUP routine detects that host configuration changes made prior to reset have been lost, then:

○ Restore from the last saved settings

● Clear all settings. Force a full download

Auto Save

● Enable ○ Disable

Delay before save:

30 seconds

□ Enable network diagnostic log

Card Database Size: 16MB

Step 3. Click to select Restore from the last saved settings to restore from the save point at power up, or from the reboot button on the controller.

Step 4. Click to select “Clear all settings, Force a full down” to force a controller to reload at power-up.

Enabling

Auto-save configures the controller to automatically save settings for configuration changes.

Disabling

Note: *Auto-save means that configuration changes are not automatically saved. Configuration can be manually saved.*

The auto-save delay specifies the time consumed to wait after a host configuration changes, before starting to save.

The timer is specified between 30 seconds and 30 minutes.

Checking “Enable Network Diagnostic Log” causes diagnostic information to be written to the debug file in every 15 minutes, when debug is enabled.

The Card Database Size specify size of 16MB only.

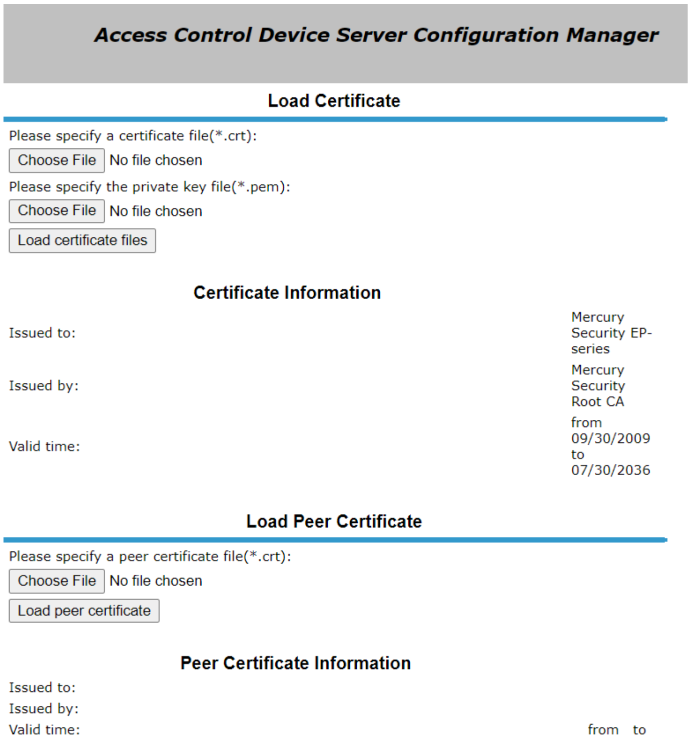
- Click on “**Save Settings**” for changes to be loaded into the controller.

Load Certificate

Step 1. Click the Load Certificate link on the navigation bar to display.

Step 2. The Load Certificate page will allow the certificates loaded at the factory to be replaced by unique custom certificates.

Figure 14: Access control Device Server Configuration Manager



Access Control Device Server Configuration Manager

Load Certificate

Please specify a certificate file(*.crt):

Please specify the private key file(*.pem):

Certificate Information

Issued to:	Mercury Security EP-series
Issued by:	Mercury Security Root CA
Valid time:	from 09/30/2009 to 07/30/2036

Load Peer Certificate

Please specify a peer certificate file(*.crt):

Peer Certificate Information

Issued to:	
Issued by:	
Valid time:	from to

The Certificate Information section of "**Peer Certificate Information**" lists the information about the currently loaded certificates.

Step 3. Click the "**Browser Button**" to select the related files to be loaded in PW-7000

Step 4. Click the **"Load Certificate Files"** to upload the files selected.

The PW-7000 series controllers allow for a maximum of 4096-bit RSA key encryption and SHA-384.

Certificate Types

The .crt file is the certificate file.

The .pem file is the Private Key file.

Note: *Settings are not permanently saved in the device until saved on the "Apply Settings" web page.*

Peer Certificates

In the controller's web interface, the "Enable Peer Certificate" option in the Host Comm configuration web page will enable/disable driver side verification in the controller. When this option is set, the controller will make a request to the Driver to send its peer certificate during the TLS handshake.

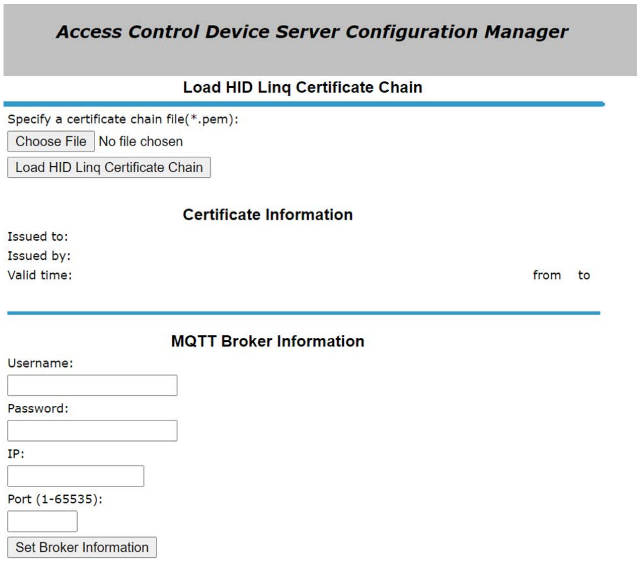
Load HID Linq Certificate

Note: *For Future Use - Not applicable for Pro-Watch. Please contact Honeywell Tech Support for more details.*

Step 1. Click the Load HID Linq Certificate link on the navigation bar to display.

Step 2. The Load HID Linq Certificate will allow load specify a certificates chain file.

Figure 15: Load HID Linq Certificate



Access Control Device Server Configuration Manager

Load HID Linq Certificate Chain

Specify a certificate chain file(*.pem):

Choose File No file chosen

Load HID Linq Certificate Chain

Certificate Information

Issued to:

Issued by:

Valid time: from to

MQTT Broker Information

Username:

Password:

IP:

Port (1-65535):

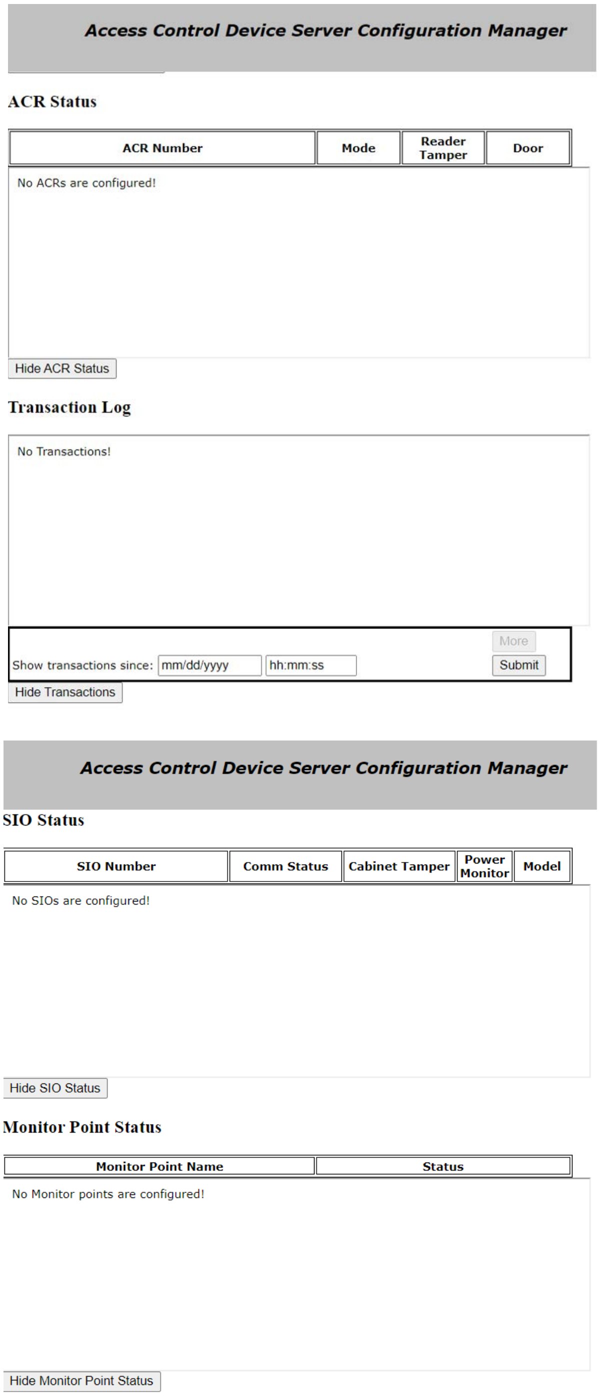
Set Broker Information

Status Display

Step 1. Click the "Status link" on the navigation bar to display.

Step 2. The Status screen will display the state of the Access Control Readers, Monitor Points and Control Points, as well as the transaction log.

Figure 16: The Access Control Readers, Monitor



Access Control Device Server Configuration Manager

ACR Status

ACR Number	Mode	Reader Tamper	Door

No ACRs are configured!

Transaction Log

No Transactions!

Show transactions since: mm/dd/yyyy hh:mm:ss

Access Control Device Server Configuration Manager

SIO Status

SIO Number	Comm Status	Cabinet Tamper	Power Monitor	Model

No SIOs are configured!

Monitor Point Status

Monitor Point Name	Status

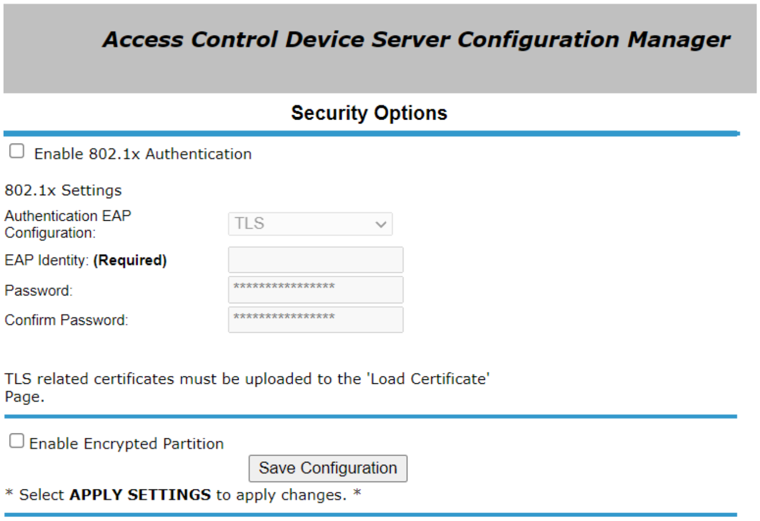
No Monitor points are configured!

Note: *The status display is only available in firmware revisions 1.8.0 and later.*

Security Options

Step 1. Click the "**Security Options**" link on the navigation bar to display the choose, if Enable 802.1x Authentication.

Figure 17: Security option



Access Control Device Server Configuration Manager

Security Options

☐ Enable 802.1x Authentication

802.1x Settings

Authentication EAP Configuration:	TLS
EAP Identity: **(Required)**	
Password:	****************
Confirm Password:	****************

TLS related certificates must be uploaded to the 'Load Certificate' Page.

☐ Enable Encrypted Partition

Save Configuration

* Select **APPLY SETTINGS** to apply changes. *

In order to communicate with the controller, the board must be on an isolated network (or directly talking to a PC). This is because the board cannot be communicated through the network that has an authentication server until. The Authenticated server unit must properly configured.

If The Authenticated server unit is not configured the PC configuring will not be able to communicate with it. By default, the controllers have 802.1x disabled.

Ensure the controller is using static IP and connected as "Network Settings".

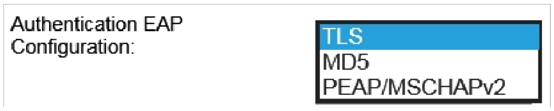
Step 1. Click "Security Options" on the menu, Once the controller is able to be communicated with browser (left-most side of the web page).

Enable 802.1x Authentication

As an added layer of local area network security, 802.1x authentication can be added to prevent unwanted access to a given network.

This allows you to enable 802.1x authentication and configure the security options for the Ethernet interface. This option is disabled by default.

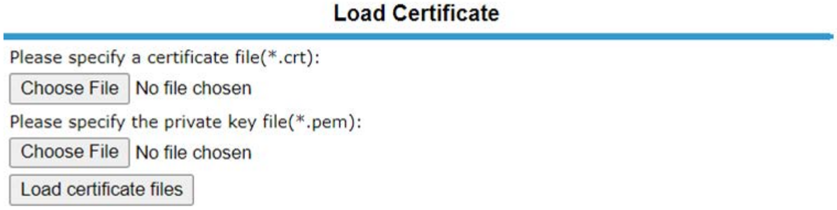
Available selections for Authentication EAP Configuration are "TLS", "MD5" and "PEAP/MSCHAPv2".



Authentication EAP Configuration:

When selecting TLS, ensure that the certificates of the controller are signed by the same root certificate that is used on the authentication server. (Skip this step if selecting MD5 or PEAP via MSCHAPV2). Go to the “Load Certificate” page and upload the necessary .crt and .pem files.

Figure18: Load Certificate



Load Certificate

Please specify a certificate file(*.crt):

No file chosen

Please specify the private key file(*.pem):

No file chosen

EAP Identity is a required field, but all fields are based on the configuration of the authentication server. Thus, the user should know the necessary settings before filling out these fields. Should the authentication server not require an EAP identity / username, any identity must be entered such as “admin”.

Enable Encrypted Partition

Selecting this option allows the configuration and data files to be encrypted, cannot be undone without a bulk erase.

Once all fields are set to the configuration corresponding to the authentication server’s.

Step 1. Click “Save Configuration” and then click on “Apply Settings” on the menu

Step 2. Click “Apply Settings, Reboot” button. The controller will now reboot.

Step 3. Once the board has rebooted, connect the controller to the network that talks to the desired network, authenticator, and authenticator server.

Step 4. The controller is now configured for 802.1x.

Disabling 802.1x

In order to disable 802.1x, first follow the steps in the “Network Settings” section above to ensure that the controller is using static IP. Once you have that information,

Step 1. Click on “Security Options” and uncheck the “Enable 802.1x

Step 2. Authentication” check box.

Step 3. Click on “Save Configuration”, then

Step 4. Click on “Apply Settings” on the menu

Step 5.]Click the “Apply Settings, Reboot” button.

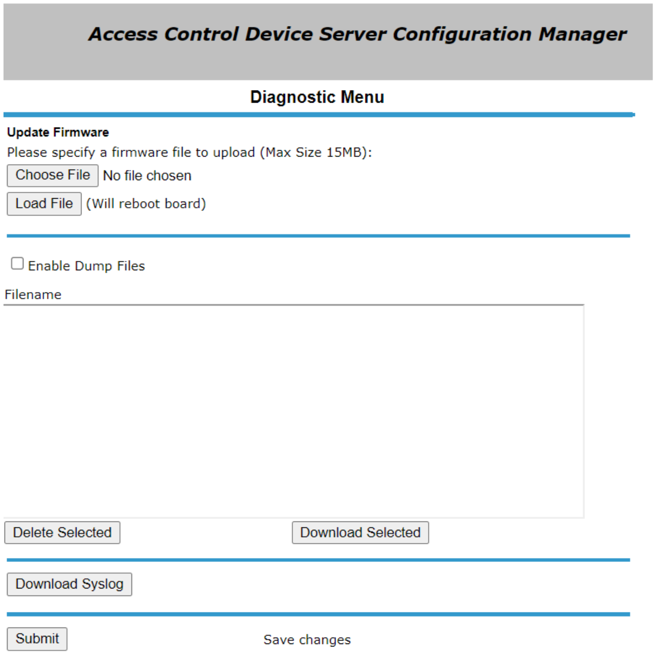
The controller will now reboot.

Note: *That if the PC configuring the board is on the authenticated network, and the controller's 802.1x is disabled, the controller will no longer be able to talk to the PC, since it is no longer authenticated. In order to communicate with the board again, follow the steps in the section "Network Settings" above.*

Diagnostics Menu

Step 1. Click the Diagnostic Menu link on the navigation bar to display where you can choose to update the firmware.

Figure 19: Diagnostic Menu



Access Control Device Server Configuration Manager

Diagnostic Menu

Update Firmware

Please specify a firmware file to upload (Max Size 15MB):

Enable Dump Files

The PW-7000 is capable of creating a core dump file. An SD card must be installed to use this feature.

Download Syslog

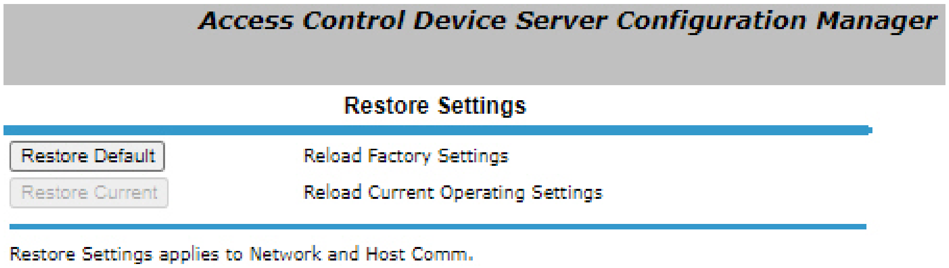
This option allows you to download the encrypted Syslog file.

Note: *The Syslog file can be analyzed and should only be downloaded if requested to assist in troubleshooting an issue.*

Restore Default Screen

Step 1. Click the Restore Default link on the navigation bar to restore the default configuration values for the PW-7000:

Figure 20: PW-7000 Web Server Restore Default Screen



Access Control Device Server Configuration Manager

Restore Settings

Reload Factory Settings

Reload Current Operating Settings

Restore Settings applies to Network and Host Comm.

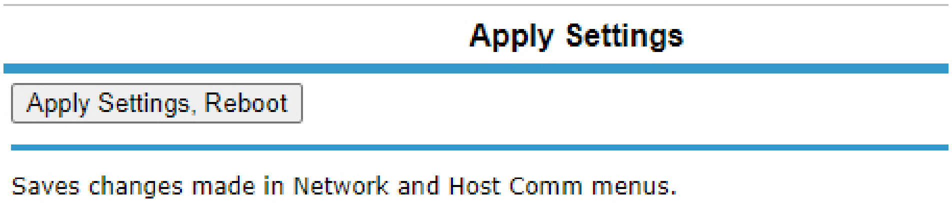
Step 2. Click **Restore Default** to reload the default factory settings for all the configuration variables.

Step 3. Click **Restore Current** to reload the current operational settings for all the configuration variables.

Apply Setting Screen

Step 1. Click the Apply Setting link on the navigation bar to apply the selected configuration values:

Figure 21: PW-7000 Web Server Apply Setting Screen



Apply Settings

Saves changes made in Network and Host Comm menus.

Step 2. Click **Apply, Reboot** to apply all the configured values and reboot the PW-7000.

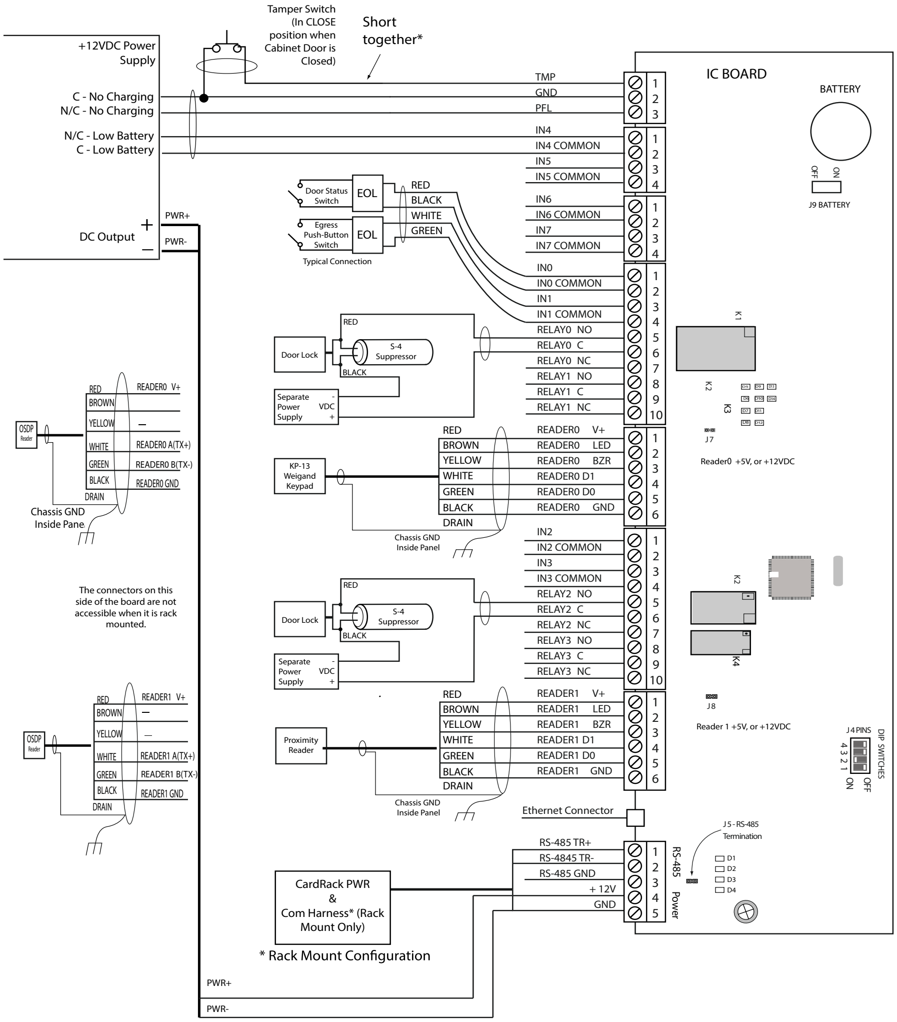
Log Out

- Click the **Log Out** link on the navigation bar to log out of the web server.

CHAPTER

4 READER MODULE

Figure 1: PW-7000 Intelligent Controller Module Wiring: TB1,TB3-9



Note: *See Status LEDs (see page 20) for descriptions of LEDs D1-D20.*

Reader Wiring

The following Honeywell reader modul numbers have been approved by UL for use with the PW7K1IC: OS20TOSDP, OS20KTOSDP, OS40TOSDP, OS40KTOSDP.

Each reader port supports a reader with TTL interface. Power to the reader is selectable as 5VDC or 12VDC (pass-through). This selection is done by setting the jumpers J7 for reader 0 and J8 for reader 1. Set jumper at position “5” for 5VDC or “12” for pass-through 12VDC. The factory defaults set J7 and J8 to “5”.

For wiring to a reader port:

Table 5: Settings for Wiring to a Reader Port

Terminal	Typical Wire Color	Wiegand Reader	Clock/Data Reader	OSDP Reader
1	Red	Power (5 or 12 Vdc)	Power (5 or 12 Vdc)	Power (12 VDC)
2	Brown	LED control	LED control	-
3	Yellow	Beeper Control	Beeper Control	-
4	White	Data 1 Signal	Clock Signal	A Signal (TX+)
5	Green	Data 0 Signal	Data Signal	B Signal (TX-)
6	Black	Common	Common	Ground

The LED control terminal in each reader port can be configured via host software to support one-wire single or bi-colored reader LED. An example of the most common configuration is shown below. If Beeper Control is not used, its terminal can be programmed to be the second wire for the two-wire bi-colored reader LED.

Table 6: Settings for Configuring an LED Control Terminal

LED Output->	High	Tri-Stated	Low
Single Color LED	LED On	LED Off	LED Off
Bi-Color LED	Green LED On	Both LEDs Off	Red LED On

To fully utilize each reader port, a 6-conductor cable (18AWG) is required. Reader port configuration is set via host software.

Input Wiring

Inputs 0 to 7 may be configured to use normally open or normally closed contacts and non-supervised or supervised (with standard ±1% tolerance 1K ohm). Four of these inputs have default functional definitions, but all eight can be configured to monitor general-purpose sensors.

By default, Input 0 is defined as the Door Status Input corresponding to reader 0 and Input 1 is defined as the REX input corresponding to reader 0. Also by default, Input 2 is defined as the Door Status Input corresponding to reader 1 and Input 3 is defined as the REX input corresponding to reader 1.

Inputs 4, 5, 6 and 7 are general purpose inputs that can be used to monitor sensors or as control inputs. Inputs 6 and 7 are not accessible when the board is rack mounted.

Inputs TMP and PFL are typically used for monitoring cabinet tamper and power failure respectively. These two inputs are not supervised and are not accessible when the board is rack-mounted. These inputs were primarily provided for the case when this board is mounted remotely and cannot take advantage of the tamper and power fail detect inputs on the controller board. If these inputs are not used, install a short piece of wire at the input to indicate safe condition.

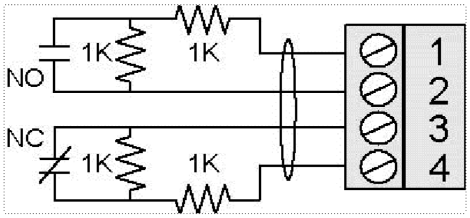
Input configuration including debounce and hold time is set via host software.

Control Output Wiring

Four form-C relay contacts are provided for controlling door strike or other devices. Each may be assigned to door-related functions or general-purpose output. They are configurable as standard (energize to activate) or fail-safe (de-energize to activate) via host software.

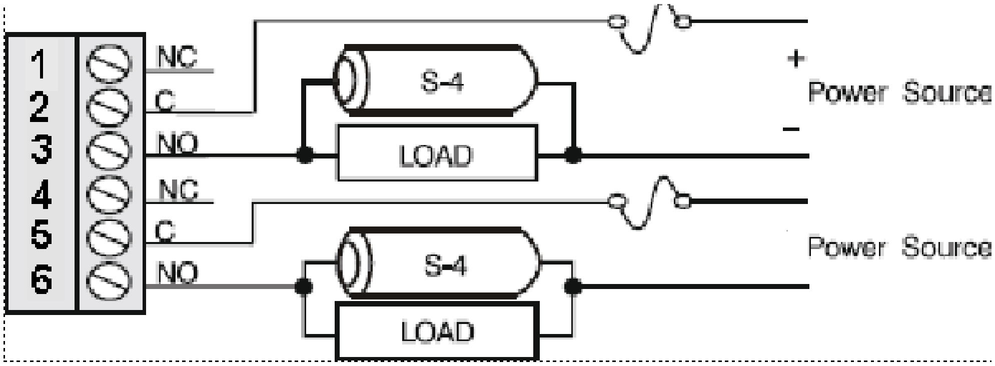
The energized or ON time of each relay can be configured using Pulse control for single or repeating pulses via host software. The energized or ON time for a single pulse can be extended up to 24 hours. For repeating pulses, the on/off time can be defined in 0.1 second increments and be repeated up to 255 times.

Relays 0 and 2 are rated for and normally used to control the door locks associated with readers 0 and 1 respectively. While Relays 0 and 2 are sized to handle the typical loads generated by electrical locks, load switching can cause abnormal contact wear and premature contact failure. Switching of inductive loads (i.e., strike) also causes EMI (electromagnetic interference) which may interfere with normal operation of other equipment. To minimize premature contact failure and to increase system reliability, a contact protection circuit is highly recommended. The following two circuits are suggested. Locate the protection circuit as close to the load as possible (within 12 inches [30cm]); the effectiveness of the circuit decreases as the distance from the load increases.



Relays 1 and 3 are dry-circuit level signal relays typically used to indicate the status of the door lock.

Use sufficiently large gauge of wires for the load current to avoid voltage loss.


1
2
3
4
5
6
NC
C
NO
NC
C
NO
S-4
LOAD
S-4
LOAD
+
Power Source
–
Power Source

CHAPTER

5 SECONDARY IP SUPPORT USING MICRO USB ADAPTER

Support for a secondary network interface via a USB to Ethernet adapter is available with the PW7K1IC controller to provide a second network interface.

Controller support

Below table details the supported micro-USB adapter and required minimum controller firmware version.

Controller Module	USB Type	Minimum Required Firmware	Supported	Adapter
PW7K1IC	USB Micro B	1.29.6.0659	Pluggable	USB-OTGE 100

Supported Functionalities

The functionality available via the primary network interface compared to the secondary network interface.

Feature	NIC 1	NIC2
Host Communication	✓	✓
Web Interface	✓	
Device Discovery	✓	
SNMP	✓	
Downstream Ethernet SIO	✓	
OTIS Compass	✓	✓
Overwatch Communication	✓	
PSTA	✓	

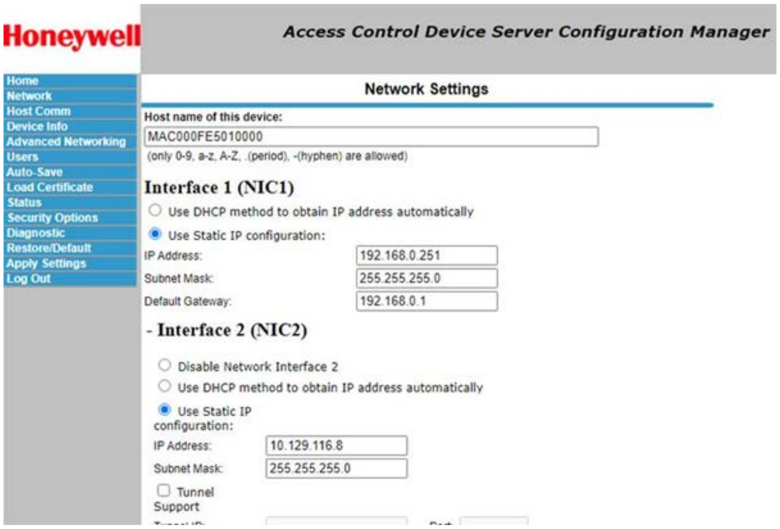
Network Settings Configure NIC2 as a Back-up for Host Communication

In case of network failure on NIC1, NIC2 can be configured as an alternate connection. If a communication failure occurs, the system reports the communication failure to the application, then automatically uses the alternate connection specified. If network communication is re-established on NIC1, NIC1 is used again, and NIC2 resumes a stand-by role.

Sample Setup Steps:

Step 1. On the Network Settings controller web page, configure NIC1 and NIC2 with static IP addresses.

Step 2. On the **Host Communication** web Page, enable the NIC2 interface.



Access Control Device Server Configuration Manager

Network Settings

Host name of this device: MAC000FE5010000

(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

Interface 1 (NIC1)

○ Use DHCP method to obtain IP address automatically

● Use Static IP configuration:

IP Address: 192.168.0.251

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

- Interface 2 (NIC2)

○ Disable Network Interface 2

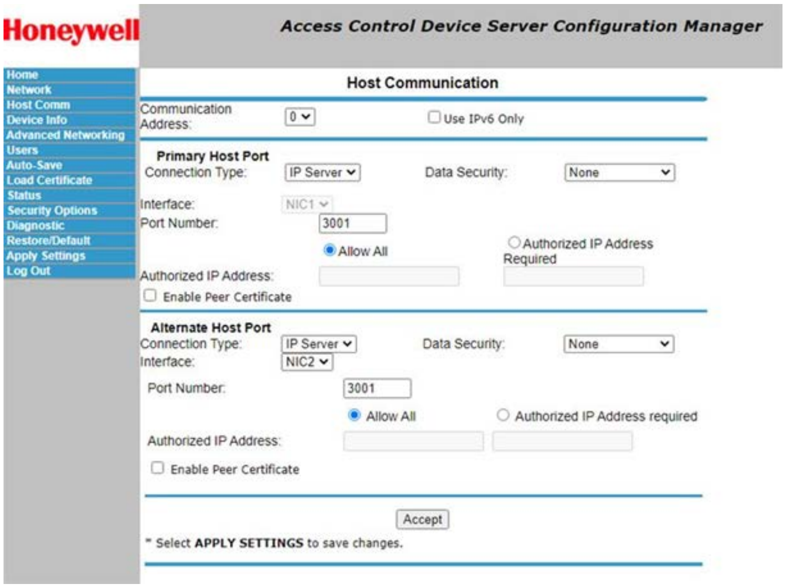
○ Use DHCP method to obtain IP address automatically

● Use Static IP configuration:

IP Address: 10.129.116.8

Subnet Mask: 255.255.255.0

□ Tunnel Support



Access Control Device Server Configuration Manager

Host Communication

Communication Address: 0 □ Use IPv6 Only

Primary Host Port

Connection Type: IP Server Data Security: None

Interface: NIC1

Port Number: 3001

● Allow All ○ Authorized IP Address Required

Authorized IP Address:

□ Enable Peer Certificate

Alternate Host Port

Connection Type: IP Server Data Security: None

Interface: NIC2

Port Number: 3001

● Allow All ○ Authorized IP Address required

Authorized IP Address:

□ Enable Peer Certificate

* Select **APPLY SETTINGS** to save changes.

Web configuration: Advanced Networking

1. Only one default gateway can be defined in the routing table as show in the **Advanced Networking** Page.
2. NIC1 and NIC2 cannot both be configured to connect on the same subnet.

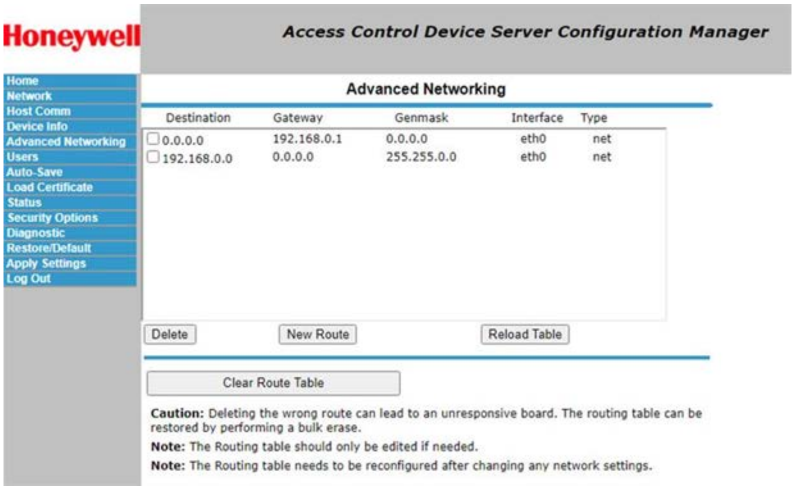
Configuring both NICs to use a static IP is recommended.

Some network configurations that use one NIC on DHCP and the other set to a static IP may result in the Creation of two default gateways.

The Advanced Networking controller web page must be used to correct this issues.

The Advanced Networking controller web page is designed to manipulate the outing table running on the Linux OS. One intended usage allows the NIC2 network to be isolated from the network used for host communication to provide more security. Many elevator implementations use this functionality to isolate the elevator system network from any outside traffic.

It is advised that DHCP not be used when using multiple NICs. Changes at the DHCP server (like netmask changes) can affect the panel's ability to connect to the network.



Advanced Networking

Destination	Gateway	Genmask	Interface	Type
□ 0.0.0.0	192.168.0.1	0.0.0.0	eth0	net
□ 192.168.0.0	0.0.0.0	255.255.0.0	eth0	net

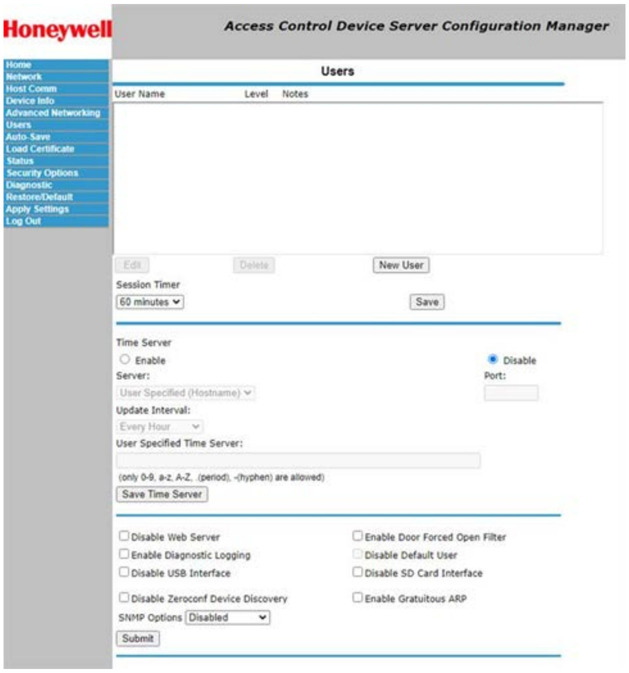
Caution: Deleting the wrong route can lead to an unresponsive board. The routing table can be restored by performing a bulk erase.

Note: The Routing table should only be edited if needed.

Note: The Routing table needs to be reconfigured after changing any network settings.

Sample controller setup

1. NIC1 (eth0) :on **Network Settings** page:
   a. Static IP : 192.168.0.251
   b. Subnet Mask : 255.255.255.0
2. NIC2 (eth1) : on **Network Settings** page:
   c. Static IP : 10.129.116.8
   d. Subnet Mask : 255.255.255.0



Access Control Device Server Configuration Manager

Users

User Name	Level	Notes

Session Timer: 60 minutes

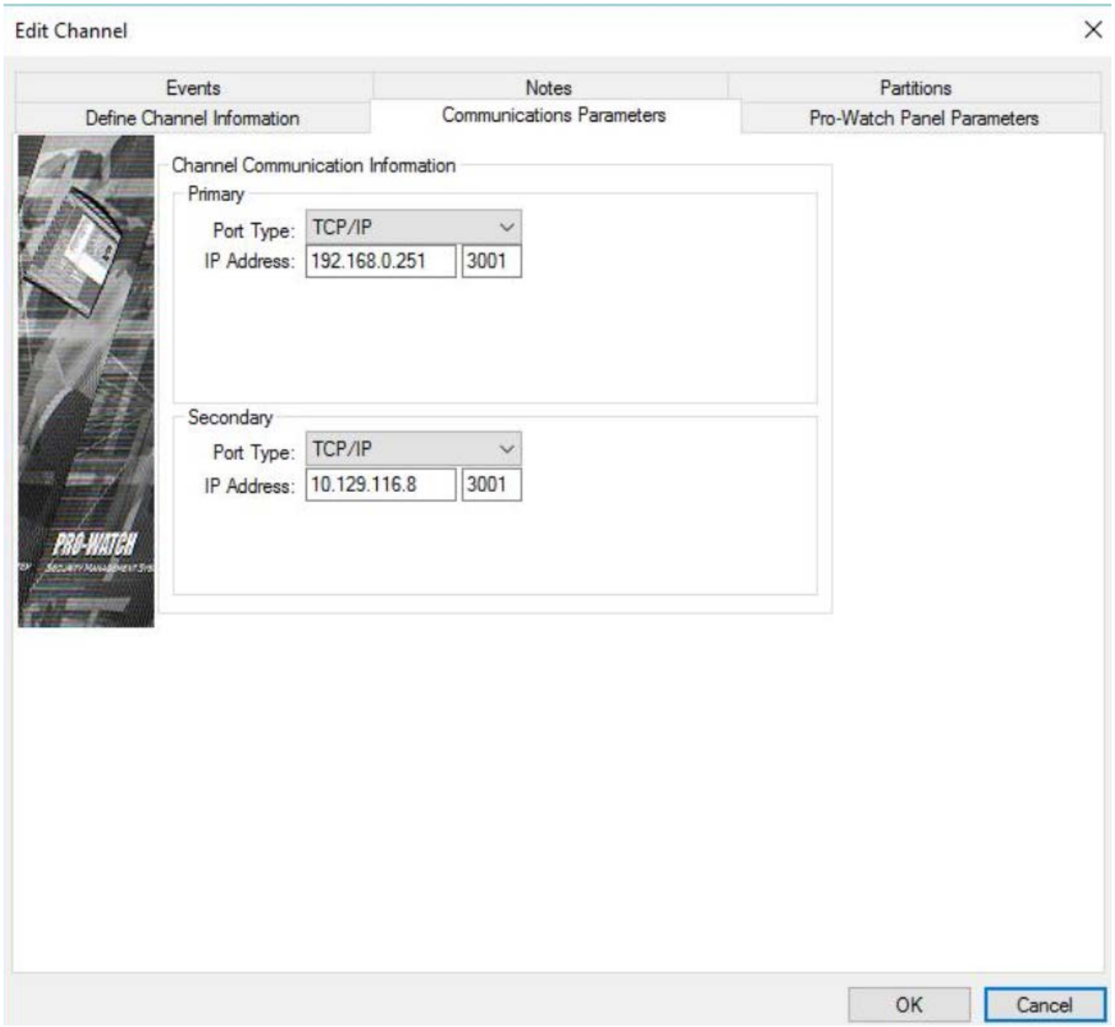
Time Server
○ Enable ● Disable
Server: User Specified (Hostname)
Port:
Update Interval: Every Hour
User Specified Time Server:
(only 0-9, a-z, A-Z, .(period), -(hyphen) are allowed)

□ Disable Web Server
□ Enable Diagnostic Logging
□ Disable USB Interface
□ Disable Zeroconf Device Discovery
□ Enable Door Forced Open Filter
□ Disable Default User
□ Disable SD Card Interface
□ Enable Gratuitous ARP
SNMP Options: Disabled

Note: *Ensure Disable USB is not selected.*

Sample Configuration in Pro-Watch

Note: *Below sample screen displays the configuration in Pro-Watch.*



Edit Channel

Events
Notes
Partitions
Define Channel Information
Communications Parameters
Pro-Watch Panel Parameters
PRO-WATCH
Security Management System
OK
Cancel

Channel Communication Information

Primary

Port Type: TCP/IP

IP Address: 192.168.0.251 3001

Secondary

Port Type: TCP/IP

IP Address: 10.129.116.8 3001

6 SD CARD SLOT AND THE MICRO-USB PORT FUNCTION

SD card slot

The purpose of SD card is to install SD card in the controller board J6 location.

Micro SD card

This is primarily used for programming the boards. In the field, it can be used to collect the diagnostic data. On the controller Diagnostic page, you can configure the settings to collect the crash dump logs and to save these dump logs a SD card is required .

Micro-USB ports

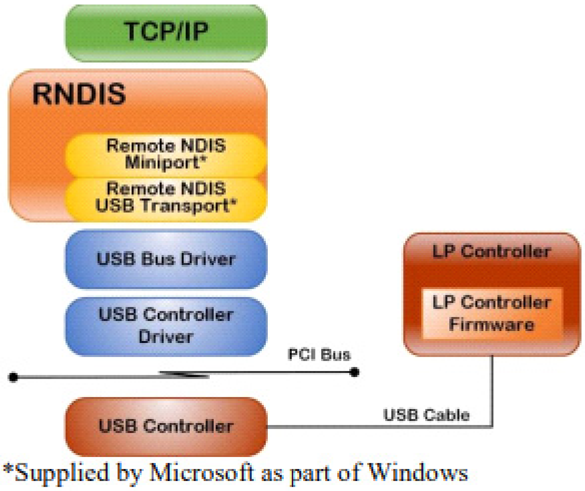
Micro USB port

Micro USB port can be used to connect a USB to Ethernet adapter and to add another NIC for redundant communications. For more details see Chapter 5 Secondary IP support using Micro USB adapter on page 41

RNDIS allows a network connection over USB to perform the initial configuration. RNDIS is used if user is unable to access the device web browser via a network connection.

RNDIS

The controllers support RNDIS (Remote Network Driver Interface Specification), which is a proprietary protocol used on top of USB. It provides a virtual Ethernet port that allows you to access the PW-7000 Series configuration web page.



Required Cable

USB cable Type-A to Micro Type-B

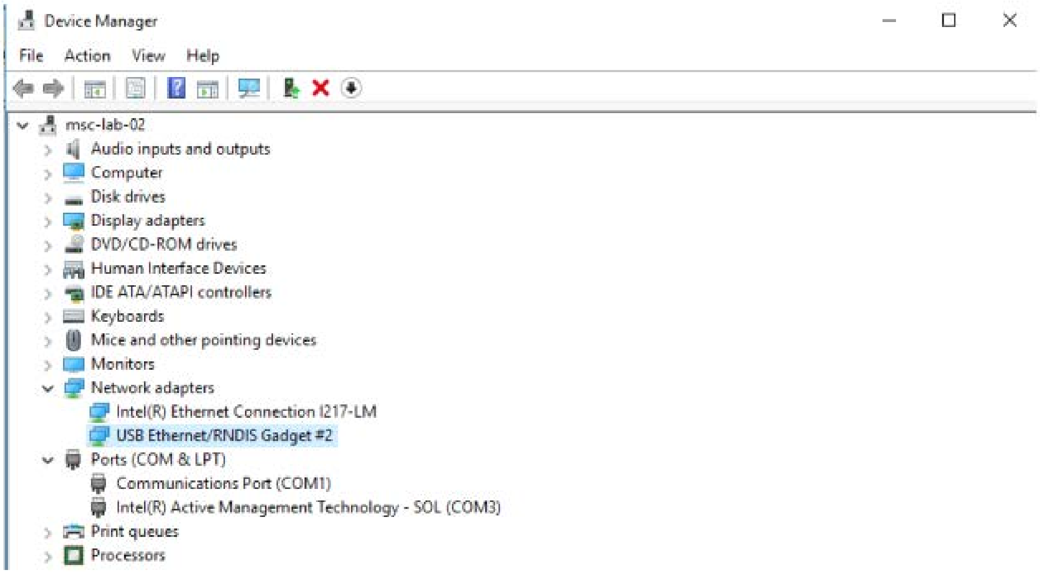
Configuring the Windows 10

Step 1. Power on the controller.

Step 2. Use the Micro Type-B USB end of the cable to connect to the controller

Step 3. Use the USB Type-A side to connect to the Windows PC.

Step 4. Navigate to the Device Manager > Network adapters and then select USB Ethernet/RNDIS Gadget #2.



- msc-lab-02
  - Audio inputs and outputs
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Intel(R) Ethernet Connection I217-LM
    - USB Ethernet/RNDIS Gadget #2
  - Ports (COM & LPT)
    - Communications Port (COM1)
    - Intel(R) Active Management Technology - SOL (COM3)
  - Print queues
  - Processors

Launch the Network and Sharing Center

Step 1. Edit the IP address of the RNDIS Gadget. To find out the IP address, unplug the USB cable and then plug it back in.

Step 2. Change the IP address to the same subnet as the controller and Netmask of 255.255.255.0

Step 3. Ping the PW-7000 controllers IP address.

Step 4. Launch a browser and type the controllers IP address. The controller's configuration login web page is displayed.

Configuring Windows 7

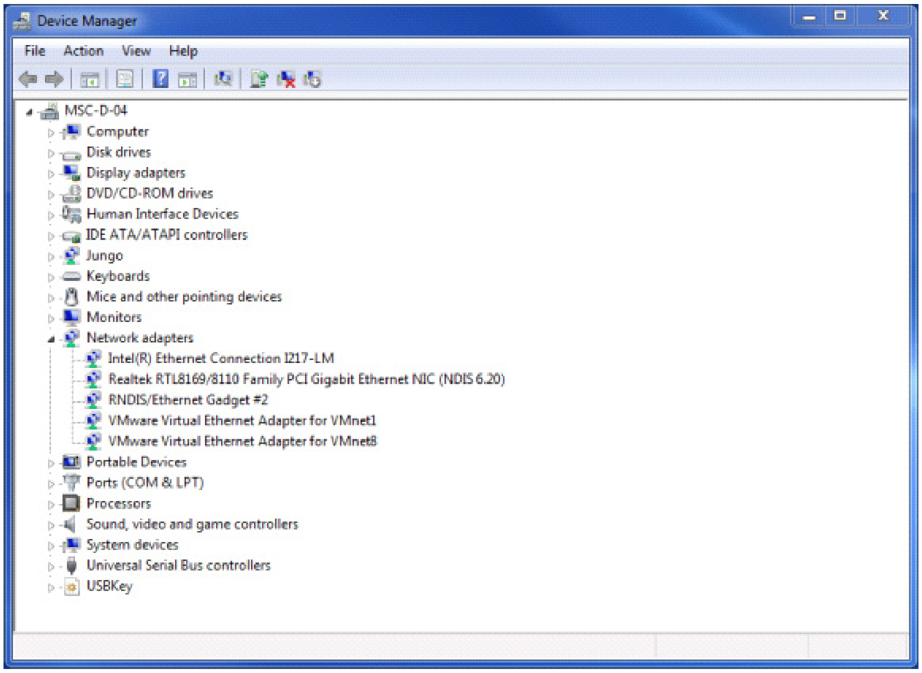
Step 1. Use the Micro Type-B USB end of the cable to connect to the controller

Step 2. Use the USB Type-A side to connect to the Windows PC.

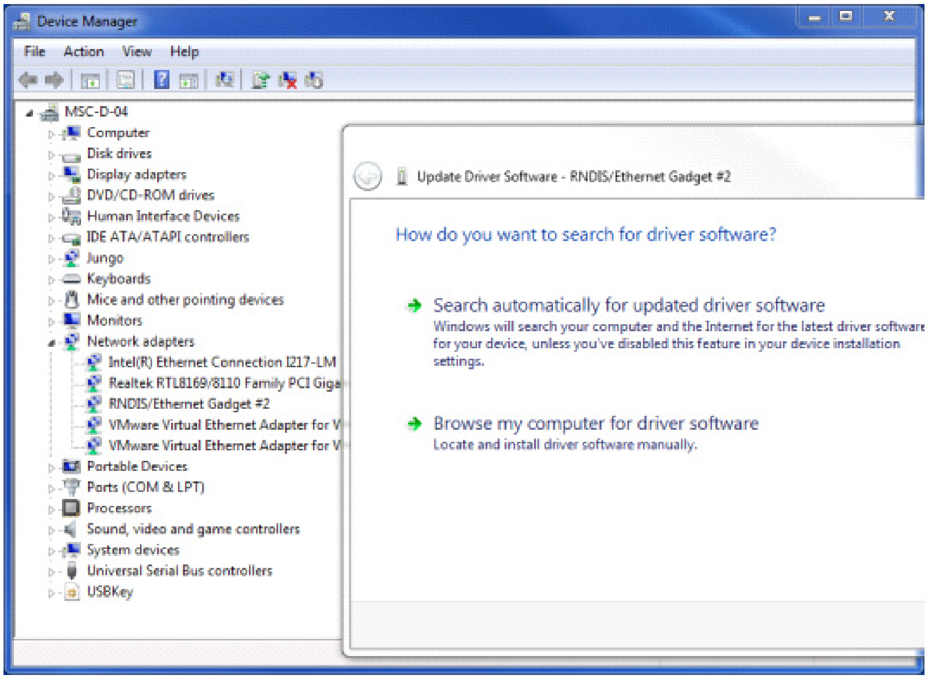
Step 3. Install the correct USB driver on the Windows host to set up a point-to-point communication via the USB cable.

Note: *Ensure the controller is up and running with the USB cable connected to your Windows host.*

Step 4. Open the Device Manager screen as shown below and locate the RNDIS network. If the RNDIS device appears under the "Network Adapters" section, then skip the “Setting the IP Address” section.


Device Manager
File
Action
View
Help
MSC-D-04
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Human Interface Devices
IDE ATA/ATAPI controllers
Jungo
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Intel(R) Ethernet Connection I217-LM
Realtek RTL8169/8110 Family PCI Gigabit Ethernet NIC (NDIS 6.20)
RNDIS/Ethernet Gadget #2
VMware Virtual Ethernet Adapter for VMnet1
VMware Virtual Ethernet Adapter for VMnet8
Portable Devices
Ports (COM & LPT)
Processors
Sound, video and game controllers
System devices
Universal Serial Bus controllers
USBKey

Step 5. Right-click the "RNDIS/Ethernet Gadget" node and the select "Update Driver Software". The Search for Driver software screen with two options is displayed.


Device Manager
File
Action
View
Help
MSC-D-04
Computer
Disk drives
Display adapters
DVD/CD-ROM drives
Human Interface Devices
IDE ATA/ATAPI controllers
Jungo
Keyboards
Mice and other pointing devices
Monitors
Network adapters
Intel(R) Ethernet Connection I217-LM
Realtek RTL8169/8110 Family PCI Giga
RNDIS/Ethernet Gadget #2
VMware Virtual Ethernet Adapter for V
VMware Virtual Ethernet Adapter for V
Portable Devices
Ports (COM & LPT)
Processors
Sound, video and game controllers
System devices
Universal Serial Bus controllers
USBKey
Update Driver Software - RNDIS/Ethernet Gadget #2

How do you want to search for driver software?

Search automatically for updated driver software

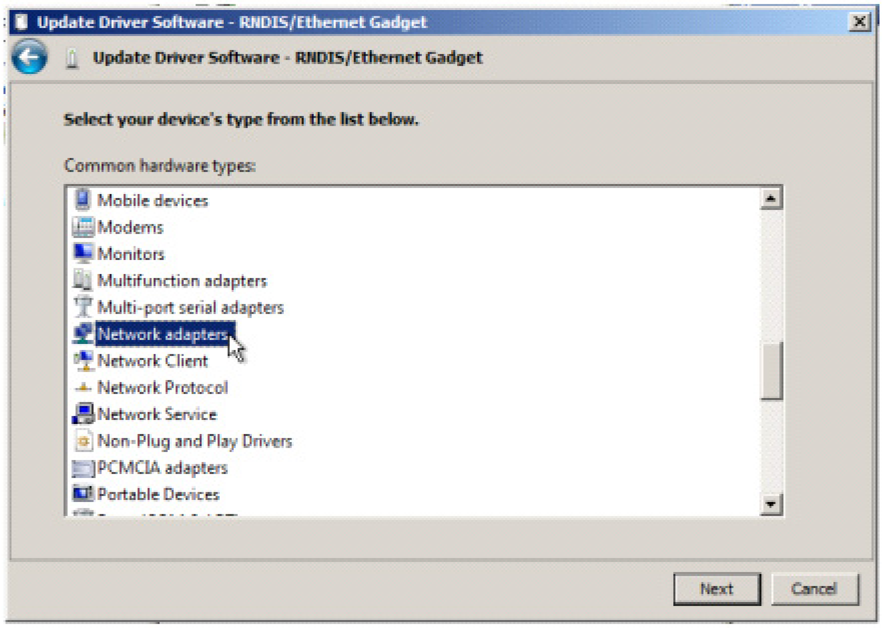
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.

Browse my computer for driver software

Locate and install driver software manually.

Step 6. Click "Browse my computer for driver software" and then click "Let me pick from a list of device drivers on my computer" option.

Step 7. Under Device type select "Network adapters" as shown below and then click "Next".



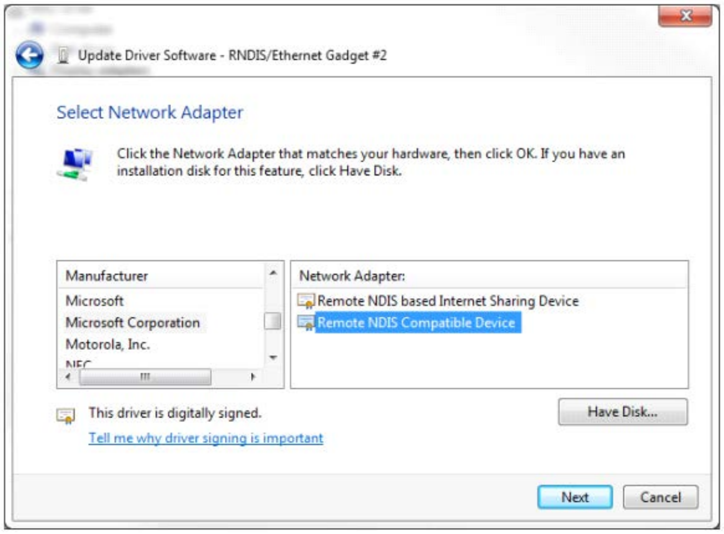
Update Driver Software - RNDIS/Ethernet Gadget

Select your device's type from the list below.

Common hardware types:

Step 8. In Network Adapter dialog box, select "Microsoft Corporation" under Manufacturer's list.

Step 9. Select "Remote NDIS Compatible Device" under Network Adapter list as shown below.



Update Driver Software - RNDIS/Ethernet Gadget #2

Select Network Adapter

Click the Network Adapter that matches your hardware, then click OK. If you have an installation disk for this feature, click Have Disk.

Manufacturer
Microsoft
Microsoft Corporation
Motorola, Inc.
NEC

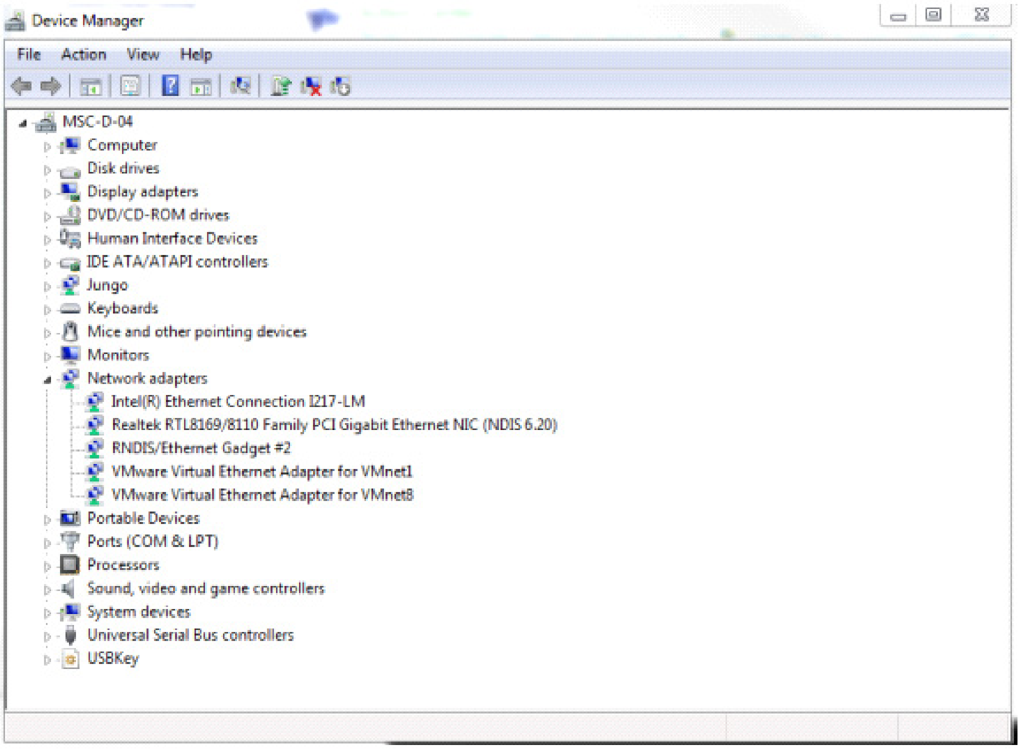
Network Adapter:
Remote NDIS based Internet Sharing Device
Remote NDIS Compatible Device

This driver is digitally signed.

Tell me why driver signing is important

Step 10. Click "Next" a warning message is displayed.

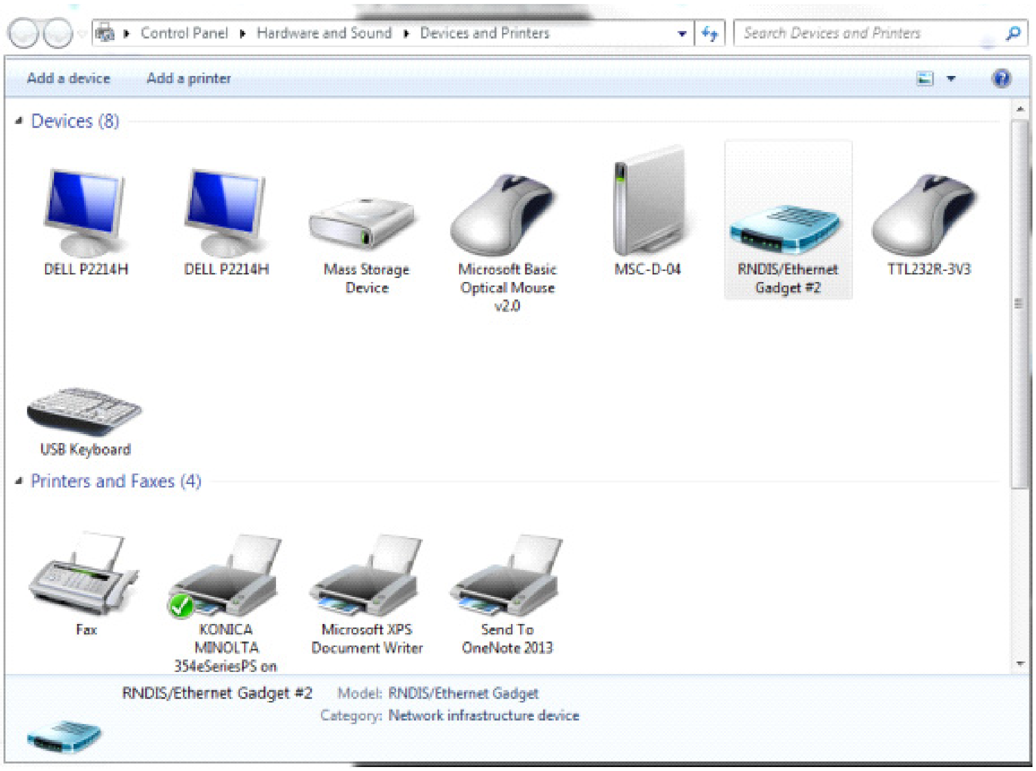
Step 11. Click on the "Update Driver Warning Dialog". The device is pushed and displayed under the "Network adapters" list as shown below:



- MSC-D-04
  - Computer
  - Disk drives
  - Display adapters
  - DVD/CD-ROM drives
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Jungo
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
    - Intel(R) Ethernet Connection I217-LM
    - Realtek RTL8169/8110 Family PCI Gigabit Ethernet NIC (NDIS 6.20)
    - RNDIS/Ethernet Gadget #2
    - VMware Virtual Ethernet Adapter for VMnet1
    - VMware Virtual Ethernet Adapter for VMnet8
  - Portable Devices
  - Ports (COM & LPT)
  - Processors
  - Sound, video and game controllers
  - System devices
  - Universal Serial Bus controllers
  - USBKey

Setting the IP Address

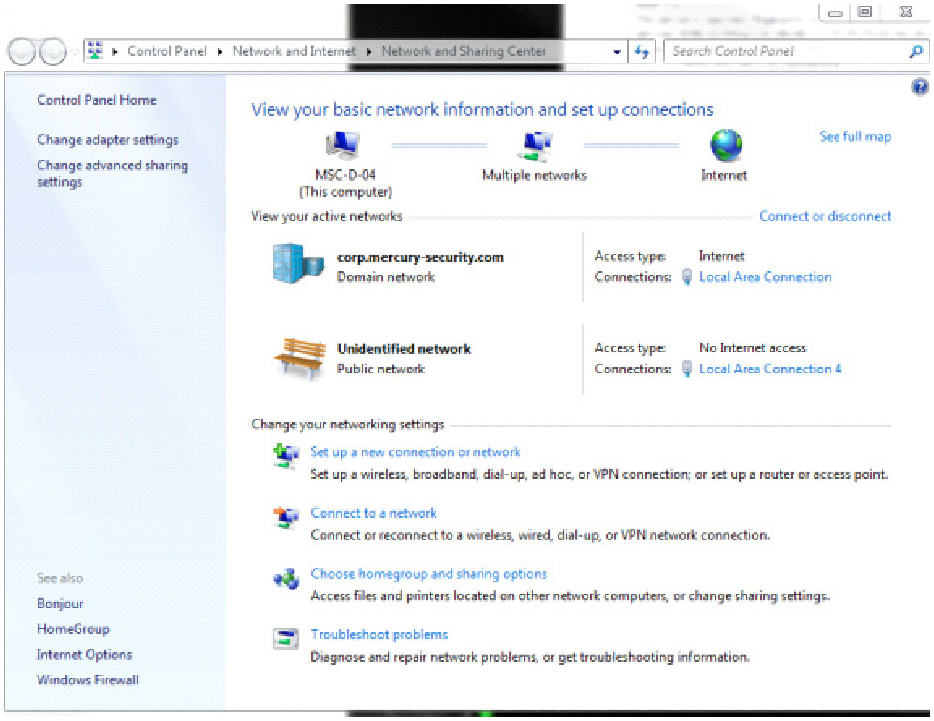
Step 1. Open the "Devices and Printers" screen from the "Start" menu as shown below.


Control Panel ▸ Hardware and Sound ▸ Devices and Printers
Search Devices and Printers
Add a device
Add a printer
Devices (8)
DELL P2214H
DELL P2214H
Mass Storage Device
Microsoft Basic Optical Mouse v2.0
MSC-D-04
RNDIS/Ethernet Gadget #2
TTL232R-3V3
USB Keyboard
Printers and Faxes (4)
Fax
KONICA MINOLTA 354eSeriesPS on
Microsoft XPS Document Writer
Send To OneNote 2013

RNDIS/Ethernet Gadget #2 Model: RNDIS/Ethernet Gadget
Category: Network infrastructure device

Step 2. Right click on the new "RNDIS/Ethernet Gadget” and then select the "Network Settings" option.

Step 3. Choose one of the Active Networks in the "Network and Sharing Center" screen. Check the “No Internet access” option on the list as shown below.



Control Panel ▸ Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

See full map

MSC-D-04
(This computer)

Multiple networks

Internet

View your active networks

Connect or disconnect

corp.mercury-security.com
Domain network

Access type: Internet
Connections: Local Area Connection

Unidentified network
Public network

Access type: No Internet access
Connections: Local Area Connection 4

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

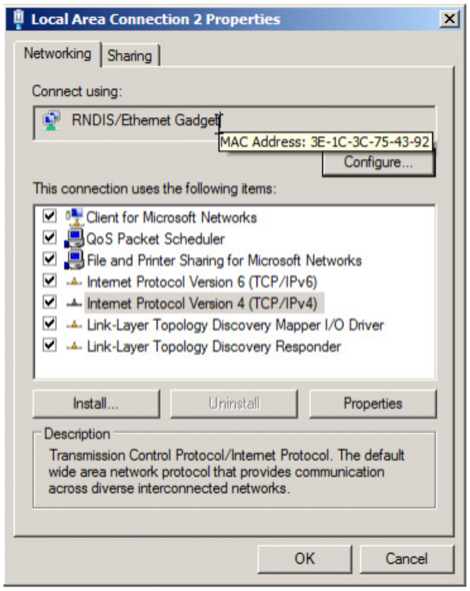
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

See also
Bonjour
HomeGroup
Internet Options
Windows Firewall

Step 4. Click “On this machine, it's "Local Area Connection 4" connection option and then click on "Properties". The properties dialog box is displayed as shown below.



Local Area Connection 2 Properties

Connect using:

RNDIS/Ethernet Gadget

MAC Address: 3E-1C-3C-75-43-92

This connection uses the following items:

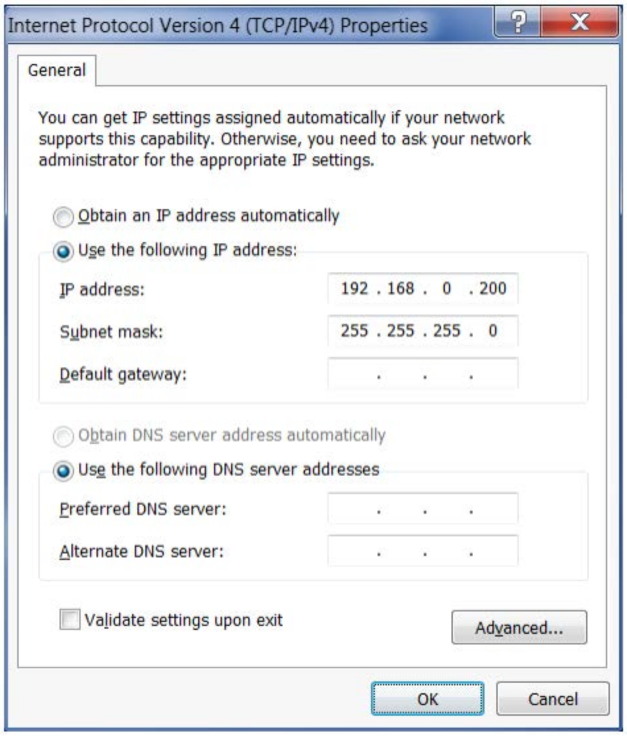
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 5. Double click the "Internet Protocol Version 4" option. The Properties dialog is displayed as shown below.

Step 6. Set the host address of the connection.
In the below example, the controller is set to the default of 192.168.0.251

with 255.255.255.0 netmask, so you should set up an IP address in the same subnet, such as 192.168.0.200.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses

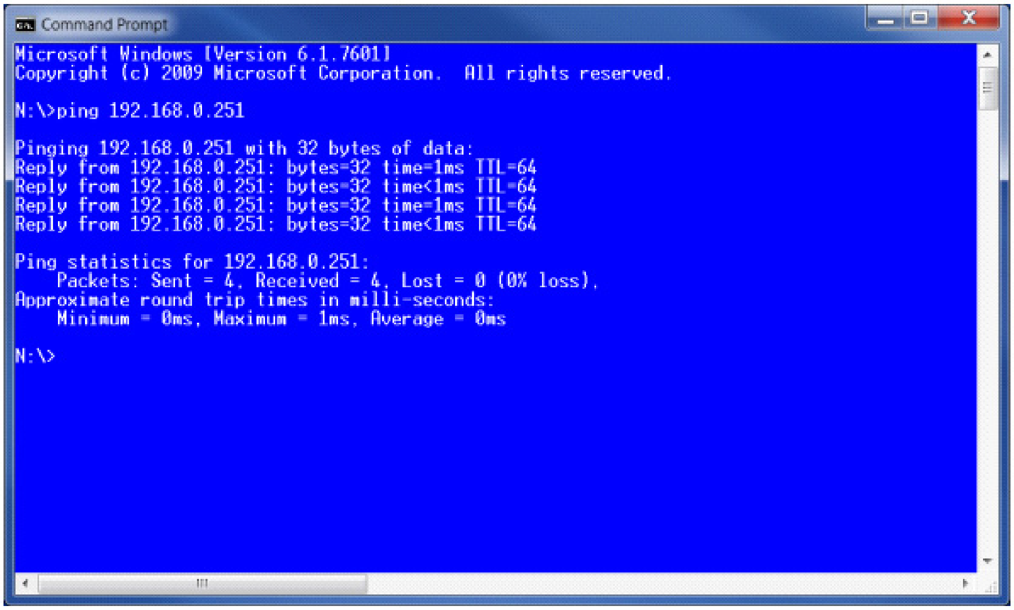
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

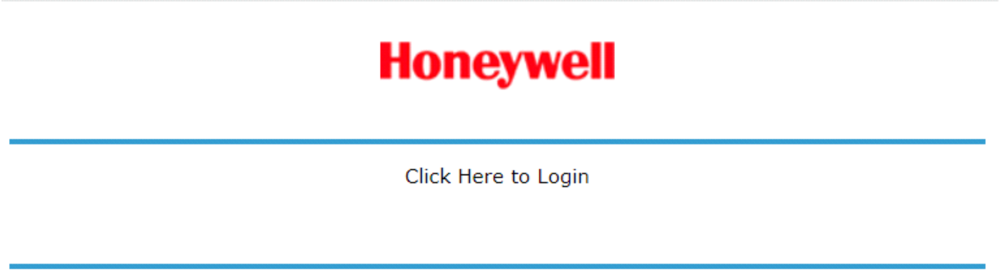
Step 7. Click "OK" after setting the address and subnet mask. The RNDIS network adapter is now set.

Step 8. Test the target address to check the connection. Ping the IP in command box as shown below.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

N:\>ping 192.168.0.251

Pinging 192.168.0.251 with 32 bytes of data:
Reply from 192.168.0.251: bytes=32 time=1ms TTL=64
Reply from 192.168.0.251: bytes=32 time<1ms TTL=64
Reply from 192.168.0.251: bytes=32 time=1ms TTL=64
Reply from 192.168.0.251: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

N:\>
```

Step 9. Launch the browser and type the controllers IP address. The controller's configuration login web page is displayed.



Honeywell

Appendix

SYSTEM REQUIREMENTS FOR IEC 60839 COMPLIANCE

To have Pro-Watch system full compliant to grade 4 of IEC 60839 regulation it is required to guarantee that the third-party devices used in the system follow specific requirements and to apply an appropriate Pro-Watch Integrated Security Suite configuration. In brackets are indicated the related regulation requirements in the IEC 60839 document.

Requirements on power supply

- The Pro-Watch controller and sub-panels must be supplied by a stand-by power source (with battery) capable to operate the device itself and the related components in full load condition for at least 4 hours. The loading conditions do not include the monitoring console or access point actuators. [Power supply requirements - 1].
- Loss of power source or restoration shall not adversely affect the normal operation of the system. [Power supply requirements - 3].
- The power source shall provide digital outputs for the monitoring of “AC presence”, “Low voltage level” and “No Battery present”. [Power supply requirements - 4].
- Such digital outputs need to be connected to the system to provide the related indications. [Indication and announcement requirements – B22].

Requirements on readers

- Readers and all other system components may be located outside the controller area shall meet, at least, IP4x and IK04. [System self-protection requirements – A7].
- Readers used must be equipped with tamper detection switch. [System self-protection requirements – A5].
- Readers must communicate using OSDP protocol with Secure channel activated (encryption and authentication are mandatory). [System self-protection requirements – 24].
- When Biometric readers are used, the Effective False Acceptance Rate (FAReff) of the reader shall not exceed 0.1%. [Recognition requirements – B20] Note: FAReff = FAR (false acceptance rate) when 1:1 comparison is performed (e.g.

biometric verification of an identity claimed by memorized information or token) FAReff = FAR × n when 1:n comparison is performed and n = number of stored templates (e.g. biometric identification without using memorized information or token).

Requirements on cards/tokens

- It is not allowed to use cards (or tokens) with the coding system structure visible. (Recognition requirements – B26).
- It is not allowed to use cards (or tokens) with identity number readable on the surface. If an identity number is printed on the card, it shall not represent the complete coding structure.(Recognition requirements – B27).

Requirements on Pro-Watch

- Operator password shall be composed, at minimum by, 8 alphanumeric characters. (System self-protection requirements – A12).

General system requirements

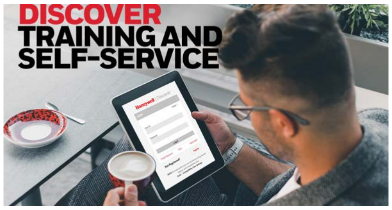
- It is not allowed to use PIN only access procedure (indication and annuciation requirements -B11, Recognition requirements – B14, B19)
- It is not allowed to use partial token information (ex. Facility code only) in case of degraded mode of operation for recognition (Recognition requirements – B25)

This page is intentionally left blank.

Honeywell Integrated Security, 135 W. Forest Hill Avenue
Oak Creek, WI 53154, United States
800-323-4576, 414-766-1798 Fax

www.security.honeywell.com

Technical Support Self-Service | Customer Portal
https://myhoneywellbuildingsuniversity.com/training/support/



YouTube | Honeywell Help and Support
https://www.youtube.com/channel/UCBEL6ouNV_LN5lEpYRujMTg/featured

THE
FUTURE
IS
WHAT
WE
MAKE IT