BEST®
dormakaba Group

Wi-Q
wireless technology

BEST WI-Q™ ONGUARD

INTERFACE USER GUIDE

Wireless Intelligence That Stands Alone

Credits/Copyright

Information in this document is subject to change without notice and does not represent a commitment on the part of dormakaba USA Inc. The software described in this document are furnished under a license agreement or nondisclosure agreement.

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. Please call dormakaba USA Inc. at (800) 392-5209 if you see any errors or have any questions. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose, without the express written permission of dormakaba USA Inc.

This document is distributed as is, without warranty of any kind, either express or implied, respecting the contents of this book, including but not limited to implied warranties for the publication’s quality, performance, merchantability, or fitness for any particular purpose. Neither dormakaba USA Inc., nor its dealers or distributors shall be liable to the user or any other person or entity with respect to any liability, loss, or damage caused or alleged to be caused directly or indirectly by this publication.

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

T85203_H February 2024

FCC/IC Certification

CAUTION: Please keep the Wi-Q Gateway 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 LICENCE-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 LICENCE. 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. This Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.Cet appareil numérique de la classe [B] respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

Approved Antennas

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

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.
    - 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 mm2) for patch cords, 24 AWG (0.21 mm2) 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.

Table of Contents

1 Overview

2 Hardware Installation

3 Software Installation

4 Software Configuration and Use

5 Advanced Troubleshooting

1 Overview

This manual is your complete guide to the integration of BEST Wi-Q wireless hardware into your BEST Access Control System. It provides detailed steps for installing hardware and software and configuring your system.

Note BEST Wi-Q Technology can also be integrated into an OnGuard system.

The information in this guide is presented in a linear manner; however, tasks to install hardware and software and configure the system for the first time do not necessarily progress in a linear manner. You will find a Setup Checklist at the end of this section to take you through the initial setup and configuration tasks in a logical sequence. If you are unfamiliar with the terms used in wireless technology, you may want to refer to the Glossary included in this manual as Appendix A.

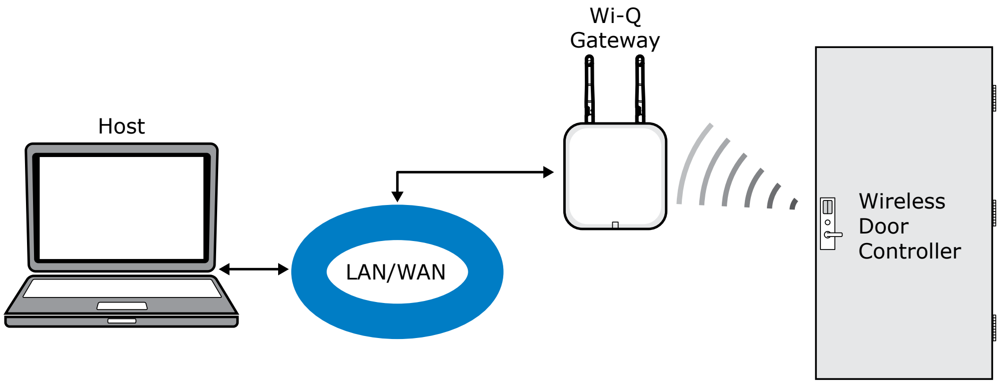
System Overview

A BEST Access Control System with integrated Wi-Q Technology combines powerful access control software with Wi-Q Gateways, Wireless Access Controllers, and multiple controller formats that work together to enable all decision making at the door. The BEST® Wi-Q system runs remotely with no need for hard wiring, providing innovative access control in any environment. The Wi-Q Interface system is versatile, so you can create a whole new system, retrofit existing hardware, and include various video camera, alarms, and inputs/outputs.

Basic Wi-Q Interface Components

A basic Wi-Q Interface system has four components: (1) a Server running the System Software, (2) a host computer with the Wi-Q Interface Software installed, (3) a Wi-Q Gateway, and (4) a Wireless Controller at the door. Figure 1 is a simple diagram showing these four components.

Figure 1 Four Basic Components



1 **Server with System Software**

Existing systems and operators can continue to work with OnGuard as normal to control Wi-Q wireless components.

Note The System Software must be installed and operational prior to the installation and operation of the Wi-Q components.

2 **Wi-Q Interface software**

Wi-Q Interface software is installed either on the same computer as the OnGuard Server or another Host computer and set up to translate data between the two systems to allow normal access control functionality.

3 **Wi-Q Gateway**

The Wi-Q Gateway is a wireless device connected to the Host computer through a secure IP address, similar to the way your computer is connected to the internet. It transfers data signals from Wireless Controllers to and from the Host computer. The

Wi-Q Gateway recognizes all Wireless Controllers within its antenna range. One Wi-Q Gateway can control as many as 64 Wireless Controllers in a system.

4 **Wireless 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 Wi-Q Gateway. The Wireless Controller grants user requests according to how they are configured in the System Software.

Note The terms “Controller” and “Lockset” are used synonymously throughout this guide. The System Software uses the term “Reader” to refer to wireless locks, while the Wi-Q Interface Software uses the term “Controller.”

Basic Operation

The system works very simply. A user enters a pass code at a Wireless Controller, either using an access card or by entering a code on a keypad. If the controller recognizes the credential from the configured settings downloaded from the Host via the Wi-Q Gateway to the controller, the door opens. The controller also sends regular signals (beacons) to the Wi-Q to let it know that it’s working properly. If a controller goes offline, the Host receives a message from the Wi-Q Gateway.

Additional System Configurations

Wi-Q Interface supports various system configurations. For example, some locations at your segment may already be hard wired with legacy equipment or additional input or output devices. You can include a Wireless Access Controller that links a hard wired strike and controller with a Wi-Q Gateway. For more information about various applications you can adapt for use with Wi-Q Interface, see “Hardware Overview” on page 13.

Software Overview

Wi-Q provides powerful tools to manage your system. The Wi-Q Interface Software allows you to add Wi-Q Gateways, Controllers and Segment Sign on Credentials to your system. The Configuration Software also allows you to send firmware updates to your Wi-Q Gateways and wireless locksets as they become available. Once your BEST® Wi-Q components are added into OnGuard, you may manage your online and wireless systems together as one.

Setup Checklist

Wi-Q Interface is set up in ten basic tasks. Completing these tasks will ensure you get your 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, you may have someone prepare your computer and install the software concurrently with site plan development and hardware installation. However, you must have the software installed and Wi-Q Gateways 'online' before you can sign on controllers.

Note System setup does not proceed in a linear manner. The following references prompt you to skip around within the Wi-Q Interface User Guide.

❑ Task 1: Develop a Site Plan
See page 17.

❑ Task 2: Position Wi-Q Gateways and Standalone Survey Mode
See page 20.

❑ Task 3: Gather and Organize Segment Data
See page 36.

❑ Task 4: Prepare your Computer
See page 37.

❑ Task 5: Install Wi-Q Interface Software
See page 50.

❑ Task 6: Configure Wi-Q Gateways
See page 67.

- ❑ Task 7: Install Wi-Q Gateways
  See page 25.

- ❑ Task 8: Install Door Hardware
  See page 29.

- ❑ Task 9: Sign on Controllers
  See page 32.

- ❑ Task 10: Configure Software
  See page 70.

2 Hardware Installation

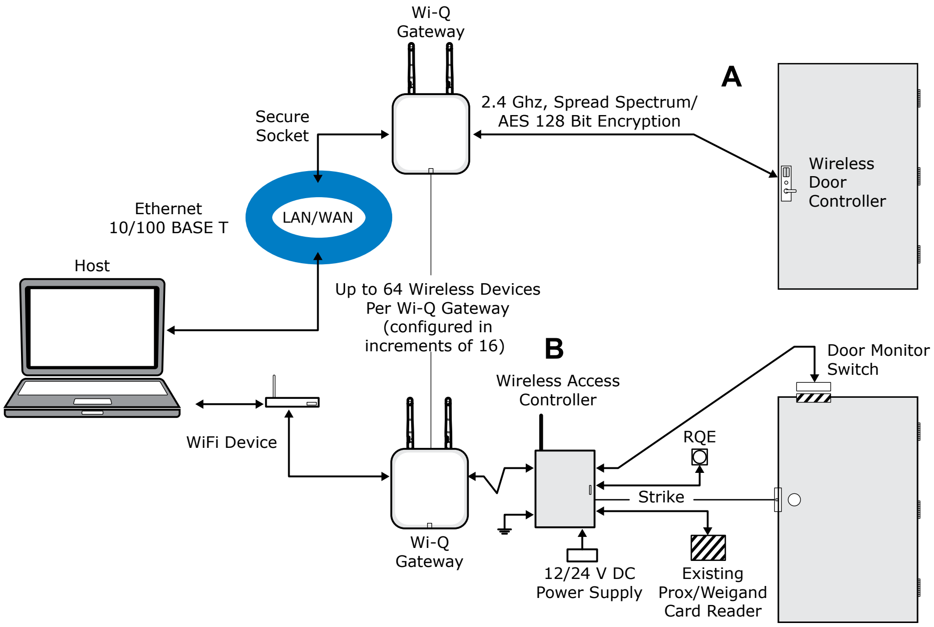
Hardware Overview

Wi-Q Interface integrates wireless hardware into your existing hard-wired system. Wi-Q Interface is designed for versatility so you can retrofit existing Wi-Gateways and include various I/O devices.

Note Once Wi-Q Technology locksets are installed, you will need to sign them on in the Wi-Q Interface Software. Therefore, it is appropriate to install Wi-Q Interface Software before or concurrent with hardware installation. For more information, see “Sign on Controllers (Task 9)” on page 32.

Figure 2 is a block diagram showing various configurations. Wi-Q Interface supports all Wi-Q Technology Wireless Controllers via Wi-Q 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.

Figure 2 Example System Configurations



Wi-Q Gateway

The Standard Wi-Q Technology Wi-Q Gateway is a wireless device connected to the Host computer through a secure IP address, similar to the way your computer is connected to the Internet. It transfers data signals from Wireless Controllers to and from the Host computer. The Wi-Q Gateway recognizes all Wireless Controllers within its antenna range. One Wi-Q Gateway can control up to 64 Wireless Controllers.

Wi-Q Gateways provide bi-directional radio frequency communication between Wireless Controllers and the associated host computer(s). All communications are via secure AES 128-Bit encrypted 2.4 HGz using spread spectrum RF Radio technology. The Wi-Q 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 Wi-Q Gateways will vary based on building construction. Directional antennas are also available to further extend range.

Wireless Controllers

Wi-Q Interface 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 Timezones (per Segment)
- 14000 User Credentials per controller (based on licensing)
- Cardholder access level definition
- Dynamic memory for IDs vs Transactions
- Locally stored and transmitted transactions
- ADA Compliant
- No AC required at door

Wireless Access Controllers

You can retrofit any existing controller configuration to communicate with BEST Wi-Q Gateways using Wi-Q Wireless Access Controllers. You can also use this device 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 12/24 V DC power supply, sealed, lead acid battery pack. They seamlessly integrate existing door hardware into the Wi-Q Interface system, supporting Wiegand-compatible keypad controller inputs.

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

Antenna Types and Applications

To optimize system performance, it is important to position Wi-Q Gateways to receive maximum signal strength from the Wireless Controllers. Once all door hardware has been installed, you will be ready to position Wi-Q Gateways using the Wi-Q Technology Site Survey Tool. 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 Wi-Q Gateways (Task 2)” on page 20.

Installing System Hardware

A system with integrated Wi-Q Technology can operate with BEST 45HQ Mortise locks, BEST 9KQ Cylindrical locks, BEST EXQ Trim, Wireless Access Controllers and Wi-Q Technology Wi-Q Gateways. Detailed installation instructions are provided in the following sections and in the lock instructions provided with the hardware which are included as Appendices to this manual.

What you will need

❑ Engineering drawings or segment map

❑ Wi-Q Technology Site Survey Kit

❑ For keypad controllers, you will need the sign-on credential from the Wi-Q Interface Software.

❑ For magnetic stripe or proximity card readers, you will need the Temporary Operator Card (supplied with the controller) and Sign on Card (supplied in the Wi-Q Interface Software package). You will also need the appropriate magnetic stripe or proximity USB enrollment reader to create a proximity sign-on credential.

❑ Locksets to be installed on doors, including cores and keys supplied with specific model.

❑ Installation instructions for specific lockset brand and model

❑ Wi-Q Gateways

❑ Access to standby power for 120 VAC non-switch circuit for 12 VDC plug-in transformer

❑ 10/100/1 GigE Base-T network connection

❑ Crossover Ethernet cable if direct connection between Wi-Q Gateway and Host will be used.

❑ 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 your lock)

❑ Phillips-head and flat-head screw drivers

❑ Access to the Host, a networked workstation, or wireless laptop computer.

Develop a Site Plan (Task 1)

Before installing Wi-Q Gateways, it is a good idea to develop a general plan for the segment. This plan will guide you in deciding where to install the Wi-Q Gateways. You must consider the following:

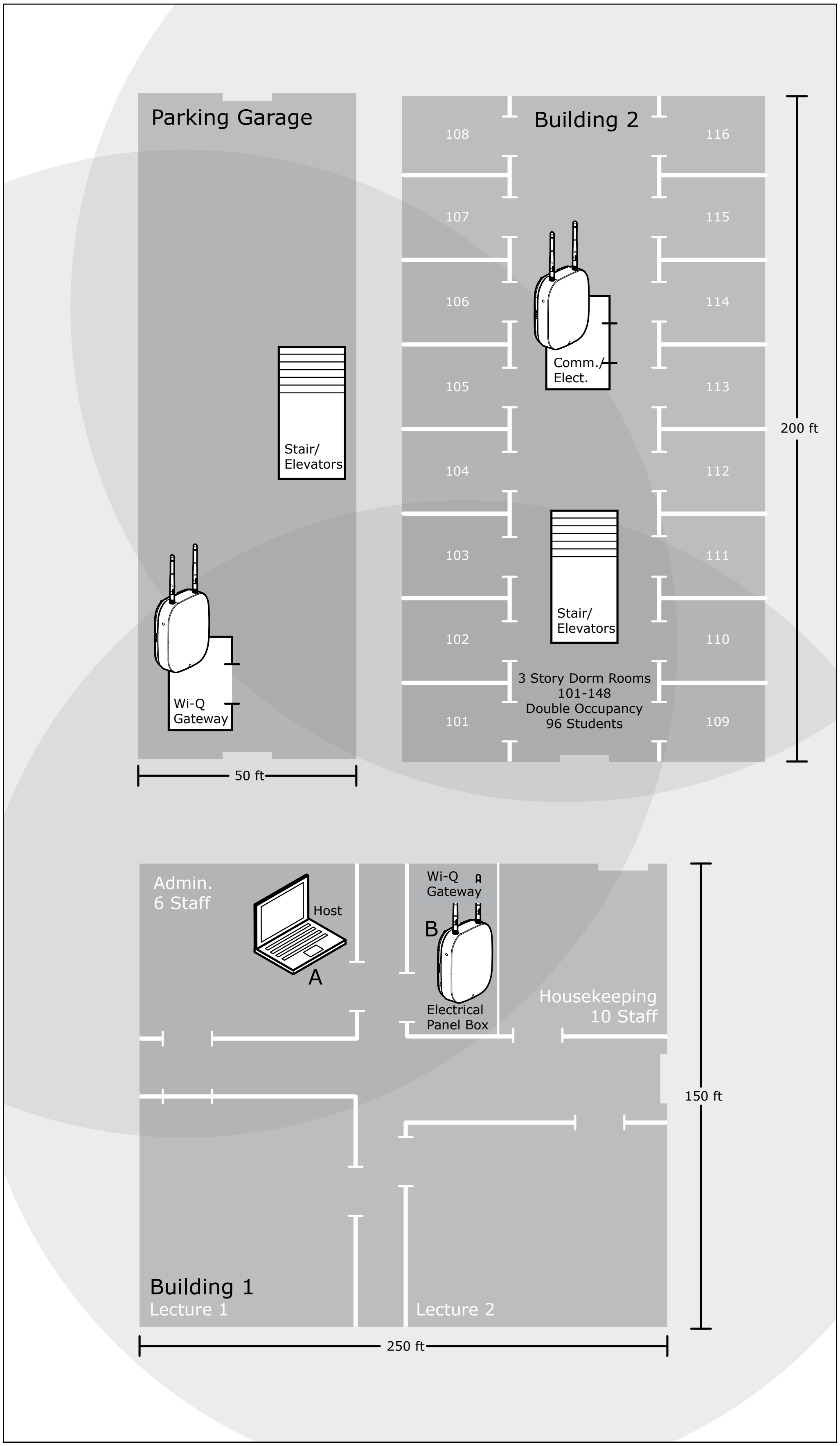
Transmit range from Wi-Q Gateway to controller varies based on building construction. Site characteristics such as reinforced concrete walls could interfere or weaken the signal; open spaces and low interference can increase signal strength.

Figure 3 shows a typical site configuration. The Host (A) is located in Building 1. The Building 1 Wi-Q Gateway (B) is located near the electrical panel in the communications/ electronics room.

The Building 2 Wi-Q 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 Wi-Q Gateway (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 Sample site installation plan



Plotting the Plan

If you don't already have a site plan indicating building dimensions, distances between buildings, possible obstructions, parking segment, and other gated access points, contact your facilities maintenance or project engineer. If none are available, you will need to visit the site, take measurements and draw up a plan of your own.

Device Identification

Each device in the system will have its own unique identity. It will be important for you 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, you must 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.

Note The MAC address is most commonly shown on the back of or inside the device, so it's important to record this number before you install the device.

When you move on to configure the Host computer, it is essential to have a list identifying each Controller and Wi-Q 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.

Interference

Wi-Q Technology transfers information between devices in the form of data packets over the 2.4 GHz ISM band. This band frequency is very heavily used in many devices such as wireless computer networks (802.11 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 Wi-Q Gateway because of interference. Interference can also reduce controller battery life due to the constant re-broadcasting of packets and lost connections to the Wi-Q Gateways. To achieve maximum efficiency in Wi-Q Interface, 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.

Extended Range

It is likely that you will have locations in your segment separated by distances greater than 300 feet. You may want to consider adding a Wi-Q Gateway with a directional antenna to extend the transmit range.

Note The recommended range is to have controllers no more than 100 feet from a Wi-Q Gateway.

Note Actual distances will vary based on building construction.

Position Wi-Q Gateways (Task 2)

Once all door hardware and controllers have been installed, you are ready to determine the final placement of Wi-Q Gateways using the results from the Wi-Q Technology Site Survey Kit. The Site Survey Kit helps you determine the number and optimum location of Wi-Q Gateways and verify signal strength before permanently installing the hardware. It is important to perform the Site Survey process as many times as needed to determine the optimal position.

The Wi-Q Gateway has a built in Survey Mode. This feature is especially handy when performing a Site Survey for Wi-Q Gateway 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.

Using the Wi-Q Gateway for a Stand-alone Site Survey

The Wi-Q 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:

1 Power on the WQXM-PG (wait for the boot process to complete).

2 Press the WiFi toggle push button of Gateway and release. The Wi-Fi is now enabled and the LED will flash on and off.

Note When the Gateway Wi-Fi is enabled, the LED will begin blinking (color?) and alternate on and off.

Note Gateway Wi-Fi access point will be disabled by default after a reboot. Once the Wi-Fi push button is pressed, the access point will remain active until the 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.

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.

7 Click on the 'Standalone Survey' button to perform a Site Survey without an ACS.

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 The 'Current Sign-on Key' field will fill with a 6-digit sign-on key (987654) to sign a demo reader onto the Gateway.

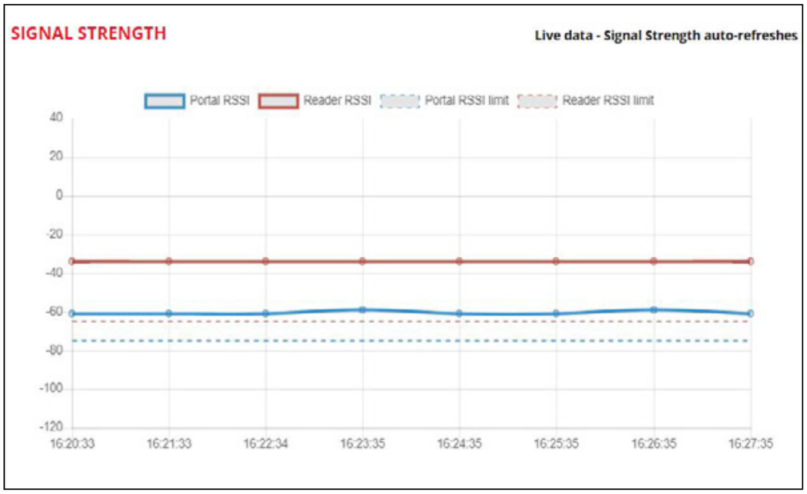
9 Noting the Gateway's sign-on key, sign on the Wi-Q Controller(s) with a keypad.

- 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.

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

The Wi-Q Gateway will begin logging the gateway packet transfer ratio, the reader packet transfer ratio as well as the signal strength at the gateway and the reader.

Figure 4 Portal Signal Strength



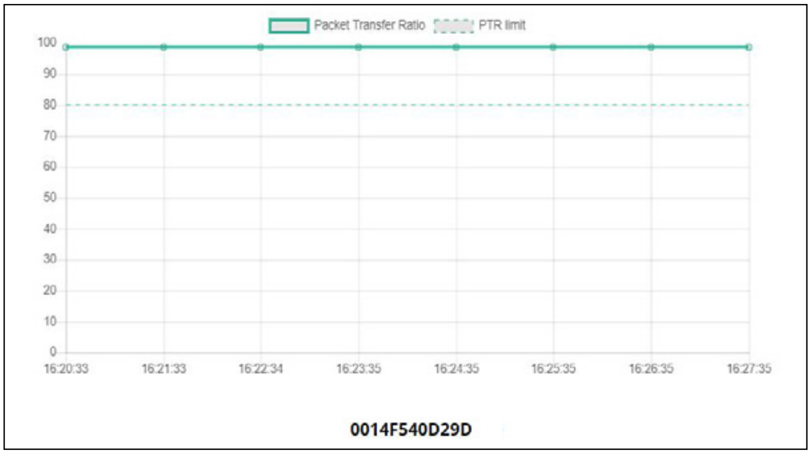
Portal Signal Strength

The Portal RSSI value indicates how well the Wi-Q Gateway receives signal from the door controller and should be -75dB or better. The Survey Mode charts in the Wi-Q Gateway 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 Wi-Q Gateway is required for adequate coverage.

Reader Signal Strength

The Reader RSSI value indicates how well the reader is receiving signal from the Wi-Q 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 Wi-Q Gateway or the antennas need to be repositioned so the reader can hear the Wi-Q Gateway more clearly.

Figure 5 Packet Transfer Ratio



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 Wi-Q Gateway 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 Wi-Q Gateway packet transfer ratio, update the reader statistics to poll every 10 seconds instead of once a day while running the survey tool in the Wi-Q Gateway.

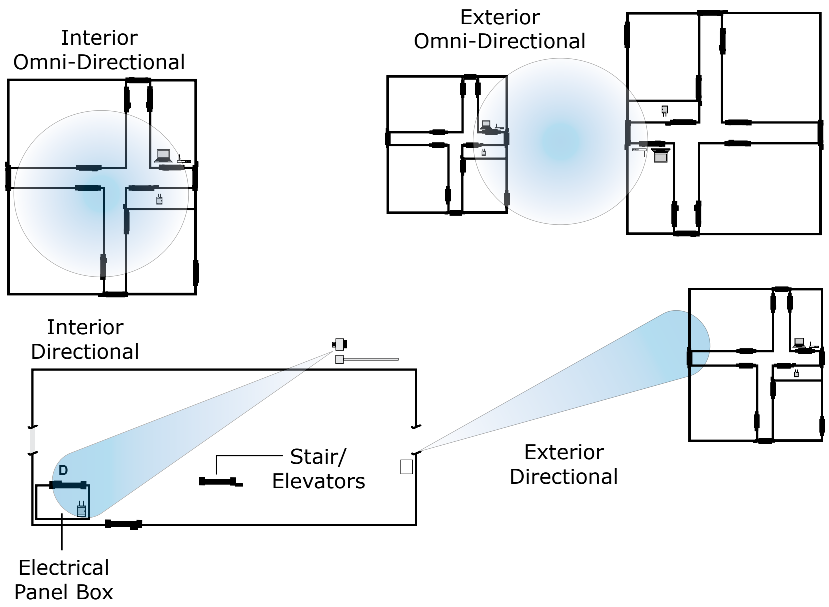
It is imperative to consider the wireless environment and the placement of the Gateway and its antennas during planning. The Gateway communicates on the 2.4 GHz frequency using the ZigBee channels. If the location has other wireless devices or networking using the 2.4 frequency, please orient the antennas 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.

Note You will need to test signal strength at all door locations near the perimeter of the coverage area as well as any location where a physical obstruction may cause interference. You can test the range and signal quality by using the built in survey mode in the Wi-Q Gateway model Wi-Q gateway.

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 you have trouble verifying signals, you may need to consider some antenna type options. Figure 6 shows two available antenna types.

Figure 6 Selecting the antenna type that best suits your needs.



Power Supply

Wi-Q Gateways must be located where they can receive 12 VDC power from a transformer plugged into a dedicated power source. If this is not possible, ensure they are plugged in to a 24/7 power circuit than cannot be turned off at a switch, such as a light switch that might be turned off by a cleaning crew. Wi-Q Gateways may also be powered with PoE instead of using the AC wall adapter.

To make your final determination, you must also consider the following:

- Access to Ethernet 10/100 Base T network connection.
- Proximity to other I/O device(s) if used.
- Placement within range of controllers.

Note Transmit range will vary based on building construction.

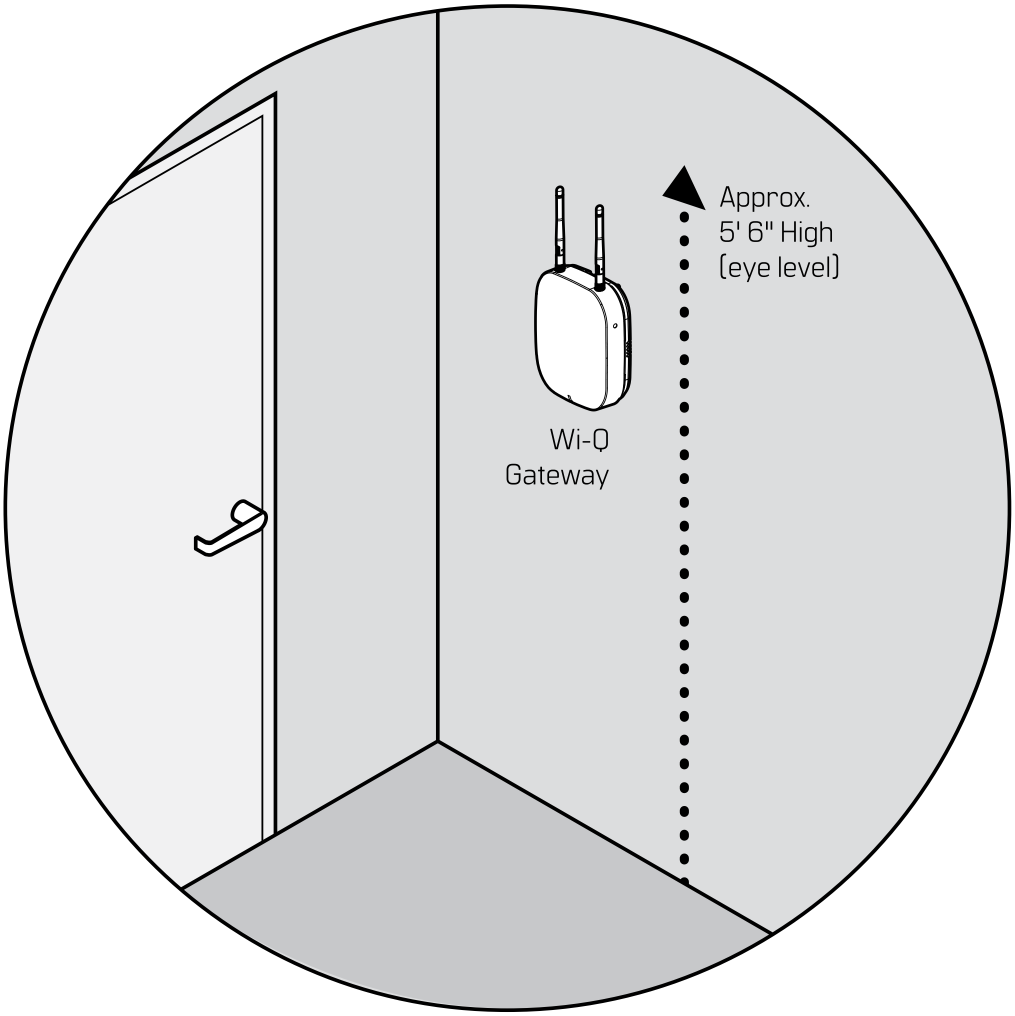
Next steps

When you are satisfied with signal performance, you can proceed to configure Wi-Q Gateways using the Wi-Q Interface Software. See "Configure Wi-Q Gateways (Task 6)" on page 67.

Install Wi-Q Gateways (Task 7)

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 you are installing inside a dealer-supplied locked enclosure, refer to the instructions provided with that equipment. Figure 7 shows a Wi-Q Gateway positioned in a protected area.

Figure 7 Installing a Wi-Q Gateway in a protected area.



1 Connect the power supply to the Wi-Q Gateway and plug the transformer into a dedicated AC power supply (wall outlet). The power indicator should come on and start blinking purple. The LED behavior should follow Table 1 (LED Behavior).

2 Insert the Ethernet cable into the Ethernet connection on the bottom of the Wi-Q Gateway.

Connecting the Gateway and Verifying Operation

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

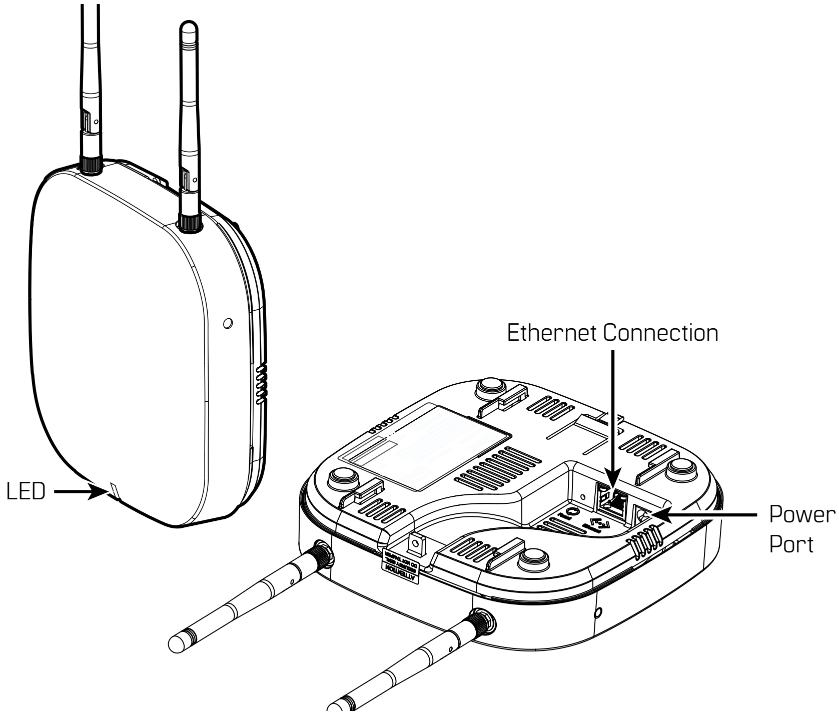
1 Connect the power supply to the Gateway and plug the transformer into a dedicated AC power supply (wall outlet) if power over Ethernet is unavailable, see Figure 8.

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.

Table 1. LED Behavior

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.

Figure 8 Connecting the Wi-Q Gateway to Power and Ethernet Connections.



Note If no protected area is available, consider positioning the Wi-Q Gateway inside a locked enclosure designed for that purpose. Contact your dealer for more information.

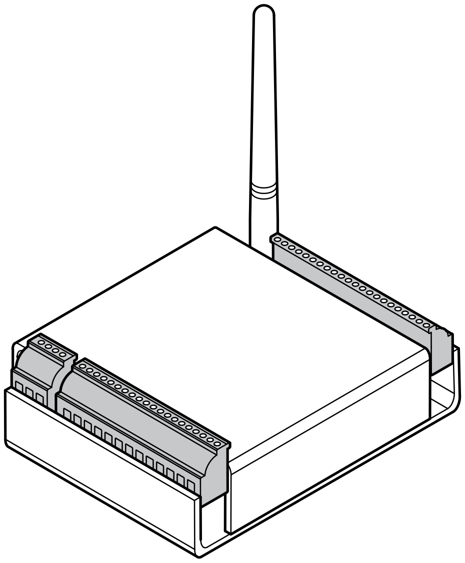
Installing a Wireless Access Controller

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 Wi-Q Interface Software, just like a standard controller.

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

Using the Wireless Access Controller (Figure"Wireless Access Controller." on page 28), you can add controllers or other I/O devices to an overall wireless solution without the high cost of installing hard-wire such as RS485 or CAT5 to the controller. You can position the controller at the door or where suitable above the ceiling tile.

Figure 9 Wireless Access Controller.



Installation

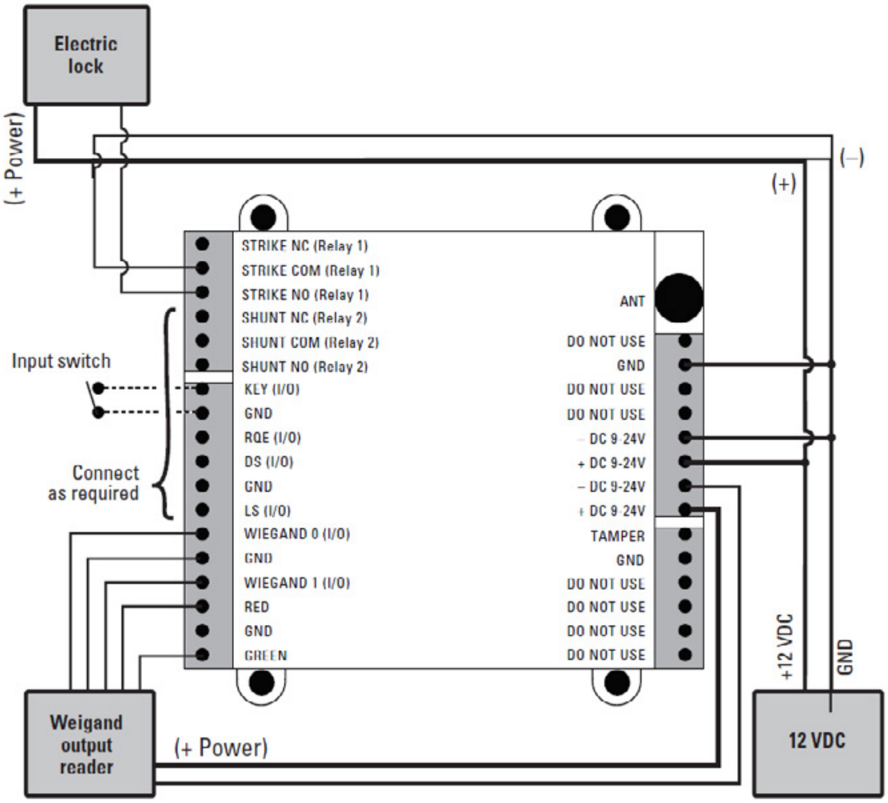
Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

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.

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 10 is a wiring diagram illustrating both configurations. Dotted lines represent optional connections for the slaved configuration.

Figure 10 Connecting devices to a WAC



Once the WAC is installed and all points connected, it will be recognized by Wi-Q Interface as a 'Controller' in the system. The WAC is configured in an almost identical manner as a Controller. For more information about configuring the WAC in the Wi-Q Interface Software, see "Controllers Tab" on page 81.

Install Door Hardware (Task 8)

This section provides general instructions for installing your controllers. Complete instructions for installing locks are packaged with the hardware. You will also find instructions for BEST Wi-Q Technology BEST 45HQ Mortise locks, BEST 9KQ Cylindrical Locks and BEST EXQ Trim as Appendices to this manual.

Before You Begin

Before you begin, take a few moments to review the following considerations:

Record device MAC address before installing device. You will need this when configuring the controller in the Wi-Q Interface Software and System Software.

- 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 you need to install 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 you are installing a left-hand door, see the instructions provided with your lockset for hand change instructions.
- If you are installing locksets on unprepared (un-drilled) doors, use the template provided with your specific lockset.

Please refer to the Appendices or the instructions provided with your particular 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 your controller type (Magnetic Card, Proximity Card or dual-validation with keypad). If the system does not operate properly, see Troubleshooting, at the end of the section.

Magnetic Card Check

If your system has a magnetic card reader (mag card), you will need the Temporary Operator Card (supplied with the controller) and Sign on Card (supplied in the Wi-Q Interface Software package) when you are ready to sign on the readers.

To perform a magnetic stripe card verification:

1 Determine if the magnetic card type is Track 2 or Track 3.

2 Select the default Programmer ID card that matches the type for your magnetic card reader.

3 Insert and remove the magnetic card. The magnetic stripe on the card should be aligned with the ‘V’ mark by the card slot. The lights on the top of the Wi-Q Technology card reader will flash green once and unlock, then during the open delay time, it will flash green five times. Once this occurs, the card reader light will flash red and lock.

4 While unlocked, check for proper lock operation.

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 WiQ Interface) 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.

Keypad Check

If your Wi-Q Technology controller is a keypad type, perform the following steps:

1. At the keypad, enter the default Programmer ID, 1234#. The green light on top of the card reader 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.

Troubleshooting mortise and cylindrical locks

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

Table 2. Troubleshooting (Mortise and Cylindrical Locks)

LEDs	Sounder	You should...
Single red flash	—	Use the card at a moderate speed.
Red flashes	3 short tones	Use the temporary operator card provided with the lock.
Green flashes	—	Check the motor connection.
—	—	Check the battery connection.

Troubleshooting EXQ Exit Hardware trim

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

Table 3. Troubleshooting (EXQ Exit Hardware Trim)

LEDs	Sounder	You should...
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 door reset to restore to the factory default settings (the lock may already be associated (programmed).
Green flashes	—	Check the motor connection.
Alternating red and green flashes	—	Check the motor connection.
—	—	Check the battery connection.

For additional troubleshooting instructions, see the Service Manual for the hardware.

Sign on Controllers (Task 9)

When all hardware is installed and tested, you are ready to sign on your system controllers. To do this, Wi-Q Interface Software must be installed on your Host computer. At a minimum, you will need to create your segment and add your Wi-Q Gateways to the segment tree before you can sign on the controllers. Once that is done you can return to the site and sign on the controllers. To complete controller sign on, you must perform steps at the Host and the controllers.

At the Host

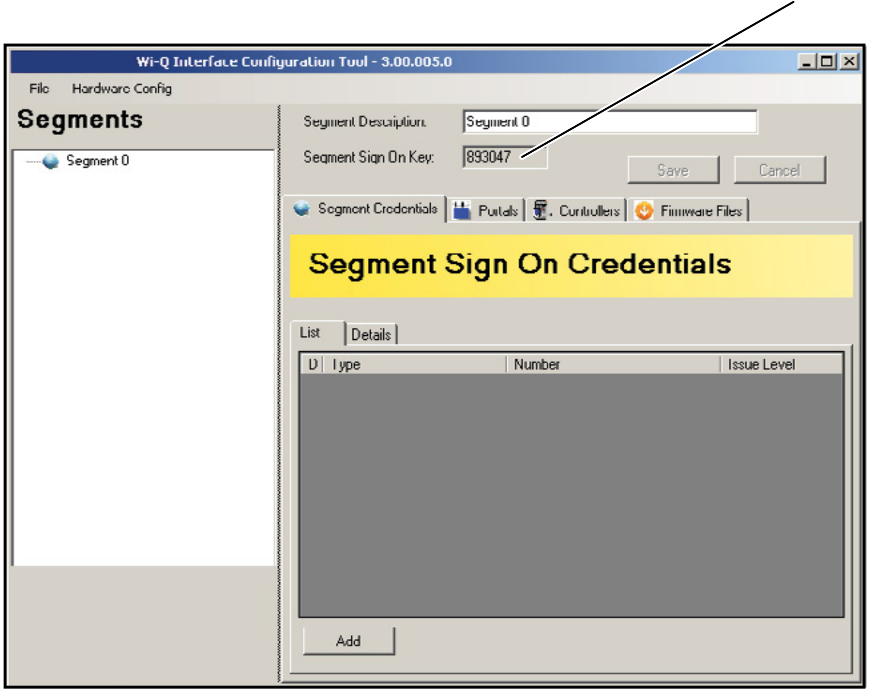
Once you have installed Wi-Q Interface Configuration Tool and created a segment, a sign-on key number is generated. You will need this number when you return to the site and sign on the controllers.

To get the Sign on Key number:

In the Wi-Q Interface Software, at the top of the screen, note the Segment Sign On Key number.

Figure 11 Locating the Segment Sign On Key.

Sign on key



Segment Description: Segment 0

Segment Sign On Key: 893047

At the Controllers

Once you have the sign on key number, you can return to the site and prepare to sign on all controllers.

Signing on Keypad Controllers

If your segment uses keypad controllers, use the following steps, in sequence, to register each controller in the system. Once this is done, the controllers will appear in the Wi-Q Interface Hardware Segment tree and Controllers tab.

Note The following sequence is timed. Be sure to have your segment sign on key ready to enter at the appropriate time.

1 Have your six-digit segment sign on key number ready.

2 At a keypad controller, press the following number sequence on the keypad: 5678# (Wireless Door Controller) or 5678 (WAC). The green light will flash three times.

3 Within five or six seconds, begin to enter the six-digit segment sign on key number, followed by #. You will have about five seconds to enter each number. The sequence will time out if more than five seconds elapses between numbers.

4 Once the key number is completed, the controller begins to alternately flash green and red to signify that it is searching for Wi-Q Gateways in range. If the sequence was completed successfully, three green flashes indicate the controller has accepted the sign on key.

5 If you see three red flashes, the controller has not accepted the number or you have exceeded the time limit. Begin again at step two and continue until you receive three green flashes.

Note Once a controller has been signed on, all sign-on functionality is disabled unless it is deep-reset.

Signing on Card Readers

If your segment uses card readers, you may want to register one of your cards with a segment credential number (See “Segments and Segment Sign On Credentials” on page 74). This card will be used to sign on card readers to the system. You can register a separate card and hold it specifically for this purpose, or register one that belongs to a user such as the Administrator’s card. Once this is done, you will use the card to sign on each card reader in the system.

Verify Signal Strength, Voltage and Packet Transfer Ratio

If you used the Wi-Q Technology Site Survey Kit, you have already verified basic controller signal strength. Once the controllers are signed on, you can use the Alarm Monitoring application to further measure controller performance, including controller voltage (battery level), and the packet ratio (the number of packets received vs the number of packets sent) of the controller. For more information about the Alarm Monitoring application, see the Alarm Monitoring User Guide.

Replacing a Controller

If you must replace an old or defective Controller with a new one, follow these steps:

1 Ensure that the Controller is online and associated with any Wi-Q Gateway. Send a deep reset to the Controller if needed.

2 Remove Wi-Q Controllers from assigned access levels in System Administration before deleting them from Readers and Doors.

3 Inside the Readers and Doors Module, Click Add button and enter the controller name followed by MAC address. Example: Controller1(0014f5123456)

4 Select OK button and confirm the changes.

5 Sign on the new controller. And the configuration should be automatically sent to it.

3 Software Installation

This chapter will guide you through performing the following tasks: :

Task 3 — Gather and Organize Segment Data

Task 4 — Prepare your Computer

Task 5 — Install Wi-Q Interface Software

Gather and Organize Segment Data (Task 3)

As the technical team works on planning and installing hardware using the Site Plan, a program administrator or other person responsible for the software side of program setup should be making plans to populate and configure the Wi-Q Interface Software and the System Software.

Device Information

You will need the MAC numbers, device names, capacities, and physical locations of all Wi-Q Gateways so that you can easily identify them and assign them to the correct location within the Wi-Q Interface Software and System Software. Ensure your site technical team will provide you this information as they work their way through the site.

User Information

To set up your Wi-Q System, you will need to gather the names of users, define their access requirements, organize user and timezone groups, and decide how you will use other features configurable within OnGuard.

It will be helpful to create a table listing what you know about each user. Starting with a list of names, think about building a table that defines basic information about each user; such as, User Type, User Group, Shift, and so on. Following is a very simple example:

Table 4. User Information

Last	First	User Type	Bldg.	User Group	Timezone	Shunt
Alverez	Alicia	Manager	A	Admin	Default	Default
Bennet	Fred	General	A	Lecture	Default	30 sec.
Ford	Aldo	General	B	Service	Service 1	30 sec.

What User Groups will help you manage security? Do you have shift workers who are allowed on site only during certain days or hours? Will there be areas off limits to certain groups? Do some users need extra time to pass through a door, such as to accommodate a food cart or wheel chair? Start thinking about these elements and begin organizing the data as soon as possible so you'll be ready when your equipment and software are ready. It is a good idea to use a spreadsheet software such as Microsoft® Excel® for this purpose. That way you can sort the data to help you plan your segment.

Importing Data

Do you have an existing database that already contains much of the information you need? It is likely you can modify a version and import it into your System using the program's System Administration feature. If you have a large organization, this will save you time and reduce data entry error. See the System Administration User Guide for more information.

Prepare Your Computer (Task 4)

To prepare your computer for the installation of the Wi-Q Interface Software, you must do the following:

- Ensure that your system is equipped with an appropriate operating system, database and server.
- Configure your Windows Firewall Ports.
- Obtain your Wi-Q Gateway Accessory Add-On.
- Stop your Communication Server (if required).
- Install your Wi-Q Gateway Accessory Add-On

It is recommended that you follow the tasks above in the order that they are presented in this guide.

Note You must have administrative rights on your computer to perform many of the tasks listed here.

Recommended System Limits

It is important to ensure your Host computer or computers are adequate to handle the system.

Computer specifications should follow OnGuard documentation.

The loading on a single OnGuard communication server should be as follows:

Table 5. OnGuard Communication Server

Element	Limit
Wi-Q Gateway Panels and Online Panels	80 maximum
Wi-Q Locks and Online Readers	500 maximum

Configure Windows Firewall Ports

Several ports must be enabled in your Windows firewall settings to allow proper communication in the Wi-Q Interface. The following ports must be enabled:

- 1433 – Default port for SQL Server
- 1434 – SQL Server
- 8000 – Portal Service Port
- 11000 – Portal Config Service Port
- 5353 – Bonjour
- 443 – HTTPS
- 80 – HTT
- 23 – Telnet (Not intended for WQXM-PG; utilized by WQX-PG)

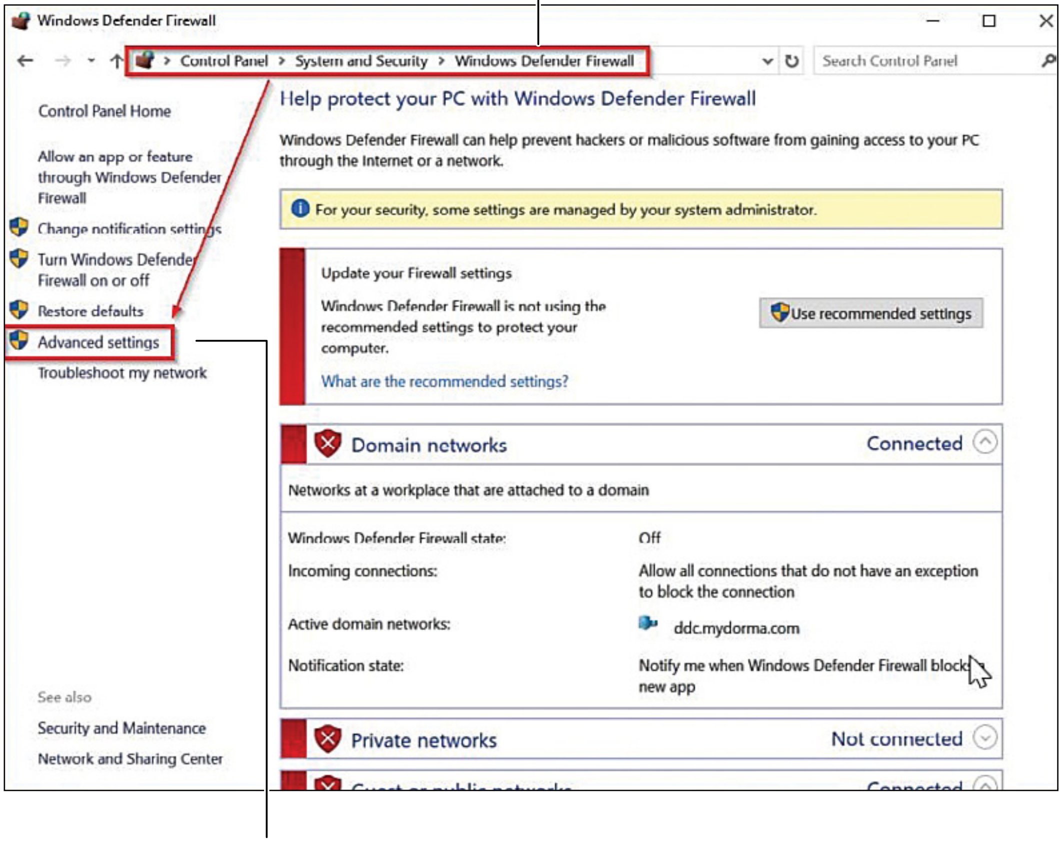
If your firewall is disabled, then all ports are open by default. If the firewall is on, perform the following steps in order to add the required ports listed above:

Note The screenshots below reflect a Windows 2007 operating system. Navigating through the firewall settings in other editions of Windows will be slightly different.

1 Navigate to your Windows Firewall settings from your PC's control panel. See Figure 12. Then, click on Advanced settings.

Figure 12 Windows Firewall

Navigate to Windows Firewall


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Use recommended settings
What are the recommended settings?
Domain networks
Connected
Private networks
Not connected

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

For your security, some settings are managed by your system administrator.

Update your Firewall settings

Windows Defender Firewall is not using the recommended settings to protect your computer.

Networks at a workplace that are attached to a domain

Windows Defender Firewall state: Off

Incoming connections: Allow all connections that do not have an exception to block the connection

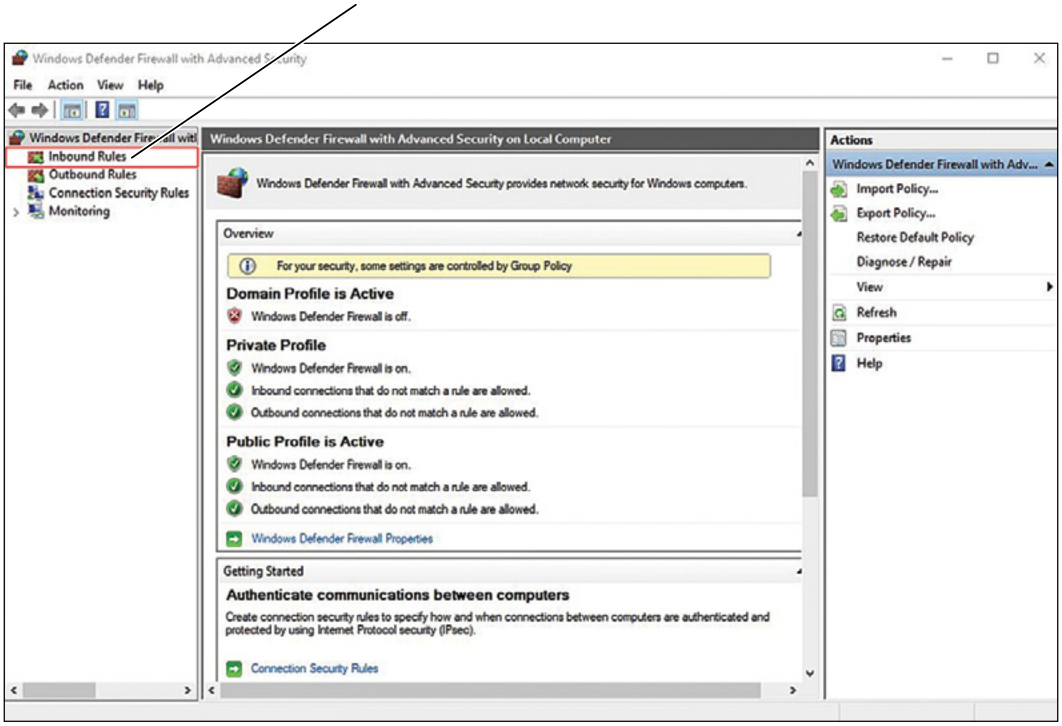
Active domain networks: ddc.mydorma.com

Notification state: Notify me when Windows Defender Firewall blocks a new app

Click on Advanced settings

2 Select Inbound Rules.

Figure 13 Inbound Rules



Select Inbound Rules

Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

For your security, some settings are controlled by Group Policy

Domain Profile is Active

Windows Defender Firewall is off.

Private Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule are allowed.

Outbound connections that do not match a rule are allowed.

Public Profile is Active

Windows Defender Firewall is on.

Inbound connections that do not match a rule are allowed.

Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

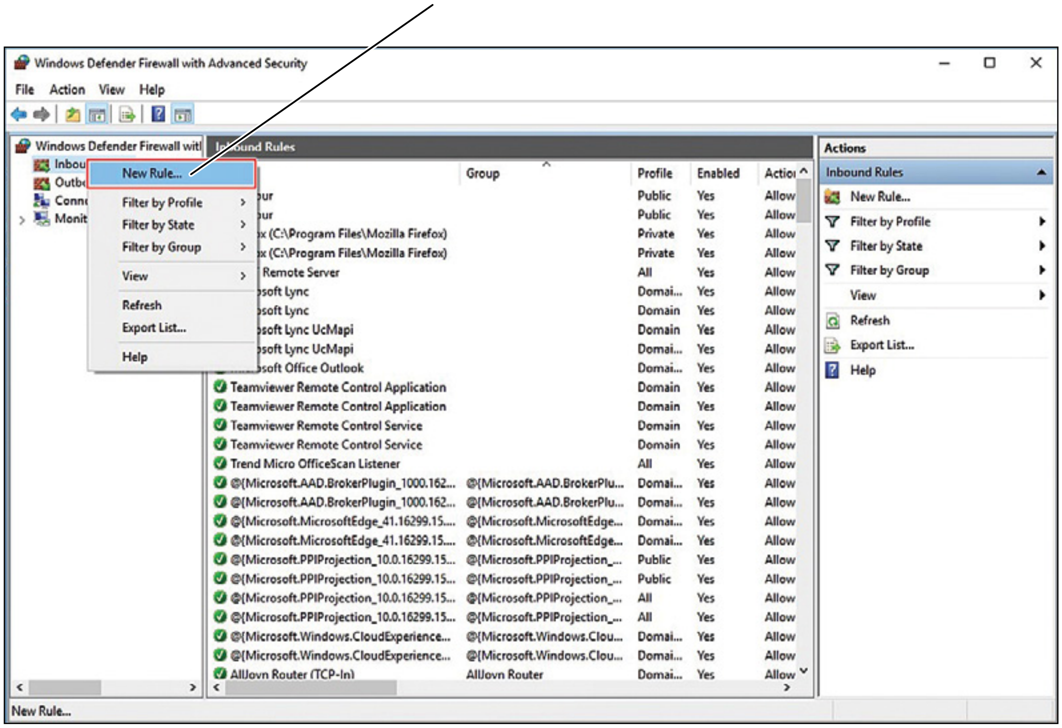
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

3 Right click on Inbound Rules to open an option menu. Select New Rule from the menu.

Figure 14 New Rule

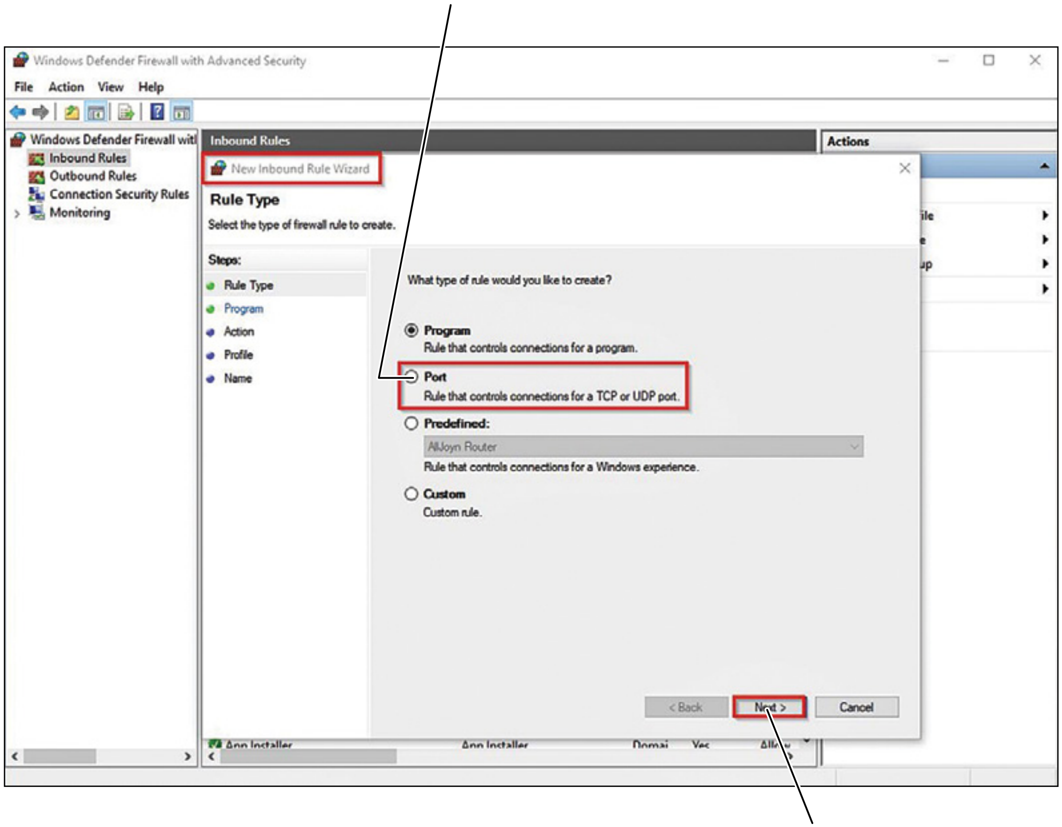
Select New Rule



	Group	Profile	Enabled	Actio
ur		Public	Yes	Allow
ur		Public	Yes	Allow
x (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
x (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Remote Server		All	Yes	Allow
soft Lync		Domai...	Yes	Allow
soft Lync		Domain	Yes	Allow
soft Lync UcMapi		Domain	Yes	Allow
soft Lync UcMapi		Domai...	Yes	Allow
soft Office Outlook		Domai...	Yes	Allow
Teamviewer Remote Control Application		Domain	Yes	Allow
Teamviewer Remote Control Application		Domain	Yes	Allow
Teamviewer Remote Control Service		Domain	Yes	Allow
Teamviewer Remote Control Service		Domain	Yes	Allow
Trend Micro OfficeScan Listener		All	Yes	Allow
@{Microsoft.AAD.BrokerPlugin_1000.162...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow
@{Microsoft.AAD.BrokerPlugin_1000.162...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow
@{Microsoft.MicrosoftEdge_41.16299.15....	@{Microsoft.MicrosoftEdge...	Domai...	Yes	Allow
@{Microsoft.MicrosoftEdge_41.16299.15....	@{Microsoft.MicrosoftEdge...	Domai...	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	Public	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	Public	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	All	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	All	Yes	Allow
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow
AllJovn Router (TCP-In)	AllJovn Router	Domai...	Yes	Allow

4 In the New Inbound Rule Wizard window, select Port. Click Next to continue.

Figure 15 Create Port Rule



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

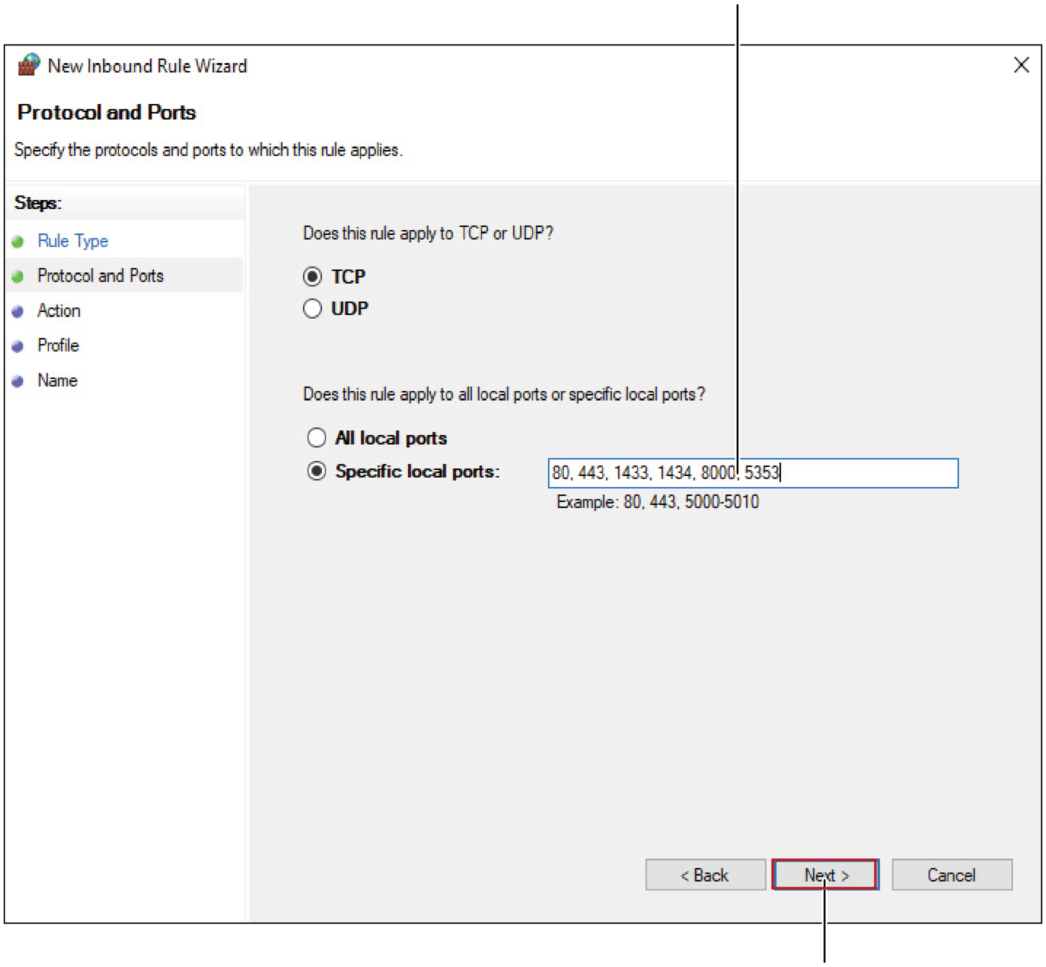
Select Port

Click Next

5 Enter the following ports into the “Specific local posts” field: 80, 443, 1433, 1434, 8000, 5353. Then, click Next to continue.

Figure 16 Enter Ports

Ports: 80, 443, 1433, 1434, 8000, 5353



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

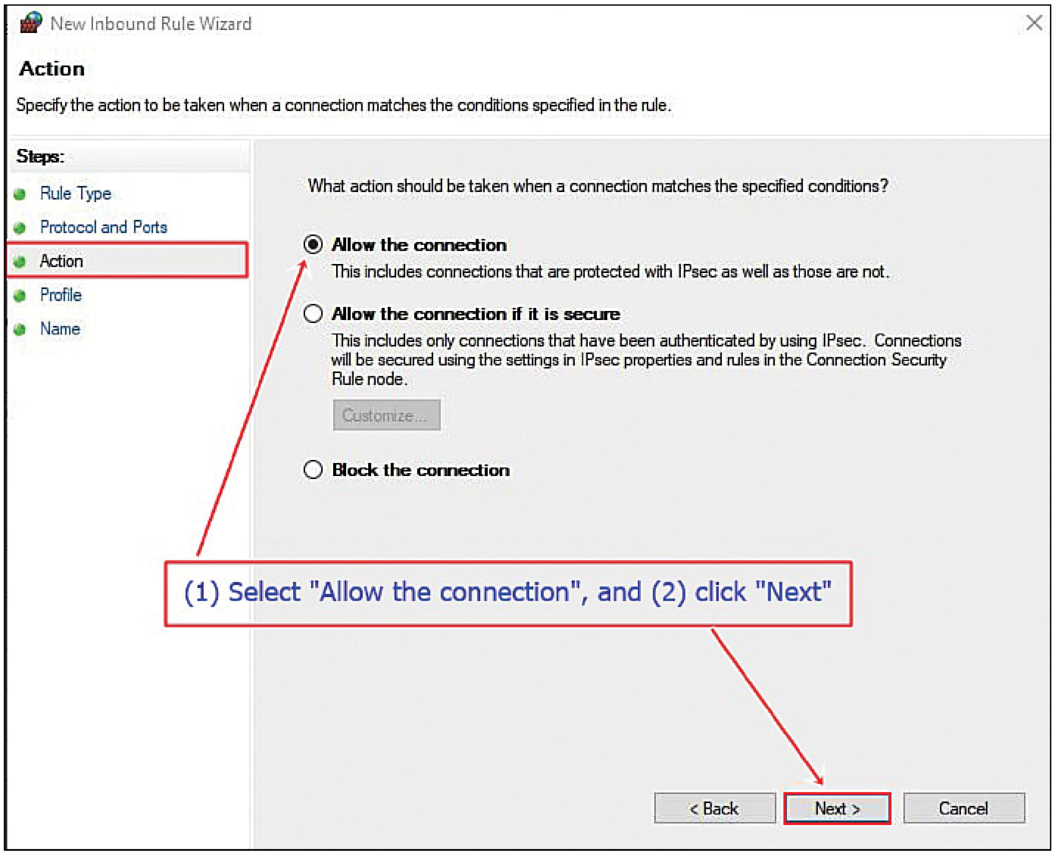
○ **All local ports**
● **Specific local ports:** 80, 443, 1433, 1434, 8000, 5353

Example: 80, 443, 5000-5010

Click Next

6 Select Allow the connection. Click Next to continue. See Figure 17.

Figure 17 Allow the Connection



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

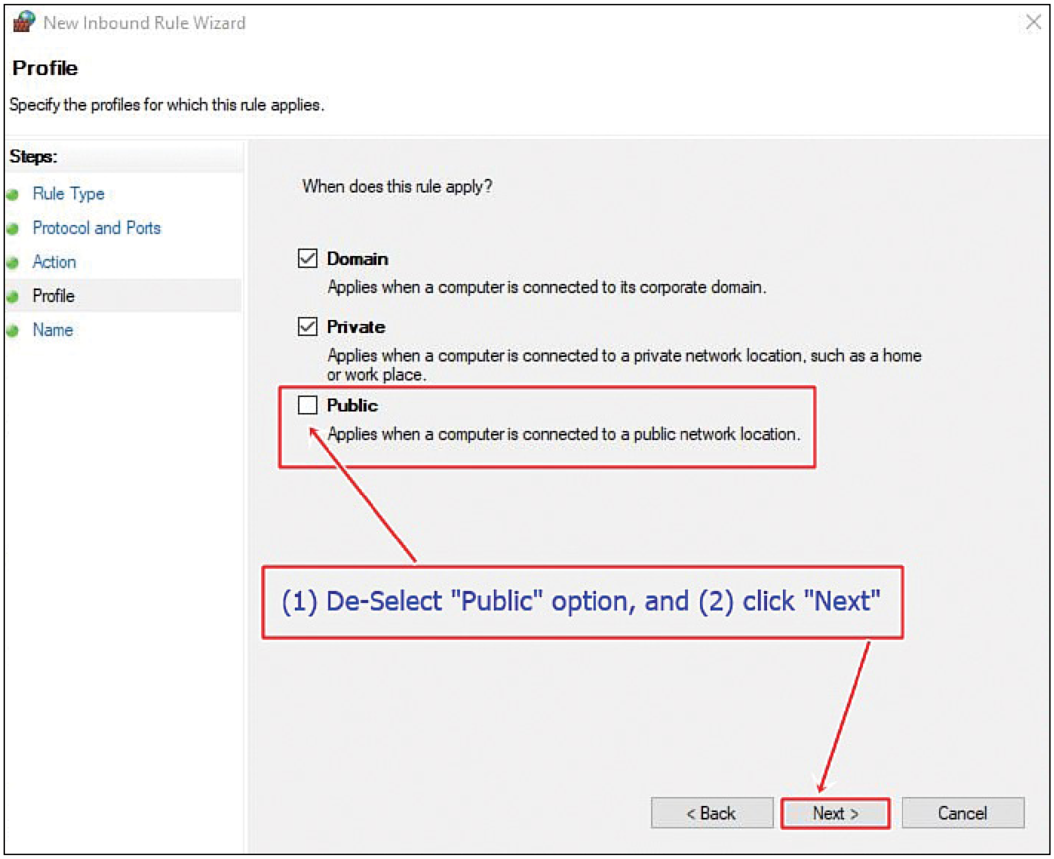
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

(1) Select "Allow the connection", and (2) click "Next"

7 De-select the Public option. Click Next.

Figure 18 De-select Public



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

☑ **Domain**

Applies when a computer is connected to its corporate domain.

☑ **Private**

Applies when a computer is connected to a private network location, such as a home or work place.

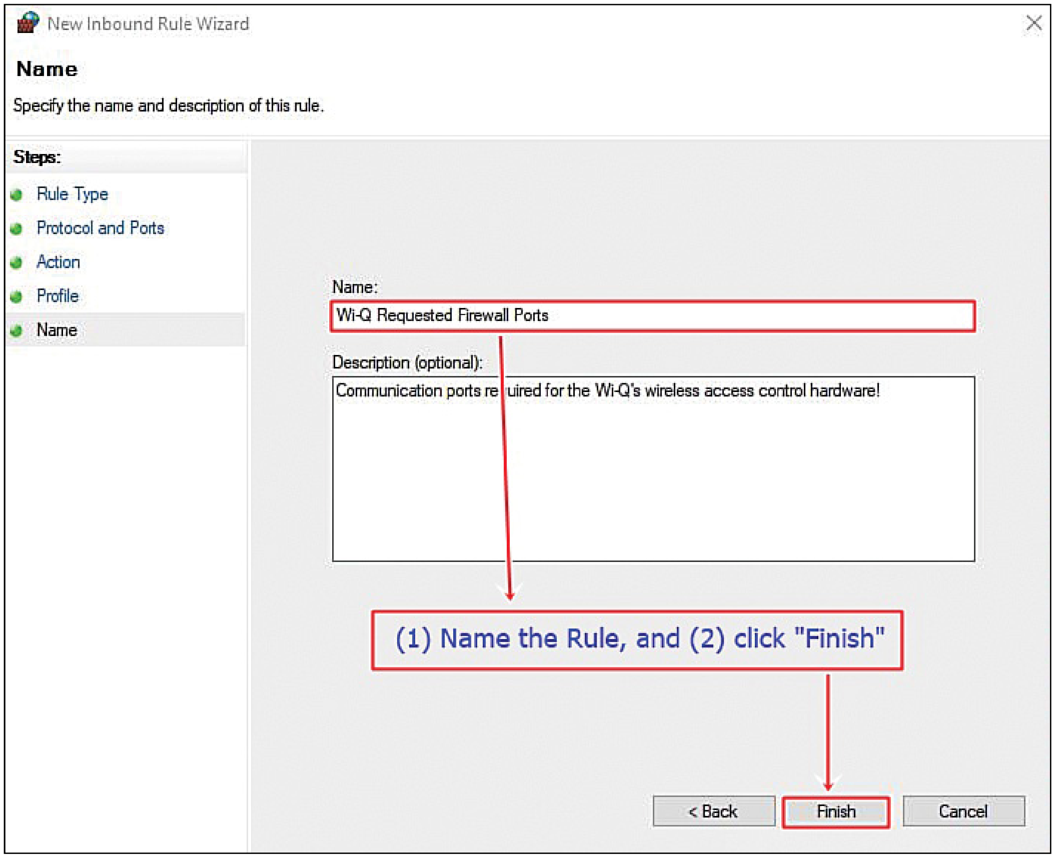
□ **Public**

Applies when a computer is connected to a public network location.

(1) De-Select "Public" option, and (2) click "Next"

8 Give the new rule a name that can be easily identified by an administrator. Once finished, click Finish. See Figure 19.

Figure 19 Name the Rule



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

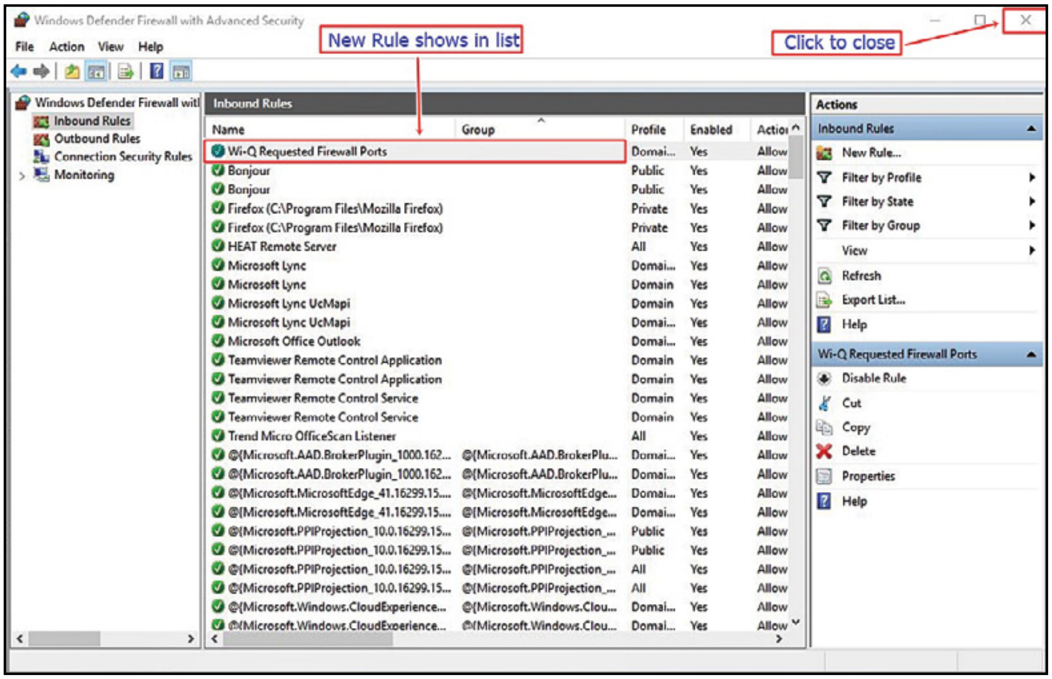
Name: Wi-Q Requested Firewall Ports

Description (optional): Communication ports required for the Wi-Q's wireless access control hardware!

(1) Name the Rule, and (2) click "Finish"

9 The new rule now appears in the list. The Firewall Settings module may now be closed. See Figure 20.

Figure 20 Inbound Rules List



New Rule shows in list

Click to close

Name	Group	Profile	Enabled	Actior
Wi-Q Requested Firewall Ports		Domai...	Yes	Allow
Bonjour		Public	Yes	Allow
Bonjour		Public	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
HEAT Remote Server		All	Yes	Allow
Microsoft Lync		Domai...	Yes	Allow
Microsoft Lync		Domain	Yes	Allow
Microsoft Lync UcMapi		Domain	Yes	Allow
Microsoft Lync UcMapi		Domai...	Yes	Allow
Microsoft Office Outlook		Domai...	Yes	Allow
Teamviewer Remote Control Application		Domain	Yes	Allow
Teamviewer Remote Control Application		Domain	Yes	Allow
Teamviewer Remote Control Service		Domain	Yes	Allow
Teamviewer Remote Control Service		Domain	Yes	Allow
Trend Micro OfficeScan Listener		All	Yes	Allow
@{Microsoft.AAD.BrokerPlugin_1000.162...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow
@{Microsoft.AAD.BrokerPlugin_1000.162...	@{Microsoft.AAD.BrokerPlu...	Domai...	Yes	Allow
@{Microsoft.MicrosoftEdge_41.16299.15....	@{Microsoft.MicrosoftEdge...	Domai...	Yes	Allow
@{Microsoft.MicrosoftEdge_41.16299.15....	@{Microsoft.MicrosoftEdge...	Domai...	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	Public	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	Public	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	All	Yes	Allow
@{Microsoft.PPIProjection_10.0.16299.15...	@{Microsoft.PPIProjection_...	All	Yes	Allow
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes	Allow

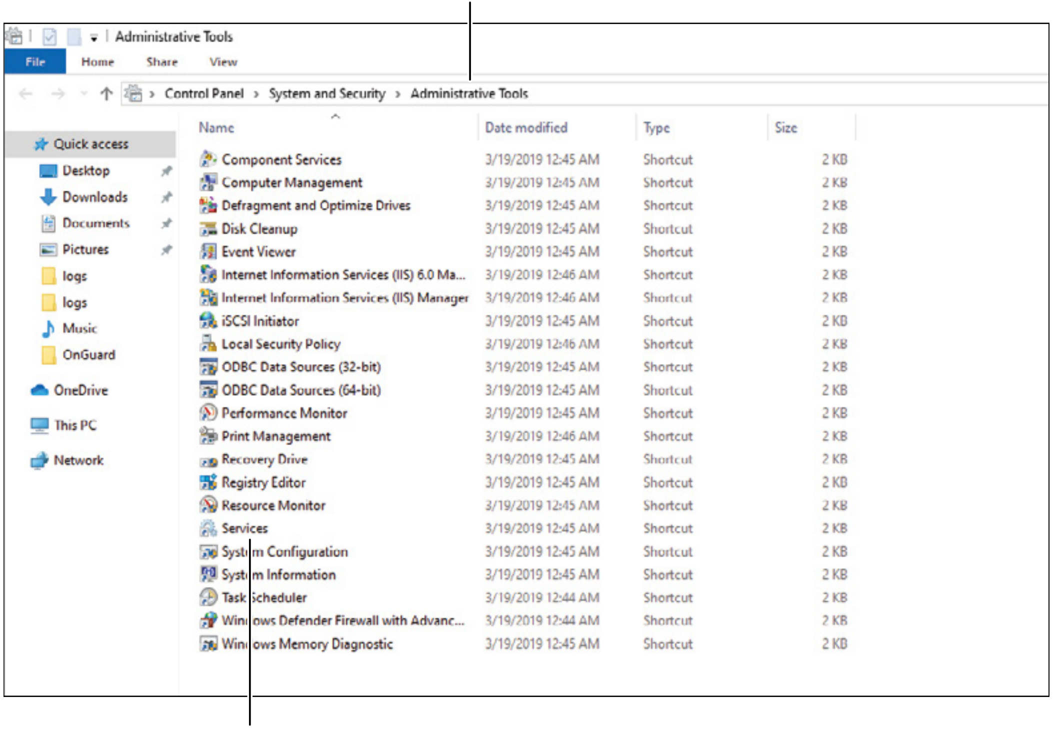
Obtain Wi-Q Gateway Accessory Add-On

Before you can install the Wi-Q Interface software, you must obtain a BEST Wi-Q Gateway Accessory Add-On from dormakaba Technical Support's secure file share available to all Wi-Q Certified technicians. This package contains necessary add-on components that enable BEST Wi-Q Gateway support. Contact dormakaba Technical Support directly at **dhw.support.us@dormakaba.com**.

Stop Communication Server

To make sure your Communication Server is not running, first, navigate to your system's Services via Administration Tools. See Figure 21.

Figure 21 Navigate to Services



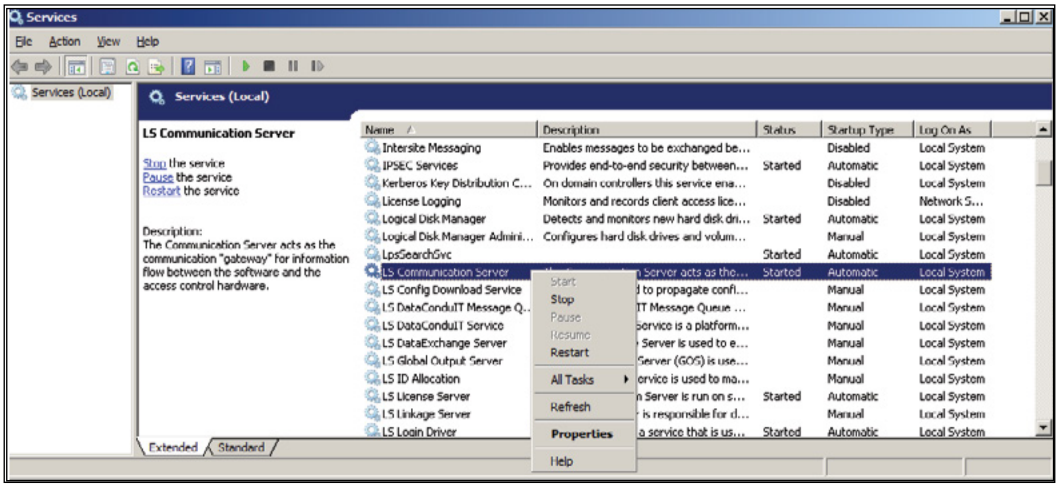
Navigate to Administrative Tools

Click to Open Services

Name	Date modified	Type	Size
Component Services	3/19/2019 12:45 AM	Shortcut	2 KB
Computer Management	3/19/2019 12:45 AM	Shortcut	2 KB
Defragment and Optimize Drives	3/19/2019 12:45 AM	Shortcut	2 KB
Disk Cleanup	3/19/2019 12:45 AM	Shortcut	2 KB
Event Viewer	3/19/2019 12:45 AM	Shortcut	2 KB
Internet Information Services (IIS) 6.0 Ma...	3/19/2019 12:46 AM	Shortcut	2 KB
Internet Information Services (IIS) Manager	3/19/2019 12:46 AM	Shortcut	2 KB
iSCSI Initiator	3/19/2019 12:45 AM	Shortcut	2 KB
Local Security Policy	3/19/2019 12:46 AM	Shortcut	2 KB
ODBC Data Sources (32-bit)	3/19/2019 12:45 AM	Shortcut	2 KB
ODBC Data Sources (64-bit)	3/19/2019 12:45 AM	Shortcut	2 KB
Performance Monitor	3/19/2019 12:45 AM	Shortcut	2 KB
Print Management	3/19/2019 12:46 AM	Shortcut	2 KB
Recovery Drive	3/19/2019 12:45 AM	Shortcut	2 KB
Registry Editor	3/19/2019 12:45 AM	Shortcut	2 KB
Resource Monitor	3/19/2019 12:45 AM	Shortcut	2 KB
Services	3/19/2019 12:45 AM	Shortcut	2 KB
System Configuration	3/19/2019 12:45 AM	Shortcut	2 KB
System Information	3/19/2019 12:45 AM	Shortcut	2 KB
Task Scheduler	3/19/2019 12:44 AM	Shortcut	2 KB
Windows Defender Firewall with Advanc...	3/19/2019 12:44 AM	Shortcut	2 KB
Windows Memory Diagnostic	3/19/2019 12:45 AM	Shortcut	2 KB

Next, locate "LS Communication Server" in the list of services (Figure 22). If the Status column reads as "Started," right-click on the line and select Stop. This step will be followed only when the LS Communication Server is run as a Service.

Figure 22 Stop Communication Server



LS Communication Server

Stop the service
Pause the service
Restart the service

Description:
The Communication Server acts as the communication "gateway" for information flow between the software and the access control hardware.

Name	Description	Status	Startup Type	Log On As
Intersite Messaging	Enables messages to be exchanged be...		Disabled	Local System
IPSEC Services	Provides end-to-end security between...	Started	Automatic	Local System
Kerberos Key Distribution C...	On domain controllers this service ena...		Disabled	Local System
License Logging	Monitors and records client access lice...		Disabled	Network S...
Logical Disk Manager	Detects and monitors new hard disk dri...	Started	Automatic	Local System
Logical Disk Manager Admini...	Configures hard disk drives and volum...		Manual	Local System
LpsSearchSvc		Started	Automatic	Local System
LS Communication Server	n Server acts as the...	Started	Automatic	Local System
LS Config Download Service	l to propagate confi...		Manual	Local System
LS DataConduIT Message Q...	TT Message Queue ...		Manual	Local System
LS DataConduIT Service	ervice is a platform...		Manual	Local System
LS DataExchange Server	Server is used to e...		Manual	Local System
LS Global Output Server	Server (GOS) is use...		Manual	Local System
LS ID Allocation	ervice is used to ma...		Manual	Local System
LS License Server	n Server is run on s...	Started	Automatic	Local System
LS Linkage Server	is responsible for d...		Manual	Local System
LS Login Driver	a service that is us...	Started	Automatic	Local System

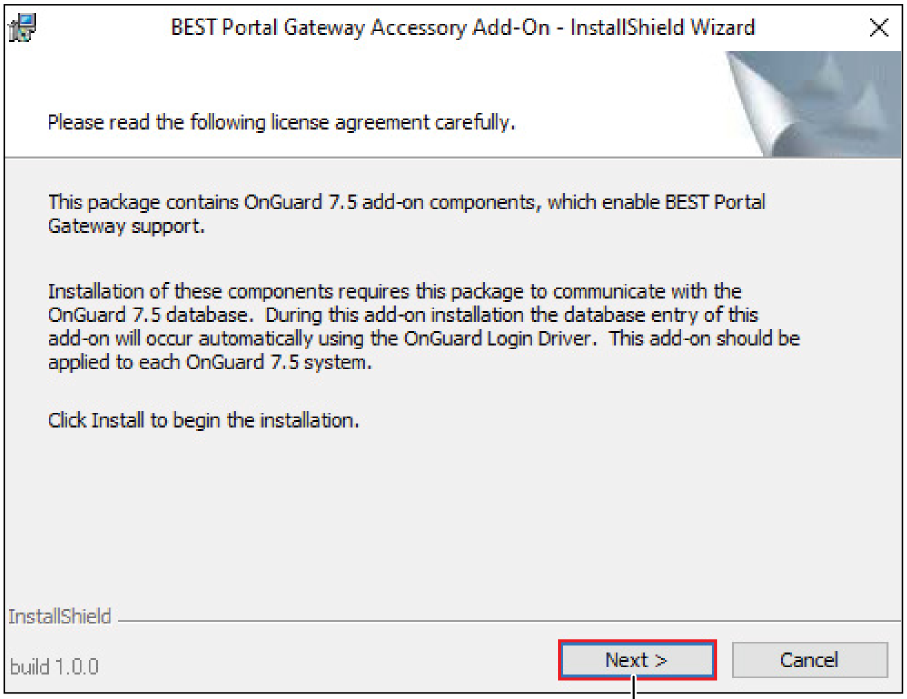
Install Wi-Q Gateway Accessory Add-On

Once you've obtained the Add-On package and associated database login information, perform the following steps to install it.

1 Navigate to the Windows Installer File (.msi extension) that you obtained from dormakaba Technical Support. Double-click to install.

2 The Accessory Add-On InstallShield Wizard will open. Read the license agreement carefully, then click Next. See Figure 23.

Figure 23 Accessory Add-On InstallShield Wizard



BEST Portal Gateway Accessory Add-On - InstallShield Wizard

Please read the following license agreement carefully.

This package contains OnGuard 7.5 add-on components, which enable BEST Portal Gateway support.

Installation of these components requires this package to communicate with the OnGuard 7.5 database. During this add-on installation the database entry of this add-on will occur automatically using the OnGuard Login Driver. This add-on should be applied to each OnGuard 7.5 system.

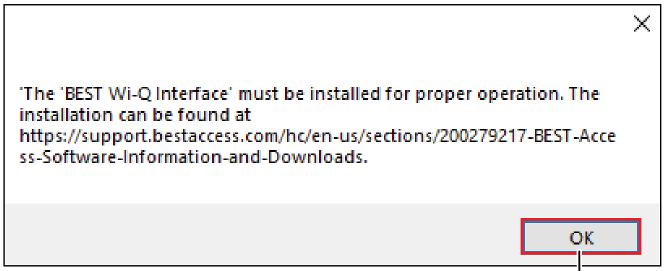
Click Install to begin the installation.

Click Next

3 The Add-On package will begin to install.

4 A window will pop up to inform you that the BEST Wi-Q Interface must be installed next. Click OK. See Figure 24.

Figure 24 Accessory Add-On Installation Reminder

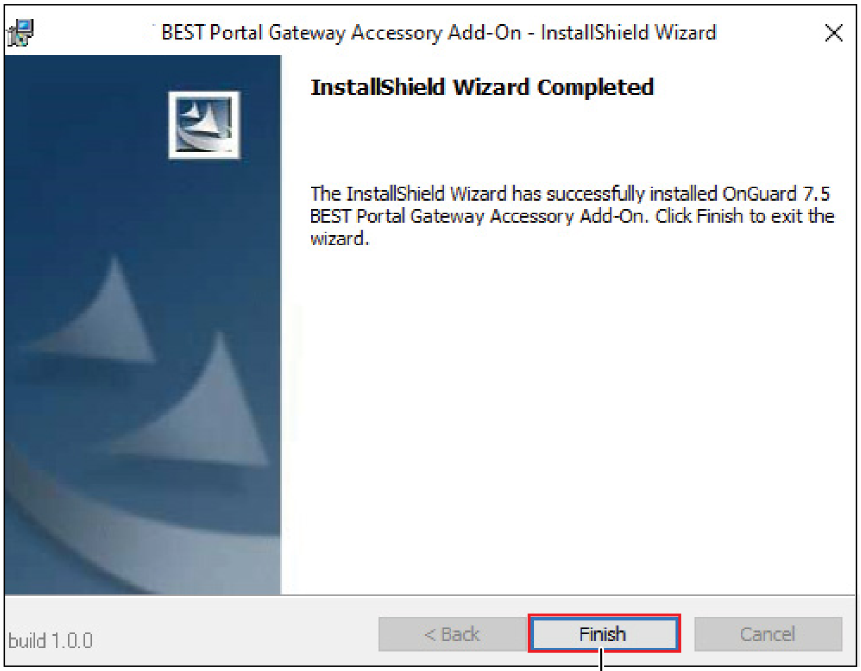


'The 'BEST Wi-Q Interface' must be installed for proper operation. The installation can be found at https://support.bestaccess.com/hc/en-us/sections/200279217-BEST-Access-Software-Information-and-Downloads.

Click OK

5 The InstallShield Wizard should now be complete. Click Finish to exit the wizard. See Figure 25.

Figure 25 Accessory Add-On Installation Complete



BEST Portal Gateway Accessory Add-On - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed OnGuard 7.5 BEST Portal Gateway Accessory Add-On. Click Finish to exit the wizard.

Click Finish

Install Wi-Q Interface Software (Task 5)

Once the Accessory Add-on has been installed, it is time to install the Wi-Q Interface Software. The Wi-Q Interface Software is a powerful tool that will help you integrate Wi-Q Technology into your system. The software consists of three parts:

- **BEST Wi-Q Interface** — Provides a communication link between the Communication Server and BEST Wi-Q Wi-Q Gateways. The Interface is responsible for transmitting and receiving all access control information.
- **BEST Wi-Q Interface Configuration Tool** — The actual software that you use to configure Wi-Q Gateways, generate Segment Sign-On Credentials, add Wireless Controllers and run Firmware Updates.
- **BEST Wi-Q Interface Database** — Contains the tables that are installed within the Access Control Database that are used by the Wi-Q Interface and Wi-Q Interface Configuration Tool.

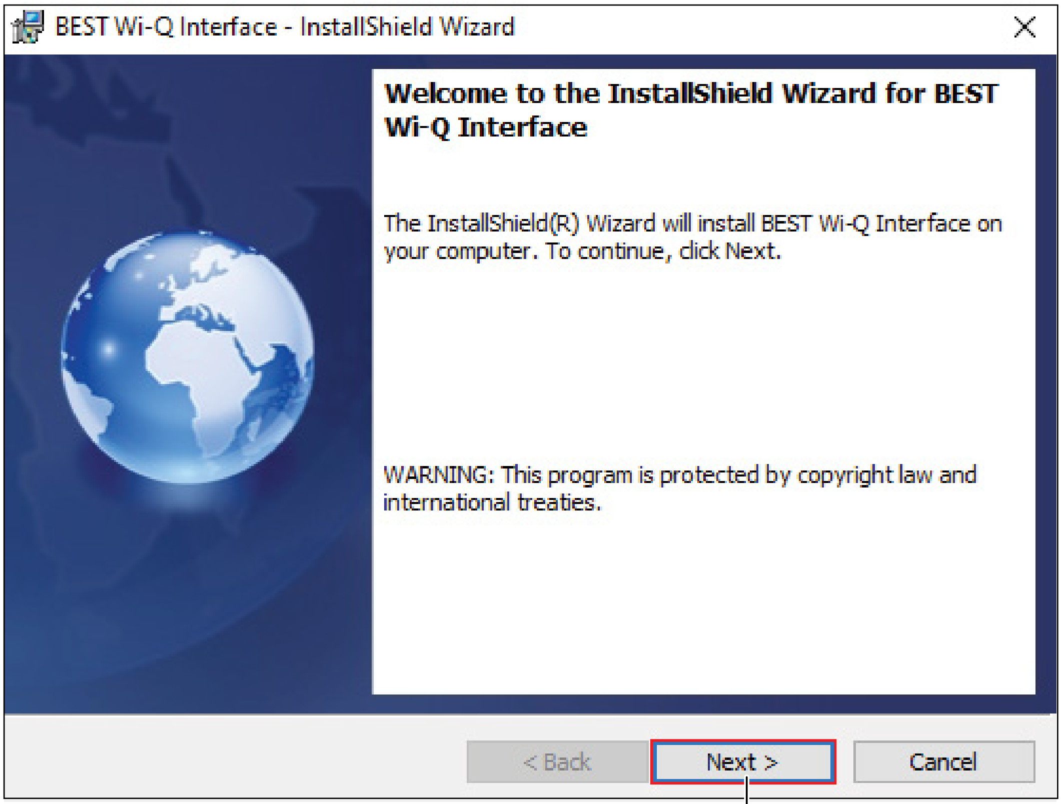
Once the software is installed, you can access this application from the Windows Start Menu. Perform the following steps to install the Wi-Q Interface Software.

1. If you have not already done so, download the Wi-Q Interface Software from the dormakaba Technical Support secure file share website available to all Wi-Q certified technicians.

   or

   Insert the software disc into your machine's disc reader.
2. Navigate to the software contents and right click on the setup.exe file and Run as administrator.
3. The BEST Wi-Q Interface InstallShield Wizard will pop up. Click Next to continue with the installation. See Figure 26.

Figure 26 Wi-Q Interface Setup Wizard



BEST Wi-Q Interface - InstallShield Wizard

Welcome to the InstallShield Wizard for BEST Wi-Q Interface

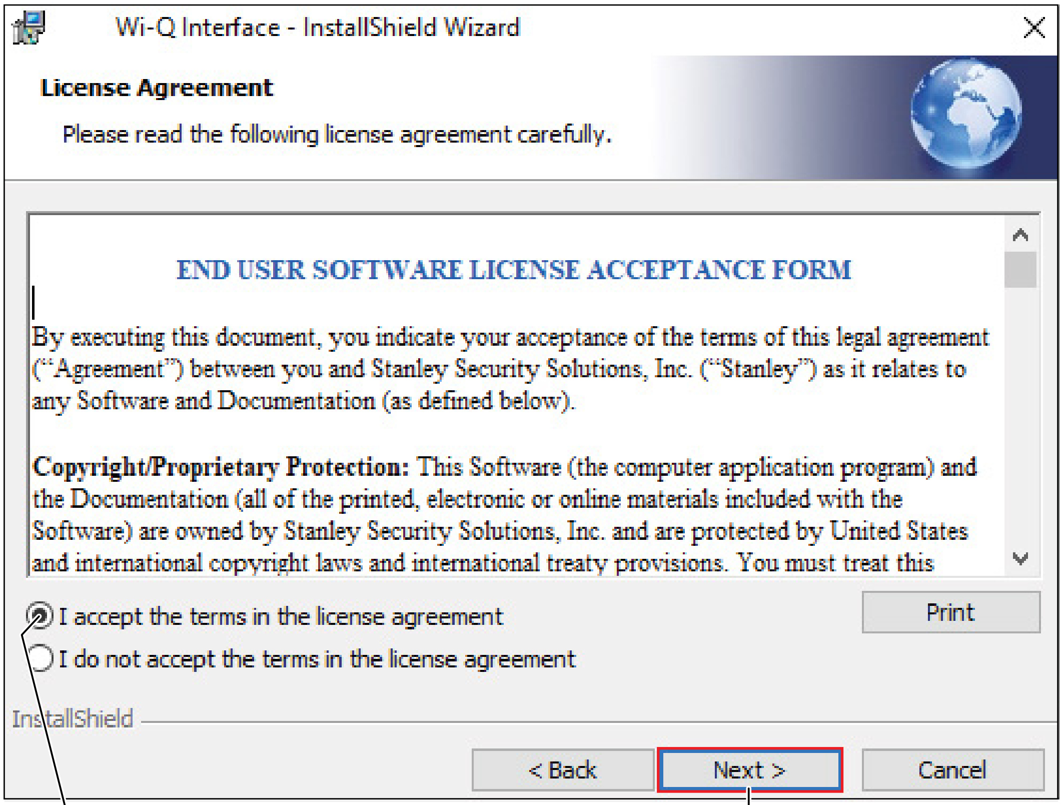
The InstallShield(R) Wizard will install BEST Wi-Q Interface on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Click Next

4 Read the License Agreement. To continue with the installation, click on “I accept the terms in the license agreement,” then press Next (Figure 27).

Figure 27 Wi-Q Interface License Agreement



Wi-Q Interface - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.

END USER SOFTWARE LICENSE ACCEPTANCE FORM

By executing this document, you indicate your acceptance of the terms of this legal agreement (“Agreement”) between you and Stanley Security Solutions, Inc. (“Stanley”) as it relates to any Software and Documentation (as defined below).

Copyright/Proprietary Protection: This Software (the computer application program) and the Documentation (all of the printed, electronic or online materials included with the Software) are owned by Stanley Security Solutions, Inc. and are protected by United States and international copyright laws and international treaty provisions. You must treat this

● I accept the terms in the license agreement

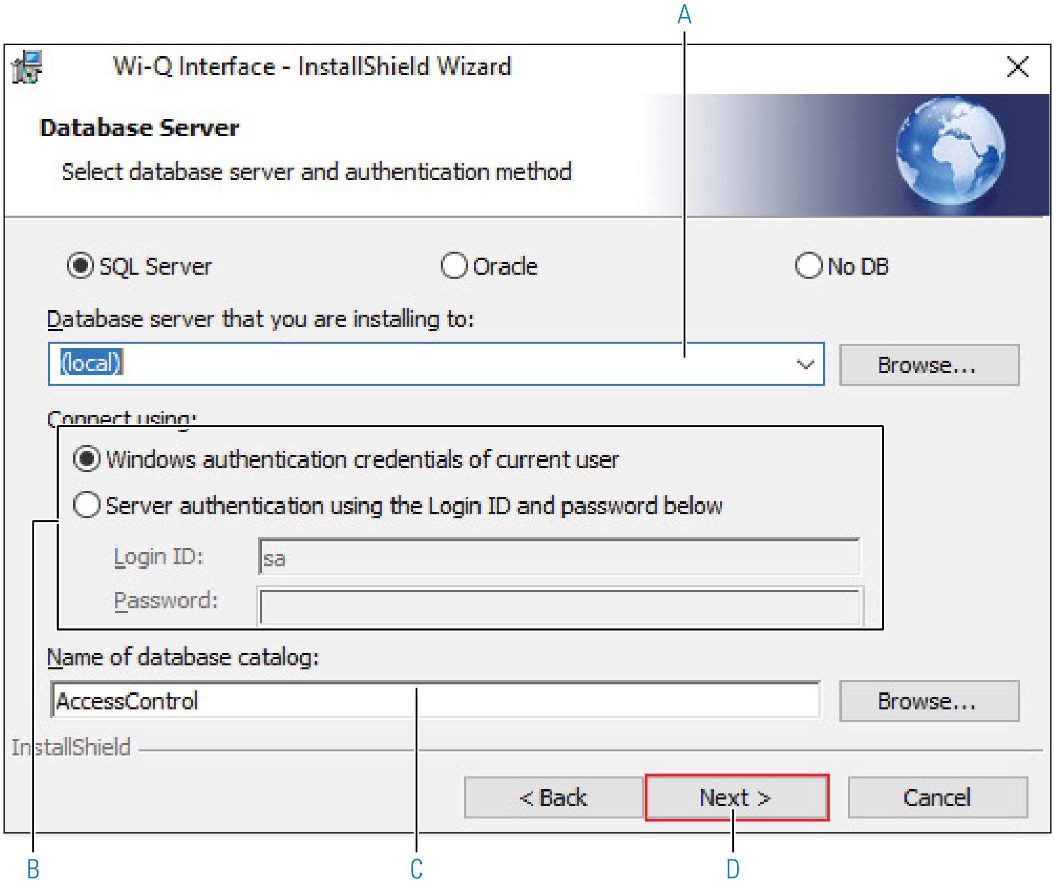
○ I do not accept the terms in the license agreement

Click to accept terms of license agreement

Click Next

5 In the “Database server that you are installing to” field, enter the computer name of your Server (Figure 28, Item A). If needed, you may browse to the server by selecting Browse.

Figure 28 Wi-Q Interface Database Server


Wi-Q Interface - InstallShield Wizard

Database Server

Select database server and authentication method

● SQL Server ○ Oracle ○ No DB

Database server that you are installing to: (local)

Connect using:

● Windows authentication credentials of current user

○ Server authentication using the Login ID and password below

Login ID: sa

Password:

Name of database catalog: AccessControl

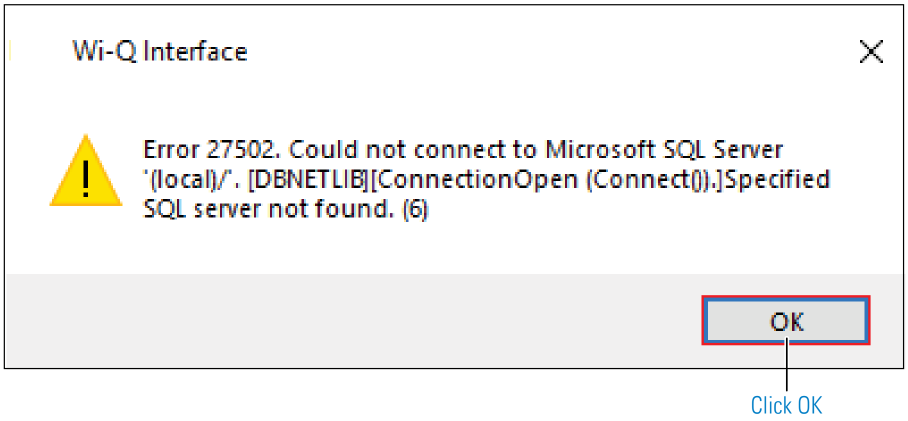
6 In the Connect Using section, choose your connection method. If you choose Server authentication, provide the Login ID and Password for the server. See Item B.

7 Enter the name of your Database in the “Name of database catalog” field. See Item C. If needed, you may browse to the database name by selecting Browse.

8 Click Next (Figure 28, Item D).

Note If you receive an error message like Figure 29, there may be an error in your database server information. Click OK, correct your information as needed, and press Next to continue. If you receive the error message again, and you have verified that all of your information is correct, contact dormakaba Technical Support.

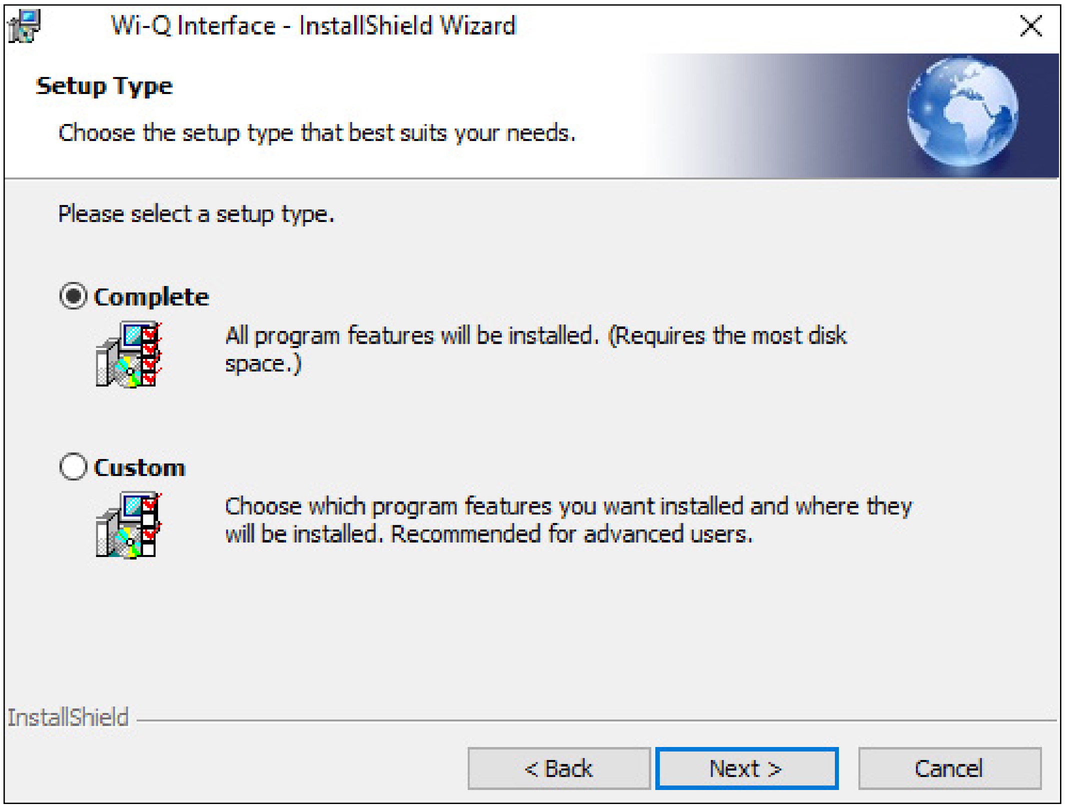
Figure 29 Connection Error Message


Wi-Q Interface

Error 27502. Could not connect to Microsoft SQL Server '(local)/'. [DBNETLIB][ConnectionOpen (Connect()).]Specified SQL server not found. (6)

9 The next step requires you to choose either a Complete Setup Type or Custom Setup Type. See Figure 30. Selecting Complete will install the BEST Wi-Q Interface, the BEST Wi-Q Interface Configuration Tool and the BEST Wi-Q Interface Database. Selecting Custom will allow you to choose which components to install. Once you've made your selection, press Next to continue.

Figure 30 Choose Setup Type



Wi-Q Interface - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Complete**

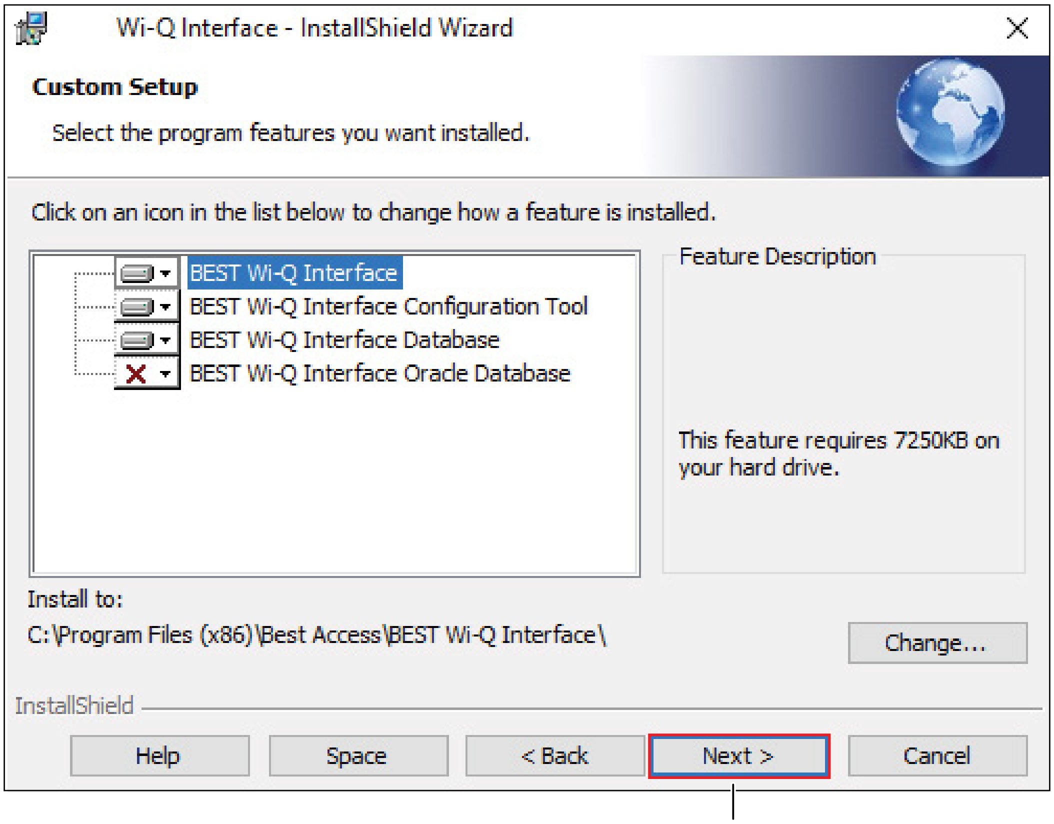
All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

Figure 31 shows the installation components available in a Custom Setup.

Figure 31 Custom Setup



Wi-Q Interface - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- BEST Wi-Q Interface
- BEST Wi-Q Interface Configuration Tool
- BEST Wi-Q Interface Database
- ✗ BEST Wi-Q Interface Oracle Database

Feature Description

This feature requires 7250KB on your hard drive.

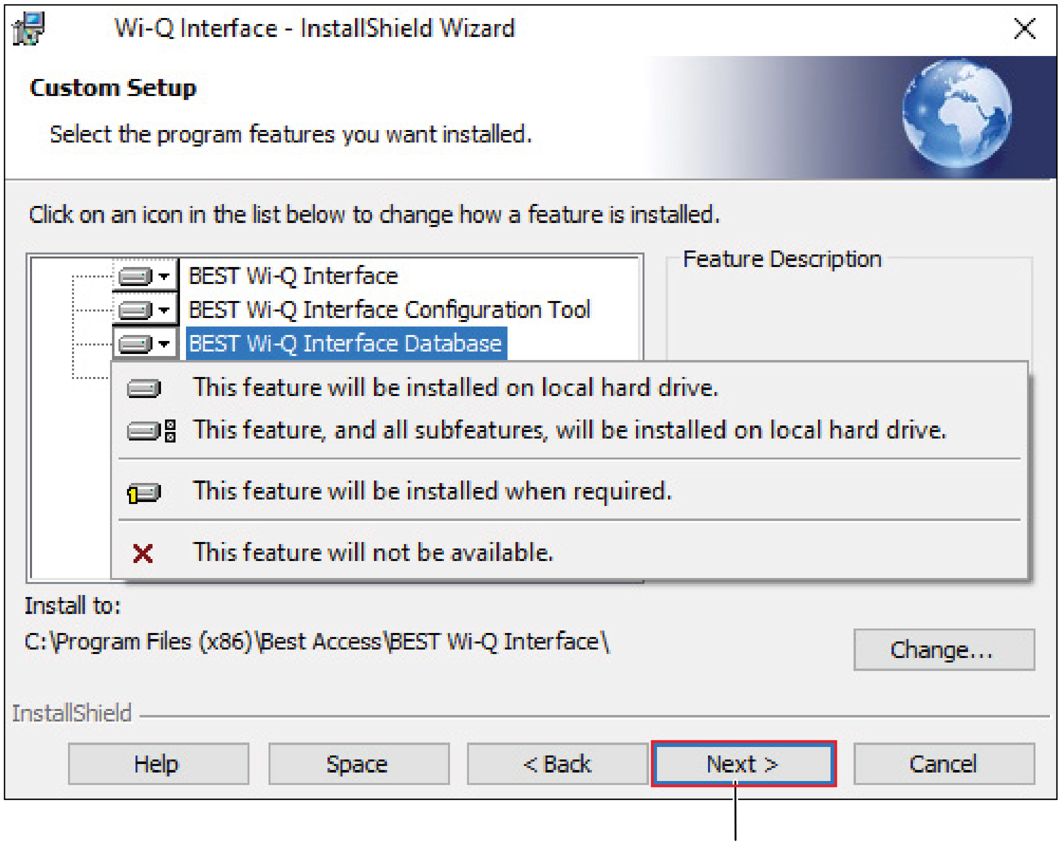
Install to:

C:\Program Files (x86)\Best Access\BEST Wi-Q Interface\

Click Next

Clicking on the icons to the left of each component will bring up installation options (Figure 32). If you decide on a Custom Setup, you must select an installation option for each component. Then click Next to continue.

Figure 32 Custom Setup Options



Wi-Q Interface - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- BEST Wi-Q Interface
- BEST Wi-Q Interface Configuration Tool
- BEST Wi-Q Interface Database

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

This feature will be installed when required.

This feature will not be available.

Feature Description

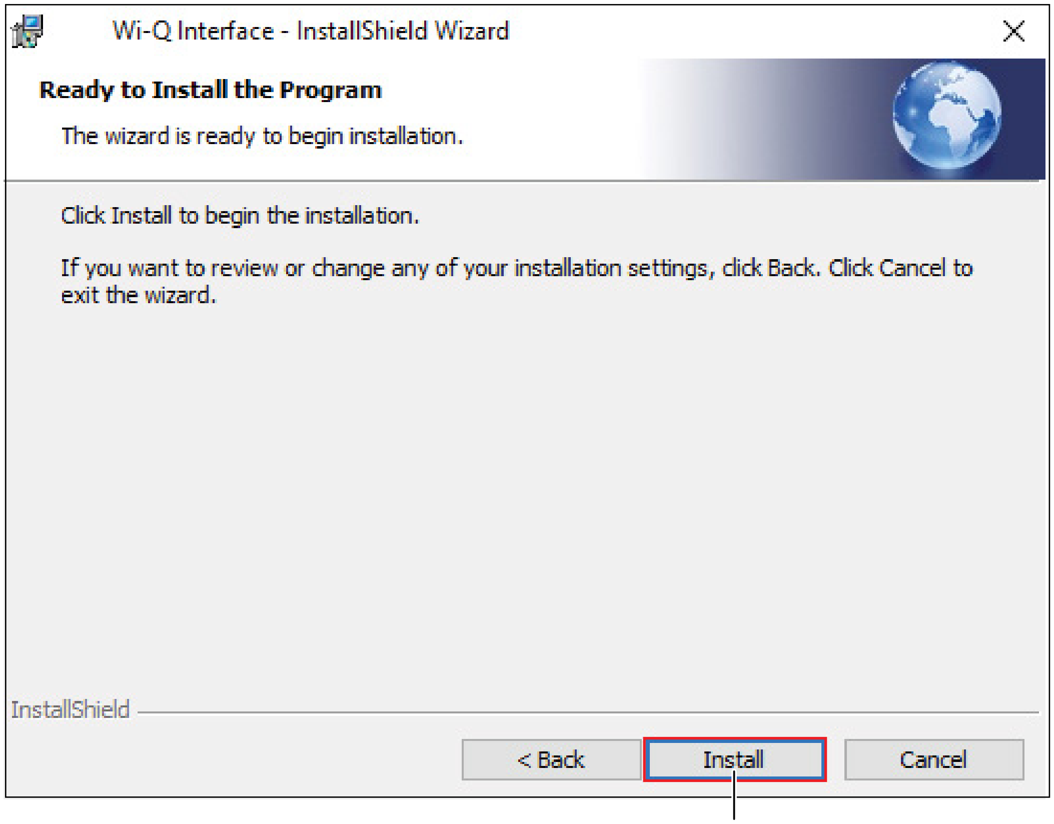
Install to:

C:\Program Files (x86)\Best Access\BEST Wi-Q Interface\

Click Next

10 The wizard is now ready to begin installation. Click Install.

Figure 33 Begin Installation



Wi-Q Interface - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

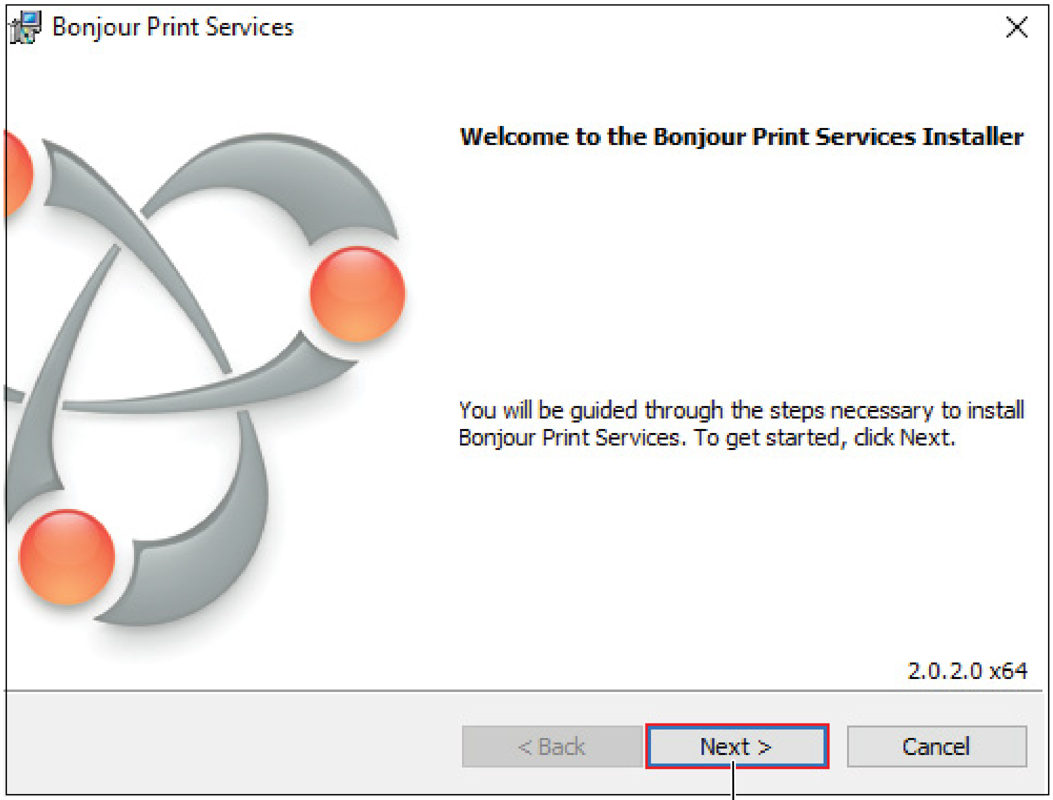
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Click Install

11 At this point, the Bonjour® Print Services Installer window will pop up. Bonjour networking technology is used by the Wi-Q Interface Configuration Tool to locate and list all Wi-Q Gateways on the network. Click Next to begin installing Bonjour.

Note If performing a Custom Setup, Bonjour will only be installed if the Wi-Q Interface Configuration Tool is being installed.

Figure 34 Bonjour Print Services Installer



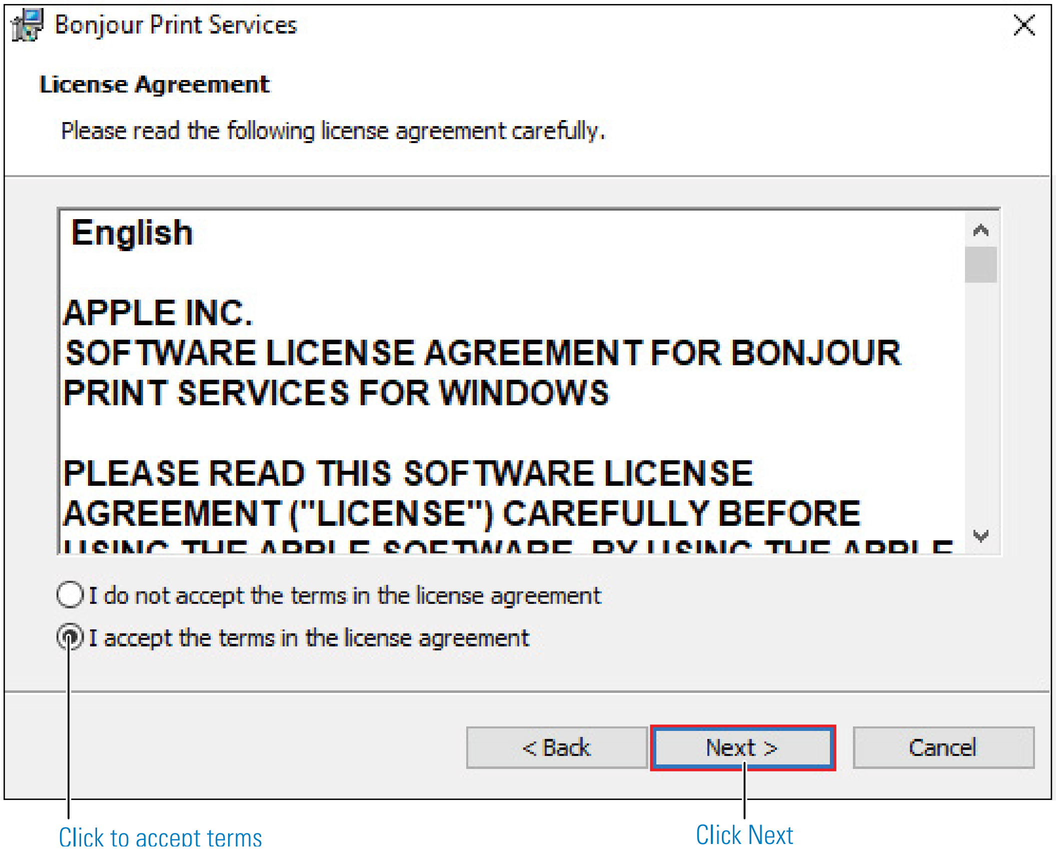
Welcome to the Bonjour Print Services Installer

You will be guided through the steps necessary to install Bonjour Print Services. To get started, click Next.

Click Next

12 Read the License Agreement. To continue with the installation, click on “I accept the terms in the license agreement,” then press Next.

Figure 35 Bonjour Print Services License Agreement



Bonjour Print Services

License Agreement

Please read the following license agreement carefully.

English

APPLE INC.
SOFTWARE LICENSE AGREEMENT FOR BONJOUR PRINT SERVICES FOR WINDOWS

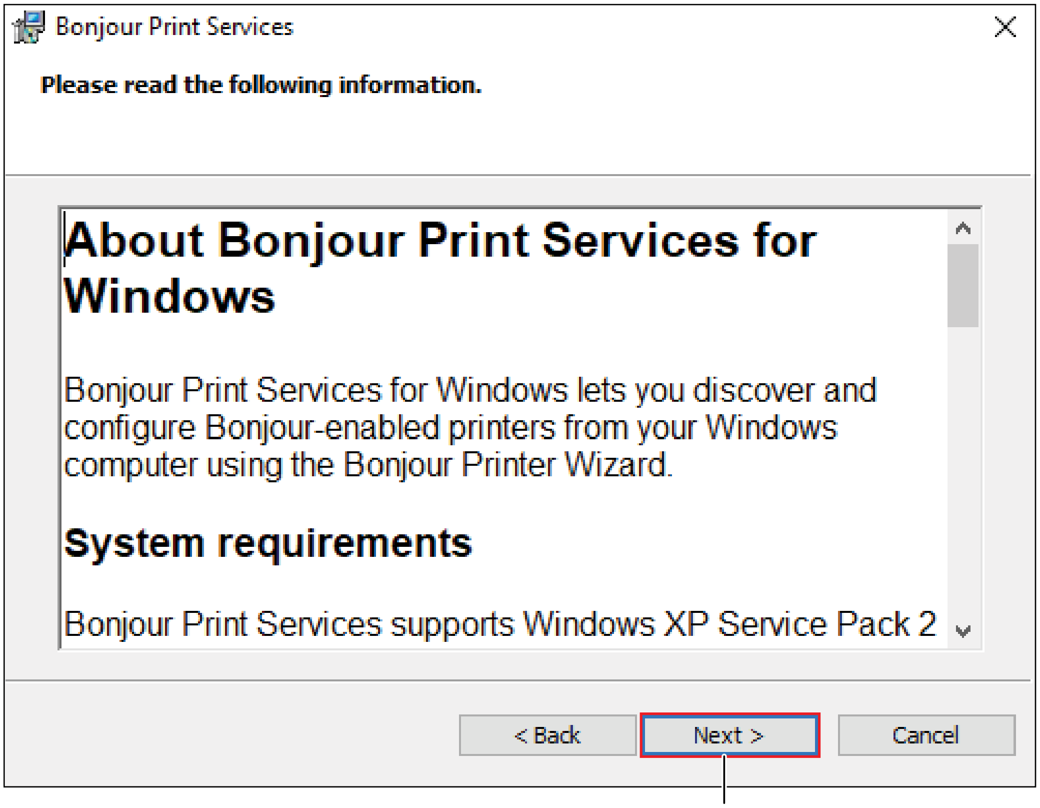
PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE

○ I do not accept the terms in the license agreement

● I accept the terms in the license agreement

13 Read the information about Bonjour Print Services. Then press Next.

Figure 36 Bonjour Print Services Information



Bonjour Print Services

Please read the following information.

About Bonjour Print Services for Windows

Bonjour Print Services for Windows lets you discover and configure Bonjour-enabled printers from your Windows computer using the Bonjour Printer Wizard.

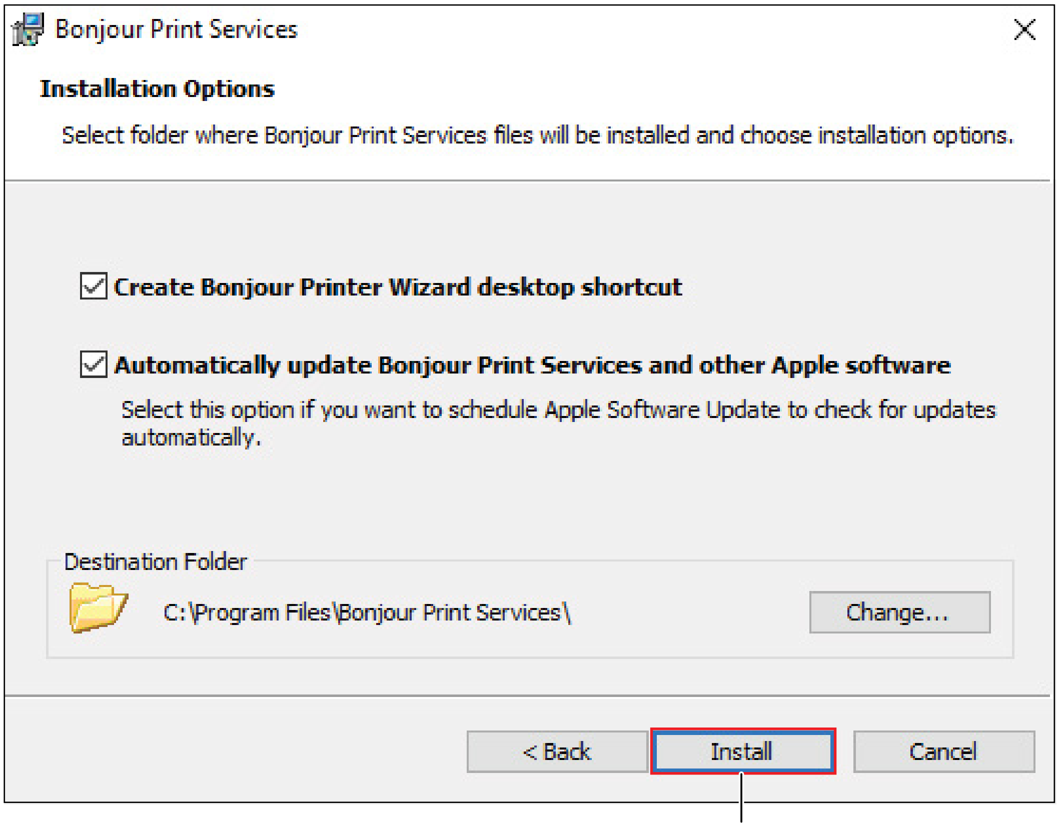
System requirements

Bonjour Print Services supports Windows XP Service Pack 2

Click Next

14 In the Installation Options section, decide whether or not to create a desktop shortcut and/or schedule automatic updates for Bonjour. Choose your destination folder and then select Install.

Figure 37 Bonjour Installation Options



Bonjour Print Services

Installation Options

Select folder where Bonjour Print Services files will be installed and choose installation options.

☑ **Create Bonjour Printer Wizard desktop shortcut**

☑ **Automatically update Bonjour Print Services and other Apple software**

Select this option if you want to schedule Apple Software Update to check for updates automatically.

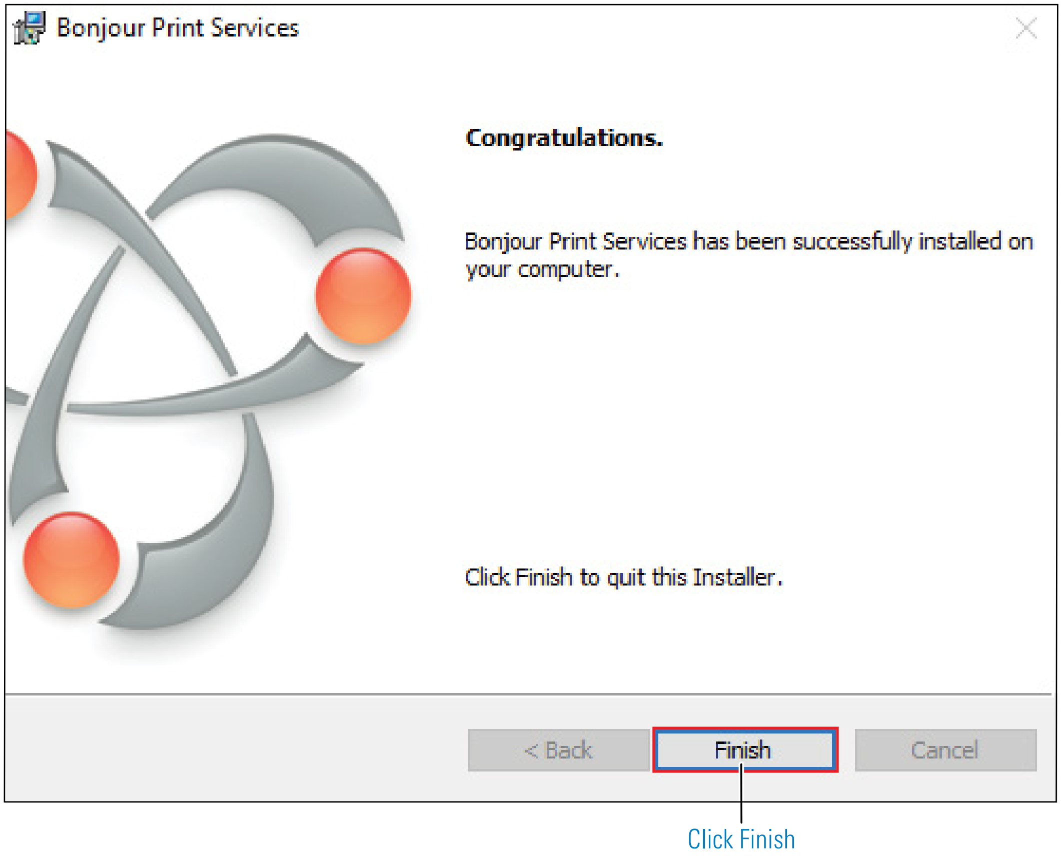
Destination Folder

C:\Program Files\Bonjour Print Services\

Click Install

15 Once the Bonjour Print Services Installation is complete, press Finish.

Figure 38 Bonjour Print Services Installation Complete



Bonjour Print Services

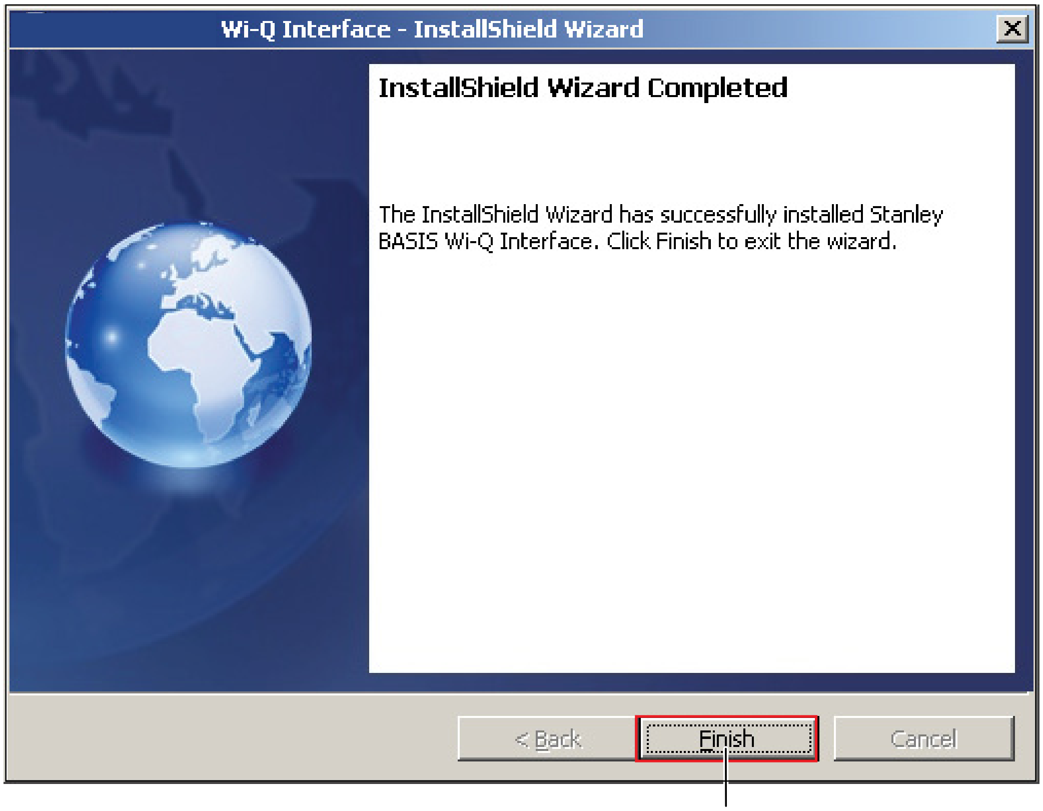
Congratulations.

Bonjour Print Services has been successfully installed on your computer.

Click Finish to quit this Installer.

16 The Wi-Q Interface components now begin to install. Once installation is complete, press Finish.

Figure 39 Wi-Q Interface Installation Complete



Wi-Q Interface - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Stanley BASIS Wi-Q Interface. Click Finish to exit the wizard.

Click Finish

17 You may now start up your Communication Server again. See “Stop Communication Server” on page 48 for more information on how to access it.

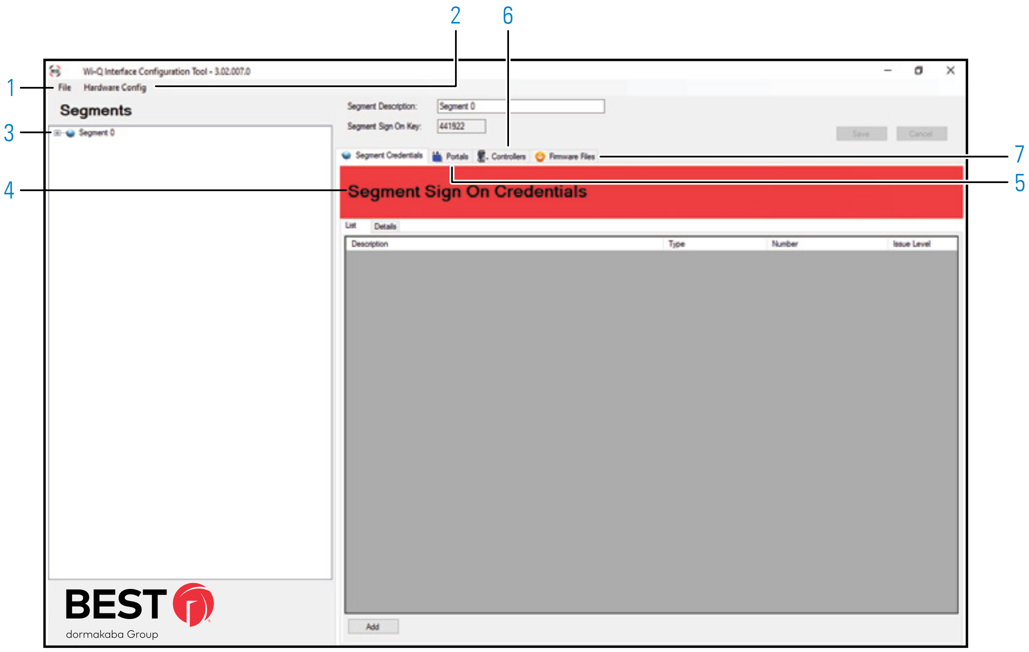
4 Software Configuration and Use

This chapter will guide you through Task 6 (Configure Wi-Q Gateways) and Task 10 (Configure Software) and Firmware Updates. It will also provide a useful term comparison chart for events and transactions in Alarm Monitoring and the Wi-Q Interface Configuration Tool.

Wi-Q Interface Configuration Tool Overview

This section will provide a brief overview of the components in the Wi-Q Interface Configuration Tool. See Figure 40.

Figure 40 Wi-Q Interface Configuration Tool



Wi-Q Interface Configuration Tool - 3.02.007.0

Segment Description: Segment 0

Segment Sign On Key: 441922

Segment Sign On Credentials

Description	Type	Number	Issue Level

1 **File menu dropdown**
Contains three options: (1) Database Connect (2) Change Password and (3) Exit. You can use Database Connect tool if you must connect to additional databases or if you move the location of the database and must connect to it again.

2 **Hardware Config menu dropdown**
Contains two options: (1) Wi-Q Gateways and (2) Firmware Reprogram. The Portals tool is used to add and configure Wi-Q gateways. The Firmware Reprogram tool is used to send firmware updates to your wireless hardware.

3 **Segments tree**
Provides a visual representation of which Wi-Q Gateways are associated with which segment and which Wireless Controllers are associated with which Wi-Q Gateways. Right-clicking on hardware items listed in the tree will provide additional options.

4 **Segment Credentials tab**
Allows you add Sign On Credentials so you can sign on wireless card readers.

5 **Portals tab**
Displays a list of BEST® Wi-Q Gateways and details about each one.

6 **Controllers tab**

Displays a list of Wireless Controllers and details about each one.

7 **Firmware files tab**

Used to upload firmware files to the database.

Configure Wi-Q Gateways (Task 6)

Wi-Q Gateways can now be added and configured within the Wi-Q Interface Configuration Tool. This can be performed on a single Wi-Q Gateway or multiple Wi-Q Gateways at a time. This task is performed in the Portal Configuration window, which utilizes Bonjour to locate and list all Wi-Q Gateways on the network.

Wi-Q Gateways are configured from the factory with an IP address of 192.168.1.200 and the gateway webpage can be accessed with IP address 192.168.3.200 (for configuration only) when connected to gateway WiFi. When configuring a Wi-Q Gateway, it is best to connect directly to the Wi-Q Gateway before placing it on the network. This removes the possibility of duplicate IP addresses on the network.

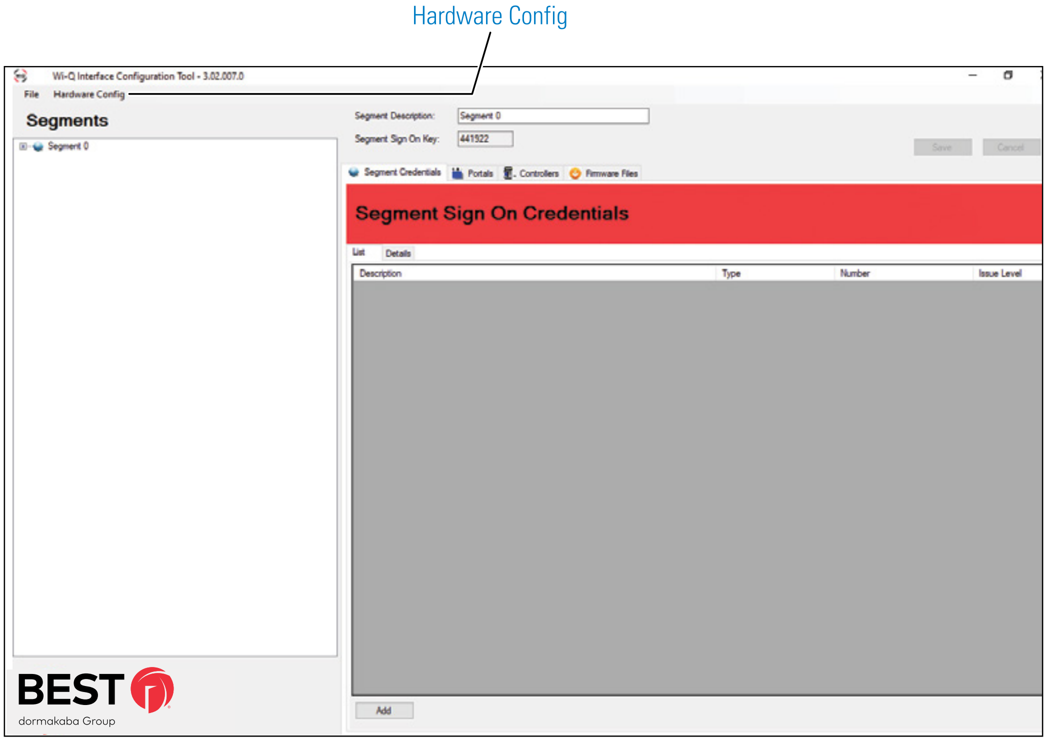
Note You will need to create and reserve a range of IP addresses for your Wi-Q Gateways before proceeding with Wi-Q Gateway configuration.

To Configure a Wi-Q Gateway:

1 Connect the Wi-Q Gateway to the Host either over LAN or WiFi or directly via crossover Ethernet cable (recommended). For more information on connecting a Wi-Q Gateway, see “Connecting the Gateway and Verifying Operation” on page 26.

2 Inside the Wi-Q Interface Configuration Tool, click on Hardware Config, and select Portals. See Figure 41.

Figure 41 Configure Wi-Q Gateway

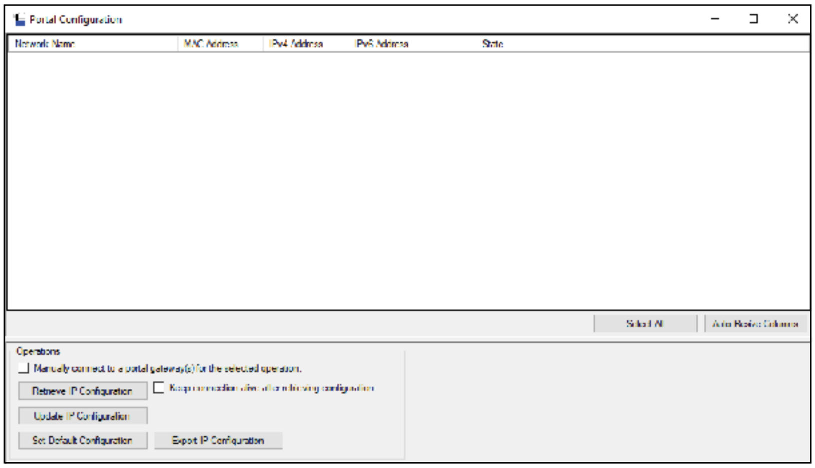


Segment Description: Segment 0

Segment Sign On Key: 441922

3 The Portal Configuration window lists the BEST® Wi-Q Gateways on the network.

Figure 42 Portal Configuration Tool

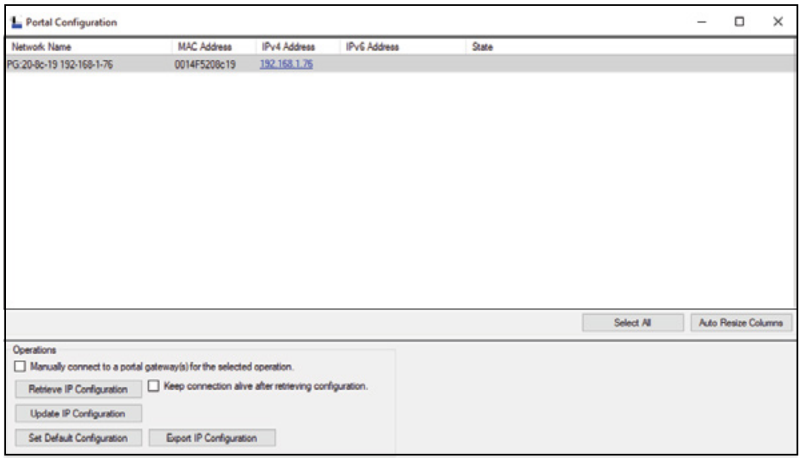


□ Manually connect to a portal gateway(s) for the selected operation.

□ Keep connection alive after retrieving configuration

4 Select a Wi-Q Gateway from the list.

Figure 43 Portal Configuration Tool with PG



Portal Configuration

Network Name	MAC Address	IPv4 Address	IPv6 Address	State
PG:20-8c-19 192-168-1-76	0014F5208c19	192.168.1.76		

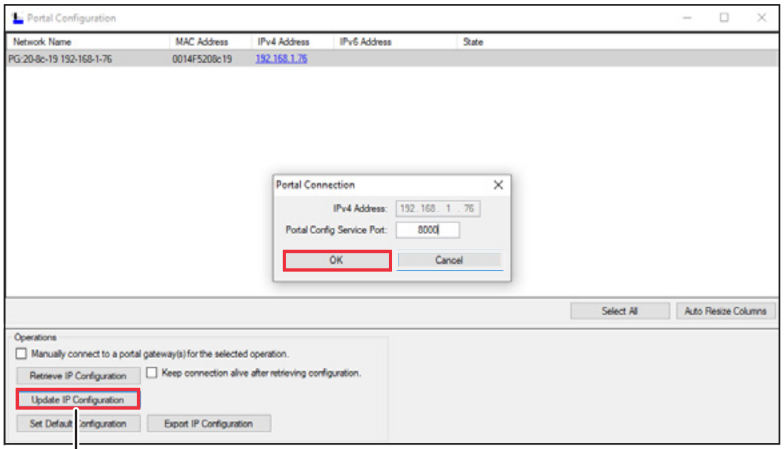
Operations

□ Manually connect to a portal gateway(s) for the selected operation.

□ Keep connection alive after retrieving configuration.

5 At this point, you may change the IP address from the factory setting to one from the range you've created. Select Update IP Configuration button and change the Portal Config Service port to 8000, click OK button.

Figure 44 Update IP Address



Portal Configuration

Network Name	MAC Address	IPv4 Address	IPv6 Address	State
PG:20-8c-19 192-168-1-76	0014F5208c19	192.168.1.76		

Portal Connection

IPv4 Address: 192 . 168 . 1 . 76

Portal Config Service Port: 8000

Operations

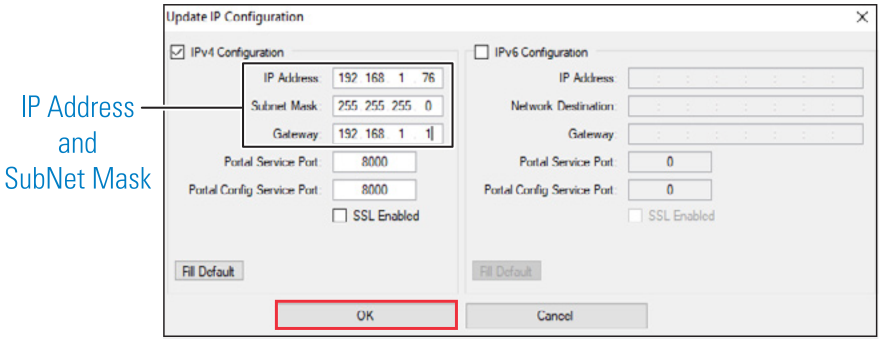
□ Manually connect to a portal gateway(s) for the selected operation.

□ Keep connection alive after retrieving configuration.

Update IP Configuration

6 You may need to adjust the SubNet Mask to match your network. Consult your network administrator for details.

Figure 45 Update IP Configuration



IP Address and SubNet Mask

Update IP Configuration

☑ IPv4 Configuration

IP Address: 192 . 168 . 1 . 76

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 1 . 1

Portal Service Port: 8000

Portal Config Service Port: 8000

☐ SSL Enabled

☐ IPv6 Configuration

IP Address:

Network Destination:

Gateway:

Portal Service Port: 0

Portal Config Service Port: 0

☐ SSL Enabled

Note Change the Portal Config Service Port to 8000.

7 If you have a direct connection to the Wi-Q Gateway, and you have changed the IP address, click on the OK button to update the selected Wi-Q Gateway.

Configure Software (Task 10)

The sub-tasks below are required to configure your software to communicate with your Wi-Q hardware. These should be performed in the order presented here.

1 Add Wi-Q Gateways as Access Panels in OnGuard.

2 For Wireless Card Readers only — Add Segment Sign on Credentials in Wi-Q Interface Configuration Tool

3 Add signed on Wireless Controllers to Readers and Doors

4 Configure Wi-Q Gateways and Controllers in Wi-Q Interface Configuration Tool

Also in this section, you will find additional notes for configuring Cardholder Options, Card Formats, Timezones, Timezone/Reader Modes, Cardholders and Segments. You will also find information about Firmware Updates in the Wi-Q Interface Configuration Tool. Finally, you will be provided with a term comparison chart of events/transactions that are viewable in Alarm Monitoring and the Controllers tab of Wi-Q Interface software.

Add Wi-Q Gateways as Access Panels

Perform the following steps to add your Wi-Q Gateways as Access Panels in System Administration. For more information on Access Panels and/or System Administration, see the System Administration User Guide.

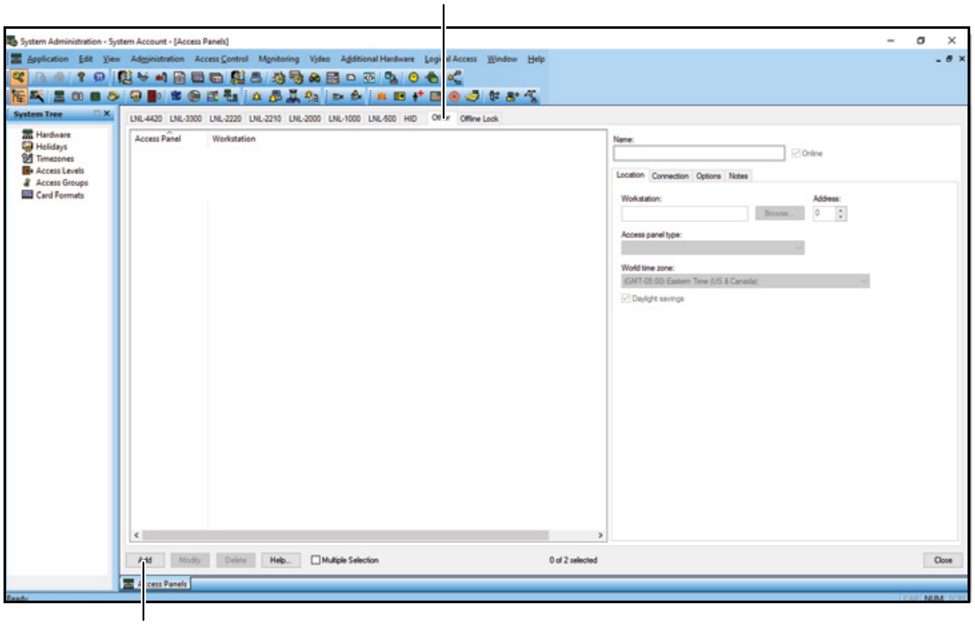
Note A Access Panel corresponds to a single BEST® Wi-Q Gateway. By default in OnGuard, the controller capacity is set to 64 controllers.

1 Open System Administration and navigate to the Access Panels module (Access Control > Access Panels).

2 Click on the Other tab, then click Add. (Figure 46).

Figure 46 Add Access Panel

Click Other



System Administration - System Account - [Access Panels]

Name:

☑ Online

Workstation:

Address: 0

Access panel type:

World time zone: (GMT-05:00) Eastern Time (US & Canada)

☑ Daylight savings

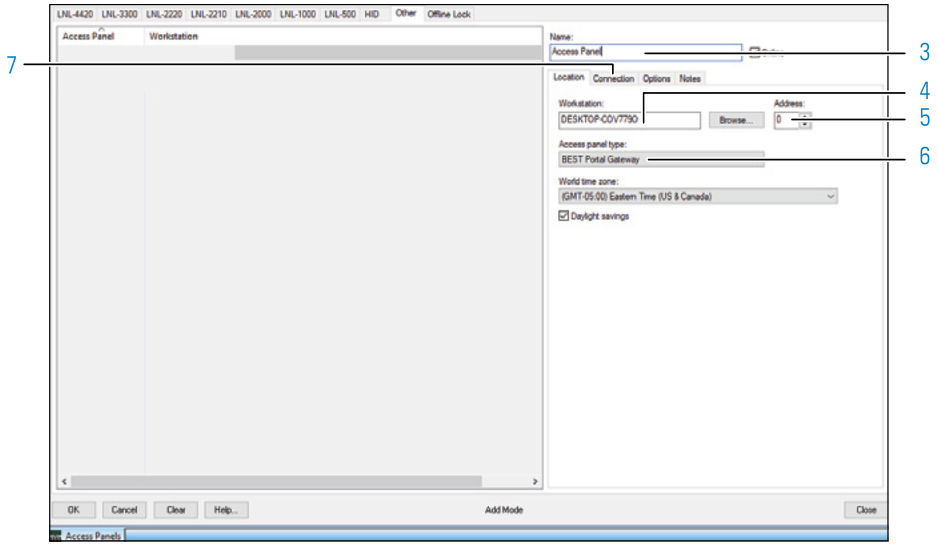
☐ Multiple Selection

0 of 2 selected

Click Add

3 In the Name field, type a unique name for your Wi-Q Gateway (Figure 47).

Figure 47 Access Panel Location Tab



Name: Access Panel

Workstation: DESKTOP-COV7790

Address: 0

Access panel type: BEST Portal Gateway

World time zone: (GMT-05:00) Eastern Time (US & Canada)

☑ Daylight savings

4 Type in or browse to the computer name of the server.

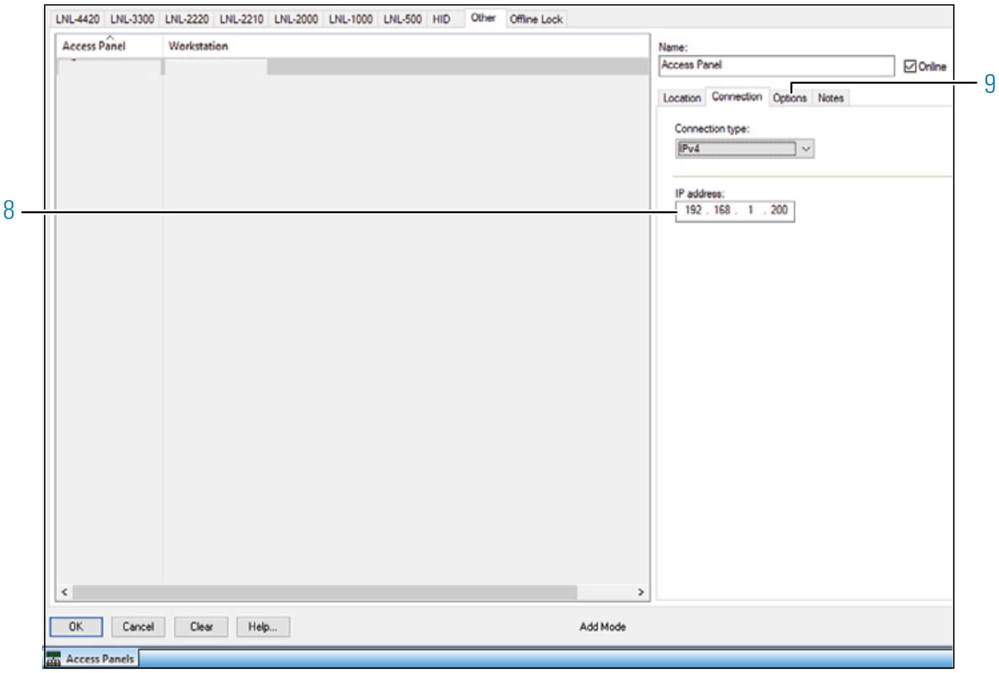
5 Set the Address field to a number between 0 and 7.

6 From the Access Panel Type dropdown list, select BEST Wi-Q Gateway.

7 Next, click on the Access Panels Connection tab.

8 Select LAN and enter the unique IP address of the Wi-Q Gateway. See Figure 48.

Figure 48 Access Panels Connection Tab



Name: Access Panel

☑ Online

Connection type: IPv4

IP address: 192 . 168 . 1 . 200

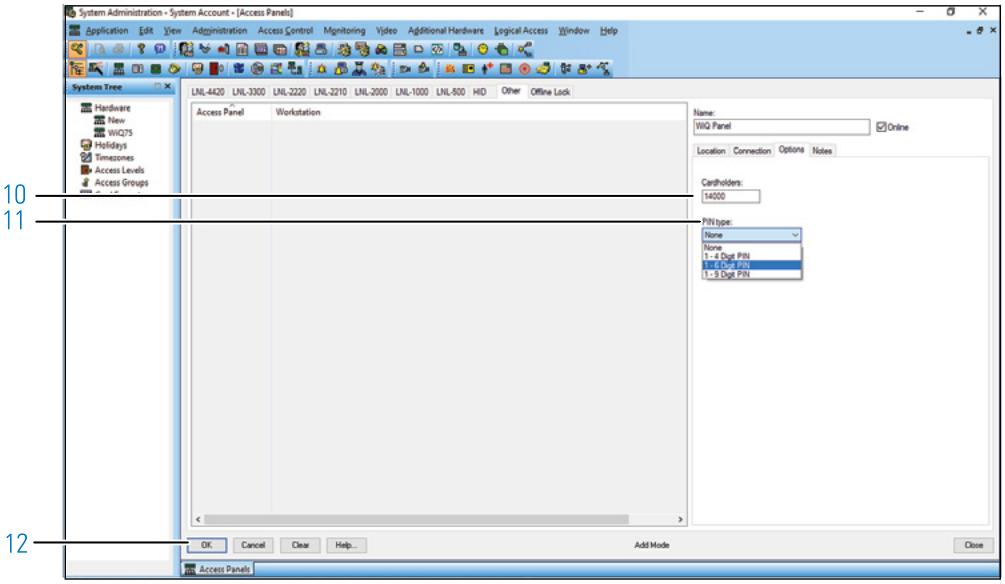
9 Next, click the Options tab.

10 In the Cardholders field, type in 14000 (Figure 49).

11 From the PIN type dropdown, select either “1-4 Digit PIN” or “1-6 Digit Pin.”

Note BEST Wi-Q technology does not support PINs longer than 6 digits.

Figure 49 Access Panels Options Tab



System Administration - System Account - [Access Panels]

Name: WIQ Panel ☑ Online

Cardholders: 14000

PIN type: None

12 Then, click OK.

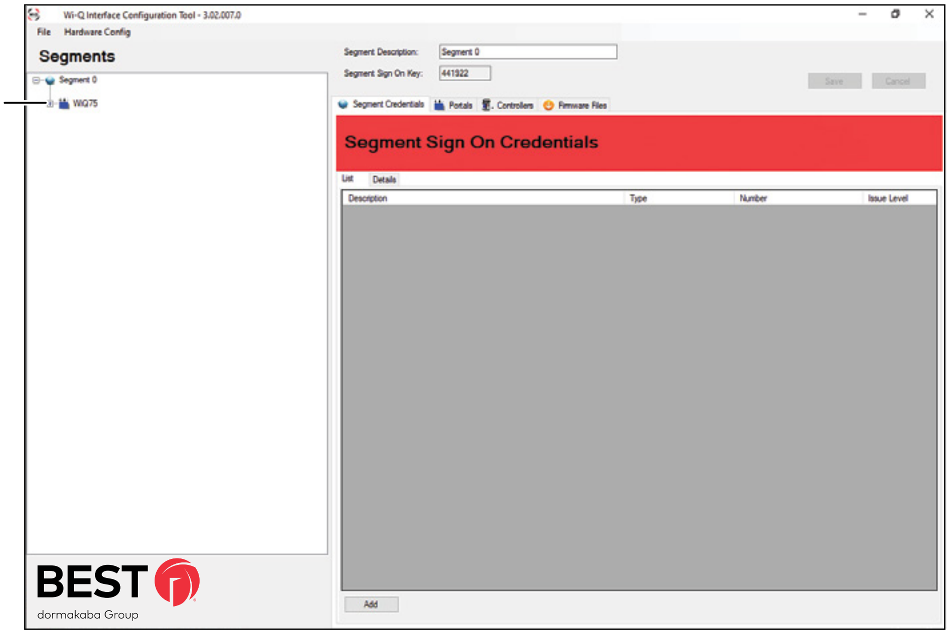
Once you have created Access Panels in OnGuard to match the Wi-Q Gateways that you configured in the Wi-Q Interface Configuration Tool (and your Wi-Q Gateways are on the network), the Wi-Q Gateways will become visible in the Segments Tree and Portals tab of the Wi-Q Interface Configuration Tool. See “Portals Tab” on page 78.

Segments and Segment Sign On Credentials

When a panel is created in OnGuard, it is assigned to a segment. In the Wi-Q Interface Configuration Tool, the Segments tree (Figure 50) provides a visual representation of which Wi-Q Gateways are associated with which segment. There are no limitations to the number of Wi-Q Gateways that can be assigned to one segment, and there are no limitations to the number of segments.

Note The option to delete a segment from the Segment tree becomes available when you right-click from within the tree.

Figure 50 Segments Tree



Segments Tree

Wi-Q Interface Configuration Tool - 3.02.007.0

Segment Description: Segment 0

Segment Sign On Key: 441922

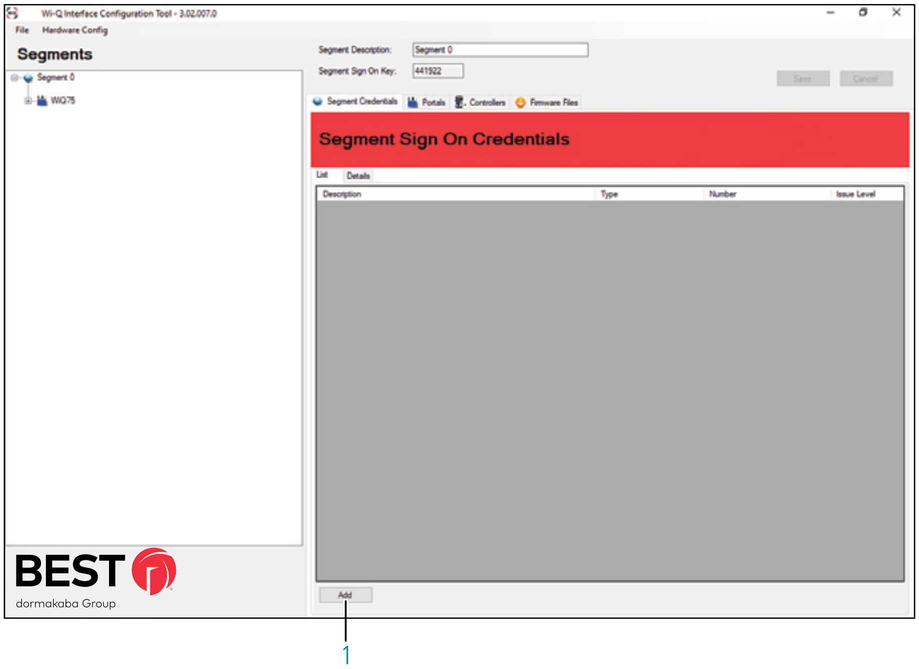
For each segment, the Wi-Q Interface Configuration Tool creates a unique Segment Sign On Key that is used to sign Wireless Controllers onto a segment. This Sign On Key is used when signing on Wireless keypad controllers (See “Signing on Keypad Controllers” on page 33).

The Segment Credentials tab allows you add Sign On Credentials so you can sign on wireless card readers.

To add a new Sign On Credential

1 Select Add.

Figure 51 Add Segment Sign On Credential

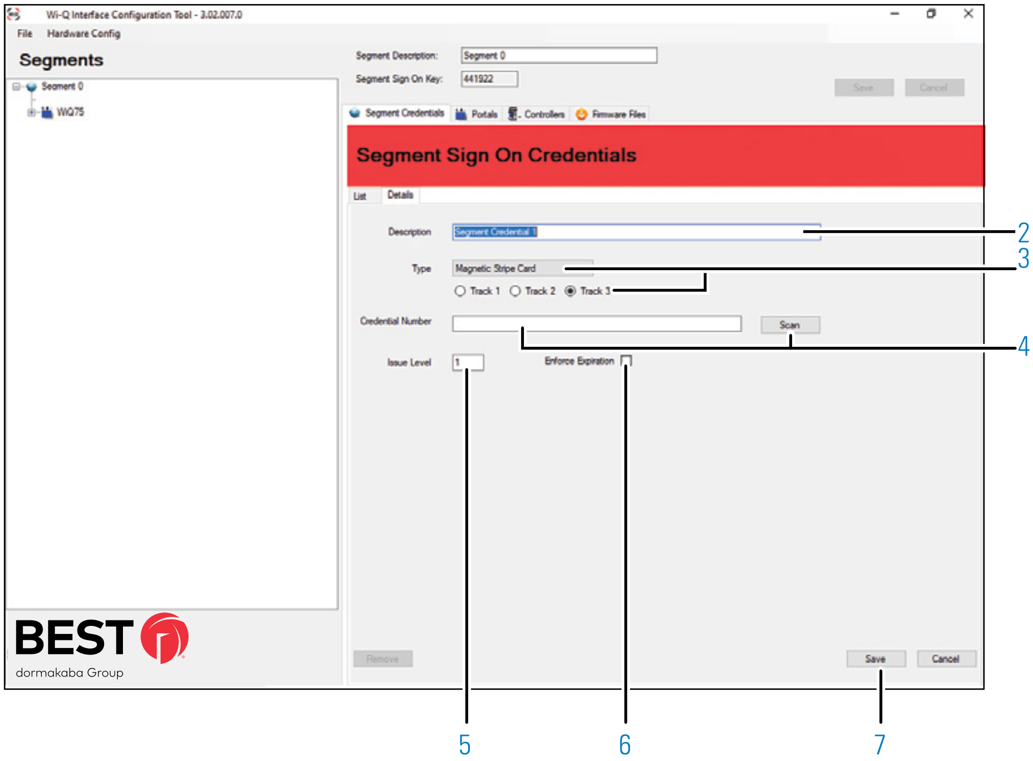


Segment Description: Segment 0

Segment Sign On Key: 441922

Description	Type	Number	Issue Level

Figure 52 Segment Sign On Credentials



Wi-Q Interface Configuration Tool - 3.02.007.0

Segment Description: Segment 0

Segment Sign On Key: 441922

Segment Sign On Credentials

Description: Segment Credential 1

Type: Magnetic Stripe Card

○ Track 1 ○ Track 2 ● Track 3

Credential Number:

Issue Level: 1

Enforce Expiration □

2 Enter a unique description in the Description field.

3 Select an option from the Type dropdown menu. If you've selected Magnetic Stripe Card, select the corresponding Track location.

4 Enter a credential number in the Credential Number field, or attach a USB card reader, press Scan, and scan the card with the reader.

5 Enter an issue code in the Issue Level field (if applicable).

6 If needed, check the Enforce Expiration checkbox to enforce an expiration date.

7 Select Save. This will trigger your Wi-Q Gateway(s) to download the saved information.

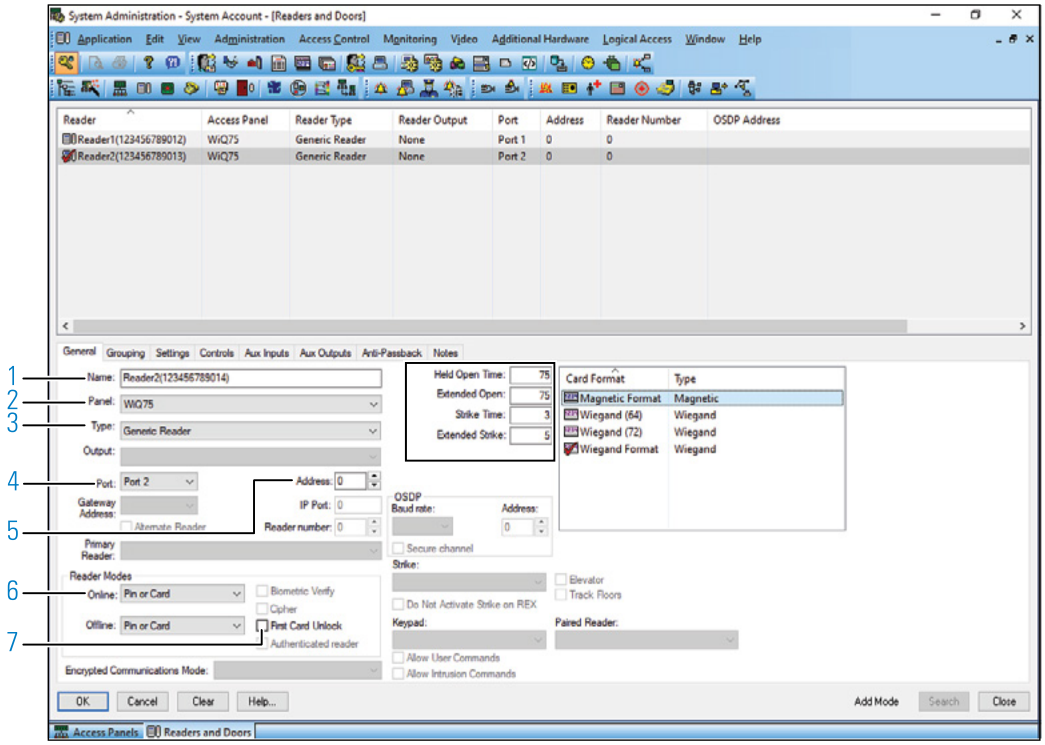
To sign on your card readers, see "Sign on Controllers (Task 9)" on page 32. Once you've signed on your Wireless Controllers, they will be visible in the Wi-Q Interface Configuration Tool Segment tree and Controllers tab.

Now, you can set up your Wireless Controllers in the Reader and Doors Module of System Administration.

Add Signed On Wireless Controllers to Readers and Doors

The Wi-Q Interface supports a maximum of 64 controllers per Wi-Q Gateway. Wi-Q supports a maximum of 64 controllers per panel. Perform the following steps to add your Wireless Controllers into OnGuard (Figure 53). See the System Administration User Guide for more information on Readers and Doors.

Figure 53 Readers and Doors


System Administration - System Account - [Readers and Doors]
Application Edit View Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
1
2
3
4
5
6
7
General Grouping Settings Controls Aux Inputs Aux Outputs Anti-Passback Notes
OK Cancel Clear Help...
Add Mode Search Close
Access Panels Readers and Doors

Reader	Access Panel	Reader Type	Reader Output	Port	Address	Reader Number	OSDP Address
Reader1(123456789012)	WiQ75	Generic Reader	None	Port 1	0	0	
Reader2(123456789013)	WiQ75	Generic Reader	None	Port 2	0	0	

Name: Reader2(123456789014)
Panel: WiQ75
Type: Generic Reader
Output:
Port: Port 2
Gateway Address:
□ Alternate Reader
Address: 0
IP Port: 0
Reader number: 0
Primary Reader:

Reader Modes
Online: Pin or Card
Offline: Pin or Card
□ Biometric Verify
□ Cipher
□ First Card Unlock
□ Authenticated reader

Encrypted Communications Mode:

Held Open Time: 75
Extended Open: 75
Strike Time: 3
Extended Strike: 5

OSDP
Baud rate:
Address: 0
□ Secure channel
Strike:
□ Do Not Activate Strike on REX
Keypad:
□ Allow User Commands
□ Allow Intrusion Commands

Card Format	Type
Magnetic Format	Magnetic
Wiegand (64)	Wiegand
Wiegand (72)	Wiegand
Wiegand Format	Wiegand

□ Elevator
□ Track Floors
Paired Reader:

1 In the Name field, enter a name for your Controller. The name must contain the MAC Address of the Controller within parenthesis (). For example: Upstairs IT Closet (123456780006)

2 From the Panel dropdown, select the Wi-Q Gateway to which the Controller is being assigned.

3 From the Type dropdown, select Generic Reader.

4 From the Port dropdown, select a unique port number (if needed).

5 In the Address field, provide a unique address (if needed).

6 In the Online field, under Reader Modes, select a default reader mode.

7 Select First Card Unlock to enable this mode. Doors configured with first card unlock will not unlock until valid personnel presents their card.

8 Select a Card Format to use. Even if you are using a keypad pin for sign-on you must select a Card Format.

9 Select OK to create the Reader.

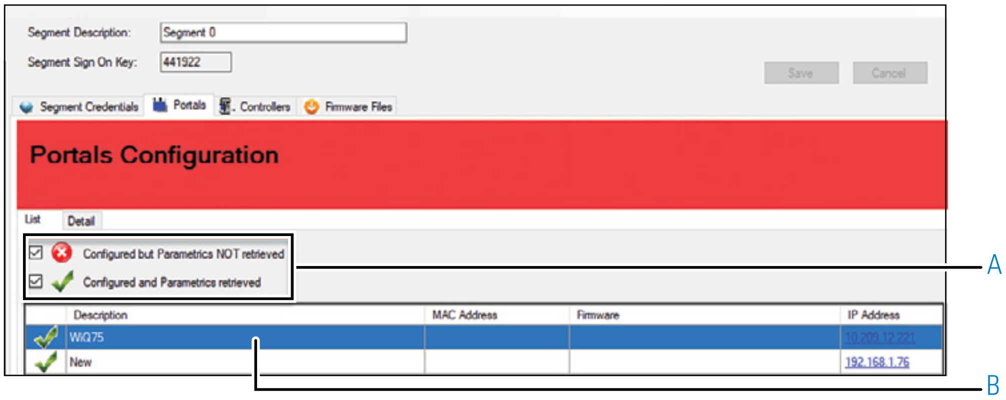
Configure Wi-Q Gateways and Controllers in Wi-Q Interface Configuration Tool

Although you already performed most of the Wi-Q Gateway and Controller configuration in OnGuard, additional configuration options can be found in the Wi-Q Gatewaysals and Controllers tabs inside the Wi-Q Interface Configuration Tool.

Portals Tab

The Portals List tab displays a list of BEST® Wi-Q Gateways along with their MAC address and current firmware version (Figure 54). The Status Legend (Item A) shows the two levels of configuration that exist for Wi-Q Gateways: (1) Configured but parametrics NOT retrieved (2) Configured and parametrics retrieved. Clicking the checkboxes next to the icons in the Status Legend will display Wi-Q Gateways matching those configurations in the Portals List (Item B) below.

Figure 54 Portals List Tab



Segment Description: Segment 0

Segment Sign On Key: 441922

☑ ✗ Configured but Parametrics NOT retrieved

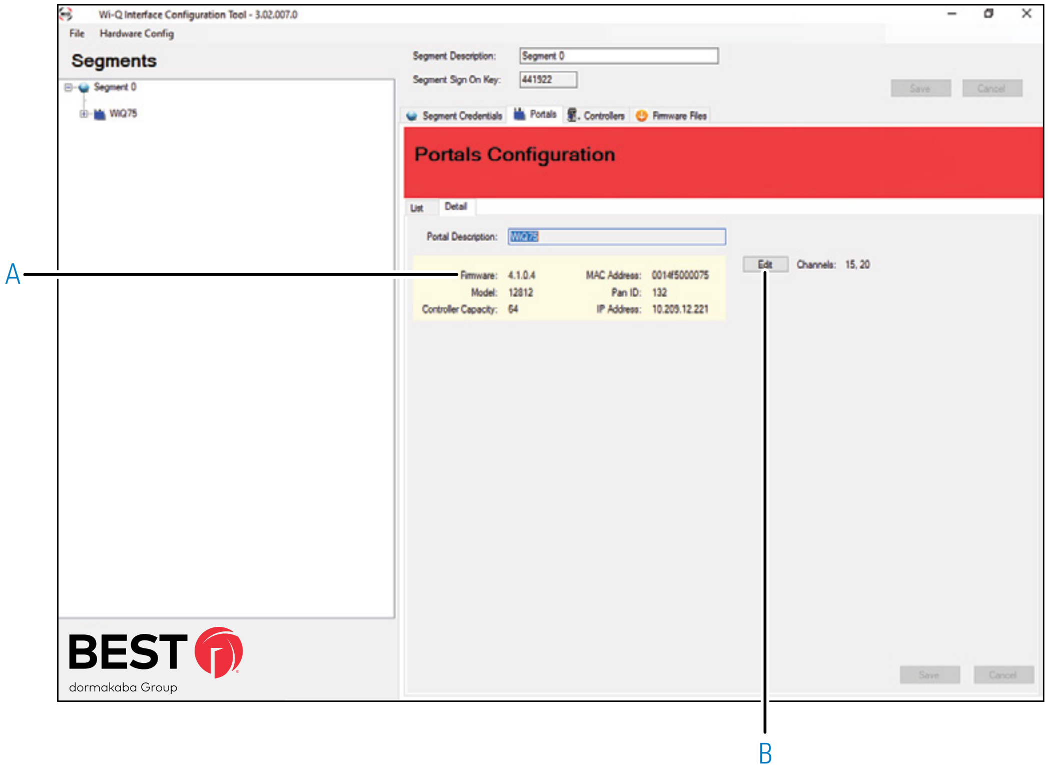
☑ ✓ Configured and Parametrics retrieved

	Description	MAC Address	Firmware	IP Address
✓	WiQ75			10.209.12.221
✓	New			192.168.1.76

Note The options to Navigate, Delete and Reset the Wi-Q Gateway become available when you right-click on it within the segment tree.

Clicking on the Description for a given Wi-Q Gateway displays detailed information about it in the Details tab (Figure 55).

Figure 55 Portals Detail Tab



Segment Description: Segment 0

Segment Sign On Key: 441922

Portal Description: WIQ75

Firmware: 4.1.0.4

Model: 12812

Controller Capacity: 64

MAC Address: 0014f5000075

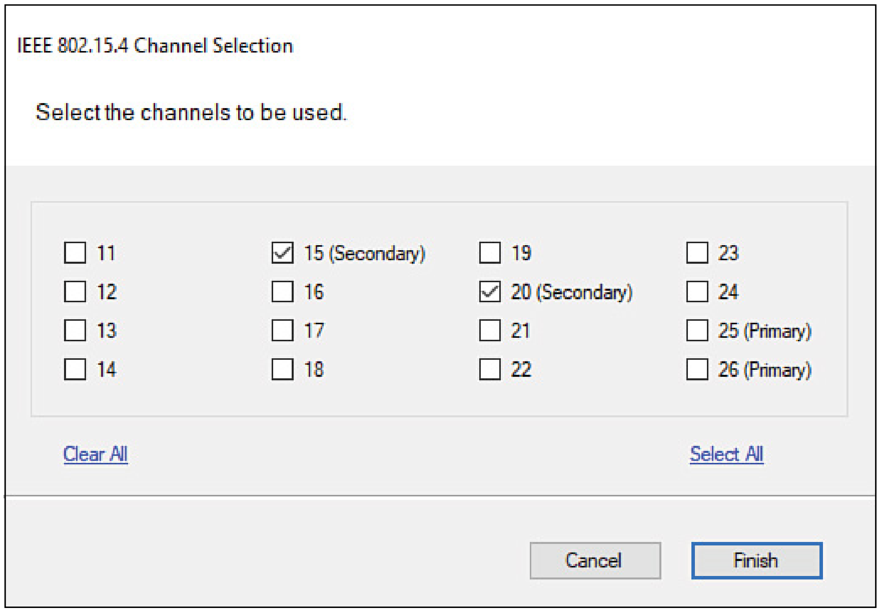
Pan ID: 132

IP Address: 10.209.12.221

Channels: 15, 20

The Details box (Item A) displays the selected Wi-Q Gateway’s Firmware version, Model number, Controller Capacity, MAC Address, and Panel ID. Clicking on Edit (Item B) will open the Channel Selection window (Figure 56).

Figure 56 Portals Channel Selection Window



IEEE 802.15.4 Channel Selection

Select the channels to be used.

☐ 11
☐ 12
☐ 13
☐ 14
☑ 15 (Secondary)
☐ 16
☐ 17
☐ 18
☐ 19
☑ 20 (Secondary)
☐ 21
☐ 22
☐ 23
☐ 24
☐ 25 (Primary)
☐ 26 (Primary)

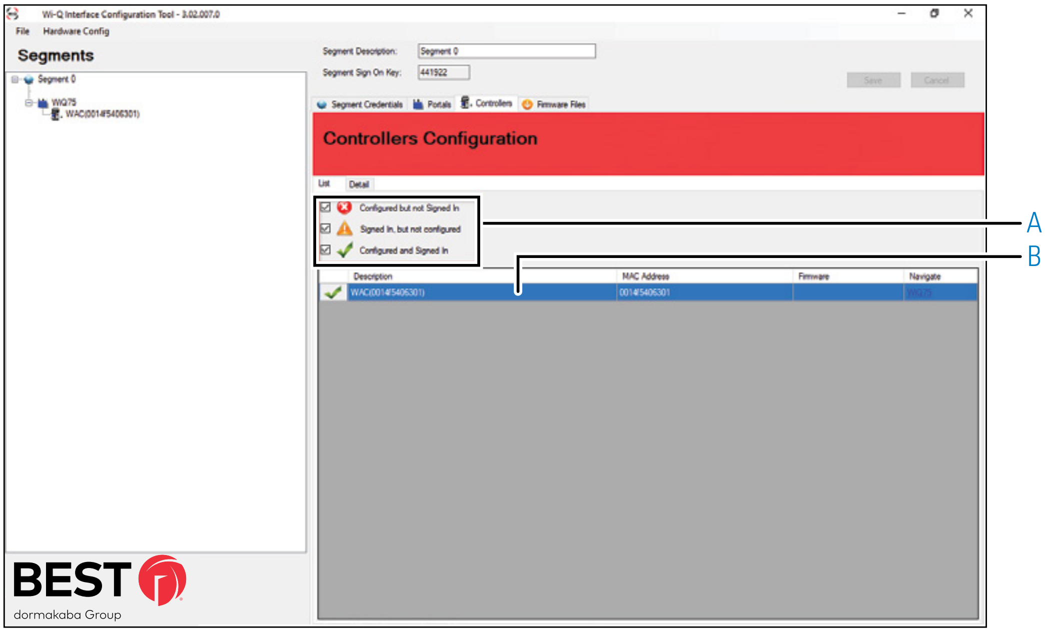
The channels selected for the Wi-Q Gateway must be enabled for the Controller as well. Channels 25 and 26 are selected by default. If you change the channel configuration, select Save to trigger the interface to send the updated information to your wireless hardware.

Controllers Tab

The Controllers List tab displays a list of BEST® Wi-Q Controllers along with their MAC address and current firmware version (Figure 57). Inside the Status Legend (Figure 57, Item A), three levels of configuration exist for Wireless Controllers: 1) Configured but not Signed In (2) Signed In, but not configured and (3) Configured and Signed In. Clicking the checkboxes next to the icons in the Status Legend will display Controllers matching those configurations in the Controllers list (Item B) below.

Note Controllers are locked to a Wi-Q Gateway the first time they are signed into the system. They can be forced to another Wi-Q Gateway using the Wi-Q Interface Configuration Tool if needed. See "Moving a Controller to a Different Wi-Q Gateway" on page 84.

Figure 57 Controllers List Tab



Segment Description: Segment 0

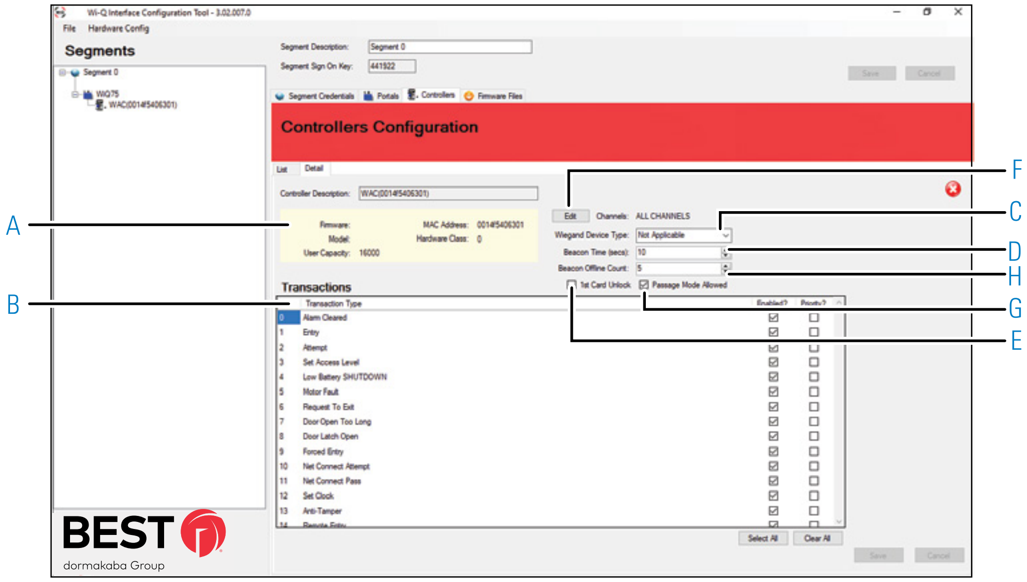
Segment Sign On Key: 441922

☑ ☒ Configured but not Signed In
☑ ⚠ Signed In, but not configured
☑ ✓ Configured and Signed In

	Description	MAC Address	Firmware	Navigate
✓	WAC(0014f5406301)	0014f5406301		WQ75

Clicking on the Description for a given Controller displays detailed information about it in the Details tab (Figure 58).

Figure 58 Controllers Detail Tab



Segment Description: Segment 0

Segment Sign On Key: 441922

Controller Description: WAC(0014f5406301)

Firmware:

Model:

User Capacity: 16000

MAC Address: 0014f5406301

Hardware Class: 0

Channels: ALL CHANNELS

Wiegand Device Type: Not Applicable

Beacon Time (secs): 10

Beacon Offline Count: 5

□ 1st Card Unlock ☑ Passage Mode Allowed

Transactions

	Transaction Type	Enabled?	Priority?
0	Alarm Cleared	☑	□
1	Entry	☑	□
2	Attempt	☑	□
3	Set Access Level	☑	□
4	Low Battery SHUTDOWN	☑	□
5	Motor Fault	☑	□
6	Request To Exit	☑	□
7	Door Open Too Long	☑	□
8	Door Latch Open	☑	□
9	Forced Entry	☑	□
10	Net Connect Attempt	☑	□
11	Net Connect Pass	☑	□
12	Set Clock	☑	□
13	Anti-Tamper	☑	□
14	Remote Entry	☑	□

The Details box (item A) displays the selected Controller's Firmware version, Model number, User Capacity, MAC Address, and Hardware Class.

The Transactions list (item B) allows transactions to be filtered and prioritized. The Enabled column enables/disables the transaction at the controller level, so if the checkbox is not checked, transactions of that type will not be sent. The Priority column enables/disables the transaction priority, which indicates whether or not the transaction is sent immediately or on the next beacon cycle. For a comparison chart of terms used here and in Alarm Monitoring, see "Events/Transactions" on page 96.

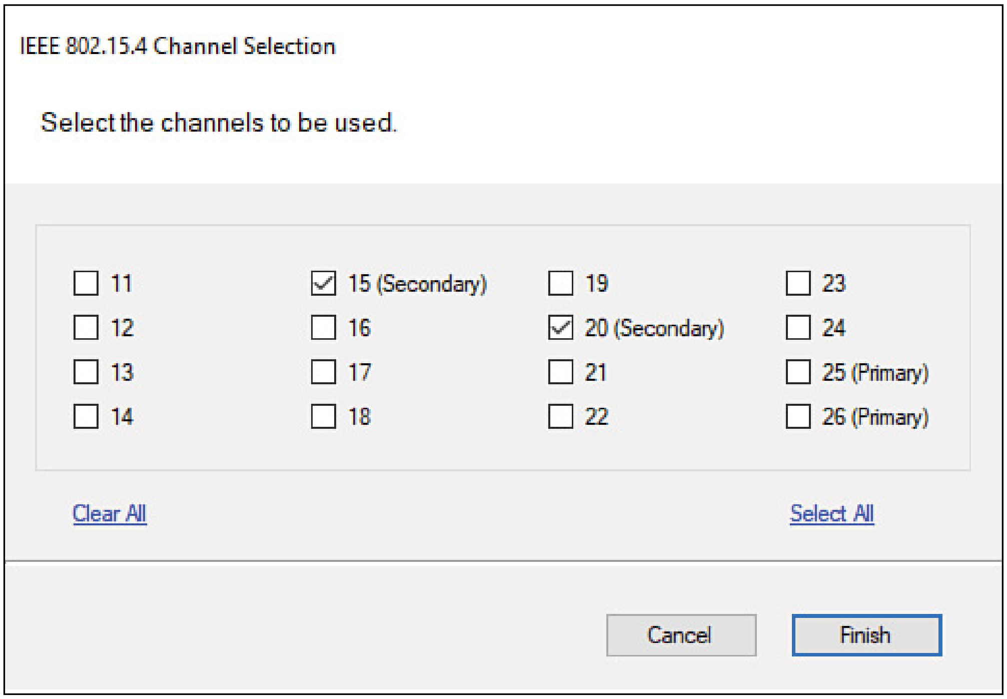
The Wiegand Device Type field (item C) is only applicable to WACs and can be set to Proximity, Magnetic or Smart Card.

The Beacon Time (Item D) is the rate at which controllers send signals to Wi-Q Gateways to look for updates and send transactions. The value set to 60 seconds by default. The setting of this value directly affects the battery life of the controller.

The 1st Card Unlock checkbox (Item E) allows the controller to unlock the door when the first valid badge is presented to the controller. If you enable this feature, it must also be enabled in Readers and Doors. See “Add Signed On Wireless Controllers to Readers and Doors” on page 77.

Selecting Edit (Item F) opens the Channel Selection window (Figure 59).

Figure 59 Controllers Channel Selection Window



IEEE 802.15.4 Channel Selection

Select the channels to be used.

☐ 11 ☑ 15 (Secondary) ☐ 19 ☐ 23
☐ 12 ☐ 16 ☑ 20 (Secondary) ☐ 24
☐ 13 ☐ 17 ☐ 21 ☐ 25 (Primary)
☐ 14 ☐ 18 ☐ 22 ☐ 26 (Primary)

The channels selected for the controller must be enabled at the Wi-Q Gateway as well. See “Portals Tab” on page 78. Channels 25 and 26 are selected by default. If you change the channel configuration, select Save to trigger the interface to send the updated information to your wireless hardware.

Segment Tree Right-Click Options

Right-clicking on items from within the Wi-Q Interface Configuration Tool Segment tree provides the following additional options.

- Segment > Delete: Allows a Segment to be deleted if no Portals or Controllers are associated with it
- Portal > Reset: Resets the Wi-Q Gateway.
- Portal>Navigate: Opens up the webpage of the WiQ Gateway. For Wi-Q Gateway, login credentials is required to view the gateway configuration details.
- Controller>Navigate: Opens up the webpage of the Wi-Q Gateway that the controller is assigned to.
- Controller > Reset: Resets a Controller
- Controller > Deep Reset: Sends a deep reset to the Controller and returns it to its factory default state.
- Controller > Remove Association with Wi-Q Gateway: Disassociates a Controller from a Wi-Q Gateway. The Controller must be signed back in if it must be reassociated with the Wi-Q Gateway.
- Controller > Unlock Association with Wi-Q Gateway: Unlocks the Controller from the Wi-Q Gateway to which it is currently assigned. This option does not automatically remove it from the Wi-Q Gateway.
- Controller > Lock Association with Wi-Q Gateway: Locks a Controller to a Wi-Q Gateway. Selecting this option will bring up a Wi-Q Gateway dropdown list.

Moving a Controller to a Different Wi-Q Gateway

If you need to move a Controller to a different Wi-Q Gateway, perform the following steps:

1 Right-click on the Controller in the Segment Tree, and select Lock Association with Wi-Q Gateway.

2 Select the desired Wi-Q Gateway from the dropdown list and click OK. It can take up to 60 seconds for the message to be sent to the hardware and for the Controller to become locked to the desired Wi-Q Gateway.

3 In Alarm Monitoring, you will see that the Controller will fall offline beneath the Wi-Q Gateway to which it was originally associated.

4 Once the controller goes offline in Alarm Monitoring, delete the Controller from the Readers and Doors module.

Note You must wait to delete the Controller from OnGuard until after it goes offline in Alarm Monitoring. Failure to wait will result in a deep reset being sent to the Controller.

5. Add a new Controller in the Readers and Doors module, and assign it to the desired Wi-Q Gateway (Access Panel dropdown list).
6. Wait for the changes to be communicated to the system hardware, and then check that the Segment Tree reflects your update.

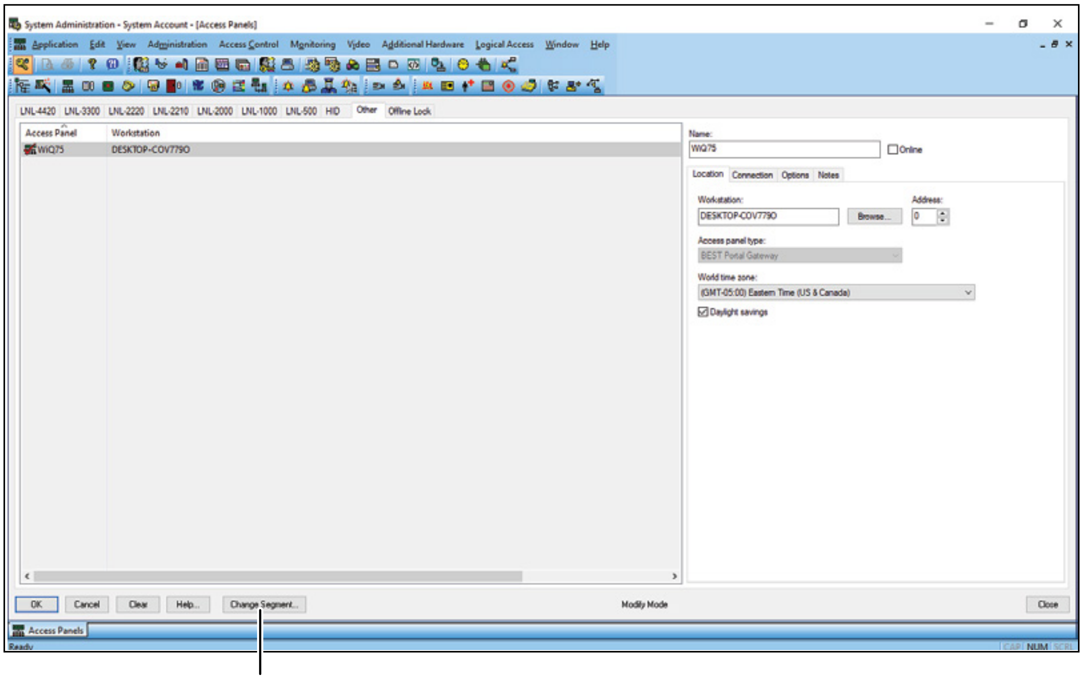
Moving a Wi-Q Gateway to a Different Segment

If you need to move a Wi-Q Gateway to a different Segment, perform the following steps in System Administration:

1. Make sure that you have segmentation enabled in (Administration > Segments > Segment Options).
2. Add additional segments as needed. See the System Administration User Guide for more information on adding segments.
3. In the Access Panels module, navigate to the Wi-Q Gateway that must be relocated. Click Modify.
4. Uncheck the Online checkbox next to the Name field.
5. Press OK and wait for the Wi-Q Gateway to go offline in Alarm Monitoring.
6. Once the Wi-Q Gateway is offline, click Modify on the Wi-Q Gateway again.

7 Click on Change Segment and select the segment to which the Wi-Q Gateway must be moved. See Figure 60.

Figure 60 Change Segment


System Administration - System Account - [Access Panels]
Application Edit View Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
LNL-4420 LNL-3300 LNL-2220 LNL-2210 LNL-2000 LNL-1000 LNL-500 HID Other Offline Lock
Location Connection Options Notes
Browse...
OK Cancel Clear Help... Change Segment...
Close
Access Panels
CAP NUM SCRL

Access Panel	Workstation
WIQ75	DESKTOP-COV779O

Name: WIQ75 □ Online

Workstation: DESKTOP-COV779O

Address: 0

Access panel type: BEST Portal Gateway

World time zone: (GMT-05:00) Eastern Time (US & Canada)

☑ Daylight savings

Modify Mode

Ready

Change Segment

8 Check the Online checkbox again so that the Wi-Q Gateway will go back online.

9 When finished, click OK.

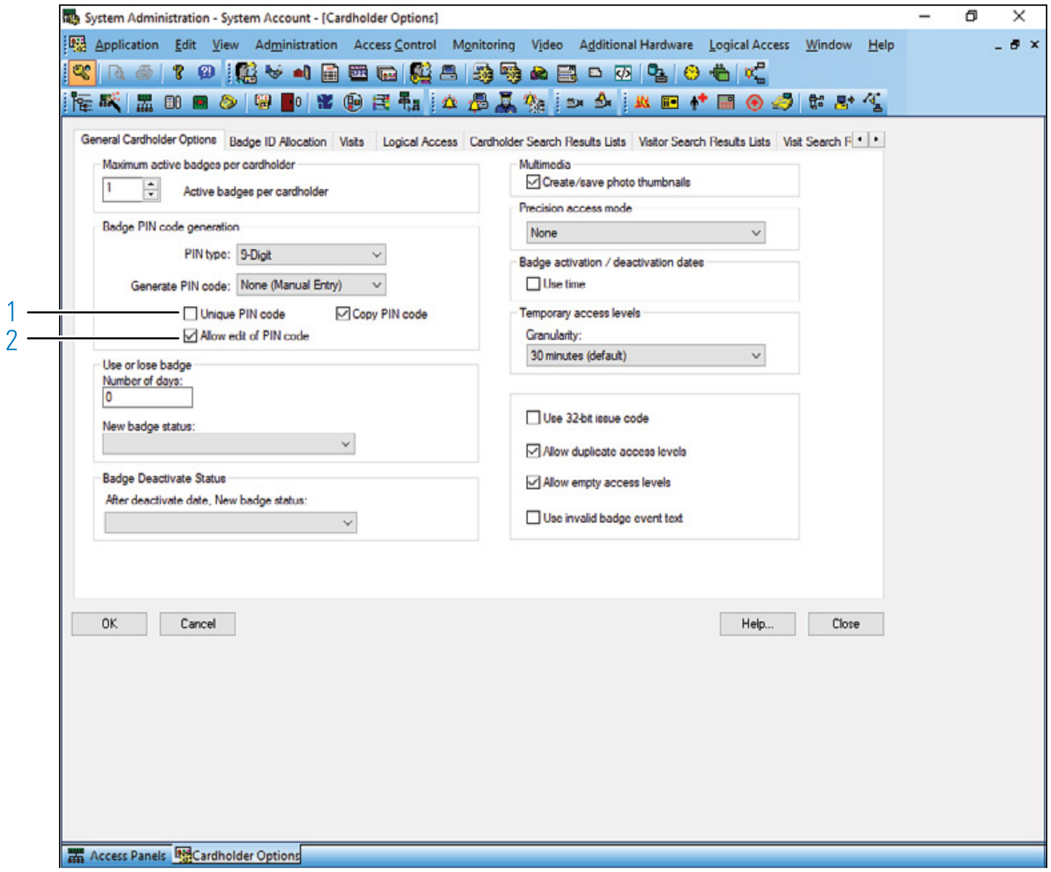
Note After segmentation or moving the Wi-Q Gateway to a new segment, a restart of the LS Communication Server service (or restart the OnGuard Communication Server if it was started as an application) is recommended. Then reset the Wi-Q Gateway to allow it to obtain its configuration for the new segment.

System Administration: Additional Notes

The following sections provide additional configuration information for System Administration.

Cardholder Options

Figure 61 Cardholder Options



Maximum active badges per cardholder

1 Active badges per cardholder

Badge PIN code generation

PIN type: 9-Digit

Generate PIN code: None (Manual Entry)

□ Unique PIN code ☑ Copy PIN code

☑ Allow edit of PIN code

Use or lose badge

Number of days: 0

New badge status:

Badge Deactivate Status

After deactivate date, New badge status:

Multimedia

☑ Create/save photo thumbnails

Precision access mode

None

Badge activation / deactivation dates

□ Use time

Temporary access levels

Granularity:

30 minutes (default)

□ Use 32-bit issue code

☑ Allow duplicate access levels

☑ Allow empty access levels

□ Use invalid badge event text

Due to the translation of badges and PINs between OnGuard and Wi-Q, you must select the Unique Pin Code option (Figure 61, Item 1).

If Allow Edit of PIN Code is enabled (Item 2), see “Changing PIN values” on page 93.

Card Formats

The following card formats are supported by Wi-Q hardware within the OnGuard System:

- Magnetic
- Wiegand
- Smartcard
- I-Class Card

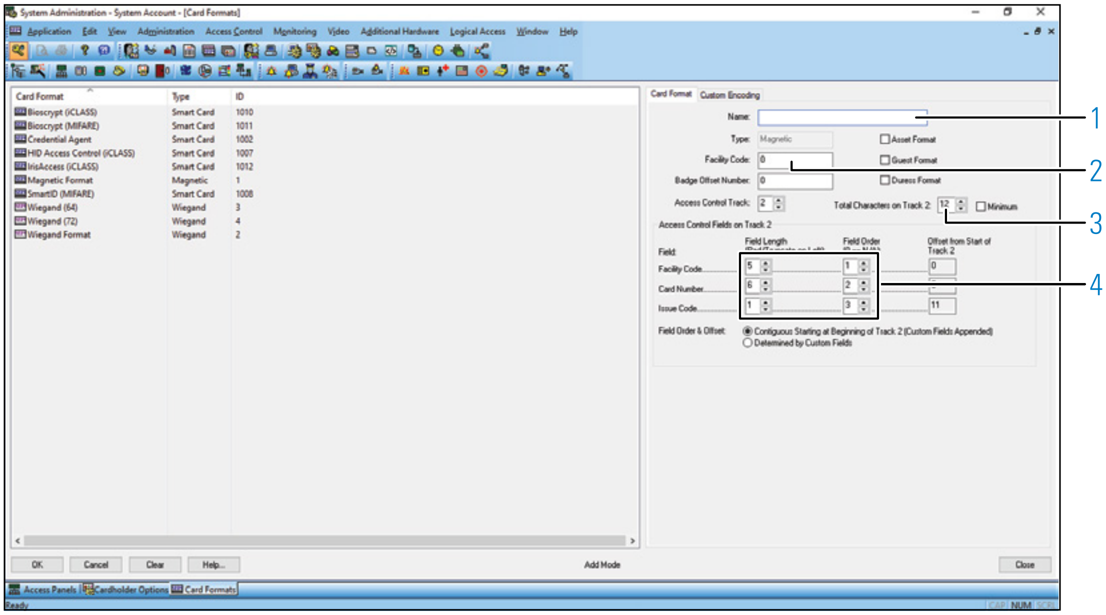
Note Smartcards and I-Class cards are configured in standard fashion in OnGuard, but Wi-Q hardware will recognize them as Wiegand format cards

All card formats supported by Wi-Q hardware must have IDs that range between 1 and 8. Wi-Q card formats match standard card formats. See the System Administration User Guide for more information on Card Formats.

If you need to add a new Magnetic card format or modify an existing one for your Wi-Q hardware in your existing OnGuard system, make sure to provide the following information (Figure 62).

Magnetic Card Format

Figure 62 Magnetic Type Card Format Configuration



Card Format	Type	ID
Bioscrypt (iCLASS)	Smart Card	1010
Bioscrypt (MIFARE)	Smart Card	1011
Credential Agent	Smart Card	1002
HID Access Control (iCLASS)	Smart Card	1007
IrisAccess (iCLASS)	Smart Card	1012
Magnetic Format	Magnetic	1
SmartID (MIFARE)	Smart Card	1008
Wiegand (64)	Wiegand	3
Wiegand (72)	Wiegand	4
Wiegand Format	Wiegand	2

Name:

Type: Magnetic

□ Asset Format

Facility Code: 0

□ Guest Format

Badge Offset Number: 0

□ Duress Format

Access Control Track: 2

Total Characters on Track 2: 12 □ Minimum

Access Control Fields on Track 2

Field	Field Length	Field Order	Offset from Start of Track 2
Facility Code	5	1	0
Card Number	6	2	[illegible]
Issue Code	1	3	11

Field Order & Offset: ● Contiguous Starting at Beginning of Track 2 (Custom Fields Appended)
○ Determined by Custom Fields

1 **Name**

Provide a unique name for your application.

2 **Facility Code**

Add your facility code.

3 **Total Characters on Track X**

Set this to the number of characters on the given track.

Note This field corresponds with the track number in the Access Control Track field.

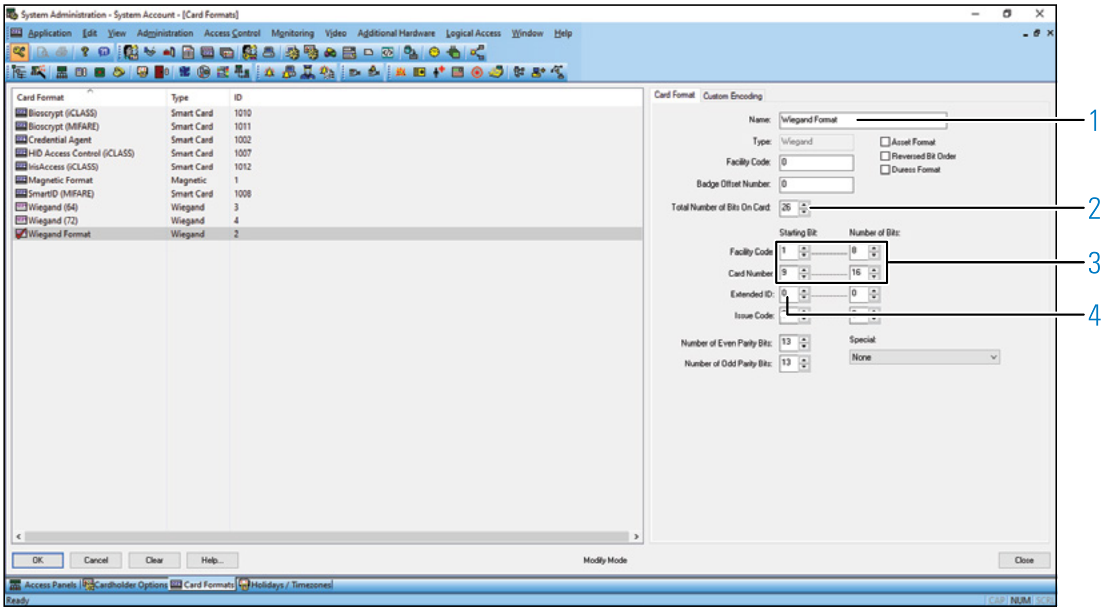
4 **Field Length and Field Order**

Fill in these fields for Facility Code, Card Number, and Issue Code.

Wiegand Card Format

If you need to add a new Wiegand card format or modify an existing one for your Wi-Q hardware in your existing OnGuard system, make sure to provide the following information (Figure 63).

Figure 63 Wiegand Type Card Format Configuration



System Administration - System Account - [Card Formats]
Application Edit View Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
Card Format Custom Encoding
OK Cancel Clear Help...
Modify Mode
Close
Access Panels Cardholder Options Card Formats Holidays / Timezones
Ready
CAP NUM SCRL
1
2
3
4

Card Format	Type	ID
Bioscrypt (iCLASS)	Smart Card	1010
Bioscrypt (MIFARE)	Smart Card	1011
Credential Agent	Smart Card	1002
HID Access Control (iCLASS)	Smart Card	1007
IrisAccess (iCLASS)	Smart Card	1012
Magnetic Format	Magnetic	1
SmartID (MIFARE)	Smart Card	1008
Wiegand (64)	Wiegand	3
Wiegand (72)	Wiegand	4
Wiegand Format	Wiegand	2

Name: Wiegand Format
Type: Wiegand
Facility Code: 0
Badge Offset Number: 0
Total Number of Bits On Card: 26
□ Asset Format
□ Reversed Bit Order
□ Duress Format

	Starting Bit	Number of Bits:
Facility Code:	1	8
Card Number:	9	16
Extended ID:	0	0
Issue Code:		

Number of Even Parity Bits: 13
Number of Odd Parity Bits: 13
Special: None

1 **Name**
Provide a unique name for your application.

2 **Total Number of Bits on Card**
Change this field to the number of bits used.

3 **Starting Bit and Number of Bits**
Fill in these fields for Facility Code and Card Number

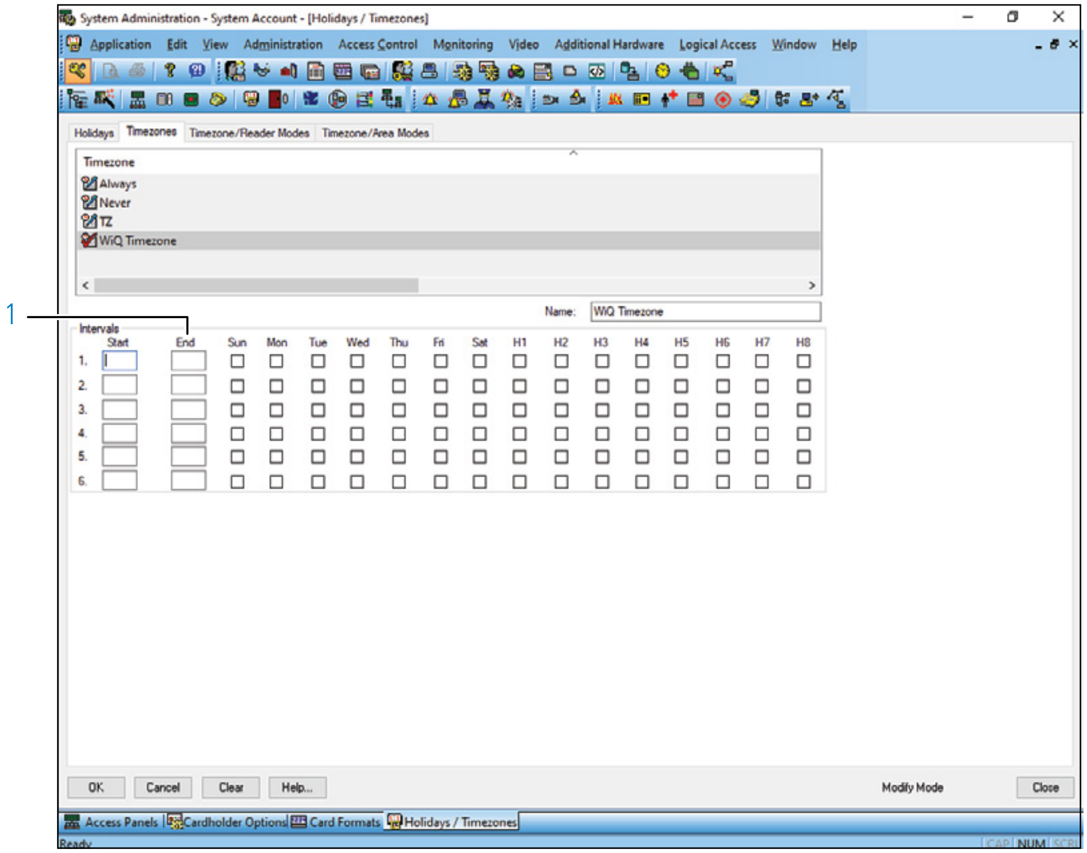
Note A Starting Bit offset is not required.

4 **Issue Code**
This field is not supported by Wi-Q hardware.

Timezones

See the System Administration User Guide for more information on setting up Timezones.

Figure 64 Timezones


1
System Administration - System Account - [Holidays / Timezones]
Application Edit View Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
Holidays Timezones Timezone/Reader Modes Timezone/Area Modes
Intervals
Start End Sun Mon Tue Wed Thu Fri Sat H1 H2 H3 H4 H5 H6 H7 H8
1. 2. 3. 4. 5. 6.
OK Cancel Clear Help...
Modify Mode
Close
Access Panels Cardholder Options Card Formats Holidays / Timezones
Ready
CAP NUM SCRL

Timezone
- Always
- Never
- TZ
- WiQ Timezone

Name: WiQ Timezone

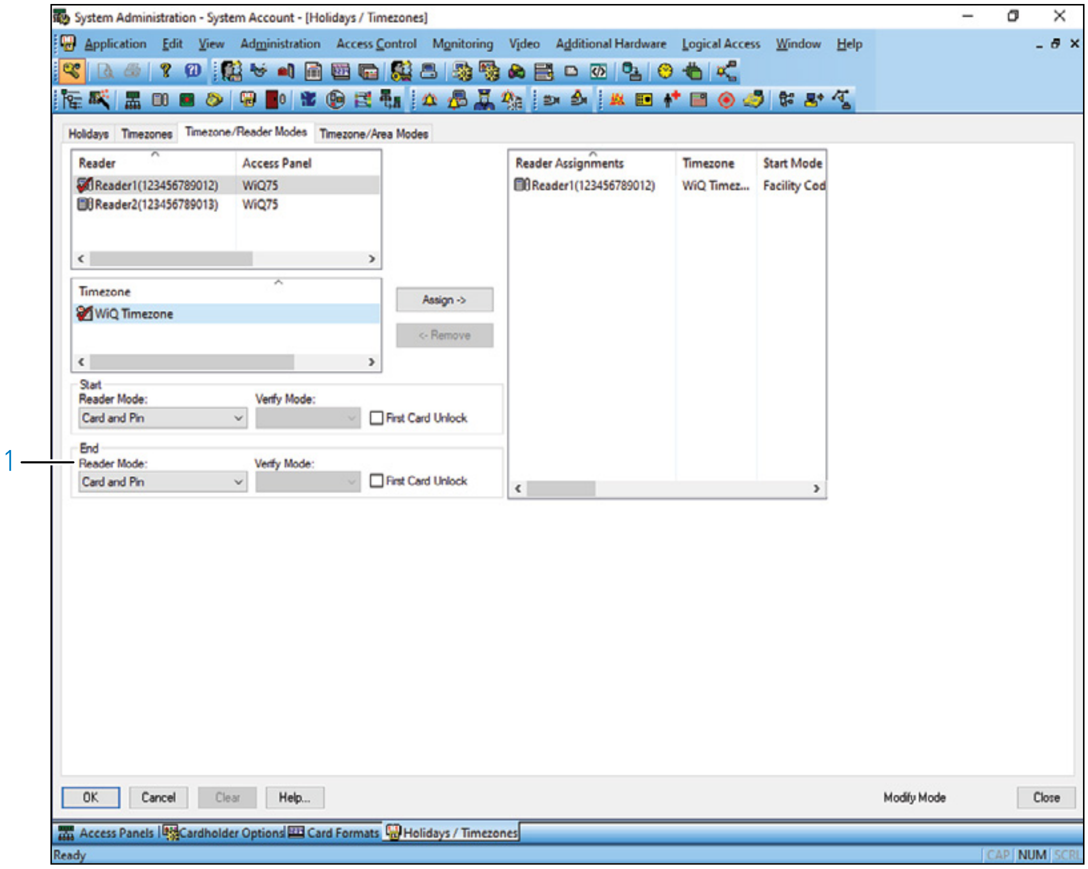
1 **End**

OnGuard only allows hours and minutes to be set. The Wi-Q Interface appends 0 seconds to the start and end times, with the exception of 23:59, which translates to 24:00:00.

Timezone/Reader Modes

See the System Administration User Guide for more information on timezone reader modes.

Figure 65 Timezone/Reader Modes



Reader	Access Panel
Reader1(123456789012)	WiQ75
Reader2(123456789013)	WiQ75

Timezone
WiQ Timezone

Start
Reader Mode: Card and Pin
Verify Mode:
□ First Card Unlock

End
Reader Mode: Card and Pin
Verify Mode:
□ First Card Unlock

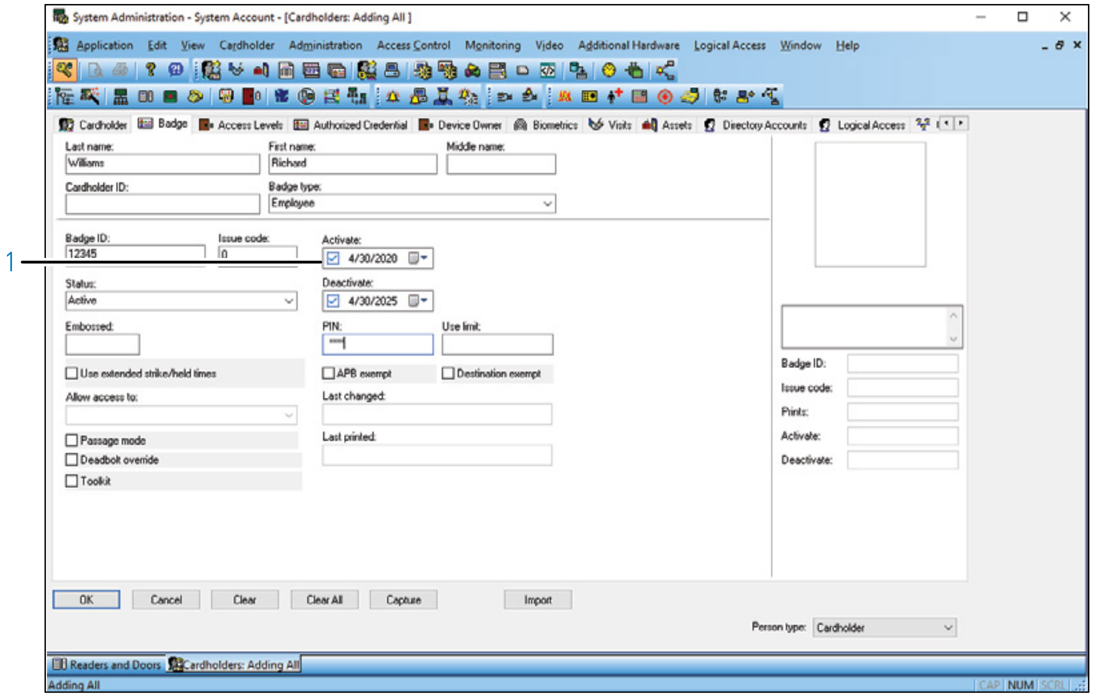
Reader Assignments	Timezone	Start Mode
Reader1(123456789012)	WiQ Timez...	Facility Cod

1 **End Reader Mode**
This feature is not supported by Wi-Q Interface. The controller will default back to the online reader mode set in the Readers and Doors configuration.

Cardholders

See the System Administration User Guide for more information on cardholders.

Figure 66 Cardholders


1
System Administration - System Account - [Cardholders: Adding All]
Application Edit View Cardholder Administration Access Control Monitoring Video Additional Hardware Logical Access Window Help
Cardholder Badge Access Levels Authorized Credential Device Owner Biometrics Visits Assets Directory Accounts Logical Access
OK Cancel Clear Clear All Capture Import
Readers and Doors Cardholders: Adding All
Adding All
CAP NUM SCRL

Last name: Williams
First name: Richard
Middle name:
Cardholder ID:
Badge type: Employee
Badge ID: 12345
Issue code: 0
Activate: ☑ 4/30/2020
Status: Active
Deactivate: ☑ 4/30/2025
Embossed:
PIN: ****
Use limit:
□ Use extended strike/held times
□ APB exempt
□ Destination exempt
Allow access to:
Last changed:
□ Passage mode
□ Deadbolt override
□ Toolkit
Last printed:
Badge ID:
Issue code:
Prints:
Activate:
Deactivate:
Person type: Cardholder

Activate Date (1) is not supported by BEST® Wi-Q Hardware.

Changing PIN values

If Allow Edit of PIN Code is enabled in Cardholder Options (Figure 61), perform the following steps when changing the PIN value in order to have the old PIN removed from the controller:

1 Navigate to the Cardholders screen in System Administration (See Figure 66). Select the Badge tab, and click Modify for the badge on which you're changing the PIN.

2 From the Status dropdown list, select Lost. Then, click OK. This will trigger a "Delete Badge" event and remove the badge from all associated controllers. You must wait for an "Updated Credential Parameters" event to display in Alarm Monitoring application occur for each controller to ensure that the badge has been completely deleted.

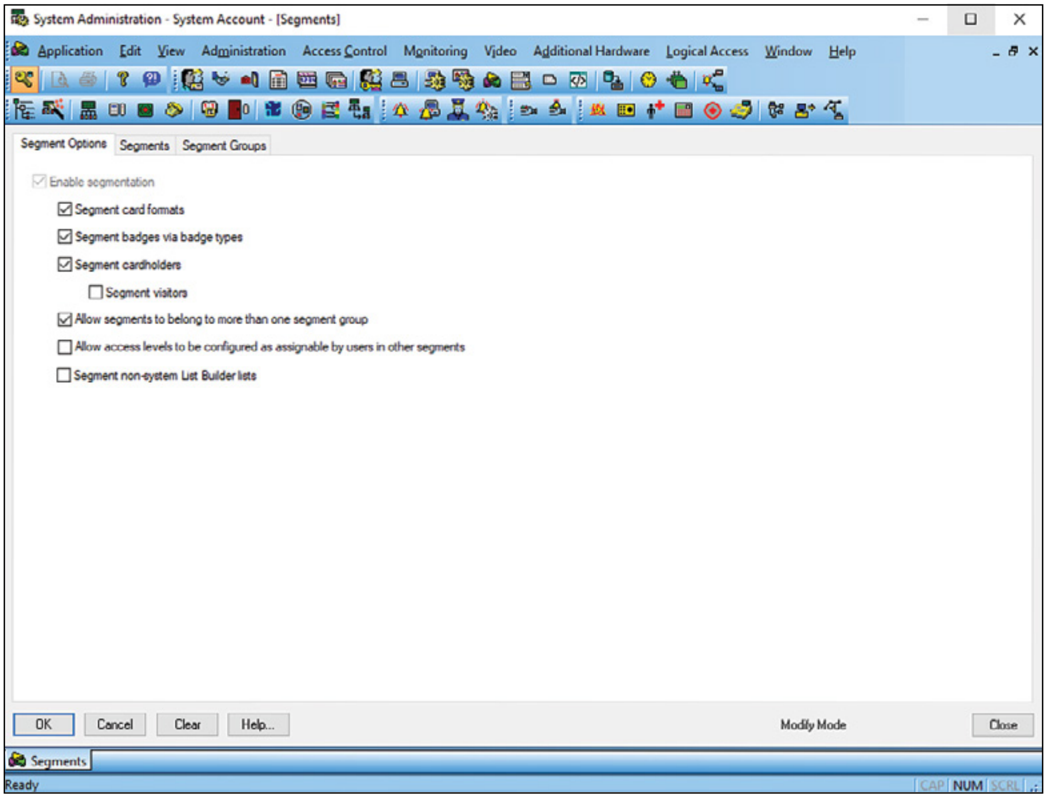
3 Once this has occurred, change the PIN value. Then, select Active from the Status dropdown list and click OK. The badge and new PIN will now be added to the associated controllers.

Note You must change the PIN value before you click OK. Failure to do so will cause the old PIN to be sent back to the controllers.

Segments

See the System Administration User Guide for more information on segments.

Figure 67 Segments



☑ Enable segmentation
☑ Segment card formats
☑ Segment badges via badge types
☑ Segment cardholders
□ Segment visitors
☑ Allow segments to belong to more than one segment group
□ Allow access levels to be configured as assignable by users in other segments
□ Segment non-system List Builder lists

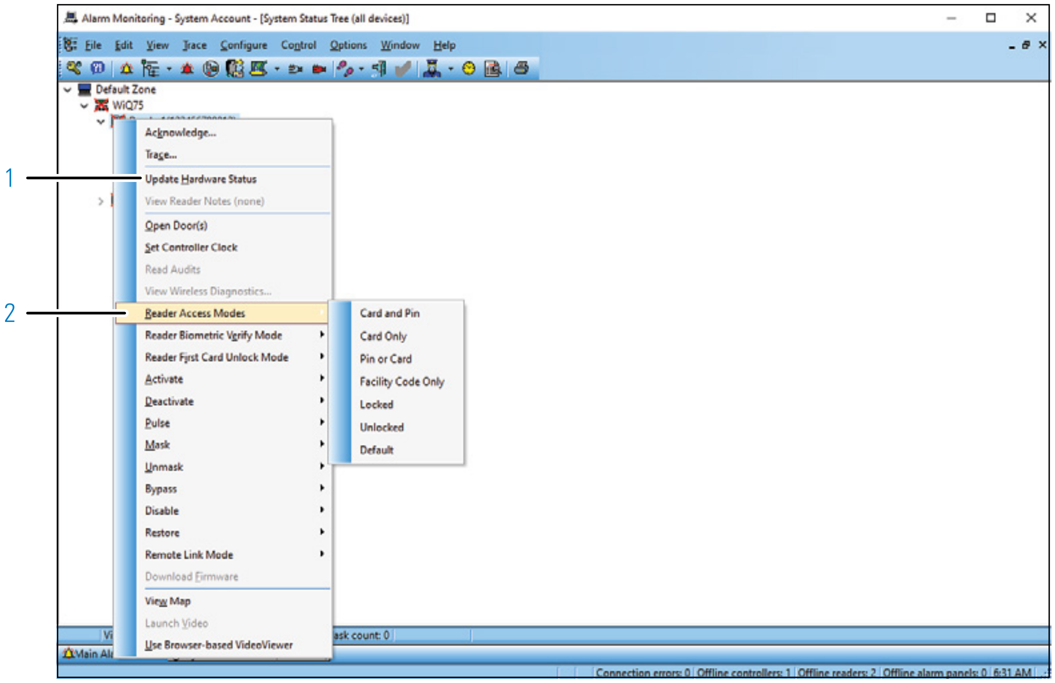
The boxes checked in Figure 67 are the only configurations supported by BEST® Wi-Q. Other configurations may yield unexpected system behavior.

Note After segmentation or moving a Wi-Q Gateway to a new segment, a restart of the LS Communication Server service (or restart the OnGuard Communication Server if it was started as an application) is recommended. Then reset the moved Wi-Q Gateway to allow it to obtain its configuration for the new segment.

Alarm Monitoring

Alarm Monitoring receives events from BEST Wi-Q hardware. See Items 1 and 2 below for Alarm Monitoring features that are tailored for Wi-Q hardware. Consult the Alarm Monitoring User Guide for additional information.

Figure 68 Alarm Monitoring



1 **Update Hardware Status**

This option is available when right-clicking on a Controller or Wi-Q Gateway in the System Status Tree. Update Hardware Status will retrieve the current status of the selected Wi-Q Gateway or Controller (online or offline), and it will retrieve the current access mode of the selected Controller.

2 **Reader Access Modes**

Selecting a Reader Access Mode in Alarm Monitoring will override the Controller’s access mode.

Note A change in timezone will force the Controller back to its default state.

Events/Transactions

The terms used for events in Alarm Monitoring differ from the terms used for transactions in the Wi-Q Interface Software Controllers Tab. The following chart compares these terms.

Table 6. Wi-Q Event/Transaction Comparison

Event Name	**Wi-Q Transaction Name**	**Generic Message Text**	**Description**
Door Forced Open Canceled	Alarm Cleared		The door status contact was in alarm mode and has been returned to the normal state when the door is closed.
Access Granted	Entry		Normal entry
Invalid Badge	Attempt		Attempt was made but the badge is invalid
	Set Access Level		System Access level changed
Reader Low Battery	Low Battery SHUTDOWN		Batteries are too low to operate the controller board. Controllers will enter the failed low battery shutdown state at 4.3V.
	Motor Fault	Motor Failure	Motor failure at the door
Request to Exit	Request To Exit		Handle depressed and door opened without motor operation
Door Held Open	Door Open Too Long		Door switch monitor open at end of shunt time
Door Contact Tamper	Door Latch Open		Latch monitor open at end of shunt time
Door Forced Open	Forced Entry		Door switch monitor open with no REX or shunt
	Net Connect Attempt	Sign on attempt	Network connection was attempted (5678) or card
	Net Connect Pass	Sign on success	Controller associated with portal
	Set Clock	Set Clock	The date and time have been set at the controller. This is determined by the communication server's date and time.
	Anti-Tamper	Anti-Tamper	Maximum invalid attempts (6) has been reached
Valid Remote Access	Remote Entry		Remote entry through the door
Key Override	Key Bypass		Key was used to open door
Reader Low Battery	Low Battery		Controller battery is getting low
Access Granted on Facility Code	Entry Facility Code		Card user entered on segment match
	Toggle Unlock	Access Granted — Toggle Access Level Entry to Unlock	Toggle access level entry to unlock
	Toggle Lock	Access Granted — Toggle Access Level Entry to Lock	Toggle access level entry to lock
Access Granted	Entry Group Valid		Time zone group enabled
	Entry System	Access Granted — The system caused an entry	The system caused a entry (override at controller level)
	Issue Code Update Needed	Access Granted — Issue code advanced on entry	User issue code advanced on entry
	Entry with Low Battery	Access Granted — Low Battery	Allowed access with low battery warning in effect
Invalid PIN Number	Failed Invalid PIN		Access denied due to invalid pin
Invalid Facility Code	Failed Facility Code		Access denied due to invalid facility code

Event Name	Wi-Q Transaction Name	Generic Message Text	Description
Invalid Issue Code	Failed Issue Code		Access was not granted due to the issue code being out of range from what the device was expecting to see. For example, the issue code on the badge is 4 but the Reader is expecting 1.
Inactive Badge	Failed Card Expired		Access denied due to expired badge
Access Denied	Failed Invalid Card		The badge is not assigned to an access level that grants access to this door or during the time interval.
Invalid Access Level	Failed Group Violation		The badge has access to the reader via a timezone controlled group assignment but has tried the card outside of permitted timezone.
Denied Low Battery	Failed Low Battery Shutdown		Low battery shutdown in progress
Denied Low Battery	Failed Low Battery Warning		Batteries are too low to operate the controller board. If the battery voltage falls below 4.3V then the controller will delay entry and make a sound. If the battery voltage falls below 3.6 volts then the controller will go into alarm mode and deny entry.
Inactive Badge	Failed Expired Credentials		Access denied due to expiration date on credential
	Group Level Change Enabled	Access Level Enabled	Group Access level changed
	Group Level Change Disabled	Access Level Disabled	Group Access level changed
	Update User Parameters	Updated credential parameters	This unit has updated its Users
	Update Facility Parameters	Updated segment information	The unit has received the segment information.
	Update Timezones	Updated timezones	This unit has updated its Timezones
	Update Input Points	Updated I/O	This unit has updated its I/O
	Update Card Formats	Updated card formats	This unit has updated its Formats
	Update Configuration	Updated controller configuration	This unit has updated its Controller Configuration.
Reader Module Firmware Upgraded	Reader Firmware Update		Controller firmware has been updated
Door Held Open Canceled	Clear Door Open Too Long		Clear a door open too long alarm
Door Forced Open Canceled	Clear Forced Entry		Clear a forced entry alarm
Door Contact Tamper Canceled	Clear Latch Stuck		Clear a door latch stuck alarm
	Input Point — Normal	I/O input triggered with importance of normal	I/O input triggered with importance level of normal
	Input Point — Warning	I/O input triggered with importance of warning	I/O input triggered with importance level of warning
	Input Point — Alarm	I/O input triggered with importance of alarm	I/O input triggered with importance level of alarm
	DLP Supervision Fault	Door contact supervised input is faulted	Door latch position supervised input is faulted
	DPS Supervision Fault	Door position supervised input is faulted	Door position switch supervised input is faulted

Event Name	Wi-Q Transaction Name	Generic Message Text	Description
	REX Supervision Fault	Request To Exit supervised input is faulted	Request to exit supervised input is faulted
	KEY Supervision Fault	Key detect supervised input is faulted	Key detect supervised input is faulted
	Using Battery As Power Source	External Power Source	This unit has switched Power sources: external to battery power
	Using External Power Source	Battery Power Source	This unit has switched Power sources: battery to external power
	Bootloader Active	Bootloader Status	Contact Stanley Technical Support, and provide code and description.
	Firmware Update Failed	Firmware update failed	Contact Stanley Technical Support, and provide code and description.
	Set Preferred Portal Passed	Set preferred portal passed	A command to change Wi-Q Gateways was sent and the change was successful
	Set Prefered Portal Failed	Set preferred portal failed	A command to change PGs was sent and change failed
	Near User Capacity	Number of badges is nearing maximum allowed	75% of of 333 user overflow pages are assigned
	User Capacity Reached	Number of badges has reached maximum allowed	0 user overflow pages are available
	FIPS140 Connected	FIPS 140 connected	FIPS140 mode enabled and connected to FIPS140 PG

Firmware Updates

Firmware updates will be sent to you periodically by dormakaba Technical Support. You can upload these firmware files to your database by using the Firmware Files Tab in the Wi-Q Interface Configuration Tool. Then, you can Use the Firmware Reprogram feature inside the Configuration Tool to send the files to your wireless hardware. This section will guide you through the firmware update process.

Firmware File Types

Every Controller has two firmware files:

- Application File: Software that provides the access control decision-making functionality on a Controller
- Bootloader File: Software that executes the reprogramming session on the Controller

The application file is what is typically reprogrammed by the BEST Team, but it is possible that the bootloader file will require reprogramming as well. Controller firmware files will always have a ".binhe" file extension.

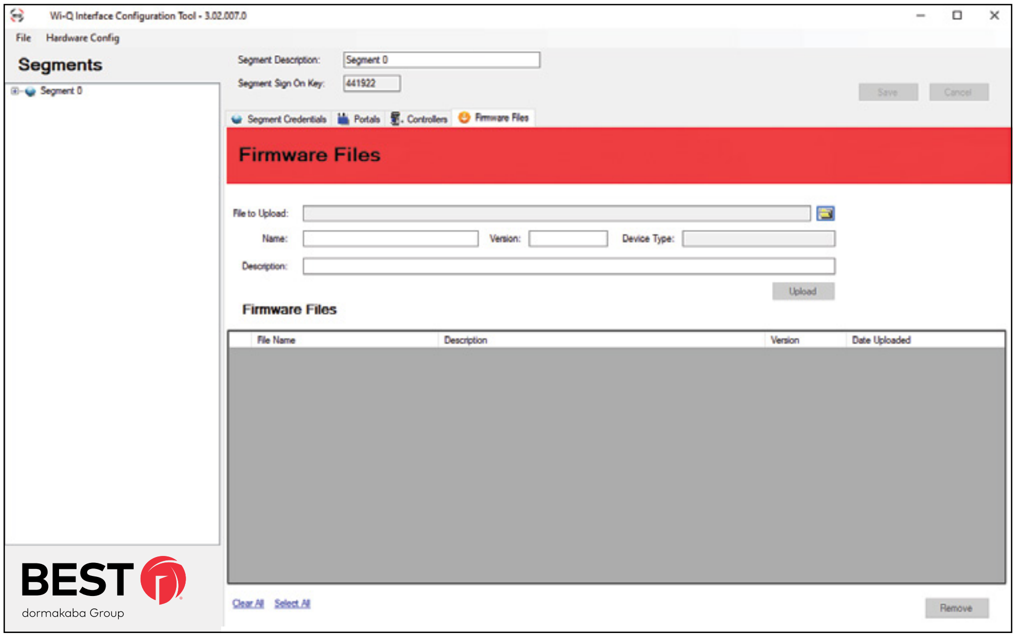
For Wi-Q Gateways, only one file is required for reprogramming, and the file name begins with the version number and ends with "image.bin.gzhe."

Firmware Files Tab

Click on the Firmware Files tab in the Wi-Q Interface Configuration Tool, and perform the following steps to upload firmware files to your database.

1 Click on the Folder Icon to the right of the File to Upload field and browse to the location of your firmware files. See Figure 69.

Figure 69 Firmware Files Tab



Segment 0

Segment Description: Segment 0

Segment Sign On Key: 441922

2 If you are uploading a Controller firmware file, the firmware name, version number and device type are automatically populated.

If you are uploading a WiQ Gateway firmware file, the firmware name, version number and device type are automatically populated.

Note The version number of a Wi-Q Gateway firmware file is visible in the path to the file.

3 Provide a unique description of the firmware file in the Description field. If you are uploading a Controller firmware file, it is recommended that you build either “Boot” or “Application” into your description name, depending on the file type.

4 Click Upload. The files will then be added to the list of Firmware Files below and added to your database.

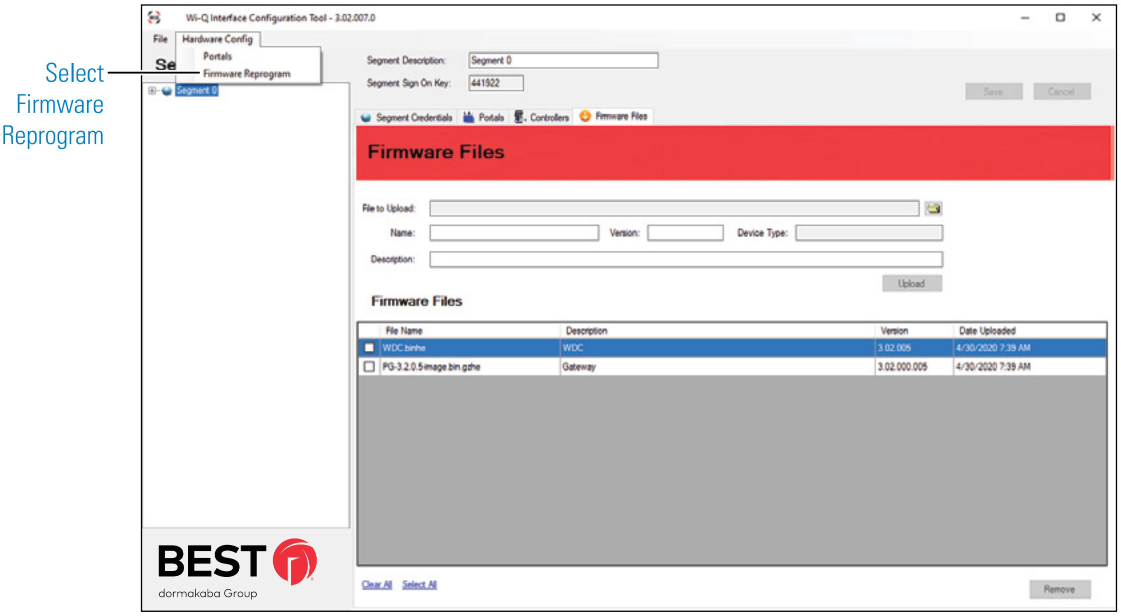
To avoid confusion between updates, it is recommended that you only keep the latest firmware files in your list. To remove older files, select the file (Check the checkbox of the file) you wish to delete and click on Remove.

Firmware Reprogram

Before you can reprogram your hardware, you must turn your Wi-Q Gateway offline in Access Panels of OnGuard application and then confirm that it is offline in Alarm Monitoring. Once your Wi-Q Gateway is offline, you are ready to reprogram your hardware with the latest firmware files. Perform the following steps.

1 Inside the Configuration Tool, click on Hardware Config at the top left of the screen and select Firmware Reprogram. See Figure 70.

Figure 70 Navigate to Firmware Reprogram



Segment Description: Segment 0

Segment Sign On Key: 441922

File to Upload:

Name:

Version:

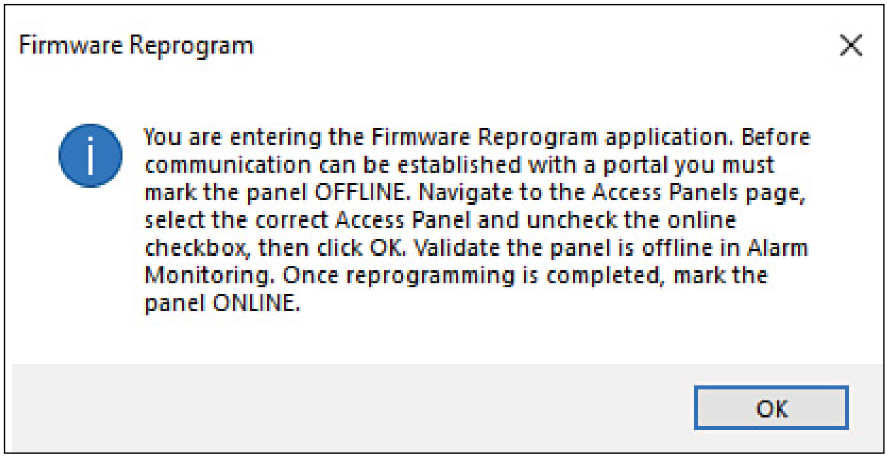
Device Type:

Description:

	File Name	Description	Version	Date Uploaded
□	WDC.binhe	WDC	3.02.005	4/30/2020 7:39 AM
□	PG-3.2.0.5image.bin.gzhe	Gateway	3.02.000.005	4/30/2020 7:39 AM

2 The following message will pop up to remind you that your Wi-Q Gateways must be turned offline in OnGuard. If you have not done so already, mark them offline and confirm that they are off in Alarm Monitoring. Then click OK.

Figure 71 Reminder message to turn Wi-Q Gateways offline

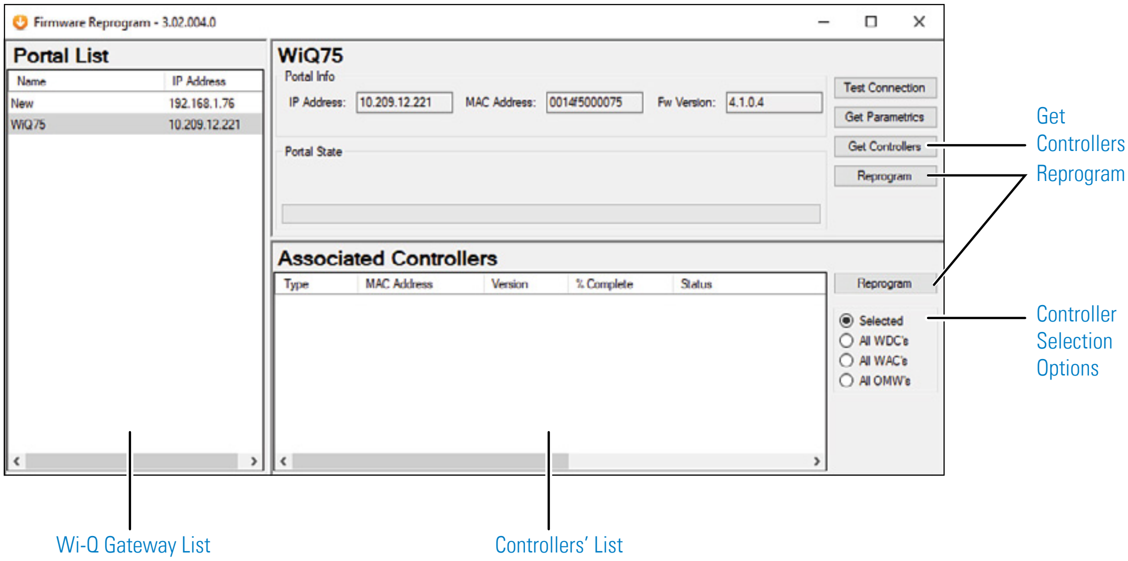


Firmware Reprogram

You are entering the Firmware Reprogram application. Before communication can be established with a portal you must mark the panel OFFLINE. Navigate to the Access Panels page, select the correct Access Panel and uncheck the online checkbox, then click OK. Validate the panel is offline in Alarm Monitoring. Once reprogramming is completed, mark the panel ONLINE.

3 The Firmware Reprogram window will open. A list of all Wi-Q Gateways in your system is located on the left side of the screen. Selecting a Wi-Q Gateway will change the top section of the window to show the selected Wi-Q Gateway's IP address, MAC address and current firmware version. See Figure 72.

Figure 72 Firmware Reprogram



Firmware Reprogram - 3.02.004.0

Portal List

Name	IP Address
New	192.168.1.76
WiQ75	10.209.12.221

WiQ75

Portal Info

IP Address: 10.209.12.221 MAC Address: 0014f5000075 Fw Version: 4.1.0.4

Portal State

Associated Controllers

Type	MAC Address	Version	% Complete	Status

● Selected
○ All WDC's
○ All WAC's
○ All OMW's

4 **If you are reprogramming a Wi-Q Gateway**, select the Portal and click Reprogram. You may reprogram multiple Portals simultaneously, but you must select them individually and click on Reprogram for each one.

If you are reprogramming a Controller, select the Portal that your Controller is associated with and click Get Controllers. A list of online Controllers associated with your Portal is generated at the bottom of the screen. If a Controller is offline, it will not show up in the list. Choose your selection option on the right. Then click Reprogram.

Note You can only reprogram one type of Controller at a time.

5 A window will pop up with a dropdown list of available firmware files. Select your file and press OK.

Note If you are reprogramming both the Bootloader and Application files on a Controller, you must update the Bootloader file first.

6 Hardware reprogramming can take between three and five minutes. Wi-Q Gateway update progress is visible in the Portal State section. Controller update progress and status is visible in the Controllers section.

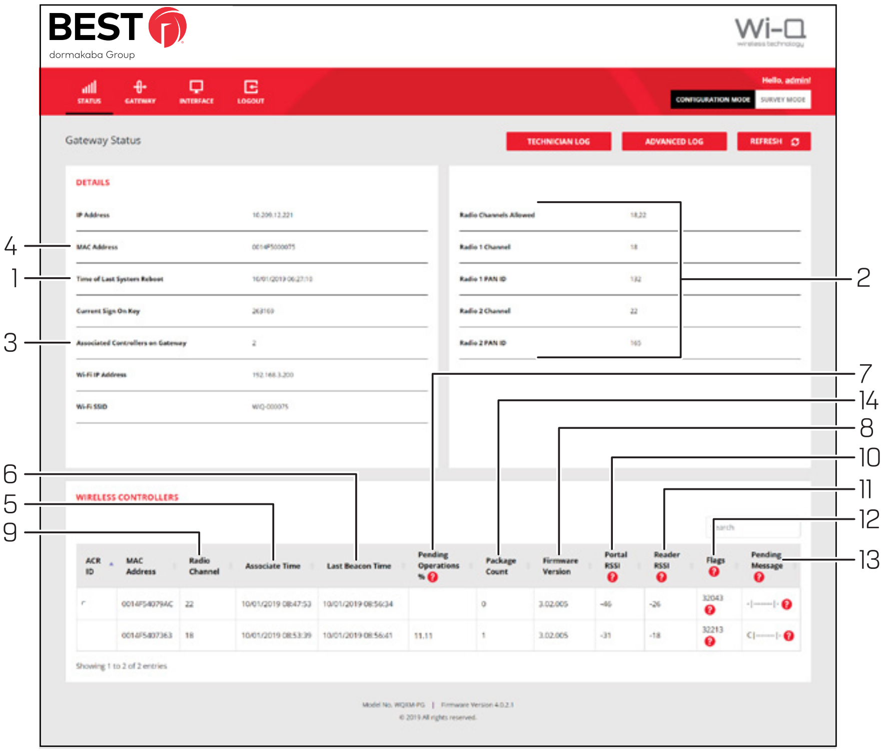
5 Advanced Troubleshooting

This section provides an overview on the Wi-Q Gateway status webpage. You can access the status webpage for a specific Wi-Q Gateway in one of two ways:

- Inside the Portal Configuration Module, locate the desired Portal in the list and click on its hyperlink. See Figure 43 on page 69.
- Type your desired Wi-Q Gateway's IP address directly into your internet browser.

Your browser will display the status of your Wi-Q Gateway and associated devices. See Figure 73 on page 104.

Figure 73 Wi-Q Gateway Status Webpage



Gateway Status

DETAILS

IP Address	10.206.12.221
MAC Address	0014F5000075
Time of Last System Reboot	10/01/2019 06:27:10
Current Sign On Key	263169
Associated Controllers on Gateway	2
Wi-Fi IP Address	192.168.3.200
Wi-Fi SSID	WIQ-000075

Radio Channels Allowed	18,22
Radio 1 Channel	18
Radio 1 PAN ID	132
Radio 2 Channel	22
Radio 2 PAN ID	165

WIRELESS CONTROLLERS

search

ACR ID	MAC Address	Radio Channel	Associate Time	Last Beacon Time	Pending Operations % ?	Package Count	Firmware Version	Portal RSSI ?	Reader RSSI ?	Flags ?	Pending Message ?
	0014F54079AC	22	10/01/2019 08:47:53	10/01/2019 08:56:34		0	3.02.005	-46	-26	32043 ?	-|------|- ?
	0014F5407363	18	10/01/2019 08:53:39	10/01/2019 08:56:41	11.11	1	3.02.005	-31	-18	32213 ?	C|------|- ?

Showing 1 to 2 of 2 entries

Model No. WQXM-PG | Firmware Version 4.0.2.1
© 2019 All rights reserved.

Clicking on Hyperlink will open the login page of the gateway webpage. You need login credentials to view the status page.

The Wi-Q Gateway Status webpage provides the following information:

1 **Time of Last System Reboot**
Last time Wi-Q Gateway was reset or rebooted.

2 **Radio and Channel**
Shows the channel associated with each radio in the Wi-Q Gateway.

3 **a) Associated Controllers on Gateway in the Details section**
b) Wireless Controllers section will display the complete details of associated controllers
Shows which devices are associated with the Wi-Q Gateway.

4 **MAC Address**
Column shows the MAC Address of the Wi-Q Gateway.

5 **Associate Time**
Column shows the time that the Controller last associated with the Wi-Q Gateway.

6 **Last Beacon Time**

Column shows the time of the last Controller beacon.

7 **Pending Operations %**

Column shows progress percentage of pending operations.

8 **Firmware Version**

Column shows the firmware version number of associated Controller.

9 **Radio Channel**

Column shows which radio the Controller is connecting to in the Wi-Q Gateway. Radio 18 is on the right side of the Wi-Q Gateway and Radio 22 is on the left side of the Wi-Q Gateway.

10 **Portal RSSI**

Column shows the signal strength of the Controller as received at the Wi-Q Gateway. This signal strength ranges from -18 (highest) to -91 (lowest).

11 **Reader RSSI**

Column shows the signal strength of the Wi-Q Gateway as received at the Controller. This signal strength ranges from -18 (highest) to -91 (lowest).

12 **FLAGS**

Column shows the current operational status of the associated device.

13 **Pending Message**

Column shows the abbreviation of the message currently in operation.

14 **Package Count**

Displays the number of packets being sent to the controller.

Status Flags in the FLAGS Column

The following is a list of the bits in the FLAGS column and their corresponding Wi-Q Gateway status flags and definition.

Note The typical Wi-Q device status code is 00032043. This is the example used in the chart below.

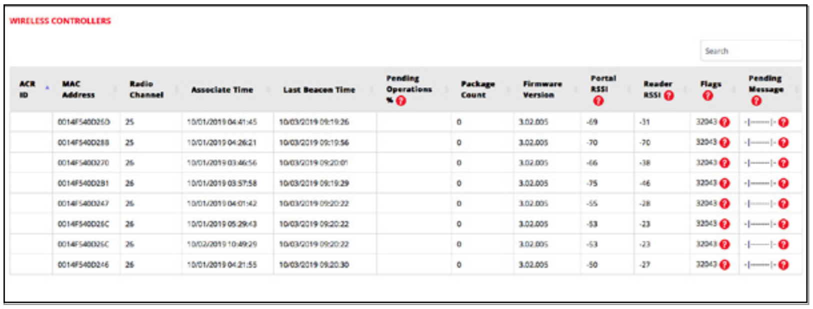
Table 7. Example Chart

Table 7. Bit			Table 7. Wi-Q Gateway Status Flag	Table 7. Definition
Right END	3	Bit 0	CONTROLLER_IS_ASSOCIATED	Set when the Controller is first associated with the Wi-Q Gateway.
		Bit 1	CONTROLLER_IS_VALID	Set during association, after the Wi-Q Gateway receives a beacon from the Controller.
		Bit 2	CONTROLLER_CONFIG_REQUIRED	Set during association, cleared by Wi-Q Gateway Communication Service after Controller configuration.
		Bit 3	CONTROLLER_ASSOC_PENDING_LIF	Set during association to indicate that Wi-Q Gateway requires LIF (Lock Information Frame) data.
	4	Bit 4	CONTROLLER_BEGIN_TRANSMISSION	Set when Wi-Q Gateway first transmits data to the Controller.
		Bit 5	CONTROLLER_DEEP_RESET_PENDING	Wi-Q Gateway must disassociate Controller when it receives the next beacon.
		Bit 6	CONTROLLER_VALID_INTERVALS	Set when Controller interval assignment has been received from the PC Communication Service.
		Bit 7	NOT USED	
	0	Bit 8	CONTROLLER_RETRY_LIMIT_EXCEEDED	Set when the retry limit on any command has been hit; used to limit downloads to firmware only.
		Bit 9	NOT USED	
		Bit 10	NOT USED	
		Bit 11	NOT USED	
	2	Bit 12	NOT USED	
		Bit 13	CONTROLLER_PREFERRED_PG_ENABLED	Set when Controller is locked to the Wi-Q Gateway.
		Bit 14	CONTROLLER_FIRMWARE_PENDING_DN	Set when the firmware commit has been sent to indicate that the disassociation is pending.
		Bit 15	CONTROLLER_FIRMWARE_PENDING	Set when firmware update is scheduled for the Controller, cleared when firmware commit is sent.
	3	Bit 16	CONTROLLER_REPORT_TIME _UPDATED	Set during association and when report time is updated.
		Bit 17	CONTROLLER_LIF_IS_VALID	Set when a LIF beacon is received.
Left END		Bit 18-31	NOT USED	

Update Flags in the PEND Column

At the bottom of the Gateway Status webpage will display the list of associated Wi-Q Controllers and their attributes.

Figure 74 Wi-Q Controllers



WIRELESS CONTROLLERS

Search

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 ?	-|------|- ?
	0014F540D288	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 ?	-|------|- ?
	0014F540D281	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 Wi-Q Gateway is in Mercury Mode. 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.
- **Portal RSSI** – Wi-Q Gateway 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 Wi-Q Gateway 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 Wi-Q Gateway.

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)

A Glossary

access level An access control relationship made between a reader or readers and a time zone or time zones. An access level is assigned to a badge ID for the purpose of granting access through a reader or readers during a specified time.

activation/deactivation date The date that a credential becomes active or expires.

badge The credential or token that carries a cardholder’s data.

badge ID Part of the access control information that is encoded to a token. This information, usually numerical, is unique to a particular credential holder.

card format The way that data is arranged and ordered on the card.

cardholder An individual who is issued a particular credential.

chassis type The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.

communication server The server application designed to provide network services to access panels, readers, PCs and PDAs.

credential A physical token, usually a card or fob, encoded with access control information.

cylindrical Lock chassis that installs into a circular bore in the door.

directional antenna An antenna type optimized to focus signal from point-to-point over longer distances and through obstacles.

ethernet The most common networking standard in the world, formally known as IEEE 802.3.

exit hardware Lock chassis type that supports exit hardware trim lock.

extended unlock The extra period of time the lock will unlock when an authorized credential with extended unlock privileges is presented.

guest A feature that enables you to add and delete cardholders to and from a lock without having to go out to a lock to reprogram it.

Host the computer on which Wi-Q Interface software is installed and set up to integrate Wi-Q gateways and readers into OnGuard.

IP address The numeric address (like 192.168.1.1) that identifies each device in a TCP/IP network. input A hardware connection point used for status reporting of a particular sensor.

issue code Part of the access control information contained on a credential that allows reuse of the badge ID when a credential is lost, damaged, or stolen. Usually one or two digits in length, this code increments forward when creating a new credential. Access is granted only when the badge ID and the issue code match the current database information.

MAC address The Media Access Control number (MAC). A unique, 12-digit number assigned by the manufacturer of a network device.

mortise A lock chassis that installs into a mortised cavity in the edge of a door.

omni-directional antenna An antenna type optimized to provide signal coverage in all directions.

packet A discrete chunk of data, being transferred on a TCP/IP or other addressable network.

Wi-Q gateway The Wi-Q Gateway is a wireless device connected to the Host computer through a secure IP address to transfer data signals from wireless reader locks to and from the Host computer.

request to exit A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation.

segment code Part of the access control information that can be encoded to a credential. This information, usually numerical, is unique to a group of credentials. Usually this feature is used to authenticate a credential to a particular organization.

sign-on key Number generated within Wi-Q Interface Software to establish the connection between the readers and the Wi-Q Gateway, and ultimately to a segment in the software.

site survey kit The Wi-Q Technology Site Survey Kit tool used to determine optimum Wi-Q Gateway location to verify signal strength before permanently installing the Notes hardware.

time interval A specific range of time, which corresponds to a particular day or days of the week. A time zone can be comprised of several, individual intervals.

timezone A defined range of time for assignment to various access control activities. A time zone may be applied to a reader or readers when creating an access level, to a reader to change the mode of operation, to a relay to activate and deactivate, to an input to mask and unmask, and a host of other operations. Dual access The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening.

unlock duration The time that the lock momentarily unlocks. Use limit A configuration limiting a credential to a defined number of uses.

Wi-Q Technology Provides efficient, online access control decisions at the door.

wireless access controller Wireless access controller provides additional capability to connect stand-alone controllers and locks.

wireless controller The wireless lockset that controls user access at the door and grants user requests according to how they are configured in OnGuard.