Honeywell

**Honeywell Commercial Security**
715 Peachtree St.NE
Atlanta, GA 30308
https://buildings.honeywell.com/security

September 29, 2023

To whom it may concern,

The following information is provided in response to requests on CIP information on PW Series Controllers.

**CIP-007 R1**
PW-Series Controllers protect against the use of unnecessary physical input/output ports used for network connectivity, console commands or removable media. Port usage is as follows:

| Port # | Port Type | Usage | Applicable Controller(s) | Can Be Disabled? |
|---|---|---|---|---|
| 67 | UDP | DHCPS | PW6K , PW7K | No |
| 68 | UDP | DHCPC | PW6K , PW7K | No |
| 80 | TCP | HTTP | PW6K , PW7K | Yes - Use the "Disable Web Server" option on the Users web configuration page |
| 123 | UDP | NTP | PW6K , PW7K | Yes – Uses by default but can be set to different port via web configuration page. |
| 161 | UDP | SNMP | PW6K , PW7K | Yes - Use the "Disable SNMP" option on the Users web configuration page |
| 443 | TCP | HTTPS | PW6K , PW7K | Yes - Use the "Disable Web Server" option on the Users web configuration page. |
| 3001 | TCP | Mercury Host Protocol (MSP2) | PW6K , PW7K | 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) | PW6K , PW7K | Yes – Use the “Disable Zeroconf Device Discovery” option on the Users web configuration page |
| 47808 | TCP | BACnet | PW7K | Yes. BACnet is disabled by default. - Not currently supported. |
| 47307 | UDP | OTIS | PW7K | Yes (only when OTIS integration is enabled). Not currently supported |
| 45303 | UDP | OTIS | PW7K | Yes (only when OTIS integration is enabled). Not currently supported |
| 46303 | UDP | OTIS | PW7K | Yes (only when OTIS integration is enabled). Not currently supported |
| 46308 | UDP | OTIS | PW7K | Yes (only when OTIS integration is enabled). Not currently supported |
| 45308 | UDP | OTIS | PW7K | Yes (only when OTIS integration is enabled). Not currently supported |
| 10200 | TCP | pivCLASS® Embedded | PW7K | Yes (configure through the pivCLASS embedded web page).- Not currently supported |

**CIP-007 R2.1**
There have been security patches/fixes related to PW7K series Controller firmware issued as a new firmware version. All updates to date provided to the Controller firmware have served to provide additional functionality or modifications to existing functionality. Any newly recommended firmware for PW7K series Controller would be referenced in the monthly Patch Release Letter. Release notes are available upon request on new firmware releases.

There have been no security patches related to PW6K series Controller firmware issued in the past and there will not be any.

**CIP-007 R2.2**
A monthly Patch Release Letter is provided upon request via email.

**CIP-007 R3.1**
The PW Series controllers are implemented as a single body executable file developed for a dedicated embedded application. They are not capable of accepting any external programs for execution (useful or otherwise). Therefore, the PW series controllers do not require virus protection software running on the controller. Any updates in Malicious Code prevention will be included in the monthly Patch Release Letter.

**CIP-007 R4.1**
The PW7K Controllers are capable of logging events related to cyber security incidents that at a minimum include detected successful login attempts and failed login attempts in Pro-Watch version 5.5 and above.

The PW7K Series Controllers are not capable of generating alerts for security events that include detected malicious code anddetected failure of event logging

The PW6K Series Controllers are not capable of logging events related to cyber security incidents that include at a minimum detected successful login attempts, detected failed access attempts and failed login attempts, detected malicious code

**CIP-007 R4.2**
The PW Series Controllers are not capable of generating alerts for security events that include detected malicious code and detected failure of event logging
.

**CIP-007 R4.3**
The PW Series Controllers are not capable of retaining applicable event logs.

**CIP-007 R5.1, R5.2, R5.5**

The PW7K1IC , PW7K1ICE , PW6K1IC and PW6K1ICE have the following default accounts:

*Username:* admin
*Password:* password

The admin user account on PW-Series Controllers is only enabled if DIP switch 1 is set to on. To disable default account access, follow this recommended process –

1. Log on to the Controller from the web interface with the default admin account.
2. Create a new admin user with a complex password.
3. Turn off DIP switch 1.

The Controller should be in a secure location to prevent unauthorized access to the DIP settings.

Web access to the Controller can be disabled by turning the feature off on the Users screen of the web interface and setting DIP switch 1 to off.

Note - If no users have been created then the default account will work regardless SW1. Once at least one user account has been created then the default account will only work with SW1 on. The option for disabling the web server is only enabled when you are logged on and SW1 is on. You will need to have SW1 ON, log on, set this option, log out, and then turn SW1 OFF.

The Controllers have three password Strength levels

Low Password Strength – minimum of 6 characters
Medium Password Strength – minimum of 6 characters and passes two of the password strength tests below.
High Password Strength – minimum of 8 characters, passes three of the password strength tests below, and password not based on user name.

Password Strength Tests – contains characters from any of the following categories:

Uppercase alphabet characters (A–Z)
Lowercase alphabet characters (a–z)
Arabic numerals (0–9)
Symbol characters (`! $ ? ^ * ( ) _ - + = { [ } ] : ; @ ' ~ # | < , > . /)"

The Maximum Password length is 10 characters.

The Controllers are not capable of technically enforcing password length, complexity requirements, or required annual password changes.

**CIP-007 R5.7**
The PW7K controller can issue an alert based on unsuccessful login attempts
The PW7K Controller will lock out a web login after three (3) invalid login attempts for one (1) minute.
The PW6K controller cannot issue an alert based on unsuccessful login attempts.
The PW6K Controller will lock out a web login after six (6) invalid login attempts for five (5) minutes

**CIP-009 R1.5**
The PW Series Controllers are not capable of monitoring system events related to cyber security. In the event of a Cyber Security Incident, standard Server backup and recovery procedures would apply to the PACS system to be followed if necessary, by a reset and download of the PW Series Controllers.

Respectfully,

Rajeev Dubey

Sr. Offering Manager

Rajeev.Dubey@honeywell.com