BEST

dormakaba Group

Wi-Q

wireless technology

WI-Q™ MERCURY

SETUP AND USER GUIDE

**Wireless Intelligence
That Stands Alone**

BEST

WIRELESS INTELLIGENCE THAT STANDS ALONE

CREDITS | COPYRIGHT

CREDITS | COPYRIGHT

Written and designed at dormakaba USA Inc.
6161 E. 75th St.
Indianapolis, IN 46250

T91416_K December 2023

FCC | IC CERTIFICATION

FCC/IC CERTIFICATION

CAUTION: **Please keep the PG antenna 20cm away from people to ensure that FCC RF exposure compliance requirements are not exceeded.**

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.

Operation is subject to the following two conditions:
1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for Class B Digital Device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, you can try to correct the interference by taking one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

THIS DEVICE COMPLIES WITH INDUSTRY CANADA LICENSE-EXEMPT RSS STANDARD(S).

Operation is subject to the following two conditions:
1. This device may not cause interference, and
2. This device must accept any interference, including any interference that may cause undesired operation of the device.

This Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

CET APPAREIL EST CONFORME À LA NORME RSS INDUSTRIE CANADA EXEMPT DE LICENSE.

Son fonctionnement est soumis aux deux conditions suivantes:
1. Cet appareil ne doit pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interferences pouvant causer un mauvais fonctionnement du dispositif.

Cet appareil numérique de la classe [B] respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

FCC | IC CERTIFICATION AND UL EVALUATION

APPROVED ANTENNAS

Approved antennas are listed below, and antennas not included in this list are strictly prohibited for use with these devices.

Configuration Description	Antenna Part Number
Gateway with rubber duck antennas	Pulse W1030W
Gateway with ceiling mount omni-directional antenna	PCTEL (Maxrad) MC2400PTMSMA
Gateway with interior/exterior wall mount directional antenna	Mobile Mark (Comtelco) CMTB36247V
Gateway with exterior omni-directional mast mount antenna	Mobile Mark (Comtelco) CMTBS2400XL3

WARNING: Changes or modifications not expressly approved by dormakaba could void the user's authority to operate the equipment.

UL EVALUATION

- Not evaluated by UL for use with Mercury Controller Board or Wireless Door Controller.
- Evaluated by UL for supplemental use (i.e. not in the path of the access control decision making) between the Listed Access Control Equipment and a supplemental monitoring station for monitoring and configuration.
- Evaluated by UL with the "Wi-Q" Integrated Wireless Access Controller.
- To be mounted in the protected area
- DC power to be provided by GlobTek GT-41080-1817.9-5.9 plug in power supply only.
- 0-49°C, 85% humidity

Electrical Ratings		
Source	Voltage	Current
DC	12VDC	1A
PoE	44-52VDC (mode B)	84mA

- Wiring methods used shall be in accordance with the National Electrical Code, ANSF/NFPA70.
- UL evaluated with standard antennas.
- For UL installations using PoE, the following must be observed:
  - Compliance with IEEE 802.3 (at or af) specifications was not verified as part of UL 294.
  - Locations and wiring methods which shall be in accordance with the National Electrical Code, ANSI/NFPA 70.

FCC | IC CERTIFICATION AND UL EVALUATION

UL EVALUATION (CONTINUED)

- This product is not intended for outside wiring as covered by Article 800 in the National Electrical Code, NFPA 70.
- Category 5e cabling is the minimum performance category recommended.
- The minimum conductor gauge permitted to connect between the PSE or power injector and the PD shall be 26 AWG (0.13 mm^2) for patch cords, 24 AWG (0.21 mm^2) for horizontal or riser cable.
- Connected through standard eight-pin RJ-45 connectors.
- Evaluated for Mode B only.
- PoE power is to be supplied by an Access Control System Unit (ALVY), Class 2 power limited, PoE injector (PSE) providing 44-52VDC and 15W for maximum output.

ACS INTEROPERABILITY NOTES

ACS INTEROPERABILITY NOTES

- Card ID offsets require special consideration in the Access Control Software when the WQXM-PG is used with a Mercury Panel.
- If multiple card formats are configured in the system, as long as there are no Card ID collisions between the multiple formats, then the Card ID offset for each format can be set to zero. (This is also called the Card Number offset, Card Format offset or Cardholder ID offset.)
- If a Card ID offset must be configured due to Card ID collisions, then non-overlapping Card ID offsets MUST be configured for each of the card formats, and each offset must be bigger than the max Card ID of all cards.
- If any of the Card ID offsets overlap and are big enough, then it may be impossible for the event (transaction) messages to properly identify the cardholder who performed an action at a door lock.

- Resets issued to the Mercury SCP or SIO (Wi-Q Gateway) from the ACS will also cause the Wi-Q Gateway to reset.
- Once the reset is received, it can take 4-5 minutes for the Wi-Q Gateway to be restored to full communication status.
- The Mercury Panel currently inserts its own timestamp in transactions sent up to the ACS. If there have been accumulated transactions in the Controller or Gateway, when those transactions are later delivered to the Mercury Panel, the panel will re-timestamp the transactions with the current time-of-day replacing the timestamp from when the event actually occurred. This issue will be fixed in a future release of the Mercury Panel firmware. Check the latest release notes from dormakaba and Mercury to see if this functionality has changed.

dormakaba TECHNICAL SUPPORT

Address

dormakaba USA Inc.

6161 E. 75th St.

Indianapolis, IN 46250

Web Page

https://dhwsupport.dormakaba.com/hc/en-us

Phone

1-800-392-5209

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

1   SYSTEM OVERVIEW

This manual is the complete guide to the integration of BEST Wi-Q Wireless Hardware with the Mercury Panel and the Access Control System. It provides detailed steps for installing hardware and configuring the Mercury LP4502 for use with Wi-Q Gateways and Controllers.

SYSTEM OVERVIEW

The information in this guide is presented in a linear manner; however, tasks to install hardware and configure the system for the first time do not necessarily progress in a linear manner. There is a "Set Up Checklist" in chapter 2 with step-by-step instructions to walk through the initial setup and configuration tasks in a logical sequence.

Figure 1 Mercury LP4502 and Wi-Q Components
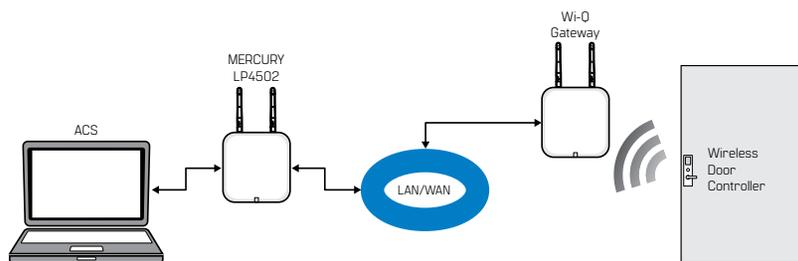
1.1 Mercury LP4502 and Wi-Q Components

1. **ACS**
   Access Control Software

2. **Optional Mercury LP4502 ACS Interface Board**
   The Mercury LP4502 Access Control Panel Interface Board can communicate with up to 32 Wi-Q Gateways with up to 64 Wi-Q Controllers. This interface board is used for third-party integration into Access Control Software.

3. **WQXM-PG Gateway**
   The Gateway is a wireless device connected to the host computer through a secure IP address, similar to the way the computer is connected to the Internet. It transfers data signals from Wireless Controllers to and from the host computer. The Gateway recognizes all Wireless Controllers within its antenna range. One Gateway can control as many as 64 Wireless Controllers in a system.

4. **Wireless Door Controller**
   The Wireless Controller is equipped with Wi-Q Technology that controls user access at the door. The basic configuration is battery operated, with either keypad or card reading capability and an internal antenna that communicates with the Gateway. The Wireless Controller grants user requests according to how they are configured in the Access Control Software.

2   SETUP CHECKLIST

The Mercury Access Panel and Wi-Q Hardware is set up in seven basic tasks. Completing these tasks will assist in getting the system up and running as quickly and efficiently as possible. Some tasks are performed at the host computer and some at the segment site. It is appropriate to perform some tasks concurrently. For example, someone may prepare the computer and install the software concurrently with Site Plan development and hardware installation. However, the software must be installed and Gateways 'online' before the controllers can be signed in.

SETUP CHECKLIST

NOTE: System setup does not proceed in a linear manner. It may be required to skip around in the process.

- ☐ Task 1: Develop a Site Plan
  See page (18).

- ☐ Task 2: Position Gateways
  See page (20).

- ☐ Task 3: Install Gateways
  See page (24).

- ☐ Task 4: Configure Gateways
  See page (25).

- ☐ Task 5: Install Wireless Access Controllers
  See page (45).

- ☐ Task 6: Install Wireless Door Hardware
  See page (47).

- ☐ Task 7: Sign On Wi-Q Controllers
  See page (50).

3   HARDWARE INSTALLATION

The Mercury LP4502 Access Panel locates the Wi-Q Gateways on the local network and integrates wireless hardware into your existing Access Control System.

HARDWARE INSTALLATION

3.1 Hardware Overview

Below is a block diagram showing various configurations. The Mercury LP4502 Interface Panel supports all Wi-Q Technology Wireless Controllers via the WQXM-PG Gateways (A); and

existing Wiegand/Prox, RQE, door strike, and door monitor switch configurations (B). Configuration types are briefly described in the following paragraphs. Full installation instructions are provided in the following sections.

NOTE: Once Wi-Q Controllers are installed, sign them on to the WQXM-PG. Therefore, it is appropriate to install and configure the Mercury Panel before or concurrent with hardware installation. For more information, see "Sign On Wi-Q Controller (Task 7)" on page 50.

3.1.1 LP4502 Controller Board

The Mercury LP4502 Access Control Panel Interface Board can communicate with up to 32 Wi-Q Gateways with up to 64 Wi-Q Controllers. This interface board is used for third-party integration into Access Control Software.

Figure 2 Hardware Overview
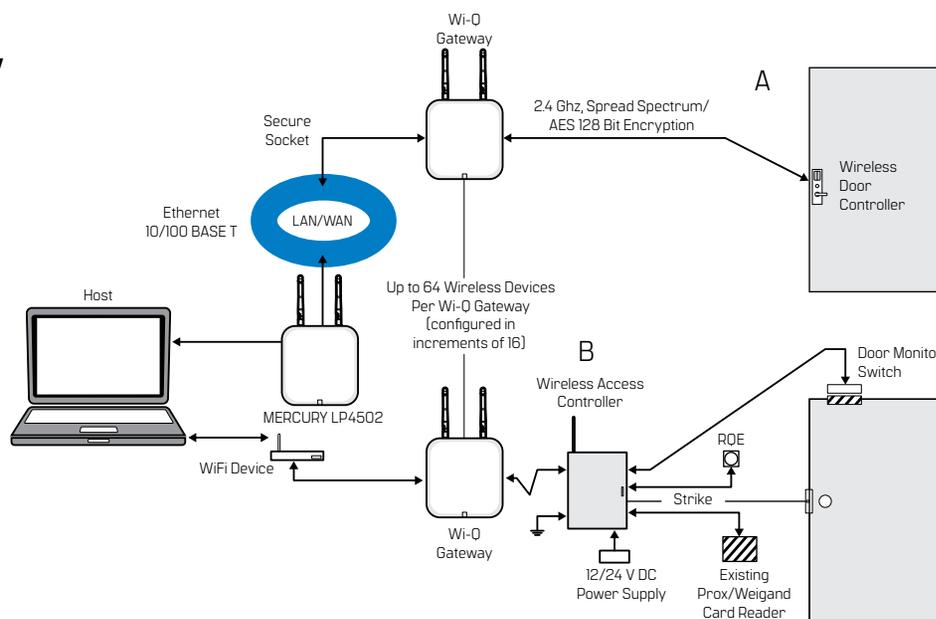
3   HARDWARE INSTALLATION

3.1.2 Gateways

The Wi-Q Gateway is a wireless device connected to the Mercury LP4502 Interface Panel or the Wi-Q Access Management Software through a secure IP address. It transfers data signals from wireless controllers to and from the host computer. The Gateway recognizes all Wi-Q Wireless Controllers within its antenna range. One Gateway can control up to 64 wireless controllers.

Gateways provide bi-directional radio frequency communication between wireless controllers and the associated host computer(s). All wireless communications are via secure AES 128-Bit encryption using spread spectrum 2.4GHz RF radio technology. Transmit range from Gateways will vary based on building construction. Cabled and directional antennas are also available to assist in managing the transmit range. The Gateway communicates to the host computer through web services via the Ethernet 10/100 Base-T.

3.1.3 Wireless Controllers

The Wi-Q Gateway is designed to operate with Wi-Q Technology BEST 45HQ Mortise and/or BEST 9KQ Cylindrical Locksets equipped with either keypad, card, or a combination of controller input devices. Door switch monitor, request to exit, and door lock position sensors are included in the locks. BEST Wi-Q Technology Controllers support a broad range of controller technologies:

- Card or Keypad ID (with PINs)
- Magnetic stripe, Prox, MIFARE (card number only)
- 512 time-zones (per segment)
- 14000 user credentials per door
- Cardholder access level definition
- Dynamic flash memory for IDs vs transactions

- Locally stored and transmitted transactions
- ADA (Americans with Disabilities Act) compliant
- No AC power required at door

3.1.4 Wireless Access Controllers

Existing controller configuration can be retrofitted to communicate with BEST Wi-Q Technology Gateways using Wi-Q Technology Wireless Access Controllers. This device can also be used to connect other I/O devices to the system. About the size of a standard double-gang box electrical box, these controllers operate on standard 12VDC or an optional 12/24VDC sealed, lead acid battery pack power supply. They seamlessly integrate existing door hardware with the LP4502 Controller Board into many Access Control Systems, supporting Wiegand-Compatible Keypad controller inputs.

NOTE: Please check with your dormakaba representative for a list of compatible controllers.

3.1.5 Antenna Types and Applications

To optimize system performance, it is important to position Gateways to receive maximum signal strength from the wireless controllers. Once all door hardware has been installed, it is time to position Gateways using the Wi-Q Site Survey feature in the Gateway.

Wi-Q Technology supports two antenna types: omni-directional, designed to provide coverage in all directions; and directional antennas that focus the signal from point-to-point over longer distances and through obstacles. For more information, see "Position Gateways (Task 2)" on page 20.

3 HARDWARE INSTALLATION

Antenna Types

Gateway Model	Configuration Description	Dormakaba Antenna Model Reference
WQXM-PG	Gateway with whip antennas	B89993
WQXM-PG	Gateway with ceiling mount omni-directional antenna	WQD-ACMO
WQXM-PG	Gateway with interior/exterior wall mount directional antenna	WQD-AWMD
WQXM-PG	Gateway with exterior omni-directional mast mount antenna	WQX-AEMO

3.2 Installing System Hardware

Many Access Control Systems can integrate the Wi-Q Technology by using the LP4502. These integrations can operate with BEST 45HQ Mortise Locks, BEST 9KQ Cylindrical Locks, BEST EXQ Trim, Wireless Access Controllers and Wi-Q Technology Gateways. Detailed installation instructions are provided in the following sections and in the lock's instructions provided with the hardware.

3.2.1 What Is Needed to Install Wi-Q Hardware

- ☐ Engineering drawings or segment map
- ☐ A Site Survey completed via the WQXM-PG Gateway
- ☐ A spectrum analysis tool to identify the best open channels for the network
- ☐ For keypad controllers, the sign-on credential from the WQXM-PG Web Interface
- ☐ For magnetic stripe or proximity card readers, the temporary operator card (supplied with the controller) and sign-on card created in the ACS or the WQXM-PG are both required. The appropriate magnetic stripe or proximity USB enrollment reader to create a proximity/magnetic sign-on credential is also required.
- ☐ Locksets to be installed on doors, including cores and keys supplied with specific model
- ☐ Installation instructions for specific lockset brand and model
- ☐ WQXM-PG Gateways
- ☐ Access to standby power for 120 VAC non-switch circuit for 12 VDC plug-in transformer or PoE
- ☐ A 10/100/1 GigE Base-T network connection
- ☐ Wireless Access Controllers, if used, and knowledge of existing hardware and switches for any retrofit installations
- ☐ Installation tools
- ☐ Drill motor/hole saw with bits appropriate for the specific lock. (See the template included in with the lock.)
- ☐ Phillips-head and flat-head screw drivers
- ☐ Access to the host, a networked workstation, or wireless laptop computer

3 HARDWARE INSTALLATION

3.2.2 Develop a Site Plan (Task 1)

Before installing Gateways, it is a good idea to develop a general plan for the segment. This plan will provide guidance in deciding where to install the Gateways. It is important to consider the following:

- The transmit range from Gateway to controller varies based on building construction.
- Site characteristics, such as reinforced concrete walls, could interfere or weaken the signal.
- Open spaces and low interference can increase signal strength.

Figure 3 shows a typical site configuration. The host (A) is located in building 1. The building 1 Gateway (B) is located near the electrical panel in the communications / electronics room.

The building 2 Gateway (C) is positioned next to the electrical panel. With 48 rooms in this three-story dorm, front and rear access doors and access to the elevator on three floors, this Gateway provides coverage to 53 controllers. Its range extends to all three floors of the building, and will also cover the pedestrian access, and elevator of the parking garage.

The parking garage portal (D) is positioned to cover the pedestrian door near the dorm and the stairway and elevator doors. Its range also extends to the entrance of buildings 1 and 2.

Figure 3 Typical Site Configuration
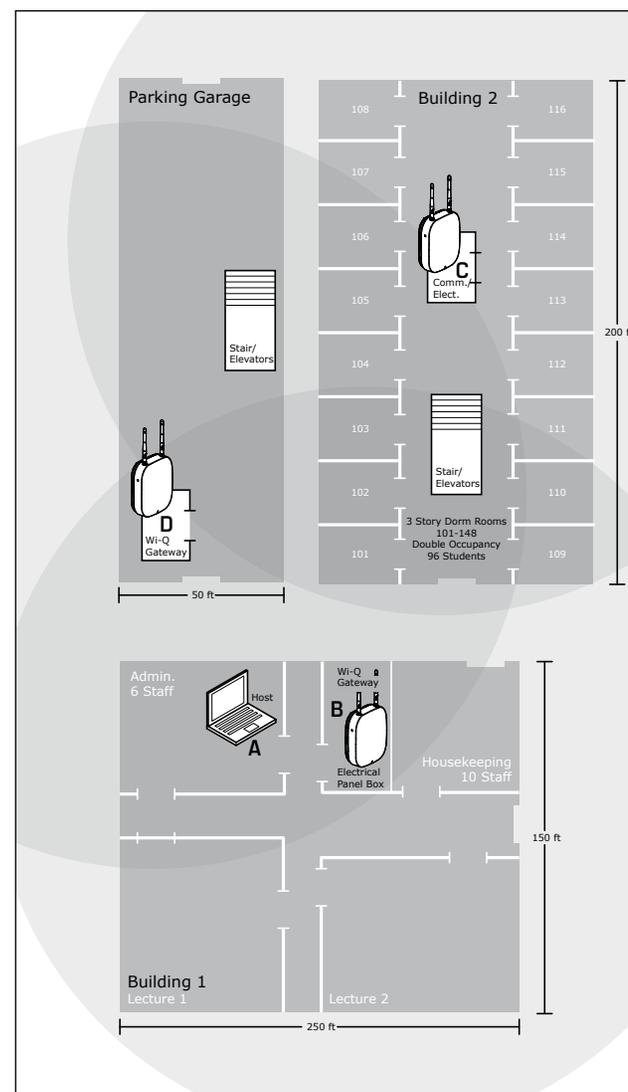
3   HARDWARE INSTALLATION

3.2.2.1 Site Survey

The WQXM-PG Wi-Q Gateway has a built in Site Survey feature. This part of the portal functionality allows the installer to conduct an on-site survey of the wireless communication between the Gateways and the Wi-Q Controllers without the use of a third-party application. This feature is useful when positioning the Gateway antennas for optimal communication with the controllers. Additionally, it helps the installer to identify the best channels to select for the Wi-Q Gateway and controllers. We recommend a Site Survey be performed during this step of the planning process. For additional information on the Survey Mode and how to use it, please see "3.2.3.3 Survey Mode" on page

3.2.2.2 Plotting the Plan

A Site Plan indicating building dimensions, distances between buildings, possible obstructions, parking segment, and other gated access points, contact the facilities maintenance or project engineer if needed. If none are available, visit the site, take measurements and draw up a plan. A sample plan is shown in .

3.2.2.3 Device Identification

Each device in the system will have its own unique identity. It will be important to document that identity, along with capacities and locations, and to give each device a common name such as "Parking Garage" or "Admin 1". At a minimum, record the Media Access Control number (MAC address) for each device. This 12-digit number is assigned by the manufacturer of a network device so that it can be recognized as a unique member of a network.

Figure 4 Sample Site Installation Plan
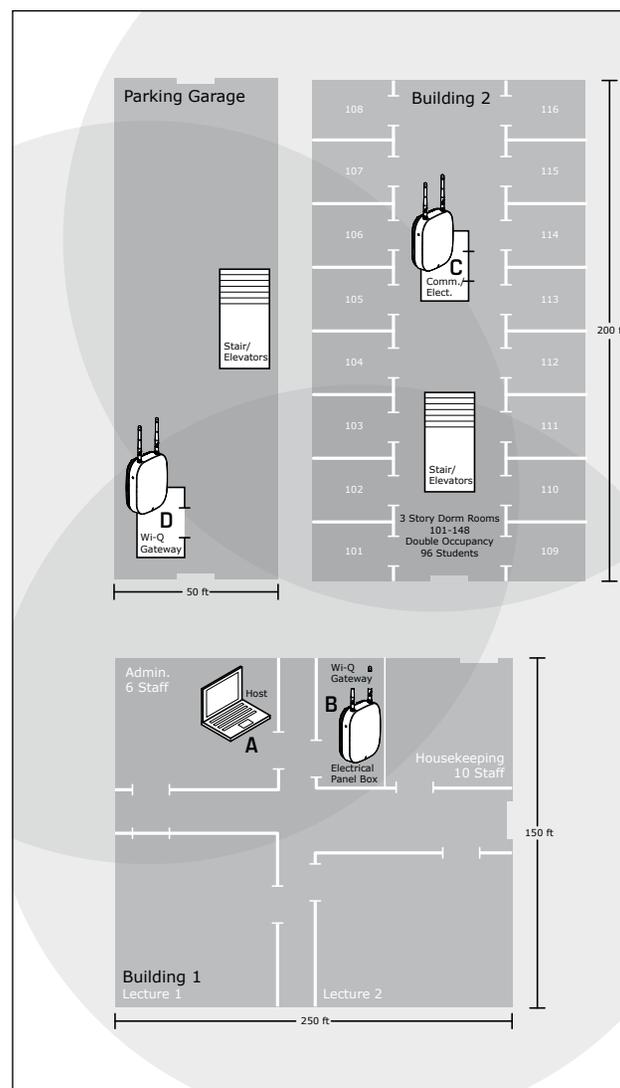
3   HARDWARE INSTALLATION

When moving on to configure the Access Control Software, it is essential to have a list identifying each controller and Gateway recognized by the system. We recommend creating a temporary label for each device that includes the MAC address, device name, location, capacity, and type of antenna so that installers on the site will have a reference for installing the correct device in a location.

3.2.2.4 Interference
Wi-Q Technology transfers information between devices in the form of data packets over the 2.4 GHz ISM band. This frequency band is very heavily used in many devices such as wireless computer networks (Wi-Fi) and cordless phones, which increases the risk of lost packets, that is, packets that do not make it from a controller to a Gateway because of interference. Interference can also reduce controller battery life due to the constant re-broadcasting of packets and lost connections to the portals. To achieve maximum efficiency with Wi-Q Communications, this frequency range must be managed effectively. Therefore, the installer must know the positions and channels of all the 2.4 GHz wireless devices in the segment and ensure channels are assigned to each device so that there is minimum frequency overlap with adjacent or nearby devices. dormakaba recommends using channels 15, 20, 25 for Wi-Q Configurations as these channels do not directly overlap Wi-Fi. Please be aware that these are not guaranteed to be interference free and it is imperative to work with the local person managing the customer wireless networking to coordinate.

3.2.2.5 Extended Range
It is likely that there will be locations in the segment separated by distances greater than 100 feet. It is important to consider adding a Gateway with a directional antenna to extend the transmit range.

NOTE: Actual distances will vary based on building construction and materials used as well as local interference.

3.2.3 Position Gateways (Task 2)
Once all door hardware and controllers have been installed, Gateway final placement is determine using the results from the Wi-Q Technology Site Survey feature built into the Wi-Q Gateway.

NOTE: The signal strength at all door locations should be verified near the perimeter of the coverage area as well as any location where a physical obstruction may cause interference.

3.2.3.1 Antenna Types
Wi-Q Technology supports two antenna types: omni-directional, designed to provide coverage in all directions; and directional antennas that focus the signal from point-to-point over longer distances and through obstacles. If there is trouble verifying signals, consider antenna type options. Figure 5 shows the two available antenna types.

3 HARDWARE INSTALLATION

Figure 5: Selecting the Antenna Type That Best Suits the Installation
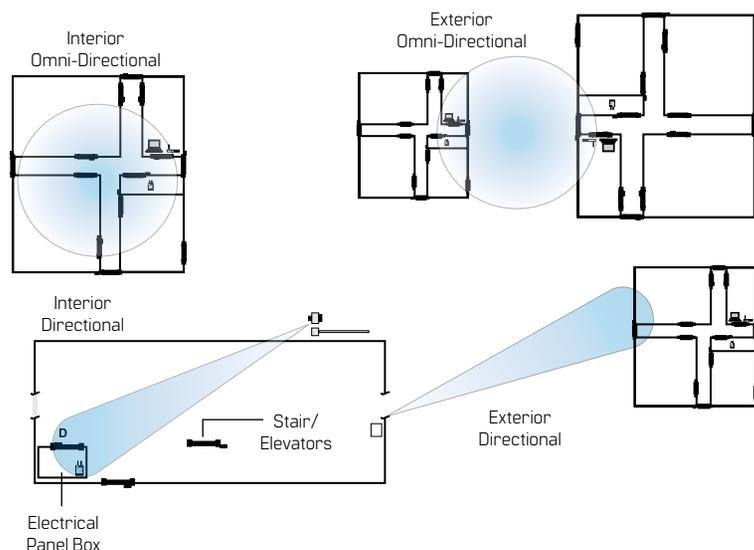
3.2.3.2 Power Supply

Gateways must be located where they can receive 110 VAC power from a transformer plugged into a dedicated power source or receive power through a PoE IEEE 802.3af compliant class 2 switch. The power draw will be around 4W or about 350mA at 12 V from the AC adapter.

To make the final determination, consider the following:

- Access to Ethernet 10/100 Base-T network connection
- Proximity to other I/O devices if implemented
- Placement within range of controllers

NOTE: Transmit range will vary based on building construction and materials used.

3.2.3.3 Survey Mode

The WQXM-PG Gateway has a built in Survey Mode. This feature

is especially handy when performing a Site Survey for portal and controller approximations for future installations as well as troubleshooting existing installations. The Survey Mode offers a live trace of signal strength and packet ratio transfer ratio.

3.2.3.3.1 Using the WQXM-PG Gateway for a Stand-alone Site Survey

The WQXM-PG Gateway can be used standalone without an ACS to perform a Site Survey to determine the Gateway antenna placement in approximation to the Wi-Q Controllers and the number of Gateway's needed for adequate coverage as well as troubleshooting signal and packet transfer ratio issues.

Using a Wireless Smart Device for Gateway WiFi:

1. Power on the WQXM-PG. Wait for the boot process to complete.
2. Press the '**Wi-Fi toggle**' push button of the Gateway and release immediately. The Wi-Fi is now enabled and the LED will flash on and off.

NOTE: The Gateway Wi-Fi access point will be disabled by default after a reboot. Once the Wi-Fi push button is pressed the Wi-Fi is enabled and the LED will flash on and off. The access point will remain active until the Wi-Fi push button is pressed again or 30 minutes have elapsed after the last Wi-Fi client disconnects.

3. Connect smart device to the Gateway WiFi access point (SSID if Gateway will be like WiQ-123456, where 123456 are the last 6 digits of the Gateway MAC address).
4. Using a smart device's browser, navigate to WQXM-PG wireless network IP address: 192.168.3.200.
5. Log in to the Gateway's webpage using the previously updated '**Username and Password**'.

3   HARDWARE INSTALLATION

NOTE: Default username and password works only with factory reset/deep reset Wi-Q Gateway. User need to change the password on a factory reset Gateway for security reasons.
Default Username: **admin**
Default Password: **password**

6. Once logged in, click on the '**Survey Mode**' button in the upper right corner of the Gateway webpage.
    Click on the '**Standalone Survey**' button to perform a Site Survey without an ACS.

7. The '**Current Sign-on Key**' field will fill with a 6-digit sign-on key (806608) to sign a demo reader onto the Gateway.

NOTE: After Standalone Survey Mode is enabled, the Web UI will be logged out. You must then log back in and return to the Survey Mode page to perform Standalone Survey Mode operations.

8. If performing the survey with a controller that has an integrated keypad, note the Gateway's sign-on key, sign on the Wi-Q Controller(s) with a keypad.
    - On the keypad enter 5 -6 -7 -8 - # immediately followed by the 6-digit sign-on key in the segment tab.
    - The LED's on the WDC will alternate red, green and blue. If the sign-on is a success, there will be 3 green LED's accompanied by 3 tones that go up in pitch.
    - If the sign-on is unsuccessful, there will be 3 red LED's with 3 tones that go down in pitch.

9. If performing the survey with door-hanger style controllers (beacons) without the integrated keypad:
    - Power on the beacons to be used and position them at the doors to be surveyed.
    - If the battery wires are disconnected, connect them.

- If the battery wires are connected, disconnect the wires; wait 10 seconds, and reconnect them.
- A tone indicates that the beacon is powered up. A second tone indicates that the beacon is communicating with the Gateway.

10. Click on '**Start log**' button to start the logging the signal strength.

The WQXM-PG Gateway will begin logging the portal packet ratio, the reader packet ratio as well as the signal strength at the portal and the reader.

Figure 6 Portal Signal Strength

Portal Signal Strength
The Portal RSSI value indicates how well the portal receives signal from the door controller and should be -75dB or better. The Survey Mode charts in the WQXM-PG denotes the lowest limit by the blue dashed line in the Signal Strength chart. If the Portal RSSI value

3   HARDWARE INSTALLATION

is below the limit, please reposition the Gateway or the antennas to improve signal strength. It may also be possible that another portal is required for adequate coverage.

Reader Signal Strength

The Reader RSSI value indicates how well the reader is receiving signal from the Gateway and should be at least -65dB or better denoted on the chart with the red dashed line. If the Reader RSSI value is below the recommended limit check the reader antenna and the gray antenna jumper cable to verify there is not damage to them. Also, it may be required that the WQXM-PG or the antennas need to be repositioned so the reader can hear the WQXM-PG more clearly.

Figure 6 (cont) Packet Transfer Ratio
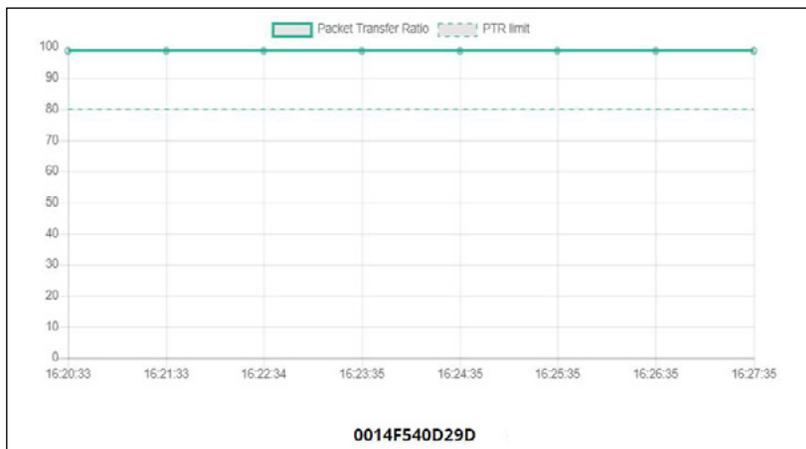
0014F540D29D

Packet Transfer Ratio

It is recommended that the packet transfer ratio rate is 80% or better. This value indicates how efficient the communication is between the readers and the WQXM-PG as well as how much interference maybe in the area. If this value is below 80%, the reader will not receive all the configuration data. To verify the portal packet ratio, update the reader statistics to poll every 10 seconds instead of once a day while running the survey tool in the WQXM-PG.

It is imperative to consider the wireless environment and the placement of the Gateway and its antennas during planning. The Gateway communicates on the 2.4 GHz frequency using the ZigBee channels. If the location has other wireless devices or networking using the 2.4 frequency, please orient the antennas away from these devices to manage interference. It may be required to work with local personnel to manage the wireless environment to prevent causing interference with other Wi-Fi installations and products.

3 HARDWARE INSTALLATION

3.2.4 Install Gateways (Task 3)

The most common installation site is inside an existing protected area such as a locked room or other secure enclosure, or above ceiling level. If a dealer-supplied locked enclosure is being installed, refer to the instructions provided with that equipment. Figure 7 shows a Gateway positioned in a protected area.

Figure 7: Installing a Gateway in a Protected Area
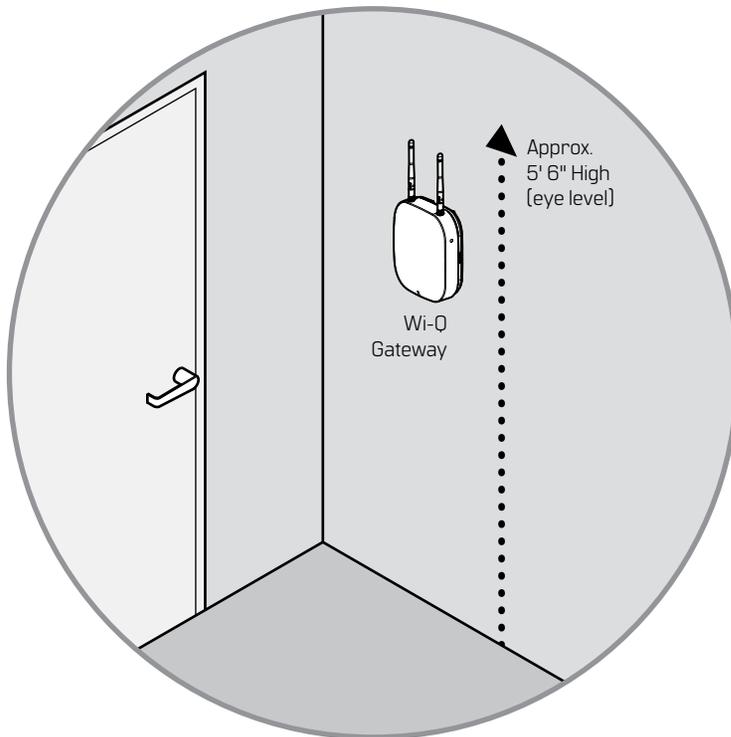

3.2.4.1 Connecting the Gateway and Verifying Operation

Once the Gateway is installed, connect and verify operation as follows:

1. Connect the power supply to the Gateway and plug the transformer into a dedicated AC power supply (wall outlet) if power over Ethernet is unavailable. See figure 8.
2. Insert the Ethernet cable into the Ethernet connection on the bottom of the Gateway. See figure 8. The link status light at the top of the Gateway will flash red while the Gateway is booting. When it flashes green, it is ready to be configured. Please see the table below for a complete list of the various LED indications and what they mean.

Mode	LED Behavior
Boot	Flashing purple, 1 flash every 2 seconds
Waiting for or lost ACS connection	Solid red
Online and connected to ACS	Solid green
Survey mode	Solid blue
Firmware update	Flashing aqua
Boot error	Solid purple
Rebooting	Flashing purple, 2 flashes per second
Factory reset	Flashing purple, 4 flashes per second
ACS connection status unchanged and Wi-Fi enabled	ACS connection status will register solid red or solid green. When the Wi-Fi button is pressed, the LED will flash red or green depending on the ACS connection status indicating that the Wi-Fi is enabled.

3 HARDWARE INSTALLATION

Ethernet Port
Power Port
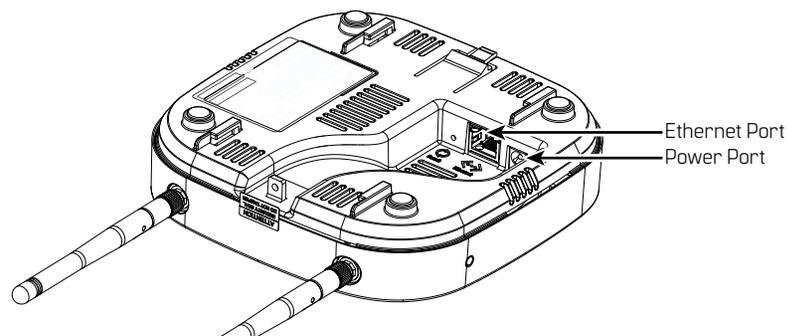
NOTE: If no protected area is available, consider positioning the Gateway inside a locked enclosure designed for that purpose. Contact your dormakaba dealer for more information.

3.2.5 Configure Gateways (Task 4)

The Gateway can be configured to work as a standalone device for use with the Wi-Q AMS Software or for use with the LP4502 Controller Board and third-party Access Control Software. The WQXM-PG model Gateways come equipped with a Wi-Fi radio and Ethernet connection. This Wi-Fi radio is used to configure the Gateway and the Ethernet connection is for communication on the customer's network. The Wi-Fi connection cannot be used to wirelessly connect the Gateway to a customer network for use with the Access Control Software.

The WQXM-PG Gateway's Wi-Fi network reserves the 192.168.3.xxx IP address space. When a device is connected to the Gateway's wireless network, it allows the device browser to connect to the Gateway via the default IP address, 192.168.3.200. Because, the Gateway's wireless network is locked down to the 192.168.3 IP address space, the hard-wired Ethernet IPv4 configuration cannot use this IP scheme for a local closed network. The 3rd octet of the IPv4

LAN connection must be something other than 3.
For example: Use 192.168.2.100, where 2 instead of 3 is used in the address's 3rd octet, when assigning an IP address to the Ethernet adapter on the Gateway if a Class C IPv4 network is in use.

The Gateway may initially be configured via wired Ethernet using the default Ethernet IP (192.168.1.200), which is displayed on the bottom of the Gateway. After the Gateway IP address is configured as described in section 3.2.5.3.1 the new Gateway IP address can now be used to connect to the Gateway web interface. This connection will allow the User to initiate future Gateway configuration changes without requiring the User to physically access the Gateway and press the Wi-Fi enable button.

3.2.5.1 Access the Gateway's Wireless Network

The WQXM-PG Gateway is equipped with a wireless network used to access the Gateway and configure it. The portal default IP address on this network is 192.168.3.200. To temporarily enable the portal's wireless network for configuration, do the following:

- Push the Wi-Fi enable button on the side of the WQXM-PG Wi-Q Gateway. See figure 9.

Wi-Fi Enable Button
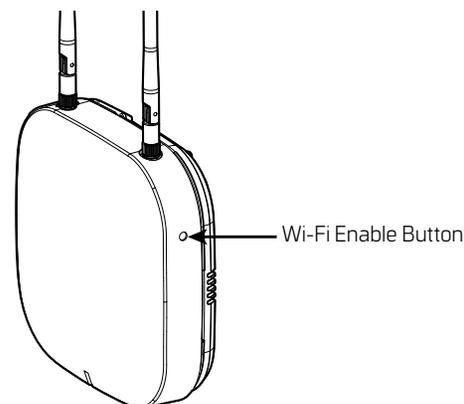
3   HARDWARE INSTALLATION

- Connect to the WQXM-PG wireless network using a smart device (e.g. tablet, cell phone) or laptop Wi-Fi connection.
- The Gateway's Wi-Fi SSID will appear in the list of available wireless connections.

NOTE: The Gateway's last 6 of the MAC address will correlate to the Wi-Fi SSID (connection name) and more than one portal's wireless network may appear in the list at a time.

Example ---> Mac address of new Gateway: 0014F500002E
                          Wi-Fi SSID to use: WiQ-00002E
Click on the network for the portal that is to be configured.

NOTE: If the portal cannot be logged in to using the steps above try the following troubleshooting steps:

1. If the SSID is not visible then press the WiFi toggle push button of Gateway and release.
2. Reconnect to the Gateway's unique wireless network connection.
3. Try to log in again.
   The Wi-Fi SSID Password = password for first time login

and will be updated each time the user login password for the gateway web UI is updated.

4. Power cycle the Gateway and attempt to log in again once it is powered back up.
5. If the power cycle is not successful and connection to the to the Gateway's webpage is still inaccessible, then perform a "Deep-Reset" by taking a pin and depressing the reset button on the Gateway for 10+ seconds at which time the LED will begin to flicker purple. See figure 10.

Figure 10 Wi-Fi Reset Button
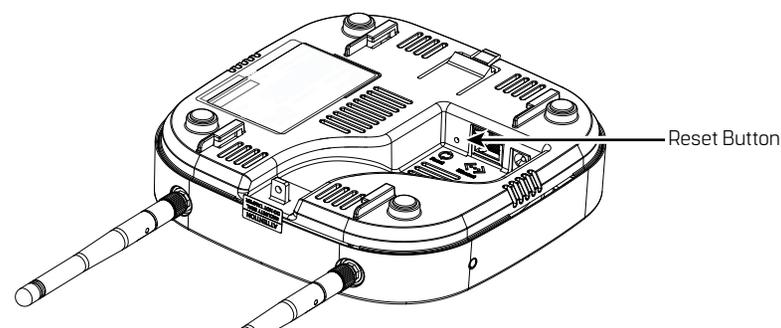
6. A purple light will flash confirming the deep reset.
7. Once the deep reset process has completed, wait 3-4 minutes before attempting to log back in to the Gateway. The gateway LED will turn solid red when it is fully booted up and ready for a Wi-Fi connection.

Follow the steps previously mentioned to enable Wi-Fi, reconnect, and log in.

NOTE: The deep reset will take the settings on the board and restore them to the factory defaults.

3   HARDWARE INSTALLATION

3.2.5.2 Configure the WQXM-PG Gateway
Open the device's browser window and navigate to the Gateway's web UI pages.

NOTE: dormakaba recommends Google Chrome as the web browser to navigate the WQXM-PG web pages.

3.2.5.2.1 Login Screen
Log in to the Gateway.
- The default Username is **admin**.
- The default Password is **password**.

NOTE: The portal will log itself out after 10 minutes of non-use.

3.2.5.2.2 Manage Profile
The first time a Gateway is logged in to, the manage profile screen will appear prompting to change the Username or Password. On the initial log in, the user must change the default Password before access is granted to any other Gateway webpage. To update the Username and Password after the initial configuration, click on the Username link in the upper right corner of the screen. In the following image, it is labeled:

Hello, admin!

Change the Default Username.

1. Click on the '**Edit**' icon next to the '**Username'** field.
2. Enter the new Username into the '**New Username**' and '**Confirm Username**' fields.
3. Click the '**Update**' button to save the changes.

4. Click on the '**Update**' button to confirm the changes in the pop-up notification.
5. Click the '**Close**' button to close the pop-up notification.

NOTE: Once you change the password any Wi-Fi connection will be terminated. You will have to go back to your mobile device and change the connection password.
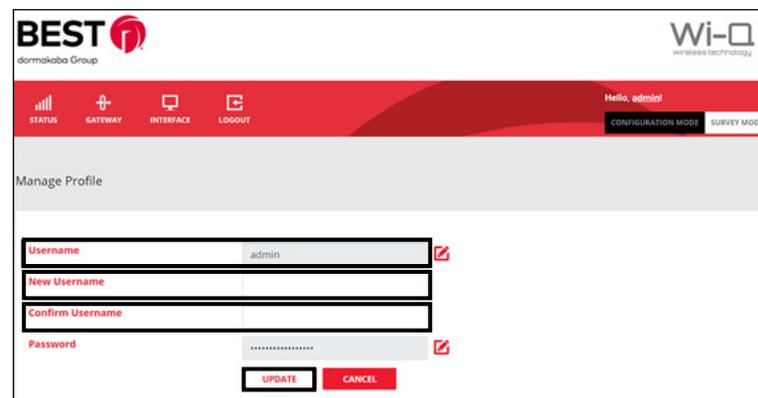
3 HARDWARE INSTALLATION

Change the Default Password.

1. Click on the '**Edit**' icon to the right of the '**Password**' field.
2. Enter the current Password in the '**Password**' field.
3. Enter the new Password in the '**New Password**' field.
4. Enter the new Password again in the '**Confirm Password**' field.
5. Click the '**Update**' button to save the changes.
6. Click the '**Update**' button in the pop-up notification window to confirm the changes.
7. Click the '**Close**' button to close the notification window.

NOTE: Once you change the password any Wi-Fi connection will be terminated. You will have to go back to your mobile device and change the connection password.

Once changes are updated, a pop-up window appears with the status of the changes being made. Click the '**Close**' button to close the pop-up window.
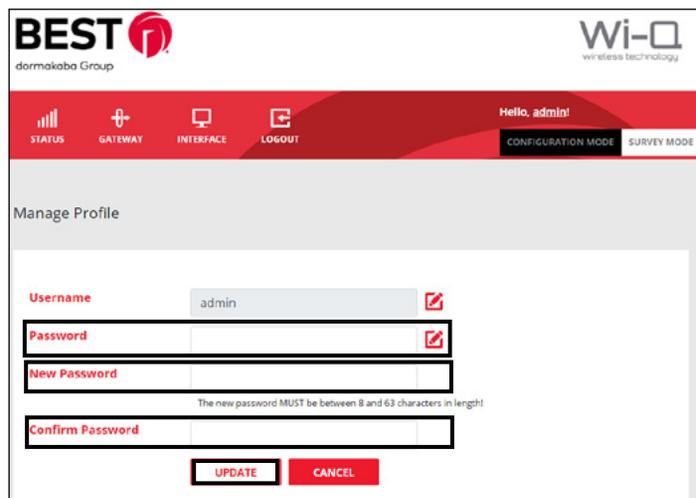
3.2.5.3 Gateway Status Window

The Gateway status page provides an overview of the WQXM-PG Gateway configuration, the sign-on key, the number of associated controllers, channels enabled, and can generate logs for trouble-shooting purposes.
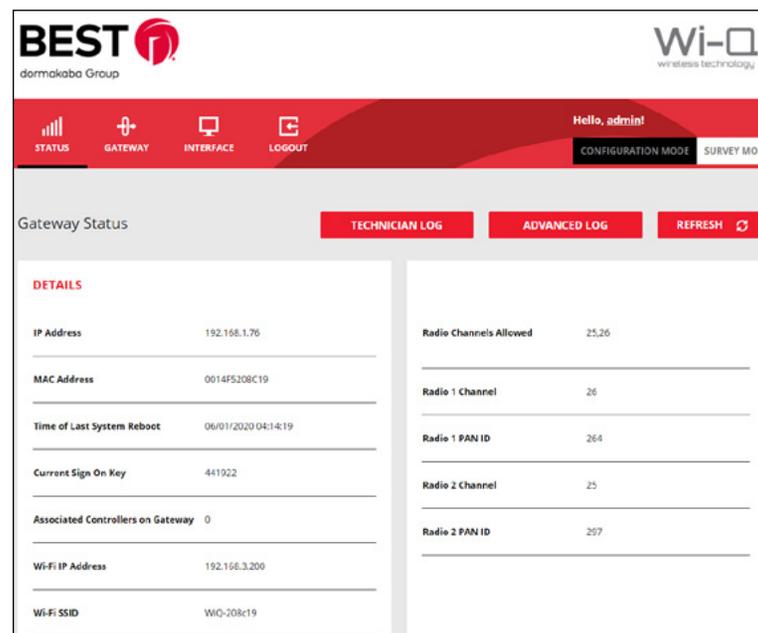
3   HARDWARE INSTALLATION

3.2.5.3.1 Details

- **IP Address** – Displays the Ethernet IP address of the Gateway as configured in its current state.
- **MAC Address** – The Gateway's unique Media Access Control address that uniquely addresses the device on the network.
- **Time of Last System Reboot** – The last date and time the Gateway was reset, or power cycled.
- **Current Sign-on Key** – A 6-digit sign-on key associated with the segment the Gateway is associated with.
- **Associated Controllers on Gateway** – Displays the number of controllers communicating with the Gateway when the view was initially displayed.
- **Wi-Fi IP Address** – IPv4 address assigned to the Wi-Fi radio on the Gateway.
- **Wi-Fi SSID** – The Gateway's wireless network name. This is always Wi-Q followed by the last six characters of the device's unique MAC address.
- **Radio Channels Allowed** – The channels currently enabled on the Gateway to connect to the Wi-Q Controllers.
- **Radio 1 Channel** – The channel assigned to Wi-Q Radio 1.
- **Radio 1 PAN ID** – The Personal Area Network ID assigned to Wi-Q Radio 1.

NOTE: Radio 1 PAN ID can be edited when in Mercury Mode. PAN IDs only need to be changed if there is a conflict with multiple Gateways within RF range of each other. Editing Radio 1 PAN ID will also change Radio 2 PAN ID. Each Gateway uses up to 66 PAN IDs.

- **Radio 2 Channel** – The channel assigned to Wi-Q Radio 2.
- **Radio 2 PAN ID** – The Personal Area Network ID assigned to Wi-Q Radio 2.

3.2.5.3.1.1 Wireless Controllers

At the bottom of the Gateway Status window is a list of the associated Wi-Q Controllers and their attributes.

- **ACR ID** – The Reader ID when the portal is in Mercury Mode with the LP4502 Access Control Board. This field will be blank when Mercury Mode is not in use.
- **MAC Address** – The Reader's unique Media Access Control address that uniquely addresses the device on the network.
- **Radio Channel** – The channel the door controller is communicating on with the Gateway.
- **Associate Time** – The date and time the Wi-Q Door Controller associated with the Gateway.
- **Last Beacon Time** – The last date and time the Wi-Q Door Controller beaconed information up to the Gateway.

3 HARDWARE INSTALLATION

- **Pending Operations** – Progress percentage of pending messages from the door controller to the Gateway.
- **Package Count** – The number of pending messages in the current queue that the Gateway has received from the Wi-Q Door Controller.
- **Firmware Version** – The current version of door controller firmware on the Wi-Q Device.
- **Portal RSSI** – Portal RSSI is the how well the Gateway received a signal from the Wi-Q Door Controller. The signal strength ranges from -18 (highest/best) to -91 (lowest/worst). Ideally, this value should be -75dB or better.
- **Reader RSSI** – Reader RSSI is the how well the Wi-Q Door Controller receives a signal from the Gateway. The signal strength ranges from -18 (highest/best) to -91 (lowest/worst). Ideally, this should be -65dB or better.
- **Flags** – The Flags indicate the device status. Common device statuses for Wi-Q Controllers when they are connected to a Gateway are below:
  - ☐ **010001 –** Controller initial connection to the Gateway.
  - ☐ **30207 –** Controller connected to the Gateway and is waiting for segment updates.
  - ☐ **30063 –** Controller has a deep reset command pending.
  - ☐ **30017 –** Controller waiting to be pulled into the segment and has not received segment updates.
  - ☐ **30007 –** Controller has received segment updates and is waiting in the "New Segment Items" folder in Wi-Q AMS Configuration software.
  - ☐ **30043 –** Controller is signed in to the ACS, connected, configured, and not locked to the Gateway.
  - ☐ **30053 –** Controller is taking configuration updates.

- ☐ **32043 –** Controller is signed in to the ACS, connected, configured, and locked to the Gateway.
- ☐ **32243 –** Controller is locked to portal but has not been added to an access level or a direct assignment to a User. No user credentials are assigned to the controller in the software.
- ☐ **38053 –** Controller has a firmware update pending.
- ☐ **38043 –** Controller is receiving a firmware update.
- ☐ **32207 –** Controller completed the firmware update and is waiting for updates from the portal.
- **Pending Messages** – The letters in the pending messages column are update messages that are being sent to the controller.
  - **S** – Segment information (pin length, DST Times)
  - **C** – Card formats
  - **L** – Controller configuration (beacon time settings, channels, transaction masks, etc.)
  - **U** – User credentials and properties
  - **T** – Timezone intervals
  - **I** – WAC I/O
  - **F** – Firmware
  - **P** – Ping (missing LIF data after association or updates)

3.2.5.3.1.2 Generate Logs
The '**Technician**' and '**Advanced**' log buttons allows the installer/technician to assist dormakaba BEST software support in troubleshooting an issue. These logs may be used by the local installer to troubleshoot or verify the credentials are all making it to the controllers or requested during a troubleshooting session with Software Technical Support.

3   HARDWARE INSTALLATION

To generate logs, do the following:

Technician Log

TECHNICIAN LOG

The '**Technician Log**' button is used to aid installers/technicians when the Wi-Q System is setup in Mercury Mode. This log provides information on when each controller was last updated with user credentials. This can aid a technician to determine if there is a problem pushing changes in user credentials to the door controllers.

The Technician Log looks like the following table.

credentialnumber	macaddress	downloadsta	lastupdate
6767	0014F540D270	1	2019-10-01 17:31:24.812
6767	0014F540D247	1	2019-10-01 17:31:25.384
6767	0014F540D246	1	2019-10-01 17:31:26.219
6767	0014F540D26D	1	2019-10-01 17:31:24.518

There are four fields in the log file: Credential Number, MAC Address, Download Status, and Lastupdate:

- **Credential Number** – Provides the credential pushed to the door controller.
- **MAC Address** – MAC address identifier for the door controller.
- **Download Status** – Shows if the door controller has received the user update. If download completed to door controller with ACK then download status = 1. If CRCs match with what is already in the controller download status will = 0.
- **Lastupdate** – Last time the door controller recognized that it received an update from the ACS.

NOTE: Adding the credentials to an access level, clearance, or reader will not automatically propagate the information to the readers. Time must be allowed for the beacon cycle and possible network lag.

Advanced Log

ADVANCED LOG

Advanced logs are used by engineering to perform advanced troubleshooting. These logs are encrypted and can only be decrypted by our engineering group. These logs may occasionally be requested by Software Technical Support during a troubleshooting session. Clicking on the '**Advanced Log**' button will download the log file to the browser's download location and should be forwarded to Technical Support via email at bas.support.best.us@dormakaba.com. The file will be named with the following naming convention: ***Portal_0014fmacaddress_201907datetime.tar.gz.enc***

3.2.5.4 Gateway Menu

The Gateway page has multiple sections with different functions as the windows are scrolled down. The primary focus of this page is to configure the Gateway for the customer network. This page allows the firmware to be upgraded on the Gateway. Should there be an updated firmware release the technician or system administrator has the ability to send a reboot command to the device. The configuration section of the Gateway menu allows the Ethernet network card configuration of the IP address, updates to the portal service port as well as SSL certificate generation and enablement.

3   HARDWARE INSTALLATION
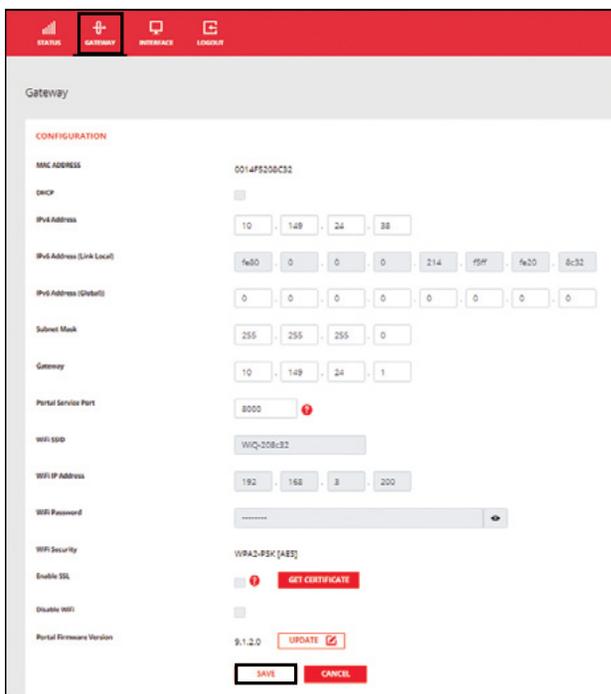
3.2.5.4.1 Assigning an IP Address

Configuration changes on the Gateway are only available via the portal's wireless network after the '**Enable Wi-Fi**' button has been pushed. The WLAN IP address for the WQXM-PG wireless network is a static 192.168.3.200 and cannot be changed.

If the 192.168.3.x subnet is required by the user for another device, the '**Disable WiFi'** box must be checked. Once WiFi is disabled, the Gateway can only be accessed via the wired network, and attempting to enable WiFi by pushing the '**Enable WiFi'** button will not be effective.

Once the LAN IP address has been updated, the '**Enable Wi-Fi**' button can be depressed for a second time to disable the Wi-Fi on the WQXM-PG. Additionally, if nothing has been connected to WQXM-PG wireless network for 30 minutes, the internal Wi-Fi network will automatically disable.

3.2.5.4.1.1 DHCP

A static LAN IP address of 192.168.1.200 is the default IP of the WQXM-PG for first time configuration via the LAN port, however, the Gateway has built in DHCP functionality allowing network administrators to assign portal IP's dynamically via DHCP. To take advantage of this feature, verify the DHCP checkbox is selected instead of manually assigning an IP address. Provide the customer's local network administrator with the list of MAC addresses and other information as required by the customer.

To complete enabling the DHCP setting, click on the '**Save**' button at the bottom of the screen to save the changes.

3.2.5.4.1.2 Static IP Assignment

The WQXM-PG Gateway has built in flexibility to use IPv4 as well as IPv6 addresses. Contact the local IT or network administrators for IP addresses available for each device. To assign the IP addresses to the devices, verify the DHCP checkbox is not selected and enter in the IP address as specified into the IP address fields. Verify that the correct subnet mask as well as default Gateway for the assigned IP schema.

To assign a static IP address configure the following fields:
- IPv4 address or IPv6 address
- Subnet mask (for IPv4 addresses only)
- Gateway (for IPv4 addresses only)

3   HARDWARE INSTALLATION

To save the changes for the static IP address, click on the **'Save'** button at the bottom of the window.

3.2.5.4.1.3 Portal Service Port
The default portal service port for the ACS to communicate to the Gateway is port 8000. The portal service port is the port used to connect to and configure the Gateway. If a port other than 8000 is required, the portal service cannot be 80, 443 nor within the range of 13000-13019. Valid ports are within the range of 0-65 or 535.

3.2.5.4.1.4 Enabling SSL

NOTE: There are two communication paths which have the option to enable SSL. One communication path is the interface to the ACS for a direct Wi-Q integration. The other communication path is for an integration involving interfacing to the ACS through Mercury panels and will be discussed in a later section.

If SSL is also required to encrypt the communication between the Gateway and the ACS as well as between the Gateway and the browser, the WQXM-PG Gateway can issue a self-sign SSL certificate for use with the ACS. To enable SSL, do the following:

1.   Click on the 'Enable SSL' checkbox in the Gateway configuration page.
2.   Click on the 'Get Certificate' button to download the portal's SSL certificate. This portal certificate will download to the predetermined location on the local browser.
3.   Click on the 'Save' button to save the SSL setting.
4.   Locate the SSL certificate on the PC where the certificate was downloaded and upload the SSL certificate into the ACS.

NOTE: SSL certificates expire after 20 years. Please take a note of the expiration date and plan to reissue the certificates and upload them before the SSL expiration to prevent disruption in communication between the ACS and the Gateways.

3.2.5.4.1.5 Update Portal Firmware
Occasionally it is necessary to upgrade the portal firmware. To upgrade the portal firmware, do the following:

1.   Navigate to the Gateway menu option in the WQXM-PG webpage.
2.   Click on the 'Update' button towards the bottom of the Gateway page.

3 HARDWARE INSTALLATION

3. In the firmware upgrade pop-up screen, click on the '**Browse**' button to browse to the firmware file.
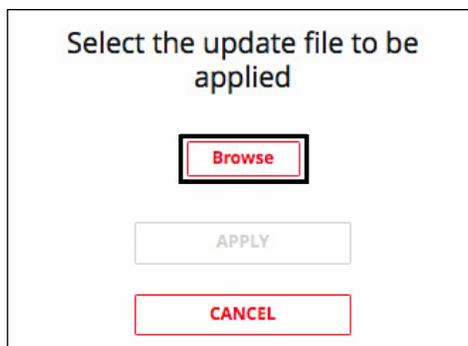
4. Browse to the previously extracted .gzhe portal firmware file and click the '**Open**' button to upload the file.
5. The selected file will be listed in the pop-up window. Verify it is correct and click the '**Apply**' button.
6. The firmware will be applied to the Gateway. The Gateway's LED will flash aqua when it downloads the firmware.

3.2.5.4.1.6 Reboot Gateway

Occasionally it may be necessary to reboot the WQXM-PG Gateway. This action can also be referred to as a reset. To reboot the Gateway do the following:

1. Navigate to the '**Gateway**' menu option of the Gateway.
2. Scroll to the bottom of the screen.
3. Click the '**Reboot Gateway**' button.
4. A pop-up window will appear asking if you are sure you want to reboot the Gateway. Any changes made and that have not been saved will be lost. Click the '**Reset**' button to continue.

5. The Gateway will reboot immediately. During a reboot, the Gateway will flash purple. Once it reconnects to the ACS, the LED will display a solid green light. See the table on page 24 for more information on the LED's.

3.2.5.4.1.7 Factory Reset the Gateway

Occasionally, situations arise that require the Gateway to be reset back to factory default settings. To perform a factory reset, do the following:

1. Remove Gateway from enclosure or from the mounted location.
2. On the back of the Gateway locate the '**Deep Reset'** button next to the Ethernet inlet. The '**Deep Reset'** button is a recessed button accessible from a pin hole. See figure 11.
3. Push and hold the '**Deep Reset'** button using a small implement such as a paper clip for more than 10 seconds.

Figure 11 Wi-Fi Reset Button

Reset Button
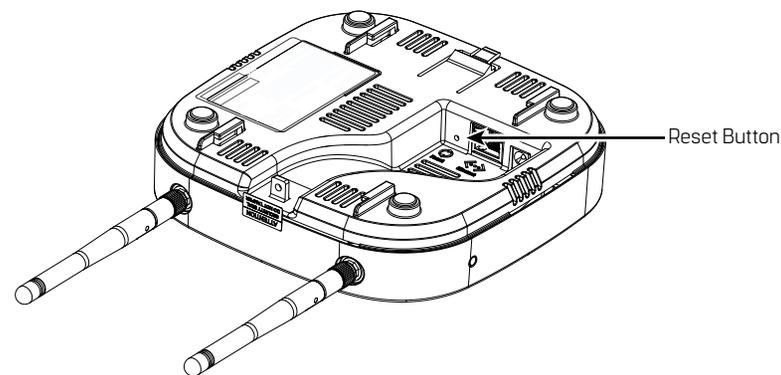
3 HARDWARE INSTALLATION

3.2.5.5 Interface Menu

The interface menu option on the WQXM-PG is for use when communicating to the ACS through a Mercury panel. This menu option will allow the WQXM-PG to be configured to communicate with the Mercury LP4502 Board.

3.2.5.5.1 Enable Mercury Mode

Mercury Mode is enabled when using the WQXM-PG with a third-party ACS and the Mercury Controller Board LP4502 or EP4502 v1.29 or higher.

1. Click on the '**Interface**' menu option at the top of the Gateway page to navigate to the Mercury Interface Configuration page.
2. Click on the '**Enable Mercury Mode**' checkbox to select it. It will turn red when selected and enabled.
3. SSL must be used to communicate to the Mercury panel (SCP). Click on the '**Enable SSL**' checkbox to enable SSL for use with the Mercury LP4502 Controller Board.
   - Click on the '**Enable SSL**' checkbox in the Gateway Configuration page.
   - If you need to revert to the default Mercury certificate, then click on the '**Use Mercury Certificate**' to use the default certificates, this certificate will work with the preloaded certificates in the Mercury panel.
   - If you wish to load your own certificate into the Wi-Q Gateway instead of using the default certificate, then click on the button to '**Load Certificate**'. If you use this option you will also need to load that certificate into the Mercury panel.
   - Click on the '**Save**' button to save the SSL setting.
4. Click on the '**Update**' button to apply the settings.
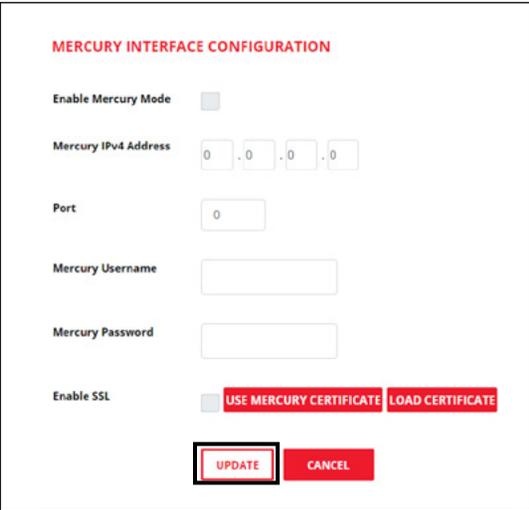
5. Once checked, the '**Enable Mercury Mode**' will validate this change and display a pop-up notification window.
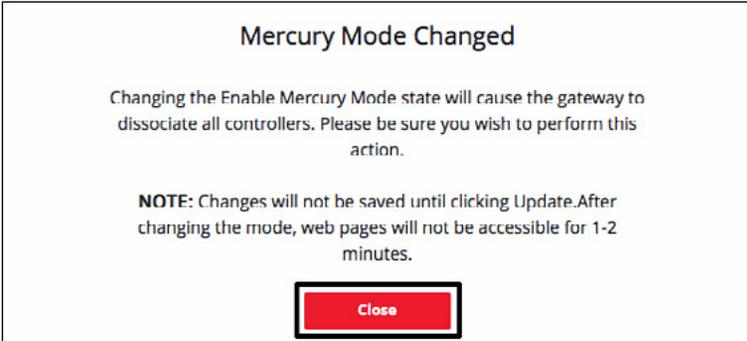
6. Click the '**Close**' button and fill out the remaining fields on the Mercury Interface Configuration screen as follows:
7. Enter the '**Mercury LP4502 IPv4 address'**.
8. Port 1883 is used for portal service communication by default. If port 1883 is already in use and the customer would prefer the port to be something else, change this

3   HARDWARE INSTALLATION

port number in the LP4502 as well as in the WQXM-PG Mercury Interface Configuration.

9. Enter the **'Mercury LP4502 Overwatch Username and Password'**. Please note this will need to be updated each time the LP4502 Overwatch Username and Password is changed.

NOTE: The WQXM-PG SSL certificate and Mercury LP4502 SSL certificate must match.
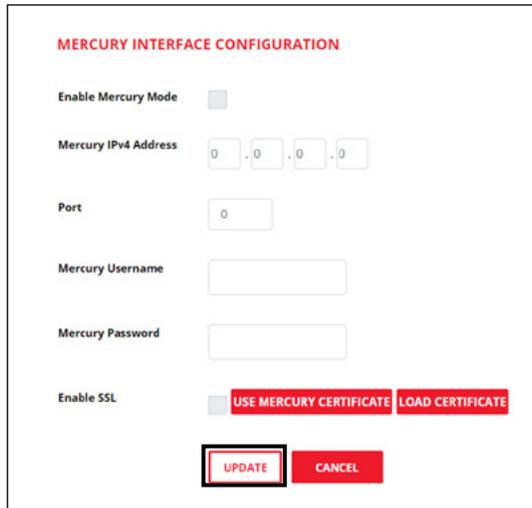
10. After making all updates, a notification window will appear to verify the updates being made to the WQXM-PG Mercury Mode Configuration.

11. Verify the changes are correct and click the '**Update**' button to commit the changes.

NOTE: If changes are required, click the '**Cancel**' button to go back and update the form.
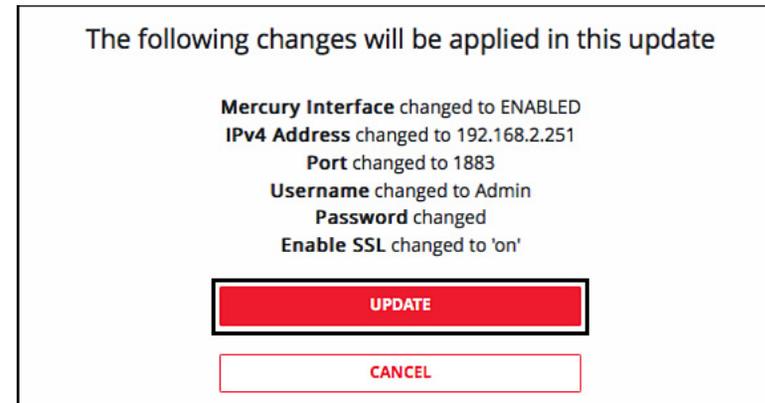
12. The system will then validate all changes and pop open a notification window showing '**Save Successful**'. Click the '**Close**' button to continue.

3   HARDWARE INSTALLATION

3.2.5.5.2 Adding Sign-on Credentials to the WQXM-PG (Gateway)

From the Portal's UI homepage click on the '**Credentials**' tab.
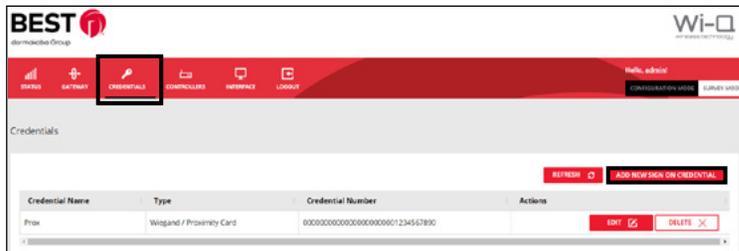
From the Credentials page, click on the '**Add New Sign-on Credential**' button on right side of screen.

NOTE: If a Wiegand/Prox card is chosen, a prompt will appear to confirm and/or edit the bit length for the card.
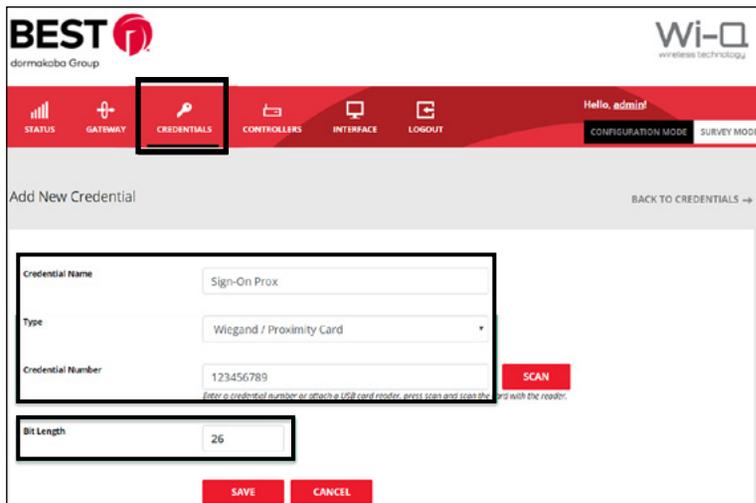
Enter credential criteria as prompted:

- **Credential Name** – Name of credentialed user to add
- **Type** – Magnetic stripe or Wiegand/Prox card
- **Credential Number** – Manually enter card number

Alternatively, attach a USB card reader, press the '**SCAN**' button, and scan the card with the reader.
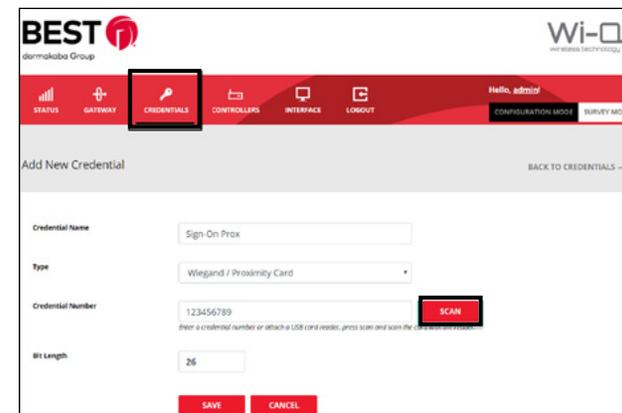
When all credential information has been entered, click '**Save**' on the Edit Credential page.

Click the '**Confirm**' button on the pop-up notification window to add the new sign-on credential.

3 HARDWARE INSTALLATION

Credentials already in the system can be edited (or deleted) by clicking the 'Edit' button on the Credentials home screen, and saved once done.

Credentials can be deleted from the Credentials screen as well. Choose the user to be removed, click the 'Delete' button.

Click 'Confirm' on the pop-up notification window when editing is complete.

3.2.5.5.3 Sign On Wi-Q Controllers to the WQXM-PG

The enrollment process for the Wi-Q Controllers requires a default token followed by a sign-on token and can take 20-30 seconds. The sign-on is also confirmed with a three-tone increasing frequency beep1-beep2-beep3 and 3 flashes of the green LED on the lock. If the sign-on fails there will be three beeps with decreasing tones and 3 red LED's.

NOTE: If the controller is a WAC or Omnilock, there will not be any audible beeps.

3.2.5.5.3.1 Keypad Method

- If a keypad is attached to the Wireless Door Controller (WDC) do the following:
  - Enter 5678# and then within 3 seconds enter the 6-digit sign-on key then the # key.
  - Example: 5678# 816645#
- If there is a keypad on the Omnilock or Wireless Access Controller (WAC) do the following:
  - Enter 5678 and then within 3 seconds enter the 6-digit sign-on key.
  - Example: 5678 816645
- The Wi-Q Controller should sign on to the WQXM-PG and display the controller's unique MAC address at the bottom of the STATUS page. (STATUS page not shown).

3 HARDWARE INSTALLATION

3.2.5.5.3.2 Magnetic Card Method

- If the WDC, WAC or Omnilock is equipped with a magnetic card reader do the following:
  - Present the magnetic temporary operator badge that comes with the Wi-Q Lock.
  - Within 3 seconds present the sign-on credential created in the Credentials screen of the WQXM-PG previously.
- The Wi-Q Controller should sign on to the WQXM-PG and display the controller's unique MAC address at the bottom of the STATUS page. (STATUS page not shown.)

3.2.5.5.3.3 Proximity Card Method

- If the WDC, WAC or Omnilock is equipped with a proximity card reader do the following:
  - Present the proximity temporary operator badge that comes with the Wi-Q Lock.
  - Within 3 seconds present the sign-on credential created in the Credentials screen of the WQXM-PG previously.
- The Wi-Q Controller should sign on to the WQXM-PG and display the controller's unique MAC address at the bottom of the STATUS page. (STATUS page not shown.)

3.2.5.5.4 Configuring the Mercury Panel for Use With the WQXM-PG

3.2.5.5.4.1 Logging in to the Mercury Board UI (User Interface)

1. Open an Internet browser. (Google Chrome is recommended.)
2. Log in to the UI for the LP-4502/MP-4502 Mercury Board by going to (**192.168.2.251**) in the URL field of the browser. Then click on the '**Click Here to Login**' link.

3. Enter the case-sensitive Username of '**admin**' and Password of '**password**' into the appropriate fields.

3   HARDWARE INSTALLATION

The Mercury Board User Interface Page will appear as follows:

NOTE: Make sure the Mercury panel has the latest firmware. It must be firmware version 1.29 or greater to work with Wi-Q. Check with Mercury for firmware update instructions.

To update the SCP panel firmware, go to the Diagnostic page. There are separate firmware files for the main SCP panel firmware and Over-Watch. If your panel doesn't have Overwatch installed then check with Mercury or your panel provider for the appropriate firmware file to load.
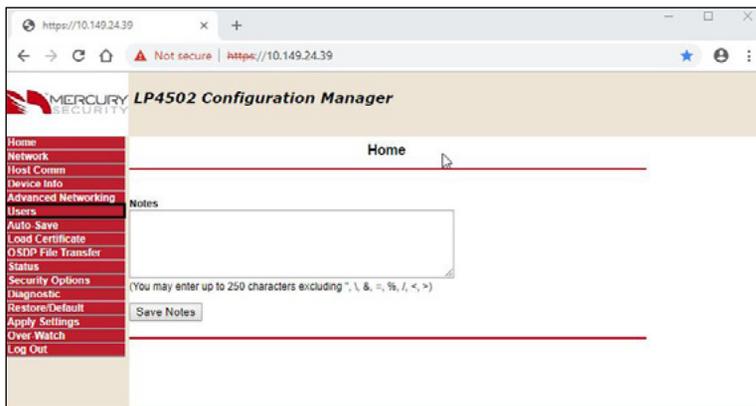
3.2.5.5.4.2 Updating/Creating Users and Passwords
1.   Log in to the LP4502 Configuration Manager.
2.   Click on the '**User**' tab on the left-side of the LP4502 home screen. As an option you may want to add your own User to the Mercury panel.
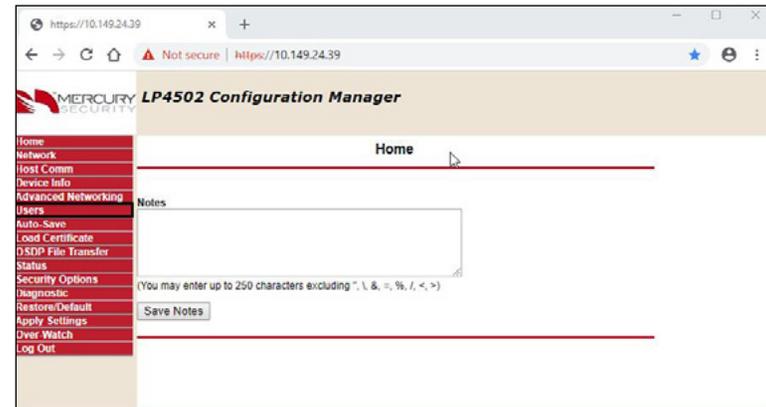
3 HARDWARE INSTALLATION

3.2.5.5.4.3 Overwatch Configuration and Loading SSL Certificates into the Mercury Panel

On the Mercury Panel some custom settings must be configured as follows:

NOTE: Steps 1-4 are one-time configurations after a hard reset of the Mercury Panel.

1. **Network** – Set IPV4 configuration as required. Make sure the IP address used in this step is the same IP address used on the Wi-Q Gateway INTERFACE page.
2. **Host Comm** – Set the '**Data Security'** drop-down to '**TLS if available**'.
3. **Users:**
   - **Option** – Create a New User, Level 1. This is for an alternate log in other than Admin/Password. This new user will not require Switch 1 to be ON to log in.
   - **Option** – Check '**Enable Diagnostic Logging**' if troubleshooting is required.
4. **Security Options** – Check '**Enable Encrypted Partition.**'
5. **Over Watch** – Create user Username and Password. This should match the Username and the Password as set in the WQXM-PG Gateway.
   - Broker Configuration Listening Port: **1883**
6. **From the Load Certificates Tab**
   If you prefer to use the Mercury SSL cert then no updates are needed, just enable SSL on the Wi-Q Gateway. If you prefer to use your own SSL certificate then follow these steps.

   - Choose certificate file: **client.crt**.
   - Choose private key file: **client.pem.**
   - Press '**Load certificate files.**'
7. **Apply Settings** – Click on the '**Apply Settings, Reboot**' button to apply the settings and reboot the Mercury Board. The board will take approximate 45 seconds to complete this process. Please wait 1 minute before attempting to log back in to the Mercury Board.

NOTE: The certificate can be generated through the WQXM-PG or through a third-party.
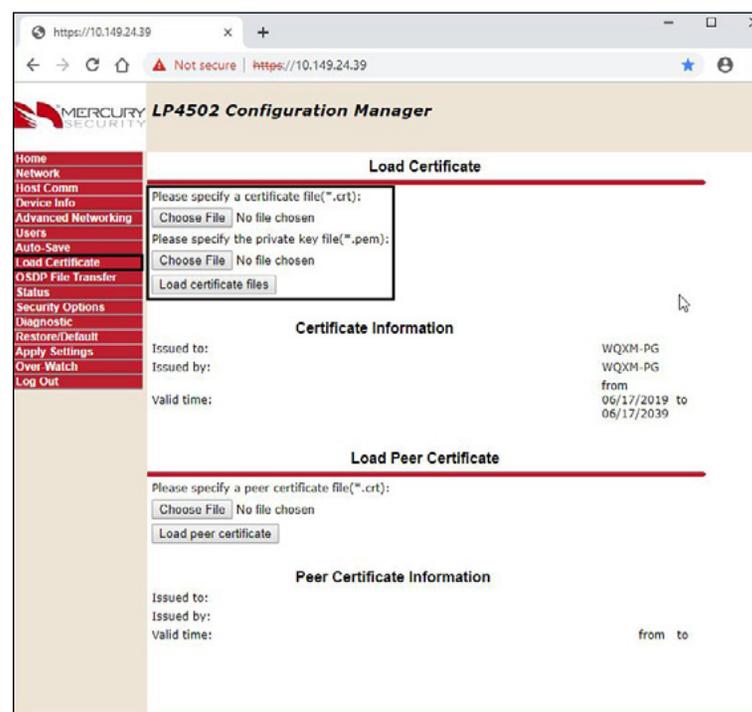
3 HARDWARE INSTALLATION

8. Click on the **Apply Settings** tab. Click on the '**Apply Settings, Reboot**' button.
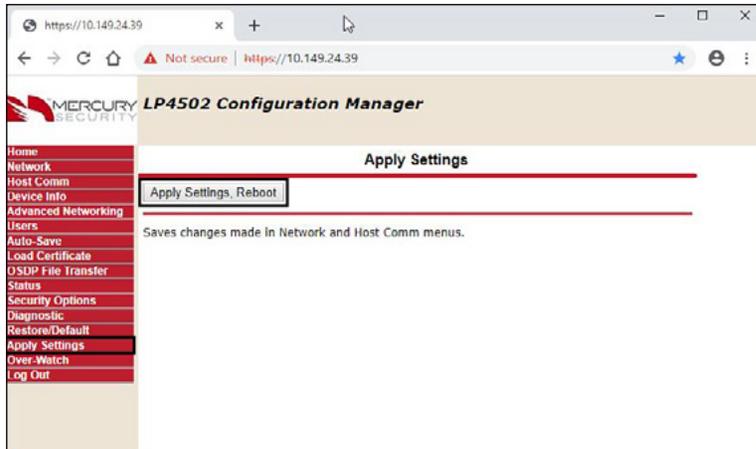
3.2.5.6 Controllers Menu

The Controllers menu option on the WQXM-PG is for configuring controllers when in Mercury Mode. This menu option can be used to verify the status and details of controllers, edit controllers, and update firmware of controllers.
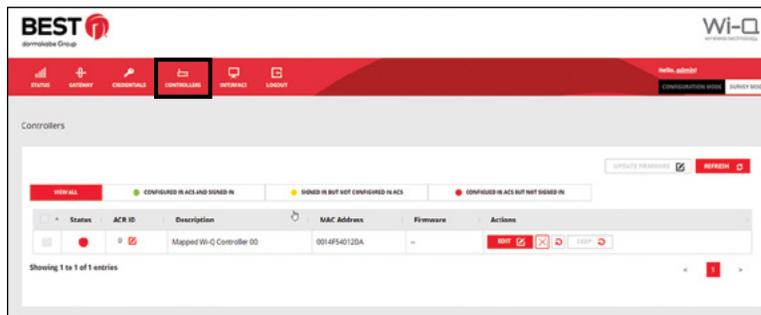
3.2.5.6.1 Filtering the List of Controllers

The top ribbon has 4 buttons that allow for viewing of all controllers, filtering only controllers that are configured in the ACS and signed in, filtering controllers that are signed in but not configured in the ACS, and filter controllers that are configured in ACS but not signed in.
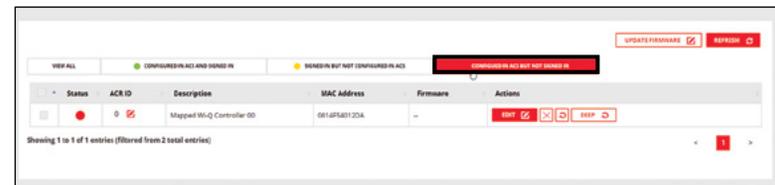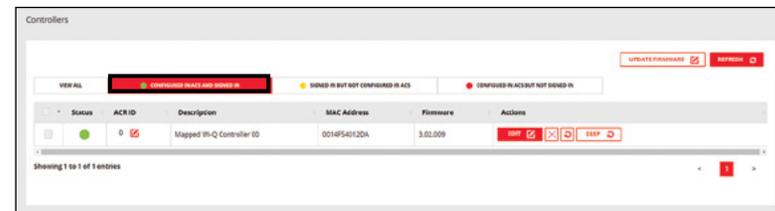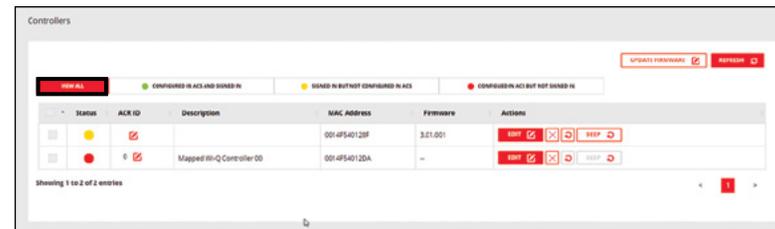
3   HARDWARE INSTALLATION

3.2.5.6.2 Controllers Information Dialog

In the center of the screen is a scrollable/selectable dialog that contains information about each controller. It contains 7 columns.

1. **Controller Selection —** This column can be used to check the box next to a controller for individually or multiply selecting controllers for updating firmware.
2. **Status —** This column shows the current status of each controller.
3. **ACR ID —** This column shows the current ACR ID and allows changing the ACR ID for each controller via the box with a pencil ✏️ in it.

    NOTE: The ACR ID can also be edited in the Controller Edit page covered in section 3.2.5.6.3.

4. **Description —** This column shows the description of each controller. The description can be changed in the Edit page.
5. **MAC Address –** This column shows the MAC Address for each controller.
6. **Firmware —** This column shows the version of firmware that each controller has loaded.
7. **Actions —** This column contains 4 buttons.
    - **Edit** `EDIT ✏️` **—** This button launches the edit menu for this controller which will be covered in section 3.2.5.6.3.
    - **Delete Controller** `✕`**—** This button will deep reset the controller and permanently remove the controller's configuration information in the WQXM-PG Gateway. If this controller were to be reassociated with the Gateway in the future all previously setup settings (ACR setting, beacon rate, etc.) would need to be reconfigured.
    - **Soft Reboot** `↻`**—** This button performs a soft reboot of the controller without deleting its configuration.

The controller will automatically re-associate with the WQXM-PG Gateway and acquire any configuration changes that may have occurred while it was offline.

- **Deep Reset** `DEEP ↻` **—** This button will deep reset a controller and disassociate it with the WQXM-PG Gateway. The controller's configuration (ACR setting, beacon rate, etc.) is saved within the Gateway and will be resent to the controller if the Gateway were to be re-associated with the Gateway in the future.

3.2.5.6.3 Controller Edit Page

The Edit Controllers page has 3 main sections.
1. The Details panel contains the following 4 pieces of information:
    - MAC Address
    - Model Number
    - ACR ID
    - Description of the Controller

NOTE: The buttons in this panel allow the ability to edit the ACR ID and the Controllers Description.

3   HARDWARE INSTALLATION

2. The Channels and Settings panel contains the following 3 config-
    urable pieces of information:
    - Selected Channels
    - Beacon Time (in seconds)
    - Beacon Offline (Count) – The number of consecutive
      Beacon Time intervals that the controller fails to commu-
      nicate with the WQXM-PG Gateway before the controller
      is flagged offline.

NOTE: Best practice is to configure this value to be 5 or above. The
Save and Cancel buttons on this panel only apply to changes on this
panel.

3. The Transactions panel contains 63 configurable types of trans-
    actions that can be enabled, disabled, and set to priority. Priority
    transactions will immediately be communicated from the con-
    troller to the WQXM-PG Gateway. Transactions not flagged as
    priority will queue up and be sent at the next beacon interval.

NOTE: Saving changes to the selected transactions is done via the
Save button at the bottom of the Transactions panel. At the bottom

of the Transactions panel are buttons to enable all the transac-
tions, disable all of the transactions, enable all transactions for
priority, and clear all priority, which removes priority from all
transactions.

3.2.5.6.4 Firmware Update
The Controller Firmware update dialog function is launched by
selecting one or more controllers from the Controllers page and
then click on the **'Update Firmware'** button.

3 HARDWARE INSTALLATION

This will launch a dialog box where the firmware update file can be browsed to.
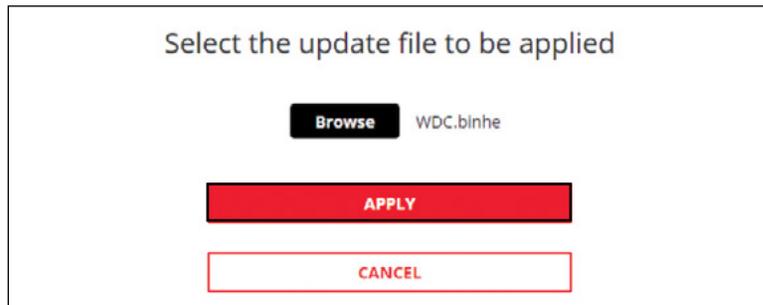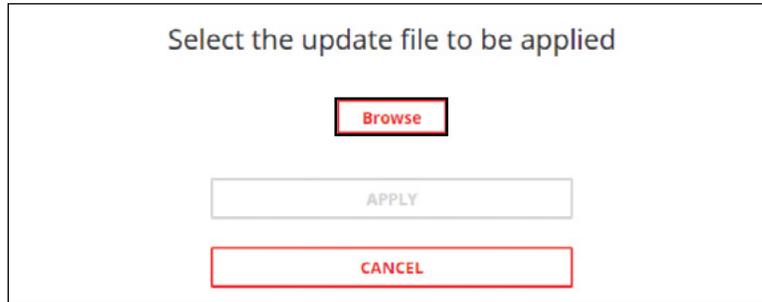
After the firmware binhe file has been selected click the '**Apply button'** to update firmware on the previously selected devices.

A message will appear confirming that the firmware update has been initiated.
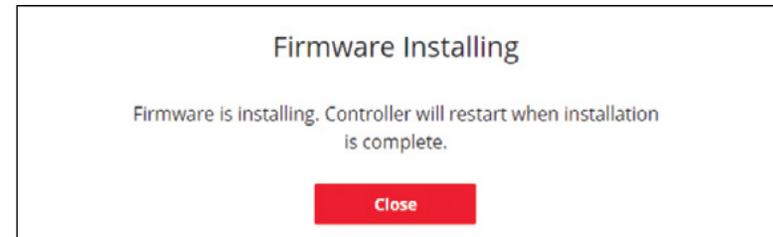
NOTE: If desired, the firmware update progress can be monitored in the Controllers section of the Status page.

3.2.6 Install Wireless Access Controllers (Task 5) Installing a Wireless Access Controller

The Wi-Q Technology Wireless Access Controller (WAC) provides an optional, cost effective way to retrofit an existing hard-wired application, or where the installed controller may be obsolete or unable to handle additional controller inputs. It supports Wiegand Compatible Keypad controllers and is configured and monitored in the Access Control Software, just like a standard controller.

NOTE: Please contact your dormakaba representative at (800) 392-5209 and select option 3, for a list of compatible controllers.

3   HARDWARE INSTALLATION
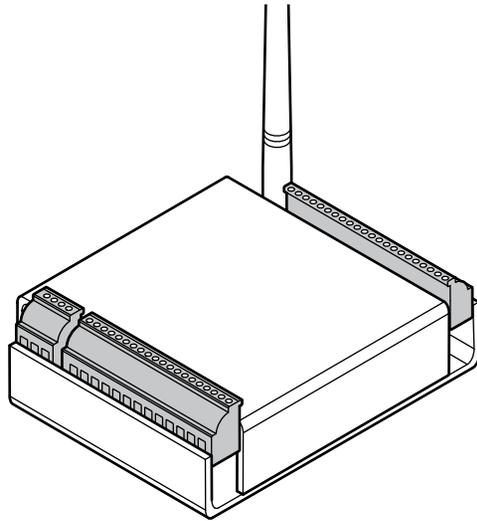
Using the Wireless Access Controller (Figure 12), controllers or other I/O devices can be added to an overall wireless solution without the high cost of installing conduit such as RS485 or CAT5 to the controller. Position the controller at the door or where suitable above the ceiling tile.

The most common installation site is inside an existing protected area such as a locked room or other secure enclosure, or above the door in the ceiling.

3.2.6.1 Installation

Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

WARNING: Wireless Access Controllers are intended for use in indoor or protected area. For other applications, such as outdoor use, contact the factory for the appropriate NEMA enclosure. Changes or modifications not expressly approved by dormakaba could void the user's authority to operate the equipment.

3.2.6.2 Wireless Access Control Wiring

The Wireless Access Controller (WAC) can be installed with its own 12 VDC power supply or slaved to the existing installation. Figure 13 is a wiring diagram illustrating both configurations.

Figure 13   Connecting Devices to a WAC
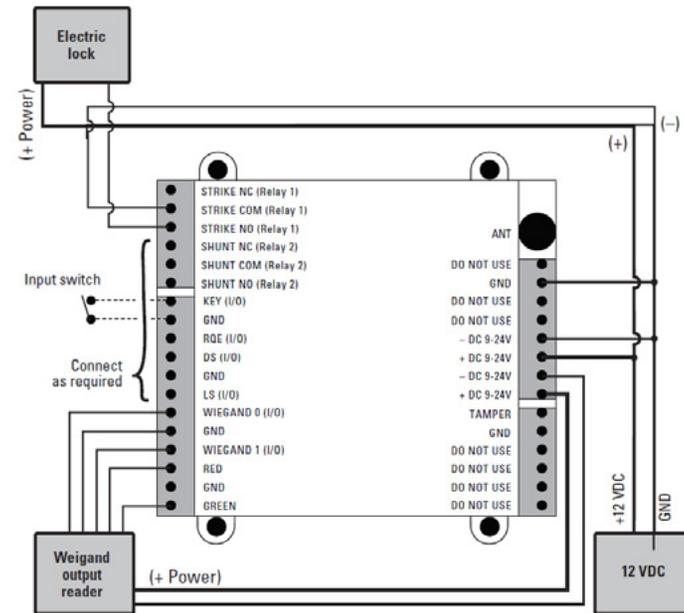
3 HARDWARE INSTALLATION

Once the WAC is installed and all points connected, it will be recognized by the ACS as a controller in the system. The WAC is configured in an almost identical manner as a controller.

3.2.6.3 Resetting the WAC
The Wireless Access Controller (WAC) may occasionally need a soft reset or a factory reset.

A soft reset would be required if the WAC has stopped communicating with the Gateway and an anti-tamper event does not re-establish communication. To reset the WAC, push and hold the reset button located on the controller board next to the antenna inlet until the first green LED flash. Release immediately after the first green LED flashes.

The deep reset restores the WAC to factory default. To deep reset the WAC, push and hold the reset button on the WAC located next to the antenna and wait until the 3 slow red LED flashes.

3.2.7 Install Wireless Door Controllers (Task 6)
This section provides general instructions for installing the wireless door controllers. Complete instructions for installing locks are packaged with the hardware.

3.2.7.1 Before Beginning
Before beginning, take a few moments to review the following considerations:
- Record the device MAC address before installing device. This is needed when configuring the controller in the ACS or the LP4502 Mercury Interface Board.

- Wi-Q and Omnilock Technology Locks will work from -31°F to 151°F.

NOTE: Extreme heat will cause a reduction in wireless signal strength and can cause a loss of connectivity while the heat remains.

NOTE: Alkaline batteries cease to operate if they reach a temperature of -20°F.

Wi-Q Technology Controllers are designed for use on 1-3/4-inch doors. If the locks will be installed on non-standard doors, contact dormakaba Customer Service for more information.

Lockset instructions are given for right-hand doors (as determined from outside the door). If the door is left hand, see the instructions provided with the lockset for hand change instructions.

If the locksets will be installed on unprepared (un-drilled) doors, use the template provided with that specific lockset.

Please refer to the instructions provided with the lock to complete these steps. Once this is done, check controller operation as described in the following paragraphs.

3.2.7.2 Check Controller Operation
Verify controller operation using the steps appropriate for the controller type (proximity card, magnetic card or keypad). If the system does not operate properly, see the troubleshooting table, at the end of the section.

3 HARDWARE INSTALLATION

Proximity Card Check

If the Wi-Q Controller has a proximity card reader, the temporary operator card (supplied with the controller) and the sign-on card (created in the ACS Software or the web interface of the LP4502 Board) are both required to sign on the readers.

To perform a proximity card verification:

1. Select the temporary operator card supplied with the controller.
2. Present the temporary operator card to the proximity bezel at the face of the reader. The light on top of the controller will flash green once and the lock will unlock. After 3 seconds, the controller will flash green and lock.
3. While unlocked, check for proper lock operation.

Magnetic Card Check

If Wi-Q Controller has a magnetic card reader, the temporary operator card (supplied with the controller) and sign-on card (created in the ACS Software or the web interface of the LP4502 Board) are both needed to sign on the readers.

To perform a magnetic stripe card verification:

1. Determine if the magnetic card type is Track-1, Track-2 or Track-3.
2. Select the temporary operator card supplied with the controller.
   - If the lock is a WDC, slide the magnetic card through the slot in the face of the reader bezel with the print facing the left and the arrow toward the door.
   - If the lock is an Omnilock, insert the magnetic card into the top of the reader with the print facing you and the arrow pointing down and pull back out.

- The magnetic stripe on the card should be aligned with the "V" mark by the card slot. The lights on the top of the controller will flash green once and unlock, then during the open delay time, it will flash green five times. Once this occurs, the card controller light will flash red and lock.

3. While unlocked, check for proper lock operation.

Keypad Check

If the controller is a keypad type, perform the following steps:

WDC

1. At the keypad, enter the default Programmer-ID, 1234#. The green light on top of the card controller will flash once and the lock will unlock, then during the open delay time, it will flash green five times. Once this occurs, the controller red light will flash and the lock will relock.
2. While unlocked, check for proper lock operation.

OMW

1. At the keypad, enter the default Programmer-ID, 1234. The green light on top of the card controller will flash once and the lock will unlock, then during the open delay time, it will flash green five times. Once this occurs, the controller red light will flash and the lock will relock.
2. While unlocked, check for proper lock operation.

3 HARDWARE INSTALLATION

3.2.7.3 Troubleshooting the Controllers

3.2.7.3.1 Troubleshooting WDC and Omnilock Locks

If the mechanism doesn't unlock, refer to the following table:

LED Lights	Sounder	Try
Single Red Flash	--------	Use the card at a moderate speed.
Red Flashes	3 short tones	Use the temporary operator card provided with the lock, or perform a deep reset to restore to the factory default settings. (The lock may already be associated/programmed.)
Green Flashes	--------	Check the motor connection on the Omnilock.
Green and Red Alternating Flashes	--------	Check that the motor connection is secured on the WDC at the connector between the wiring harnesses and at the controller board.

3.2.7.3.2 Troubleshooting the WAC/WDC

LED Lights	Sounder	Try
Single Red Flash	--------	Use the card at a moderate speed.
Red Flashes	3 short tones	Use the temporary operator card provided with the lock, OR perform a deep reset to restore to the factory default settings. (The lock may already be associated/programmed.)
Green Flashes	--------	Check the motor connection on the Omnilock.
Green and Red Alternating Flashes	--------	Check the motor connection to the WDC Board as well as the harnesses. Verify all connections are tight.

For additional troubleshooting instructions, see the service manual for the hardware components and assemblies.

Once the installed controllers have been tested, they are ready to be signed into LP4502 or ACS. To do this, the ACS must be installed on the host computer or the LP4502 configured and communicating with the ACS as well as the WQXM-PG Gateways. At a minimum, the segment should be created and the Gateways online and communicating to the ACS or the LP4502 Mercury Controller Board. For more information see the "Configure Gateways (Task 4)" section on page 25.

3 HARDWARE INSTALLATION

Once this is done, return to the site and sign on the controllers. For more information see the "Sign On and Configure Controllers (Task 7)" section on page .

3.2.8 Sign On Wi-Q Controllers (Task 7)

To successfully sign on Wi-Q Controllers, the temporary operator card as well as the sign-on cards created in the ACS or the WQXM-PG are both needed. If the Wi-Q Reader has a keypad, the keypad code can be used to sign the readers onto the WQXM-PG or the ACS.

NOTE: Card offsets other than "0" are not supported for the WQXM-PG in Mercury Mode. If a card offset other than "0" is used the end result is that the ACS will not be able to report which ACR a transaction came from.

Keypad Method

1. **Test the Reader** – Enter 1 2 3 4 # on a WDC or 1 2 3 4 on the WAC or Omnilock. The reader should display the green LED and Unlock.

2. **Prepare the Reader to Receive the Sign-on Code** – Enter 5 6 7 8# on the WDC or 1 2 3 4 on the WAC or Omnilock.

3. **Enter the Segment's Unique Sign-on Key** – Enter the 6-digit sign-on key in the ACS or on the segment tab of the WQXM-PG followed by the # key if the reader is a WDC. If the reader is a WAC or Omnilock, the # key is not needed.
   - □ **Example –** Key sequence for the WDC: 1 2 3 4 # 5 6 7 5 6 7#
   - □ **Example –** Key sequence for the WAC or the Omnilock: 5 6 7 8   5 6 7 5 6 7

NOTE: The keypad codes 5678 and the sign-on key should be presented in rapid success. It is important to not let the controller time out before entering the 6-digit sign-on code. There should be no more than a 2 second delay between the 5 6 7 8 (#) keypad entry and the 6-digit code keypad entry.

Magnetic Card Method

1. Test the reader. Swipe the temporary operator card through the reader bezel of the WDC or wall mounted magnetic reader wired to a WAC.
   - The WDC controller will display a brief green LED and unlock.
   - The Omnilock controller will display a brief green LED and unlock.
   - The WAC will display a green LED on the controller board and unlock.
2. Present the temporary operator badge to the reader, look for the green LED and the reader to unlock.
3. Immediately present the sign-on card to the reader.

Proximity Card Method

1. Test the reader. Present the temporary operator card to the face of the reader bezel on the WDC, Omnilock or wall mounted proximity reader wired to a WAC.
   - The WDC controller will display a brief green LED and unlock.
   - The Omnilock controller will display a brief green LED and unlock.
   - The WAC will display a green LED on the controller board and unlock.

3 HARDWARE INSTALLATION

2. Present the temporary operator badge to the reader, look for the green LED and the reader to unlock.
3. Immediately present the sign-on card to the reader.

If the reader does not successfully sign on to the WQXM-PG, repeat the steps above ensuring that the delay between the temporary badge or keypad code 5 6 7 8 and the segment sign-on key or card is minimal. Waiting too long between steps will result in controller sign-on failure.

Behavior	Try This
3 red flashes at the end of the sign-on sequence.	Try signing the controller in again.
Temporary card does not unlock the reader.	Deep reset the controller and try again.
Tried to sign on the reader multiple times without success.	Verify the keypad code is correct or the card that is used as the segment sign-on card is correct.

3.2.8.1 Verify Sign-on Success
Once the readers have received the sign-on sequence, the readers will each display a LED sequence indicating they are initiating the radios and will indicate sign-on success or failure.

WDC
The blue LED will illuminate when the radios are initiating. The controller will alternate the red, green and blue LED's while the controller seeks to establish communication with the WQXM-PG Radios.

If the controller sign-on was a success, the final 3 LEDs will be 3 quick green flashes accompanied by 3 tones that go up in pitch. The blue LED will flash as the controller receives information from the controller.

If the sign-on procedure was not a success, the final LEDs will be 3 quick red flashes accompanied by 3 beeps that go down in pitch. LED activity will stop.

WAC
The blue LED will illuminate when the radios are initiating. The controller will alternate the red, green and blue LED's while the controller seeks to establish communication with the WQXM-PG Radios.

If the controller sign-on was a success, the final 3 LEDs will be 3 quick green. The blue LED will continue to flash as the controller receives segment information from the WQXM-PG.

If the sign-on procedure was not a success, the final LEDs will be 3 quick red flashes. LED activity will stop.

Omnilock
The Omnilock is not equipped with a blue LED, therefore the light sequence is different than that of the WDC and WAC. The controller will alternate the red and green while the controller seeks to establish communication with the WQXM-PG Radios.

If the controller sign-on was a success, the final 3 LEDs will be 3 quick green flashes. LED activity will continue while the controller receives segment data from the WQXM-PG.

3   HARDWARE INSTALLATION

If the sign-on procedure was not a success, the final LEDs will be 3 quick red flashes. LED activity will stop.

3.2.8.2 Verify Signal Strength and Packet Ratio Using Survey Mode

Prior to installation, the Wi-Q Technology Site Survey feature in the WQXM-PG should have been used to verify basic controller signal strength. Once the controllers are signed on, the WQXM-PG Site Survey webpage can be used to verify the signal strength and packet transfer ratio to verify all information is being sent successfully to and from the Wi-Q Controllers.

To do this, please do the following:

1. Log in to the WQXM-PG by navigating to the IPv4 address using an Internet browser.
2. Click on the '**Survey Mode**' button.
3. Check the boxes next to the reader(s) connected to the Gateway to select them for the survey.
4. Click on the '**Start Log**' button to begin surveying the locks.
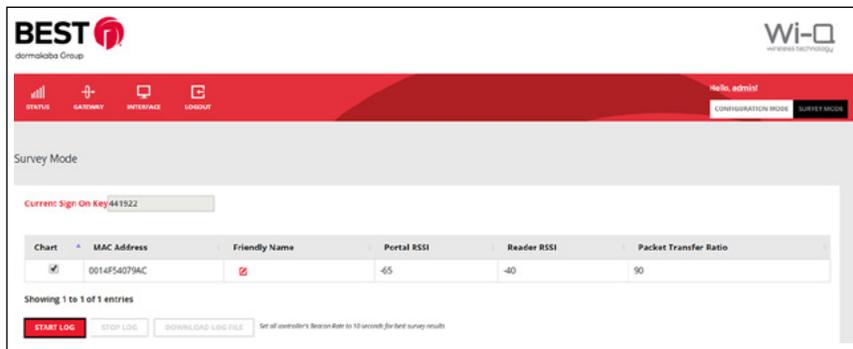
The WQXM-PG Gateway will begin logging the portal packet ratio, the reader packet ratio as well as the signal strength at the portal and the reader.

Portal Signal Strength
The Portal RSSI value indicates how well the portal receives signal from the door controller and should be -75dB or better. The Survey Mode charts in the WQXM-PG denotes the lowest limit by the blue dashed line in the Signal Strength chart. If the Portal RSSI value is below the limit, please reposition the Gateway or the antennas to improve signal strength. It may also be possible that another portal is required for adequate coverage.

3 HARDWARE INSTALLATION

Reader Signal Strength

The Reader RSSI value indicates how well the reader is receiving signal from the Gateway and should be at least -65dB or better denoted on the chart with the red dashed line. If the Reader RSSI value is below the recommended limit check the reader antenna and the gray antenna jumper cable to verify there is not damage to them.

Also, it may be required the WQXM-PG or the antennas need to be repositioned so the reader can hear the WQXM-PG more clearly.

Packet Transfer Ratio

It is recommended that the packet transfer ratio rate is 80% or better. This value indicates how efficient the communication is between the readers and the WQXM-PG as well as how much interference maybe in the area. If this value is below 80%, the reader will not receive all the configuration data. To troubleshoot the portal packet ratio, update the reader statistics to poll every 10 seconds instead of once a day while running the survey tool in the WQXM-PG. Please remember to change the reader statistics back to only poll 1 time a day once the troubleshooting is complete.

NOTE: OnGuard 7.4 and higher with Wi-Q Interfaced installations using the WQXM-PG, require global statistics update poll rates to be made during troubleshooting. Please contact dormakaba Technical Support for direction at 800-392-5209 or via email at bas.support.best.us@dormakaba.com.

It is imperative to consider the wireless environment and the placement of the Gateway and its antennas during troubleshooting. The Gateway communicates on the 2.4 GHz frequency using the IEEE 802.15.4 channels. If the location has other wireless devices or networking using the 2.4GHz frequency, please orient the antennas away from these devices to manage interference. It may be required to work with local personnel to manage the wireless environment to prevent causing interference with other Wi-Fi installations and products.

For any questions regarding the functionality of this integration please contact dhwsupport.dormakaba.com/hc/en-us with the subject line: WQXM-PG Wi-Q Gateway Setup and User Guide.

T91416_K