Wi-Q
wireless technology

WQXM-PG WI-Q™ GATEWAY
SETUP AND USER GUIDE

Wireless Intelligence That Stands Alone

BEST

dormakaba Group

dormakaba

CREDITS |COPYRIGHT

DOCUMENT DISCLAIMERS
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.

DOCUMENT DISCLAIMERS
FCC/IC Certification

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

Approved Antennas

Configuration Description	Antenna Part number
Gateway with rubber duck antennas	Pulse W1030W
Gateway with Ceiling Mount Omni-directional antenna	PCTEL (Maxrad) MC2400PTMS-MA
Gateway with Interior/Exterior Wall mount directional antenna	Mobile Mark (Comtelco) CMT-B36247V
Gateway with Exterior omnidi-rectional 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.

dormakaba TECHNICAL SUPPORT

Address

dormakaba USA Inc.

6161 East 75th Street

Indianapolis, IN 46250

Web Page

www.bestaccess.com

Phone

1-800-392-5209

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS
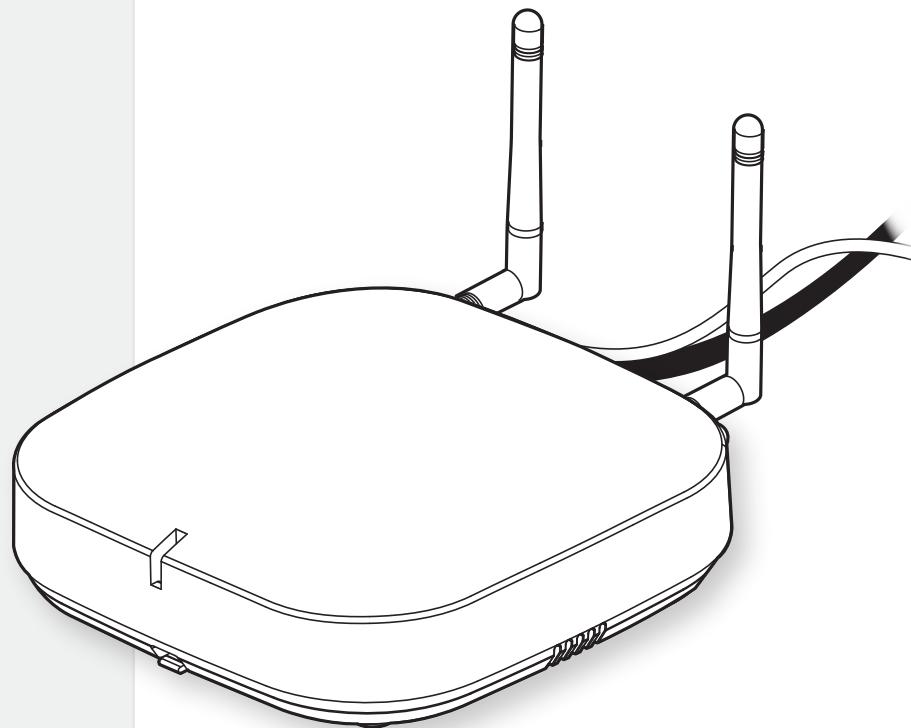
TABLE OF CONTENTS

TABLE OF CONTENTS

1 SYSTEM OVERVIEW

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
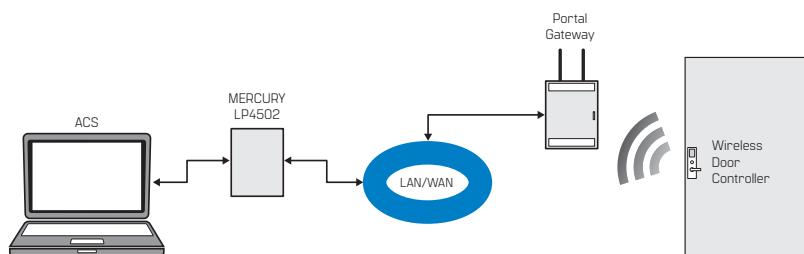
1.1 MERCURY LP4502 AND WI-Q COMPONENTS

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 128 Wi-Q controllers. This interface board is used for 3rd party integration into Access Control Software.

3. **WQXM-PG Portal Gateway**
   The Portal 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

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 (20)

❑   Task 2: Position Gateways
See Page (22)

❑   Task 3: Install Gateways
See page (25)

❑   Task 4: Configure Gateways
See page (26)

❑   Task 5: Install Wireless Access Controllers
See page (42)

❑   Task 6: Install Wireless Door Hardware
See page (44)

❑   Task 7: Sign on Wi-Q Controllers
See page (47)

3 HARDWARE INSTALLATION

3 HARDWARE INSTALLATION

The Mercury LP4502 access panel locates the Wi-Q portals 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 Prox/Wiegand, 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 before or concurrent with hardware installation. For more information, see "Sign on Wi-Q Controller (Task 7)" on page .

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 128 Wi-Q controllers. This interface board is used for 3rd 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. The Gateway communicates to the host computer through web services via either Ethernet 10/100 BaseT or an approved commercial RF carrier-enabling a wireless solution end-to-end. Transmit range from Gateways will vary based on building construction. Cabled and directional antennas are also available to manage range within the buildings.

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 retrofit 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 12V DC or an optional 12/24V DC power supply, sealed, lead acid battery pack. 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 22.

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 omnidirectional 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 Competed 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.

❑   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:

- 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
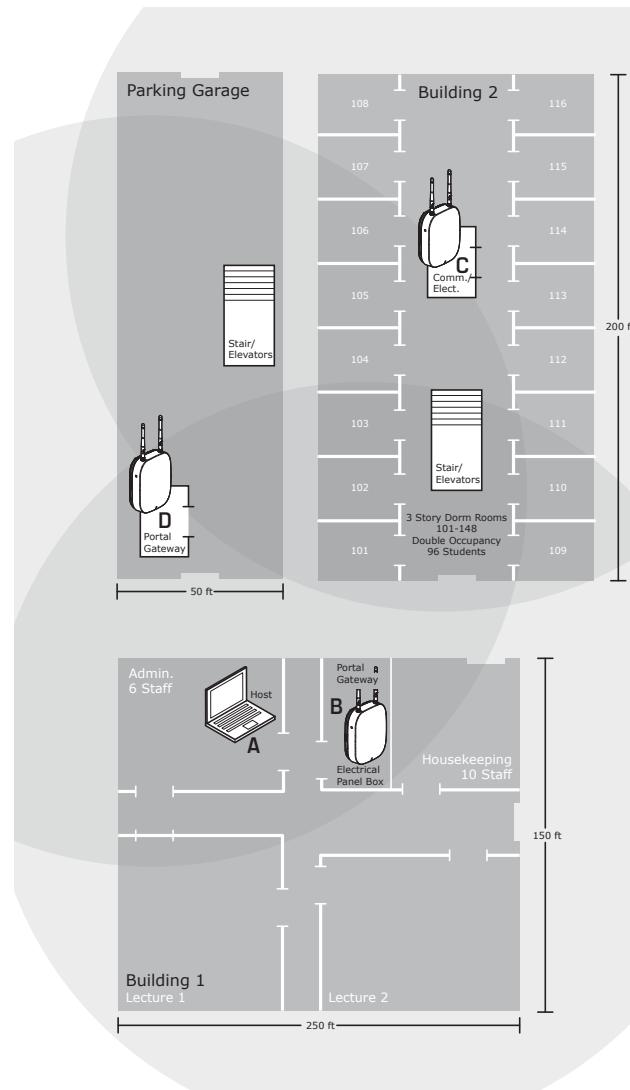
3   HARDWARE INSTALLATION

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 3rd 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 SURVEY MODE under Position Gateways (Task 2) on page (22).

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 figure 4.

Note: The MAC address is most commonly shown or inside the device. It is important to record this number before installing the device.

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
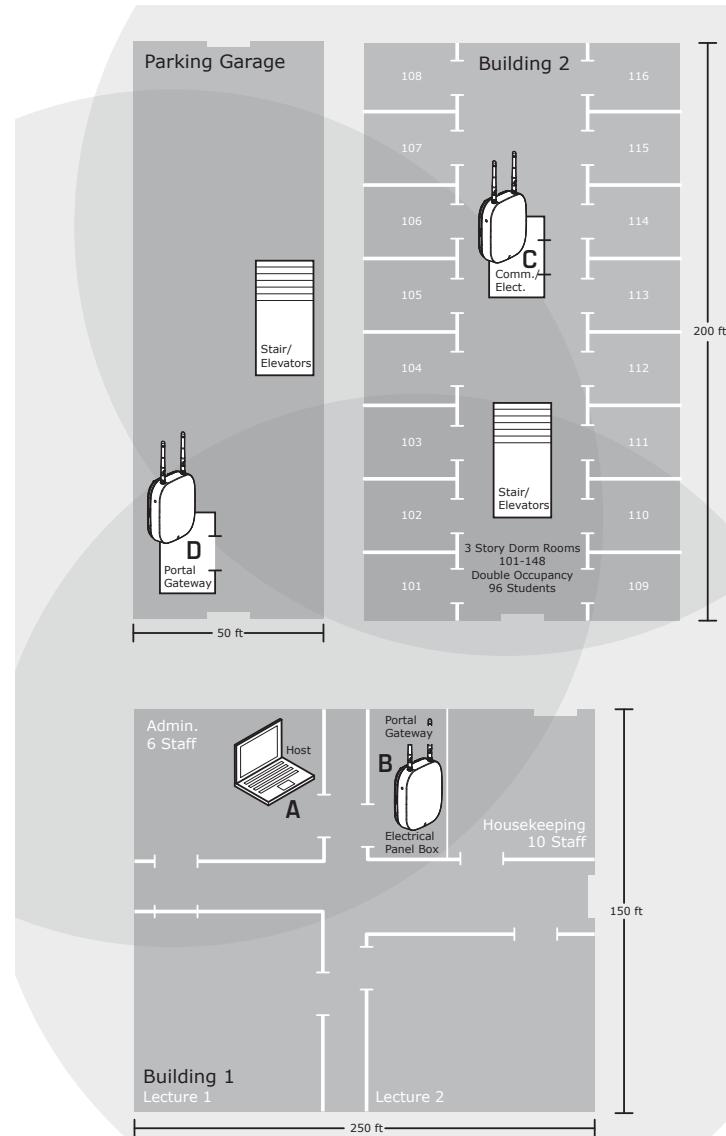
3   HARDWARE INSTALLATION

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, Gateways 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 two available antenna types.

3   HARDWARE INSTALLATION

Figure 5: Selecting the antenna type that best suits the needs of the installation.
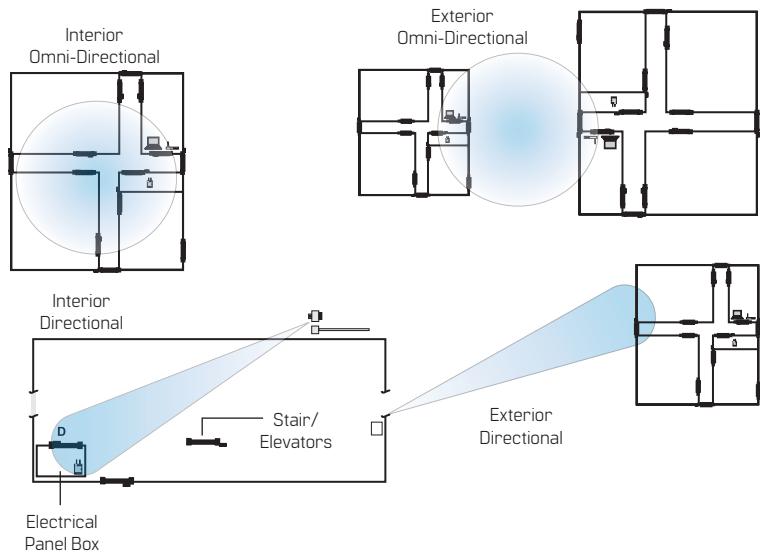
3.2.3.2 Power Supply

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(s) 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, the number of gateway's needed for adequate coverage as well as troubleshooting signal and packet transfer ratio issues.

WIRELESS

1. Power on the WQXM-PG.
2. Using the smart device's Wi-Fi, locate the WQXM-PG's wireless network and connect to it.
3. Using a smart device's browser, navigate to the WQXM-PG wireless network IP Address: 192.168.1.200.
4. Login to the Gateway's webpage using the previously updated username and password.
   - Default Username: **admin**
   - Default Password: **password**
5. Once connected, click on the 'Survey Mode' button in the upper right corner of the gateway webpage.
6. 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 static 6 digit sign on key (987654) to sign a demo reader into the gateway.

3   HARDWARE INSTALLATION

8. Noting 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.

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 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 blue 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 inter-

3   HARDWARE INSTALLATION

ference 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 pre-vent causing interference with other Wi-Fi installations and prod-ucts.

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 in-stalled, 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.

Approx. 5' 6" High (eye level)

Portal Gateway
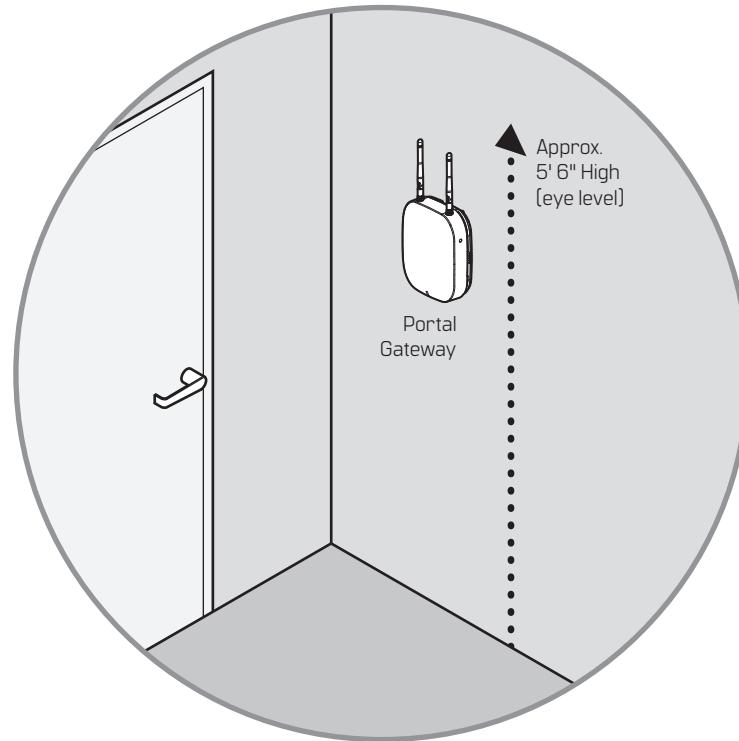
3.2.4.1 Connecting the Gateway and Verifying Operation

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.
2. Insert the Ethernet cable into the Ethernet connection on the bottom of the Gateway. The Link Status Light at the top of the gateway will flash red while the gateway is

3   HARDWARE INSTALLATION

booting. When it flashes Green, it is ready to be config-
ured. 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

Figure 8: Connecting the Gateway to Power and Ethernet Connections.

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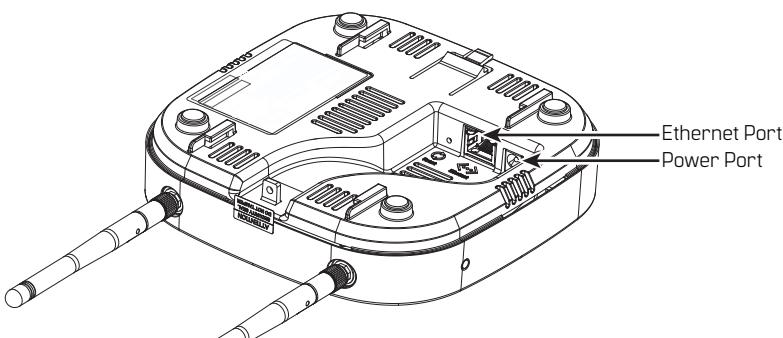
Note: If no protected area is available, consider positioning the
Gateway inside a locked enclosure designed for that purpose. Con-
tact your dormakaba dealer for more information.

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 gateway's 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 wire-
lessly 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 config-
uration 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 Eth-
ernet adapter on the Gateway if a Class C IPv4 network is in use.

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 ad-
dress on this network is 192.168.1.200. To temporarily enable the
portal's wireless network for configuration, push the Wi-Fi enable
button on the side of the WQXM-PG Wi-Q Gateway. See figure 9.

3   HARDWARE INSTALLATION

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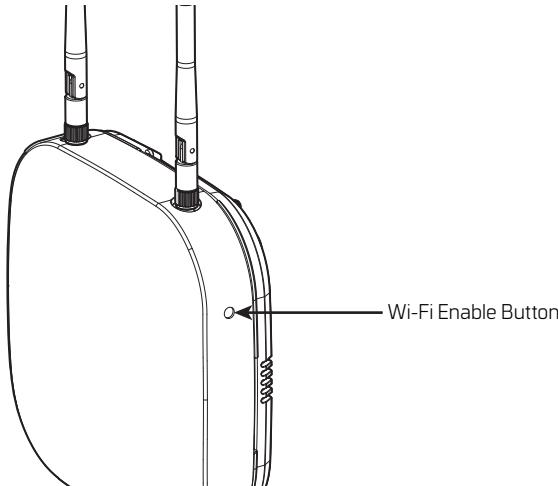
- Connect to the WQXM-PG wireless network using a smart device (ex... tablet, cell phone) or laptop Wi-Fi Connection.
- The Gateway's Wi-Fi SSID will appear in the list of available wireless connections.

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 into using the steps above try the following troubleshooting steps:
1. Press Wi-Fi button on the side of the Wi-Q Gateway.
2. Reconnect to the Gateway's unique wireless network connection.
3. Try to login again.
4. Power Cycle the Gateway and attempt to login again once 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

Reset Button
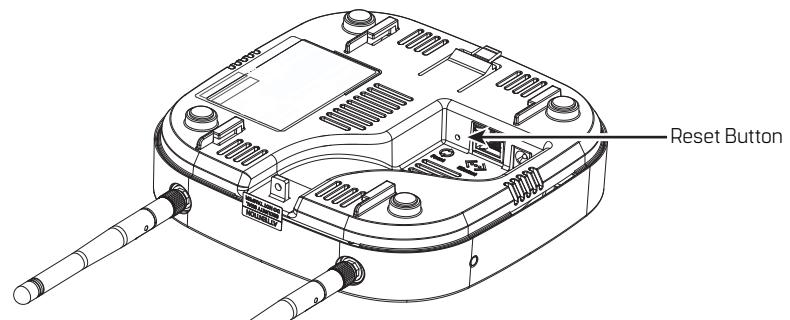
3   HARDWARE INSTALLATION

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 into the gateway. Follow the steps previously mentioned to enable Wi-Fi, reconnect, and login.

* The Deep Reset will take the settings on the board and restore them to the factory defaults.

3.2.5.2 Configure the WQXM-PG Gateway
Open the device's browser window and navigate to the gateway's default IP address: 192.168.1.200.

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

3.2.5.2.1 Login Screen
Login 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 into, the manage profile screen will appear prompting to change the username or password. The user will be prompted to change the password every time the gateway is logged into until it has been changed to something other than the default. 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.
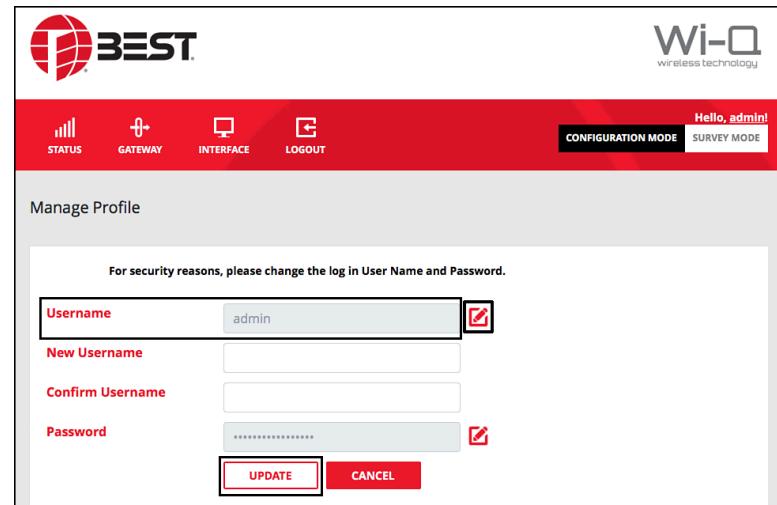
3   HARDWARE INSTALLATION

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.

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.
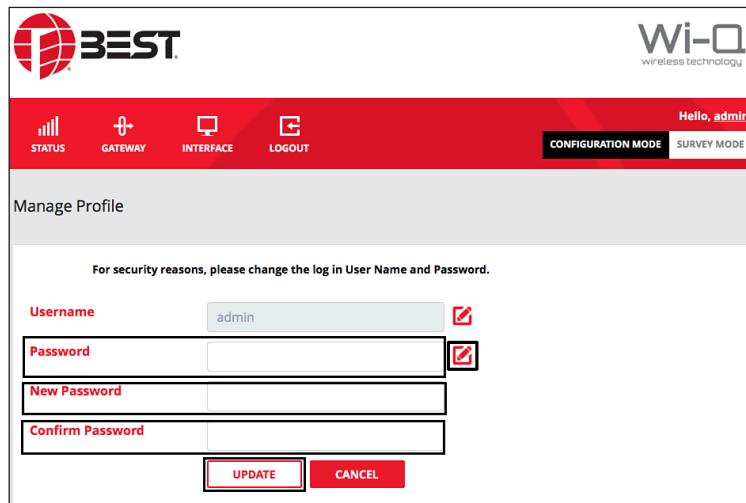
3.2.5.4 Gateway Status Window

The gateway status page provides and 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.

Gateway Status	TECHNICIAN LOG	ADVANCED LOG	REFRESH

DETAILS

IP Address	10.189.17.16
MAC Address	0014F5208C06
Time of Last System Reboot	10/01/2019 15:16:21
Current Sign On Key	887452
Associated Controllers on Gateway	8
Wi-Fi IP Address	192.168.3.200
Wi-Fi SSID	

Radio Channels Allowed	25,26
Radio 1 Channel	25
Radio 1 PAN ID	21214
Radio 2 Channel	26
Radio 2 PAN ID	21247

3 HARDWARE INSTALLATION

3.2.5.4.1 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** – 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 addressed 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.

3.2.5.4.1.1 Wireless Controllers

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

WIRELESS CONTROLLERS

ACR ID	MAC Address	Radio Channel	Associate Time	Last Beacon Time	Pending Operations %	Package Count	Firmware Version	Portal RSSI	Reader RSSI	Flags	Pending Message
	0014F540D26D	25	10/01/2019 04:41:45	10/03/2019 09:19:26		0	3.02.005	-69	-31	32043	-|------|-
	0014F540D28B	25	10/01/2019 04:26:21	10/03/2019 09:19:56		0	3.02.005	-70	-70	32043	-|------|-
	0014F540D270	26	10/01/2019 03:46:56	10/03/2019 09:20:01		0	3.02.005	-66	-38	32043	-|------|-
	0014F540D2B1	26	10/01/2019 03:57:58	10/03/2019 09:19:29		0	3.02.005	-75	-46	32043	-|------|-
	0014F540D247	26	10/01/2019 04:01:42	10/03/2019 09:20:22		0	3.02.005	-55	-28	32043	-|------|-
	0014F540D26C	26	10/01/2019 05:29:43	10/03/2019 09:20:22		0	3.02.005	-53	-23	32043	-|------|-
	0014F540D26C	26	10/02/2019 10:49:29	10/03/2019 09:20:22		0	3.02.005	-53	-23	32043	-|------|-
	0014F540D246	26	10/01/2019 04:21:55	10/03/2019 09:20:30		0	3.02.005	-50	-27	32043	-|------|-

- **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.
- **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.

3   HARDWARE INSTALLATION

- **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 into the ACS, connected, configured, and not locked to the gateway.
  - □ 30053 – Controller is taking configuration updates.
  - □ 32043 – Controller is signed into 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)

3.2.5.4.1.2 Generate Logs
Click on the '**Generate Logs**' button in the upper right corner of the gateway status screen.

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 the software technical support engineers.

3 HARDWARE INSTALLATION

To generate logs, do the following:

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.

<div style="background:#E2231A;color:#fff;display:inline-block;padding:4px 12px;font-weight:bold;">TECHNICIAN LOG</div>

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, 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

<div style="background:#E2231A;color:#fff;display:inline-block;padding:4px 12px;font-weight:bold;">ADVANCED LOG</div>

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***

3.2.5.5 Gateway Menu

The GATEWAY page has multiple sections of this page 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 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, update to the Portal Service Port as well as SSL certificate generation and enablement.

3 HARDWARE INSTALLATION
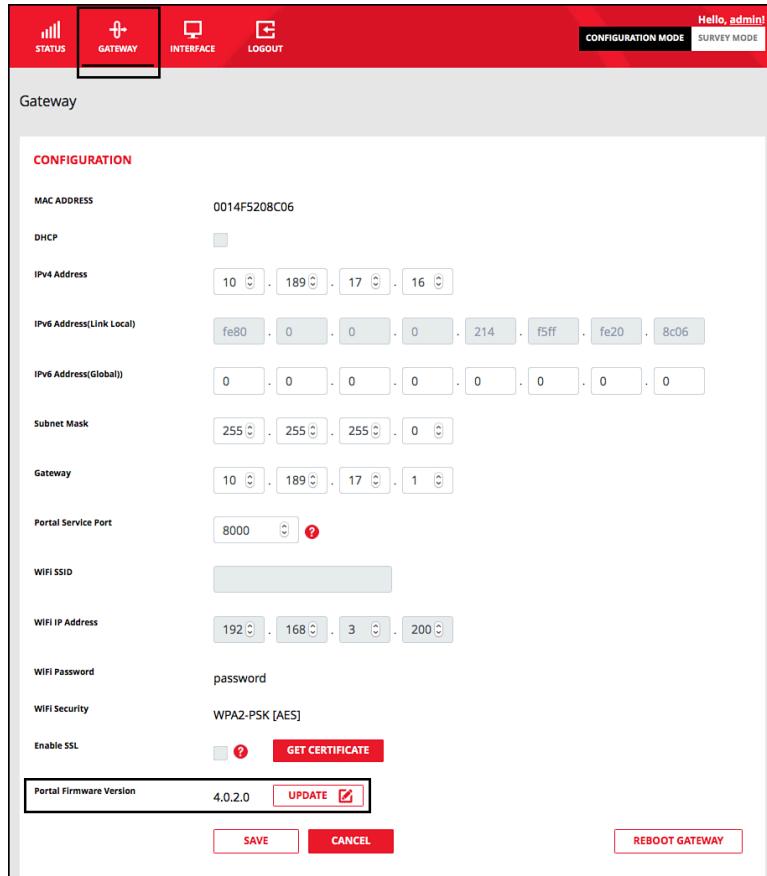
3.2.5.5.1 Assigning an IP Address

Configuration changes on the gateway are only available via the portal's wireless network after the "**Enable Wi-Fi**" button has been pushed. The IP address for the WQXM-PG wireless network is a static 192.168.3.200 and cannot be changed. Once the IP Address has been updated, the enable Wi-Fi button can be de-

pressed 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.

3.2.5.5.1.1 DHCP

A static 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.

3.2.5.5.1.2 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.

3.2.5.5.1.3 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.

3.2.5.5.1.4 Enabling SSL

AES encryption is used for the wireless communication from the gateway to the radios. 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.

3.2.5.5.1.5 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.
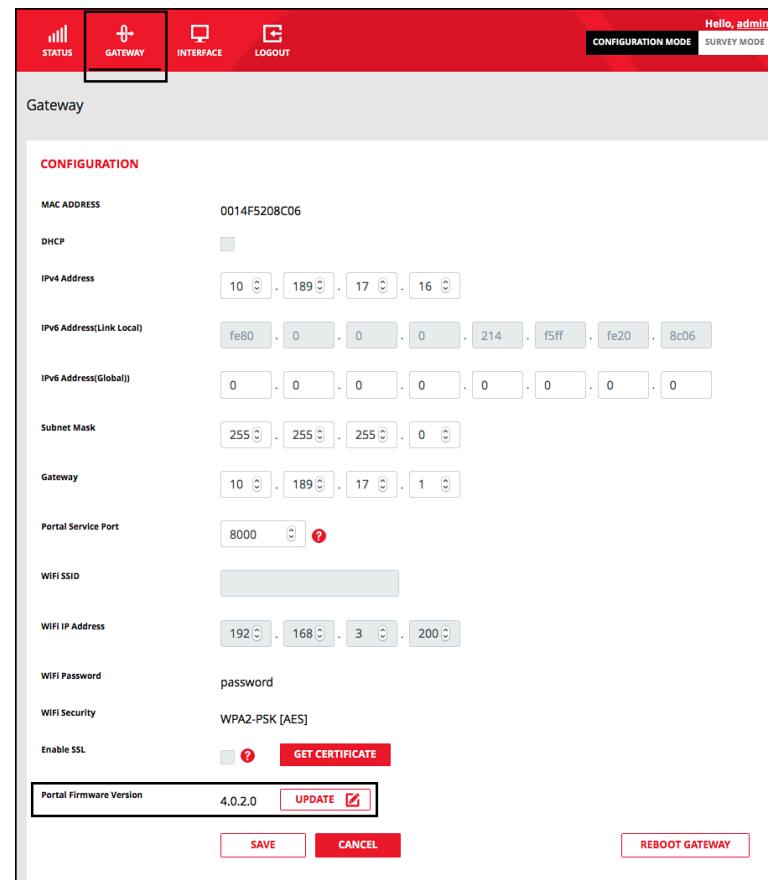
3   HARDWARE INSTALLATION

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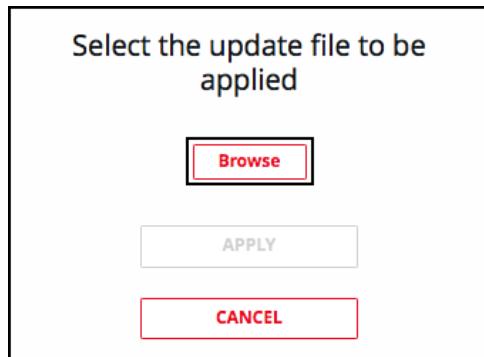
3. Browse to the previously extracted .gzhe portal firmware file and click the '**Open**' button to upload the file.
4. The selected file will be listed in the pop-up window. Verify it is correct and click the '**Apply**' button.
5. The firmware will be applied to the gateway. The gateway's LED will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

3.2.5.5.1.6 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 save 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.

3.2.5.5.1.7 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 deep reset button next to the Ethernet inlet. 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
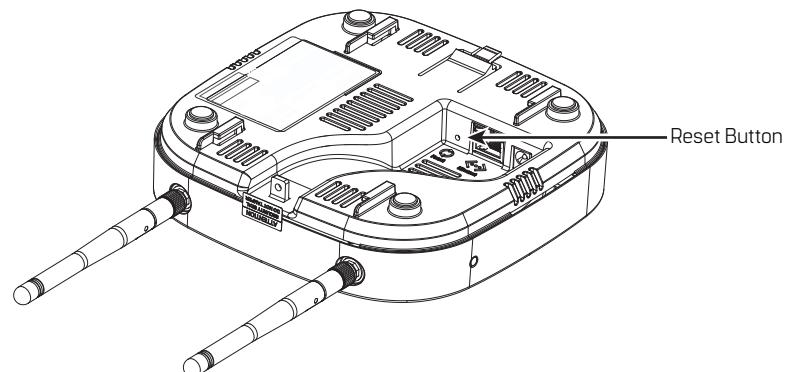
3   HARDWARE INSTALLATION

3.2.5.6 INTERFACE MENU

The interface menu option on the WQXM-PG is for use when the gateway will be used in a 3rd party ACS. This menu option will allow the WQXM-PG to be configured to communicate with the mercury LP4502 board.

3.2.5.6 1 Enable Mercury Mode

Mercury mode is enabled when using the WQXM-PG with a 3rd party ACS and the mercury controller board LP-4502 or MP-4502 v1.29 or higher.

1. Click on the **"Interface"** menu option 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. If SSL will be used, 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.
   □ Click on the **'GET CERTIFICATE'** button to download the portal's SSL certificate.
   □ Click on the **'Save'** button to save the SSL setting.
   □ Upload the SSL certificate into the ACS.
4. Click on the **"Update"** button to apply the settings.
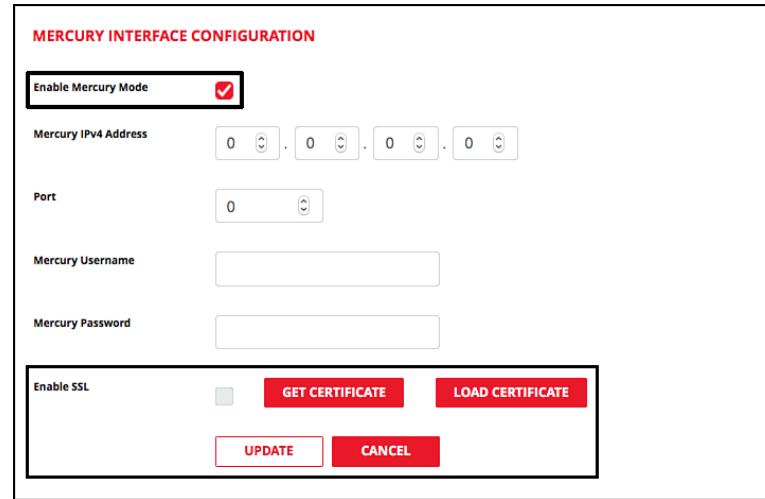
5. Once checked, the '**Enable Mercury Mode**' will validate this change and display a pop-up notification window.
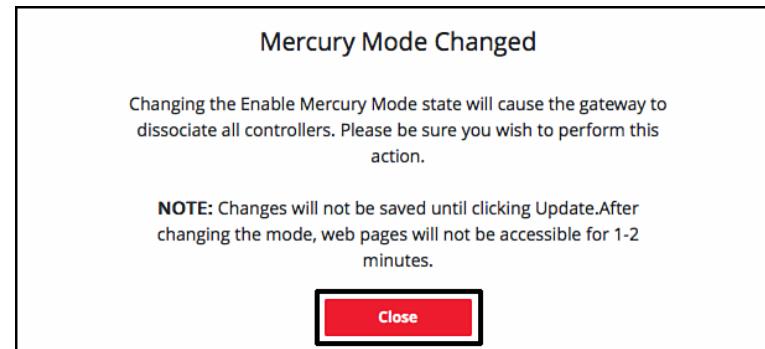
6. Click the '**Close**' button and fill out the remaining fields on the Mercury Interface Configuration screen as follows:
7. Enter the Mercury LP4502 IPv4 Address.

3 HARDWARE INSTALLATION

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

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

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.
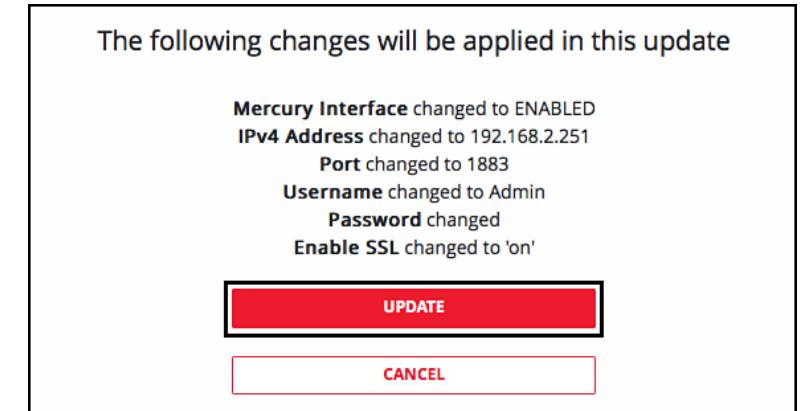
12. The system will then validate all changes and pop open a notification window showing "**Save Successfu**l". Click the "**Close**" button to continue.

3.2.5.6.2 Update the IP Configuration for the LP4502 Mercury Board

- Make sure all the dip-switches on the LP4502 Mercury board are in the OFF state/position (see below). If they are not, then turn them to the OFF position and reboot the LP4502.
- Next, go to the UI (user interface) webpage for the Mercury board by typing the IP address of the board into a web browser's URL.

3 HARDWARE INSTALLATION

3.2.5.6.3 Adding Sign-On Credentials to the WQXM-PG (Gateway)

From the Portals UI homepage click on the '**CREDENTIALS**' tab.
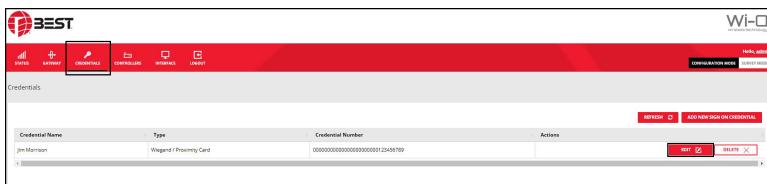
From the Credentials page, click on the '**ADD NEW SIGN ON CREDENTIAL**' button on right side of screen.

Note: If "Wiegand/Proximity" card is chosen, a prompt will appear to confirm and/or edit the "Bit Length" for the card.
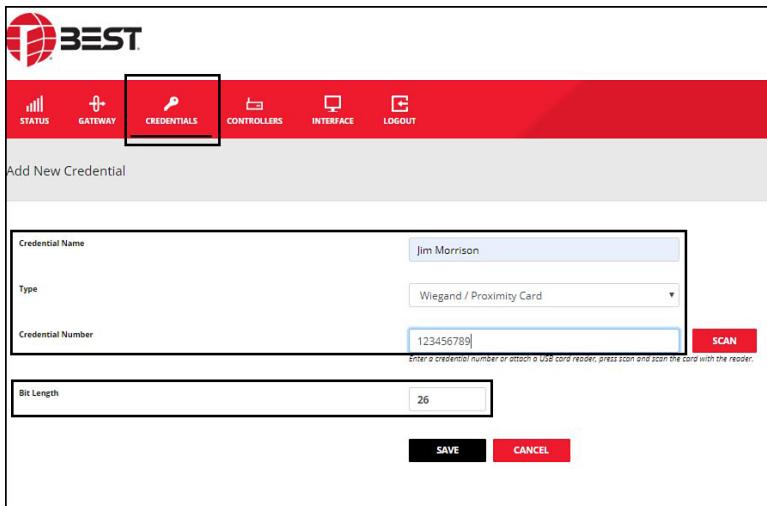
Enter credential criteria as prompted:

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

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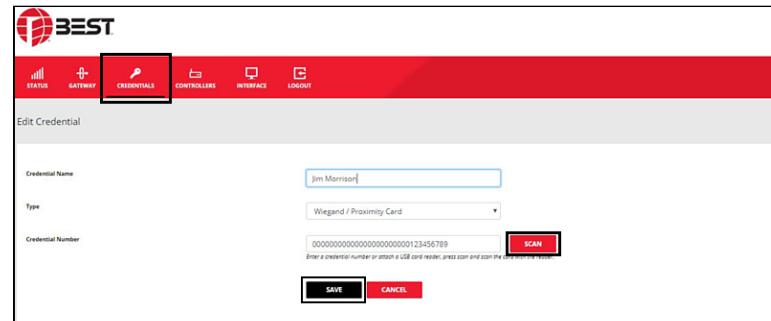
When all credential information has been entered, click '**SAVE**' on the Edit Credential page.

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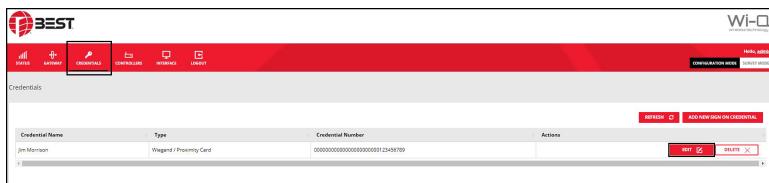
Credentials can be deleted from the Credentials screen as well. Choose the user to be removed, click the '**DELETE**' button.

Click '**CONFIRM**' on the pop-up notification window when editing is complete.
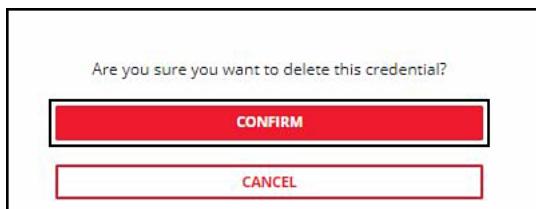
3.2.5.6.4 Sign On Wi-Q Controllers to the WQXM-PG

The enrollment process for the Wi-Q controllers requires a default token followed by a sign-on token and can take 20-30 seconds. 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 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.

3.2.5.6.4.1 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 six-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 six-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.

3 HARDWARE INSTALLATION

3.2.5.6.4.2 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.

3.2.5.6.4.3 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.

3.2.5.6 Configuring the Mercury Panel for use with the WQXM-PG

3.2.5.6.1 Logging into the Mercury Board UI (User Interface)

1. Open an internet browser (Google Chrome is recommended)
2. Log into 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 (aka...LP4502 Configuration Manager) will appear as follows:
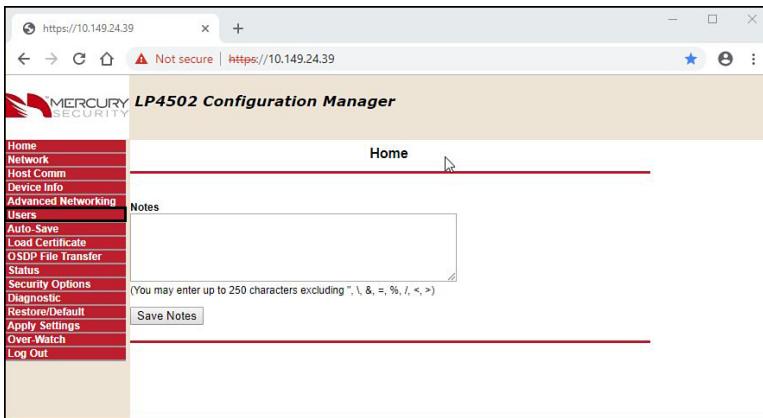

3.2.5.6.2 Updating/Creating Users & Passwords

1. Log into the LP4502 Configuration Manager (aka...LP4502 Mercury Board Interface).
2. Click on the "**USER"** tab on the left-side of the LP4502 home screen.
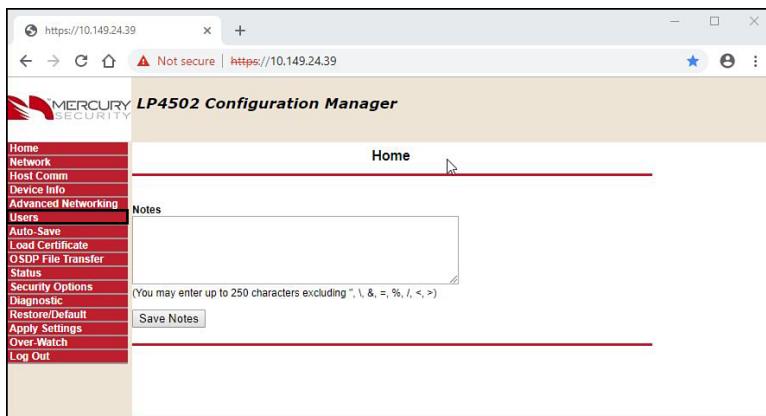
3.2.5.6.3 Load SSL Certificates into the Mercury panel

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

Note: Steps 1-4 are one-time configuration after hard reset of the Mercury panel.

1. **Network** – Set IPV4 configuration as required.
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 alternate login 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 set in the WQXM-PG.
6. **Apply Settings** – Click on the '**Apply Settings, Reboot**' button to apply the settings and reboot the Mercury board. The board will take approximate XX minutes to complete this process. Please wait X minutes before attempting to log back into the Mercury board.
7. **From the Load Certificates tab**
   □ Choose certificate file: **client.crt**.
   □ Choose private key file: **client.pem.**
   □ Press "**Load certificate files."**

Note: The certificate can be generated through the WQXM-PG or through a 3rd party.

3 HARDWARE INSTALLATION

8. Click on the **Apply Settings** tab. Click on the "**Apply Settings, Reboot**" button.

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

3 HARDWARE INSTALLATION

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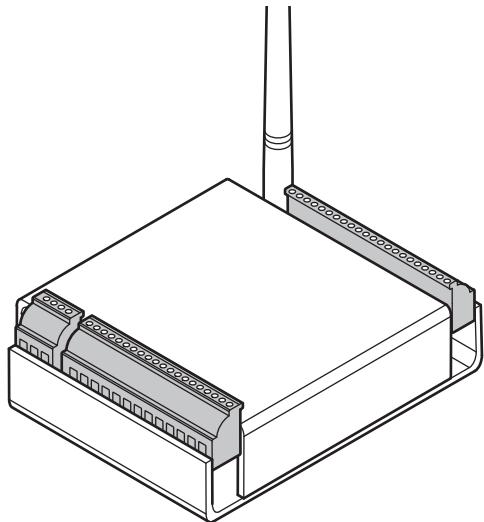
Using the Wireless Access Controller (Figure 12), controllers or other I/O devices can be added to an overall wireless solution without the high cost of installing conduit such as RS485 or CAT5 to the controller. Position the controller at the door or where suitable above the ceiling tile.

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. Dotted lines represent optional connections for the slaved configuration.

Figure 13 Connecting Devices to a WAC
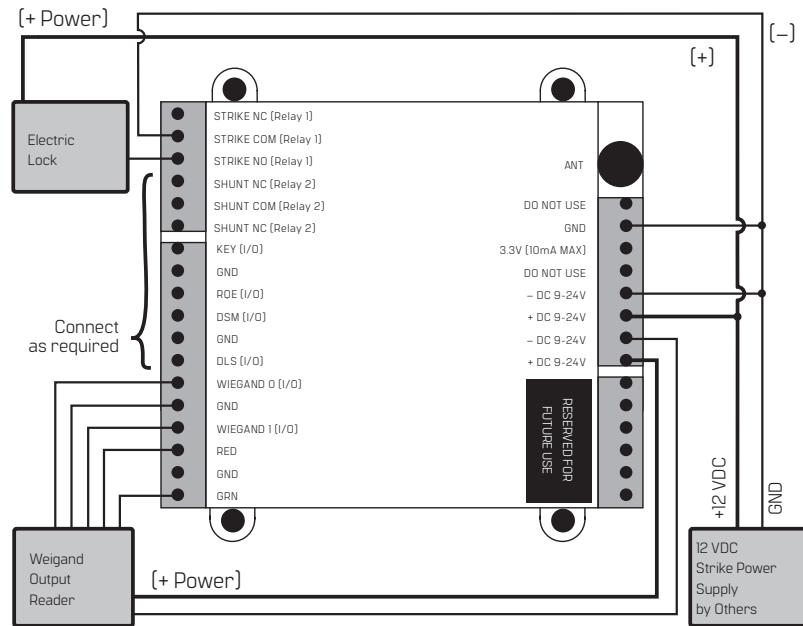
3   HARDWARE INSTALLATION

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.

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.

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

Troubleshooting WDC and Omnilock locks

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

LEDs 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 is secured on the WDC at the connector between the wiring harnesses and at the controller board.

Troubleshooting the WAC\SDC

LEDs 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, 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 (26).

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.

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 six-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.
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.

3   HARDWARE INSTALLATION

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, therefor 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.

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

3 HARDWARE INSTALLATION

3.2.8.1 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 ratio to verify all information is being sent successfully to and from the Wi-Q controllers.

To do this, please do the following:
1. Login 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 Survey**' button to begin surveying the locks.
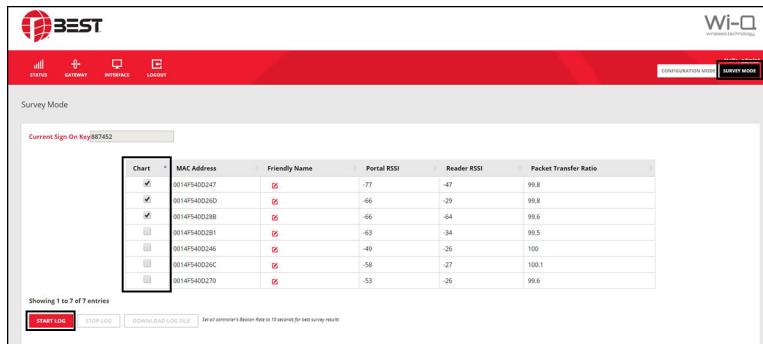
The WQXM-PG Gateway will begin logging the portal packet ratio, the reader packet ratio as well as the signal strength at the portal and the reader.

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.
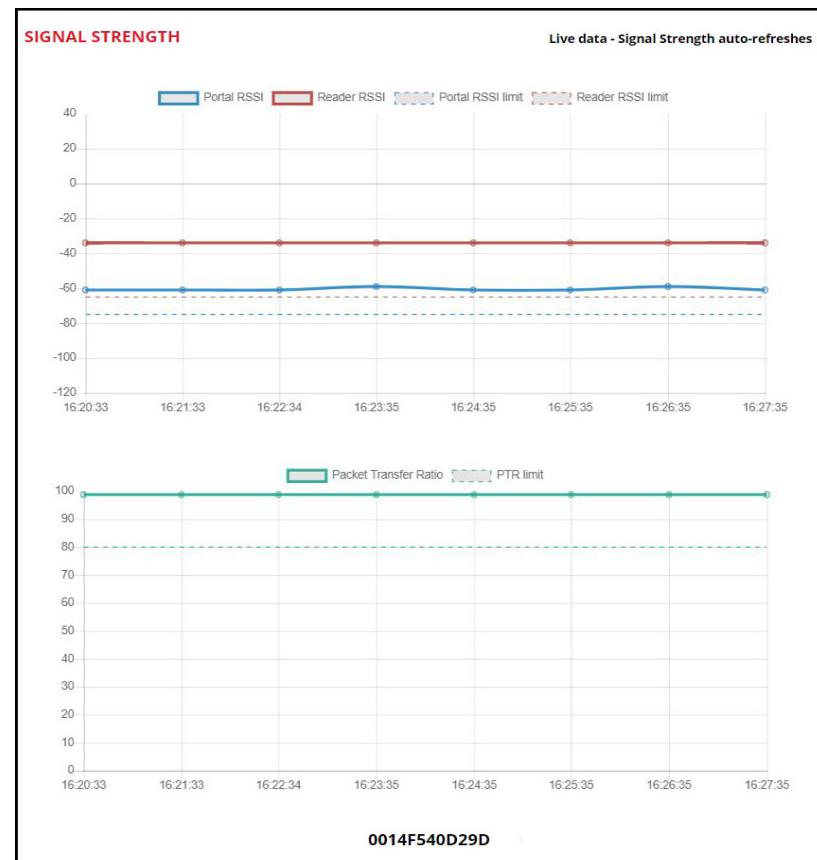
3   HARDWARE INSTALLATION

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 blue 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 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 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.