Honeywell | THE FUTURE IS WHAT WE MAKE IT

Pro-Watch 7000

Security Manual

Rev 1.0

Security Manual

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.honeywellintegrated.com to post your comments.

TABLE OF CONTENTS

NOTICE

This document contains Honeywell proprietary information.Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International.While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.Honeywell cannot be held responsible for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

This page is intentionally left blank

CHAPTER

1 INTRODUCTION

Overview

This Security manual provides information to maximize security with PW7K Access Control Panels. This guide will identify critical information on features, suggest options that should be enabled, and include best practices for using the panels.

Intended Audience

This guide provides additional information to the end user for a secure deployment and operation of the PW7K access panel.

Related Documents

- PW7K Quick Start Guide
- PW7K Installation Guide
- PW7K User Guide

This page is intentionally left blank

CHAPTER

2 INSTALLATION

Unpacking

Before installing PW7K panel on site make sure the package is received in good condition and seal is not tampered. If you find the package is tampered or not in good condition, then contact customer service and return the device through the RMA process. "Once seal is removed from the package, please make sure the panel is stored in secure place till it is installed in the enclosure with tamper protection".

Installation

Recommendations include:

- Securing Network Wiring
- Securing The Enclosure
- Ensuring The Latest Firmware
- Normal Operations

Securing Network Wiring

Security Ethernet Network

PW7K uses Ethernet for below type of communications.

- Web browser for the standalone user interface
- Panel networking
- Host/Pro-Watch access

It is recommended to use isolated/standalone network for installing PW7K panels. Cabling must be concealed in secured area and must not be freely accessible.

Caution: The PW7K panel is not recommended to connect to any untrusted network, Internet. The PW7K panel in is designed to work in trusted or protected network where known users can interact with the panel. If the panel is connected to the INTERNET, remote attacker may try to exploit or damage the panel.

Note: *The user will own the risk, if the user connects the panel to the Internet or any untrusted network*

Securing Fieldbus Wiring

The PW7K support below types of field bus protocols over three wire and RS-485 physical cables.

Protocol	Medium	Purpose	Preferred Cable
Wiegand	Three wire bus	Reader communication	CAT 6E/FSTP
OSDP	RS-485	Reader communication	CAT 6E/FSTP
SIO	RS-485	SIO Module communication	CAT6E/FSTP

Cables used for Wiegand and SIO communications must be concealed in the secured area and must not be freely accessible.

Securing The Enclosure

Install the hardware in the secure enclosure with tamper protection to generate notifications when the enclosure is opened/tampered. It is recommended to mount SIO in the same enclosure as controller board.

Ensuring The Latest Firmware

Always make sure to check for the new releases of the PW7K & SIO Interface board firmware and update panel to use latest version of the firmware. This ensures the latest changes and security improvements are installed.

Normal Operations

Set all DIP switches to OFF for normal Operation.

Settings	Secure configuration
Web Interface	Disable web interface once basic configuration is done.
Default account	Remove default user login, create a unique user account with a strong password.
USB interface	Disable USB interface.
SD Card Interface	Disable SD card interface.
SNMP communication	Disable SNMP communication.
Discovery service	Disable discovery service.
Partition encryption	Enable data encryption at rest: This is necessary to protect cryptographic keys and personal data.
Host communication	Enable only TLS encryption for host communication

Configuration

Please refer to the PW7K User Guide for detailed configuration steps.

Web Interface

The PW7K panel supports web interface for the basic installation parameter setup. It is recommended to:

- Disable web interface before leaving panel in normal operation. Refer to the PW7K User Guide for more details.
- Enable web interface and physically using dip switches only when installer is physically close to the panel.

Session Timer

The Session timer logs OFF a user when session is inactive for configured time interval.

PW7K panel is configured with fifteen (15) minutes as default session time out which is recommended value to minimize the risk of when an attacker can access active sessions. Refer to the PW7K User Guide for the detailed step by step approach for configuring “Web Session Timeout”.

Account and permission Management

The PW7K has accounts, represented by users in the PW7K configuration. It is important that these accounts are properly managed. Failure to do so can make it easier for an attacker to penetrate the system, or make it more difficult to detect that an attack has occurred.

Default User Account

The Out-of-the-box PW7K panel is preloaded with default user credentials as shown below:

- Username: admin
- Password: password

The default user credentials are the same for all Mercury Security Controllers. To prevent unauthorized use, on initial signing in with the above default login credentials, it is recommended to remove default user login, create a unique user account with a strong password. Refer to the PW7K User manual for details steps by step instructions to manage users.

Note: *Refer to the PW7K User manual for detailed steps for disabling Default User Account.*

Unique User Account

Each user account in the PW7K system should represent a single user. Different people should never share the same account. For example, rather than a general "Supervisor" user account that many Supervisors could use, each supervisor should have his own, separate account.

There are many reasons for each user to have his own individual account:

- If each user has his own account, audit logs will be more informative. It will be easy to determine exactly which user did what. This can help detect if an account has been compromised.
- If an account is removed, it does not inconvenience many users. For example, if a user should no longer have access to the PW7K System, deleting or disabling his individual account is simpler. If it is a shared account, it makes the administrator difficult to manage the account used by multiple users. The only option would be to change the password and notify all users. Leaving the account as-is not an option – the goal is to revoke the user's access.
- If each user has his own account, it is much easier to tailor permissions to precisely meet their needs. A shared account could result in users having more permissions than they should.
- A shared account means a shared password. It is an extremely bad security practice to share passwords. It makes it much more likely for the password to be leaked, and makes it more difficult to implement certain password best practices.

Each different user should have a unique individual account. Similarly, users should never use accounts intended and used for running administrative services.

Use a unique account for each project

It is a common (bad) practice that some system integrators often use the exact same system/service credentials on every project they install. If one system is compromised, the attacker could potentially have credentials for the access to many other projects installed by the same contractor.

Minimum Required Permissions

When creating a new user, think about what the user needs to do in PW7K, and then assign the minimum permissions level required to do that job. For example, a user who only needs to view current network setting does not need access to change the network setting. Giving non-required permissions increases the possibility of a security breach. The user might inadvertently (or purposefully) change settings that they should not change. Worse, if the account is hacked, more permissions give the attacker more power.

Password policies

The most popular technique for breaking into a system is to guess user names and passwords. Consequently, it is essential that passwords are difficult to guess and that they are changed often.

- The most popular technique for breaking into a system is to guess user names and passwords. Consequently, it is essential that passwords are difficult to guess and that they are changed often.
- All the passwords must be strong.
- Ensure password of minimum 8 alphanumeric characters.
- Password must not contain username. In addition passwords must contain three of the four categories characters shown below
    - Uppercase alphabet characters (A-Z)
    - Lowercase alphabet characters (a-z)
    - Arabic numerals (0-9)
    - Non-alphanumeric characters (!, $, #, or %)

Authorized IP Addresses

Restrict accessing the controller's host communication port. When there are only one or two IP addresses accessing the controller's host communication port, you can restrict where this connection originates. This filter applies to the communication port established by a host application configured in IP Server (host initiated connection) mode. In an IP Client (controller initiated connection) mode, the authorized IP addresses are programmed into the controller by the host application.

Refer to the PW7K user guide for detailed steps to configure "Authorized IP Address".

Information Services

Prevent discovery services through implementing the following guidelines.

Disable Discovery

By default the controllers supports device discovery utilizing Zeroconf through services on Windows® and Linux like Apple® Bonjour® and mDNSResponder. Once the controller is installed and configured it is recommended to turn-off discovery. This prevents someone with access to the same network from discovering the controllers.

Refer to the PW7K User manual for detailed steps for disabling Zeroconf Discovery.

Disable SNMP

By default, SNMP is disabled. If SNMP is not used, leave this setting disabled.

Refer to the PW7K User manual for detailed steps for disabling SNMP.

Disable USB

USB interface is used to add additional Ethernet interface using "USB to Ethernet adapter". It is Always recommended to disable USB interface unless used for the additional Ethernet interface.

Refer to the PW7K User manual for details steps for disabling USB interface.

Disable SD Card

SD card interface is used for uploading debug and crash dumps and piv CLASS embedded authentication database upcoming features, so it is always recommended to disable SD card interface. Refer to the PW7K User manual for details steps for disabling SD card.

Operations

System Audit

To discover any unintended activities, it is recommended to perform periodic audit to make sure PW7K panel is being used as configured and intended.

PW7K panel captures all user and major system events for the auditing purpose when panel is connected to Host audit logs are periodically synced with Host software's for the persistence and auditing purpose.

Encryption and Authentication

Utilize the following settings to improve encryption and authentication methods.

Host Controller Encryption

The controller supports AES and TLS encryption for host communications. Use TLS method to encrypt the data being transferred to and from the controller. TLS is recommended for data security over AES. There are two types of modes.

Legacy Mode

TLS

TLS is more secure host communication than AES Encrypted communication, to use TLS panel is required to be configured with certificate for panel and peer host certificate.

Refer to the PW7k User guide for the detailed steps for configuring and enabling TLS Host communication.

AES

Do not use AES method to transfer data between Host and Controller. Disable AES encryption by configuring both the host and controller.

Standard Mode

TLS

TLS is more secure host communication than AES Encrypted communication, to use TLS panel is required to be configured with certificate for panel and peer host certificate.

Refer to the PW7k User guide for the detailed steps for configuring and enabling TLS Host communication.

AES

Enable AES encryption by configuring both the host and controller. Load the encryption keys (128 or 256-bit) on both sides before enabling AES.

Encryption mechanism

The below critically sensitive data and its encryption mechanism used in the PW7K system.

Encryption in Communication

Category	Encryption Type	SSL/TLS Version	Notes
PW7K to OSDP	AES128		OSDP reader communication
PW7K to Host Software	TLS	TLS 1.2	Proprietary protocol
PW7K to Web Client	TLS	TLS 1.2	HTTPs protocol
PW7K TO SIO	AES256		Proprietary protocol

Reader Communications

OSDP (Open Supervised Device protocol) secure channel (V2) is a bi-directional secure protocol using symmetric keys shared between the reader and controller, it is recommended to use OSDP in Secure mode always.

OSDP is recommended for reader communications as it provides secure method of communication.

Wiegand Readers

Wiegand protocol based readers are vulnerable to attack. Hence OSDP is recommended for reader communications as it provides a secure method of communication.

Controllers to SIO Communication

The PW7K panel supports two types of downstream communication.

- RS485 SIO: communication on this network is encrypted using AES 128/256 pre shared keys, cables used for these communications must be concealed in the secured area and must not be freely accessible.
- IP based Downstream Modules: IP-enabled input/output modules support AES encryption (128-bit) by default. It also has provision to use TSL between the controller and downstream module. Refer to the PW7K User manual.

Data at Rest Encryption

The PW7K panel comes with the option of “Enable Encryption Partition” to protect cryptographic keys and satisfy privacy concerns for end users in the field. The encryption will allow the configuration and data files to be stored in encrypted format. It is recommended to always select “Enable Encryption Partition” option before leaving panel in normal operation.

Network Ports

Physical Ports, Protocols, and Services

The following inbound ports are used to accept the connections:

PW7K Panel Inbound Ports.

Port	Protocol	Standard/Custom	Disable
67	UDP	DHCPS	Used for DHCP
68	UDP	DHCPC	Used for DHCP
80	TCP	HTTP	Yes – Use Disable Web Server from the Users web confirmation page
443	TCP	HTTPs	Yes - Use Disable Web Server from the Users web configuration page.
161	UDP	SNMP	Yes – Use Disable SNMP from the Users web configuration page.
3001	TCP	Mercury Host Protocol(MSP2)	Yes – Set the Connection Type from the Host Comm page to an option other than IP. Note: For the best security it is recommended to change default host communication port.
5353	UDP	Zeroconf (Discovery service)	Yes – Use the Disable Bonjour option from the Users web configuration page.

Equipment Replacement/Decommissioning

When replacement/decommissioning a board, make sure to use factory default option to clear all data in the controller before discard panel. Please refer to the PW7K Installation Guide for detailed step by step instructions to put the panel in the factory default condition.

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

Honeywell

THE FUTURE IS WHAT WE MAKE IT

Rev 1.0 - 08/2020