BEST

dormakaba Group

Wi-Q

wireless technology

BEST WI-Q™

ACCESS MANAGEMENT SYSTEM

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 1-800-392-5209 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.

The BEST Wi-Q AMS and Wi-Q Technology are trademarks of dormakaba USA Inc.
Bonjour is a registered trademark of Apple Inc.

Written and designed at dormakaba USA Inc.
6161 E. 75th St.
Indianapolis, IN 46250
T85202_K, October 2023

FCC/ISED Certification

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.

ISED Compliance Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(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 interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) L'appareil ne doit pas produire de brouillage ; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)/NMB-3(B)

ISED Antenna Statement

This radio transmitters 7713A-WDCSPIN and 7713A-WXCSPIN have been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio IC: 7713A-WDCSPIN, IC: 7713A-WXCSPIN a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Manufacturer: Southwest Antenna
Antenna type: Planar antenna
Model number: 1055-036
Maximum gain: 6 dBi

This radio transmitter 7713A-WACSPIN has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Le présent émetteur radio IC: 7713A-WACSPIN a été approuvé par Innovation, Sciences et Développement économique Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est supérieur au gain maximal indiqué pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'émetteur.

Manufacturer: L-Com
Antenna type: Rubber duck
Model number: HG2402RD-RSF
Maximum gain: 2.2 dBi

ISED RF Exposure Statement

In order to comply with ISED RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

Afin de se conformer aux exigences d'exposition RF ISED, cet appareil doit être installé pour fournir au moins 20 cm de séparation du corps humain en tout temps.

FCC RF Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, this equipment should be installed and operated with minimum distance 20 cm (7.6 inches) between the antenna and your body during normal operation. Users must follow the specific operating instructions for satisfying RF exposure compliance.

Approved Antenna

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.

Contents

1 Overview

2 Hardware Installation

3 Software Installation

4 Configuring Segments, Wi-Q Gateways and Controllers

5 Configure AMS Software (Task 11)

1 Overview

This manual is your complete guide to the BEST Wi-Q Access Management System. It provides detailed steps to install hardware and software, configure and customize your system, and use and manage the system.

The information is presented in a linear manner, describing each tab, feature, and application in the system. 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 Set Up Checklist at the end of this section and in the Getting Started Guide 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.

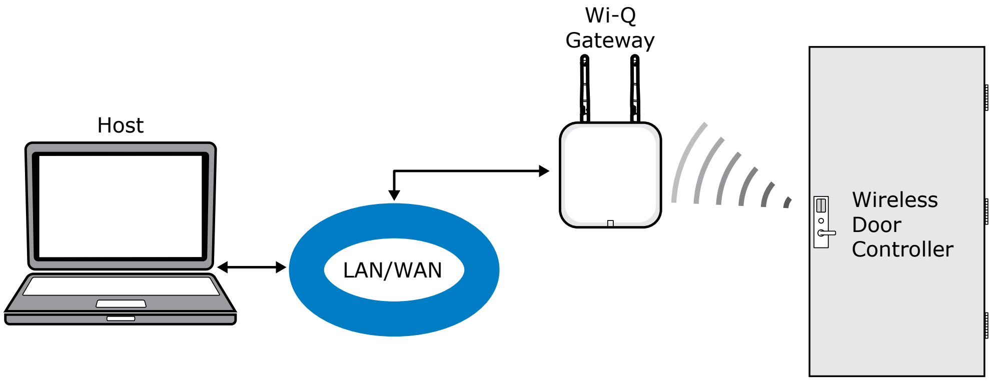
System Overview

The BEST Wi-Q Access Management System (Wi-Q AMS) integrates powerful access management software with Wi-Q Gateways, Wireless Access Controllers, and multiple controller formats that work together to enable all decision-making at the door. The system runs remotely with no need for hard-wiring, providing innovative access control in any environment. Wi-Q AMS is versatile so you can create a whole new system, retrofit existing hardware, and include various CCTV alarms, general alarms, and inputs/outputs.

Basic Hardware Components

A basic Wi-Q AMS system has three components: a host computer with Wi-Q AMS, a Wi-Q Gateway, and a controller lock at the door. Figure 1 is a simple diagram showing these three components.

Figure 1 Four Basic Components



The Host Computer

The software is installed at the Host computer and set up to tell the Wi-Q Gateways on the network which controllers to control and how to control them. It contains all User ID and access management commands. The Host transfers information to and from the Wi-Q Gateway through a standard Ethernet (LAN/WAN) connection.

The Wi-Q Gateway

The Wi-Q Gateway is a 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 controllers in a system.

Wireless Controllers

There are two types of Wi-Q and Omnilock Wireless Controllers:

Wi-Q

- Wireless Access Controller
    - PMN: WAC-SPIN
- Wireless Door Controller
    - PMN: WDC-SPIN
- Wireless Exit Device Controller
    - PMN: WXC-SPIN

Omnilock

- Single Door Controller
- Omnilock Reader

General Equipment and Service Information			
FCC Identifier:	FCC ID: WEF-WAC-SPIN	FCC ID: WEF-WDC-SPIN	FCC ID: WEF-WXC-SPIN
ISED Certification Number:	IC: 7713A-WACSPIN	IC: 7713A-WDCSPIN	IC: 7713A-WXCSPIN
Description of Product:	Wireless access controller - SPIN	Wireless Door Controller - SPIN	Wireless Exit Device Controller - SPIN
Model / HVIN:	WAC	WDC	WXC
PMN:	WAC-SPIN	WDC-SPIN	WXC-SPIN
FVIN:	WXQ-WAC	45HQ-MS, 45HQ-PKP, 45HQ-DV, 45HQ-SE, 45HQ-PH, 45HQ-PSEBH	EXQ-MS, EXQ-PKP, EXQ-DV, EXQ-SE, EXQ-PH, EXQ-PSEBH
Antenna Information:	Manufacturer: L-Com Type: Rubber duck Model: HG2402RD-RSF Gain: 2.2 dBi Internal/external: External	Manufacturer: Southwest Antenna Type: Planar antenna Model: 1055-036 Gain: 6 dBi Internal/external: External	Manufacturer: Southwest Antenna Type: Planar antenna Model: 1055-036 Gain: 6 dBi Internal/external: External
Maximum Transmit Power:	52.36 mW	1.23 mW	2.75 mW
Contains (Related Equipment):	N/A	FCC ID: T8H-SEICLASS IC: 7713A-SEICLASS Manufacturer: dormakaba USA Inc. Model: SE Technology: RFID	FCC ID: T8H-SEICLASS IC: 7713A-SEICLASS Manufacturer: dormakaba USA Inc. Model: SE Technology: RFID
Contains (Related Equipment):	N/A	FCC ID: JQ6-XTENDER IC: 2236B-XTENDER Manufacturer: HID GLOBAL CORPORATION Model: XTENDER Technology: Bluetooth	FCC ID: JQ6-XTENDER IC: 2236B-XTENDER Manufacturer: HID GLOBAL CORPORATION Model: XTENDER Technology: Bluetooth
Contains (Related Equipment):	N/A	FCC ID: T8H-BESTPM104 IC: 7713A-BESTPM104 Manufacturer: dormakaba USA Inc. Model: PKP Technology: RFID	FCC ID: T8H-BESTPM104 IC: 7713A-BESTPM104 Manufacturer: dormakaba USA Inc. Model: PKP Technology: RFID

Both controllers are equipped with Wi-Q or Omnilock 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 AMS software.

Basic Operation

The system works very simply. A user enters a pass code at a 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 Gateway 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 AMS 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 also use a Wireless Access Controller, hard-wired to a controller and strike, and wirelessly communicate back to a Wi-Q Gateway.

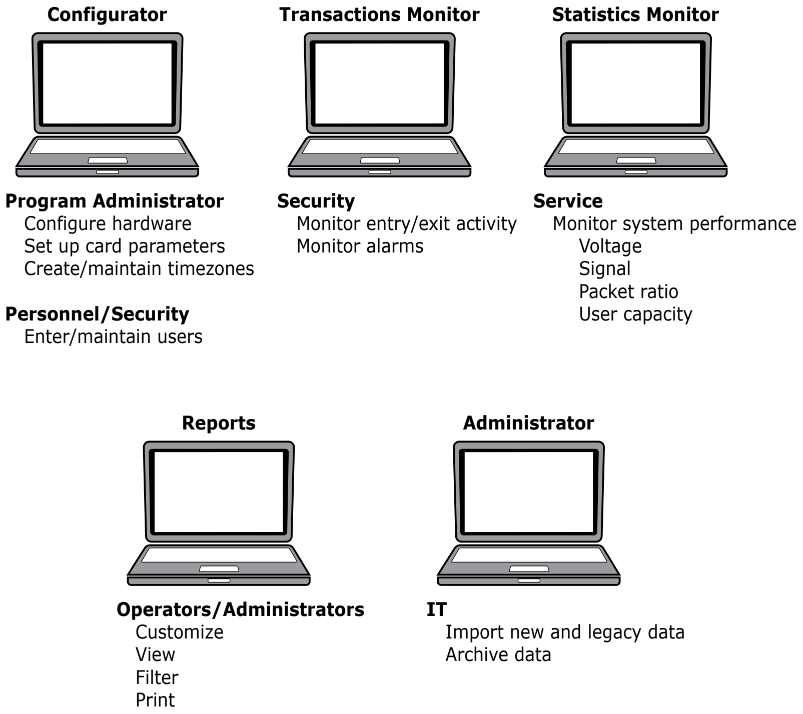
For more information about various applications, you can adapt for use with Wi-Q AMS, see "Hardware Overview" on page 13.

Software Overview

Wi-Q AMS provides powerful tools to manage your system: Wi-Q AMS Configurator, Transactions, and Statistics Monitor help you configure your settings, monitor transactions in the system, and verify system hardware performance. You can view and create reports from all applications and perform archivals and imports using Wi-Q AMS Administrator.

If you are the Program Administrator responsible for setting up communications between AMS software and system Wi-Q Gateways and controllers; you will spend most of your time using the Configurator module. If you are in personnel or security, you may be the person who adds users to the system and gives them access privileges and IDs. You will spend most of your time on the Users tab of the Configurator. If you are responsible to oversee security for your organization, you will monitor all access and alarm activity using the Transactions module. If you are a Systems Administrator responsible to ensure the wireless network is operating at maximum performance, you will use the Statistics Monitor and Administrator modules. If your organization is small, you may use all applications. Regardless of the tasks, you are responsible to perform, you can view and print reports from all applications using the Reports module.

Figure 2 Five Applications



Once the software is installed, you will find the Configurator module shortcut on your desktop. You can access all applications from the Configurator main menu. You can also access these applications from the Windows Start Menu under BEST Access.

Setup Checklist

Wi-Q AMS is set up in eleven 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 this User Guide.

- ❑ Task 1: Develop a Site Plan, page 17.
- ❑ Task 2: Position Wi-Q Gateways, page 21 .
- ❑ Task 3: Prepare your Computer, page 34.
- ❑ Task 4: Gather and Organize Segment Data, page 44.
- ❑ Task 5: Install Software, page 46.
- ❑ Task 6: Create your Segment, page 65.
- ❑ Task 7: Add and Configure Wi-Q Gateways, page 69.
- ❑ Task 8: Install Wi-Q Gateways, page 25.
- ❑ Task 9: Install Door Hardware, page 29.
- ❑ Task 10: Sign On and Configure Controllers, page 101.
- ❑ Task 11: Configure AMS Software, page 112.

2 Hardware Installation

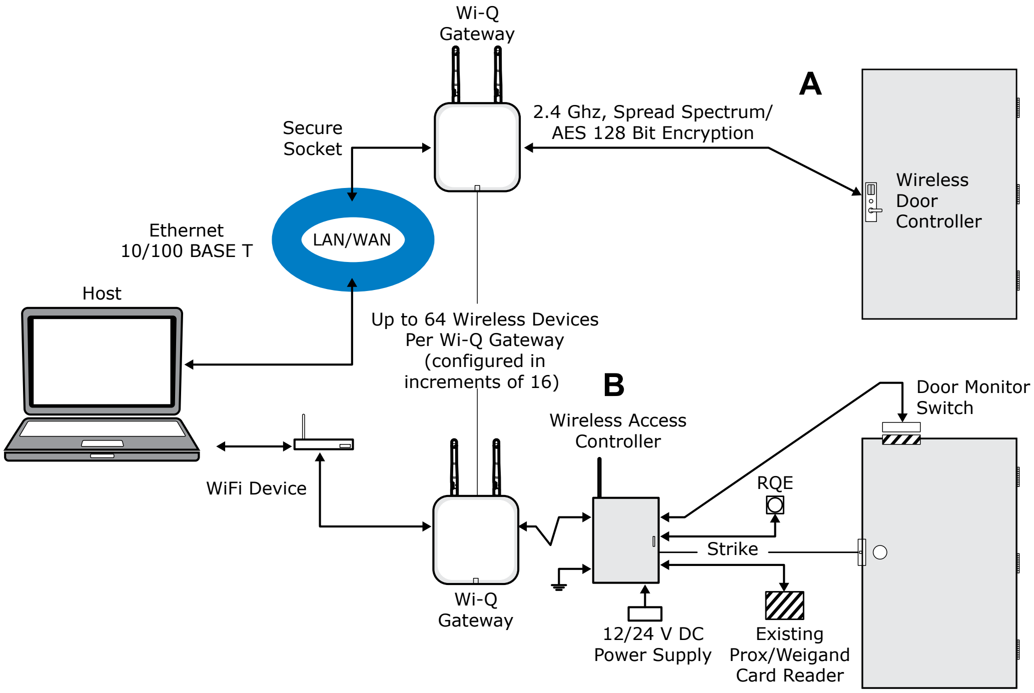
Hardware Overview

Wi-Q AMS runs remotely with no need for hard-wiring, creating a simple, innovative approach to access control in any environment.

Note Once Wireless Controllers are installed, you will need to sign them on to AMS software. Therefore, it is appropriate to install the software before or concurrent with hardware installation. For more information, see “Sign on and Configure Controllers (Task 10)” on page 101.

Figure 3 is a block diagram showing various configurations. Wi-Q AMS supports all 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 3 Example System Configurations


Wi-Q Gateway
A
2.4 Ghz, Spread Spectrum/ AES 128 Bit Encryption
Secure Socket
Wireless Door Controller
Ethernet 10/100 BASE T
LAN/WAN
Host
Up to 64 Wireless Devices Per Wi-Q Gateway (configured in increments of 16)
B
Door Monitor Switch
Wireless Access Controller
RQE
WiFi Device
Strike
Wi-Q Gateway
12/24 V DC Power Supply
Existing Prox/Weigand Card Reader

Wi-Q Gateways

The BEST 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 be upgraded to 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, approved 802.11 G wireless, or an approved commercial RF carrier-enabling a wireless solution end-to-end. All communications between Wireless Controllers and Wi-Q Gateways can be further backed up by "redundant" Wi-Q Gateways each with capacity for up to 64 Wireless Controllers.

Transmit range from Wi-Q Gateway to controller varies based on building construction. Various factors can affect the range you will see in your facility.

Wireless Controllers

Wi-Q AMS software is designed to operate with Wi-Q Technology BEST 45HQ mortise and BEST 9KQ Cylindrical locksets equipped with either keypad, card, or a combination of controller input devices. Wi-Q AMS software is also designed to work with Omnilock 9KOM cylindrical and 45KOM mortise locksets. Door switch monitor, request to exit, and door lock position sensors are included in the locks. Wi-Q and Omnilock 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 door
- Cardholder access level definition
- Dynamic memory for IDs vs Transactions
- Locally stored and transmitted transactions
- ADA Compliant
- No AC required at the door

Wireless Access Controllers

You can retrofit any existing controller configuration to communicate with Wi-Q Gateways using 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 AMS system, supporting Wiegand-compatible keypad Controller inputs. 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 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 and Omnilock Technology support 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).

Installing System Hardware

Wi-Q AMS is designed to operate with BEST Wi-Q and Omnilock Controllers and 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

❑ Wi-Spy Spectrum Analysis Tool by MetaGeek (or equivalent) to identify the best open channels for your network

❑ For Keypad Controllers, you will need the sign-on credential from the Wi-Q AMS software

❑ For magnetic stripe or proximity card controllers, you will need the Programmer ID cards supplied in the software package. You will also need the appropriate magnetic stripe or proximity USB enrollment controller 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 the 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 screwdrivers

❑ 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:

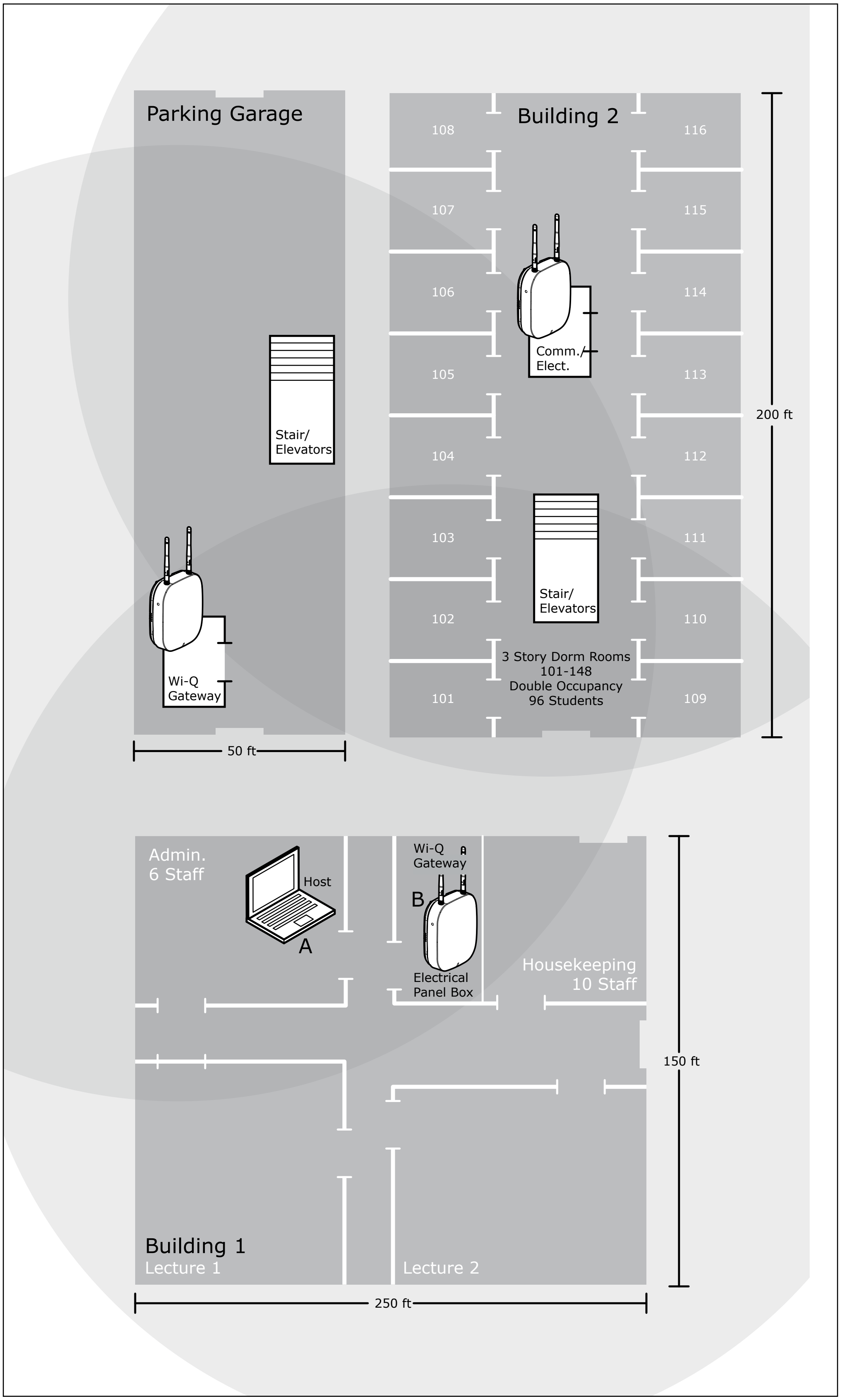
Transmit range from Wi-Q Gateway to controller varies based on building construction. Site characteristics such as reinforced concrete walls could interfere or weaken the signal; open spaces and low interference can increase signal strength.

Controllers will transmit to the nearest Wi-Q Gateway; however, if for some unforeseen event, the nearest Wi-Q Gateway goes down; the controllers are able to report to another Wi-Q Gateway in the nearby area, providing redundancy in the system.

Figure 4 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. This Wi-Q Gateway will collect transactions from the 12 controllers in Building 1. As you can see by the gray circle representing the Portal’s range, it also extends to the entrance of Building 2 and the Parking Garage. This provides redundant coverage of those areas should either of the other Portals go off line.

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 4 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 lock 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.

Redundancy

In our sample plan, approximate Wi-Q Gateway ranges are indicated by shaded circles. As you can see, these circles overlap, creating a degree of redundancy in the system. It is perfectly acceptable, in fact, desirable to create range redundancy in your plan. This will provide additional coverage should a Wi-Q Gateway go off line, intentionally or otherwise. If the controllers find that the nearest Wi-Q Gateway is down, they will "search" for the nearest Wi-Q Gateway.

Interference

Wi-Q and Omnilock 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 b and g) 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 Gateway.

To achieve maximum efficiency in AMS, 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 increase the transmit range.

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 the Wi-Q Gateways using the results from the Wi-Q Gateway built in Site Survey Mode along with the Wi-Q Technology Site Survey Kit. The Wi-Q Gateway Site Survey Mode 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.

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.

Verify Signal Strength and Packet Ratio Using Survey Mode

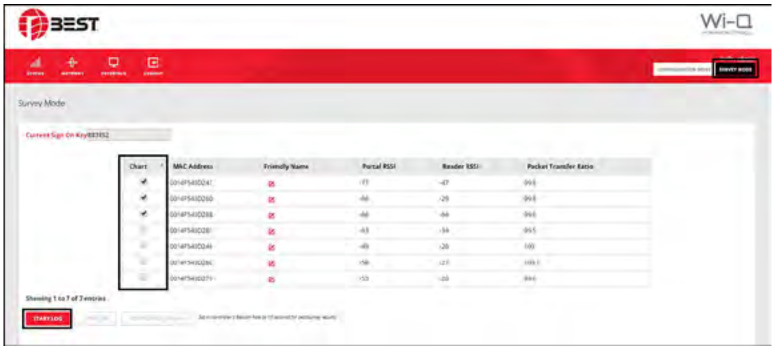
Prior to installation, the Wi-Q Technology Site Survey feature in the WQXM-PG should have been used to verify basic controller signal strength. Once the controllers are signed on, the WQXM-PG Site Survey webpage can be used to verify the signal strength and packet transfer ratio to verify all information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

To do this, please do the following:

1. Log in to the WQXM-PG by navigating to the IPv4 address using an Internet browser.
2. Click on the Survey Mode button.
3. Check the boxes next to the reader(s) connected to the Gateway to select them for the survey.

4 Click on the Start Log button to begin surveying the locks.

Figure 5 Survey Mode



Survey Mode

Current Sign On Key 883952

Chart	MAC Address	Friendly Name	Portal RSSI	Reader RSSI	Packet Transfer Ratio
✓	0014F540D241	☒	-77	-47	99.8
✓	0014F540D260	☒	-66	-29	99.8
✓	0014F540D288	☒	-66	-64	99.6
□	0014F540D281	☒	-63	-34	99.5
□	0014F540D246	☒	-49	-20	100
□	0014F540D28C	☒	-58	-27	100
□	0014F540D271	☒	-53	-20	99.6

Showing 1 to 7 of 7 entries

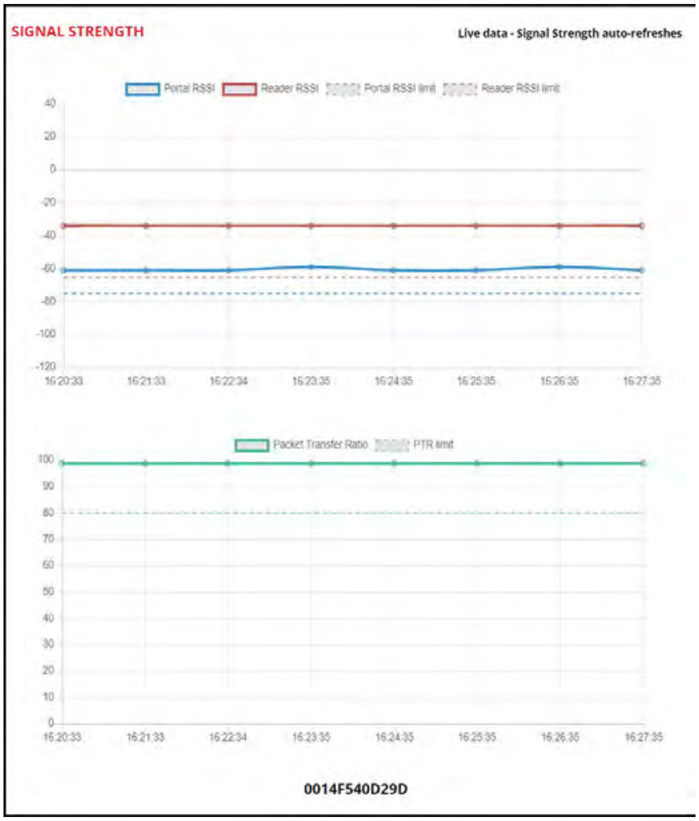
START LOG

The WQXM-PG Gateway will begin logging the Packet Transfer Ratio as well as the signal strength at the portal and the reader.

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 WQXM-PG denotes the lowest limit by the blue dashed line in the Signal Strength chart. If the Portal RSSI value is below the limit, please reposition the Gateway or the antennas to improve signal strength. It may also be possible that another portal is required for adequate coverage.

Figure 6 Portal Signal Strength



Reader Signal Strength

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

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

Packet Transfer Ratio

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

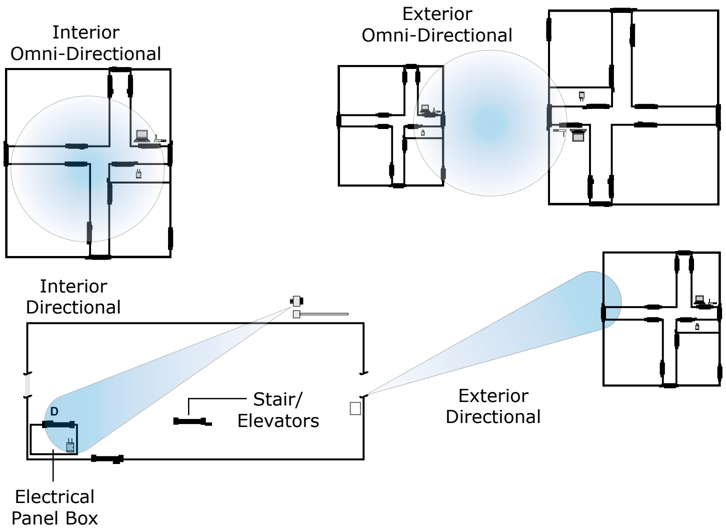
Note OnGuard 7.4 and higher with Wi-Q Interfaced installations using the WQXM-PG, require global statistics update poll rates to be made during troubleshooting. Please contact dormakaba Technical Support for direction at 800-392-5209 or via email at bas.support.best.us@dormakaba.com.

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

Antenna types

Wi-Q and Omnilock Technology provide 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 7 shows two available antenna types.

Figure 7 Selecting the antenna type that best suits your needs.



Power Supply

The Wi-Q Gateways can be powered using PoE. The Wi-Q Gateway is a class 1 PoE device. If PoE is not available from the network, then 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 into a 24/7 power circuit that cannot be turned off at a switch, such as a light switch that might be turned off by a cleaning crew.

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

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

Note Actual distances will vary based on building construction.

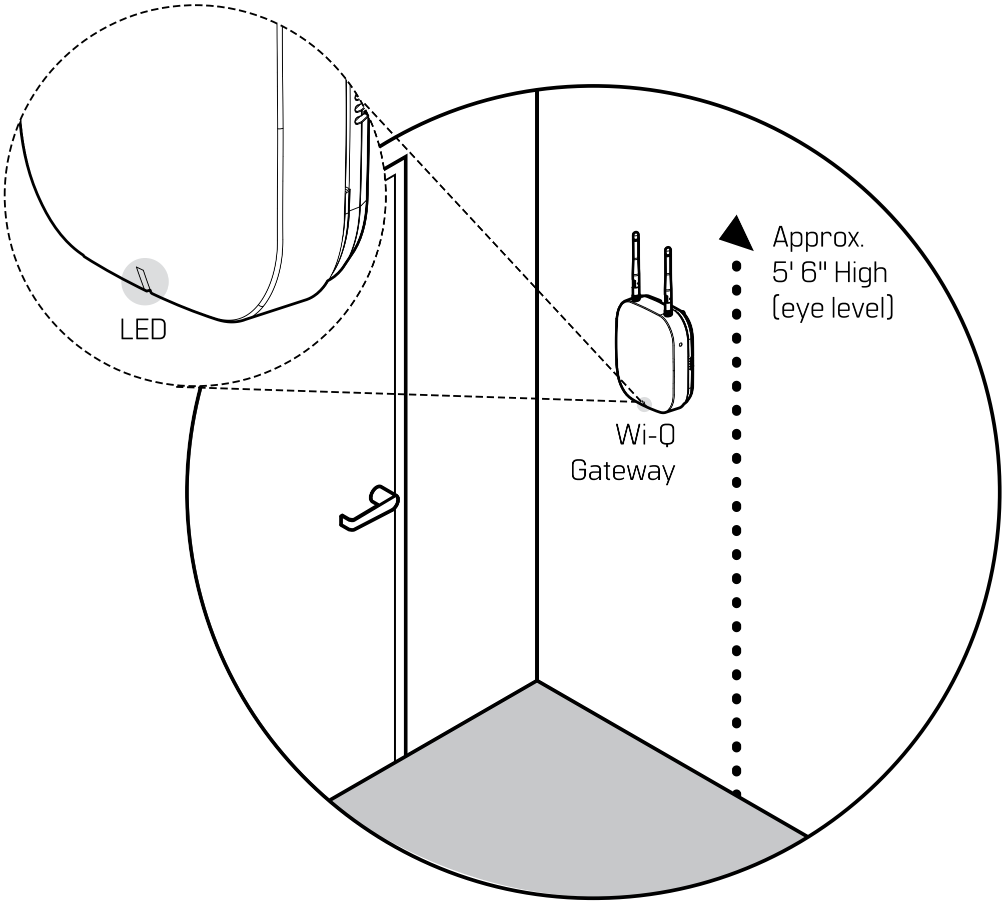
Next steps

When you are satisfied with the signal performance, you can proceed to configure Wi-Q Gateways using Wi-Q AMS.

Install Wi-Q Gateways (Task 8)

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 8 shows a Wi-Q Gateway positioned in a protected area.

Figure 8 Installing a Wi-Q Gateway in a protected area.



Connecting the Wi-Q Gateway and Verifying Operation

Once the Wi-Q Gateway is installed, connect and verify operation:

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

2 If using the AC adpator to power the Wi-Q Gateway then connect the AC adapter power

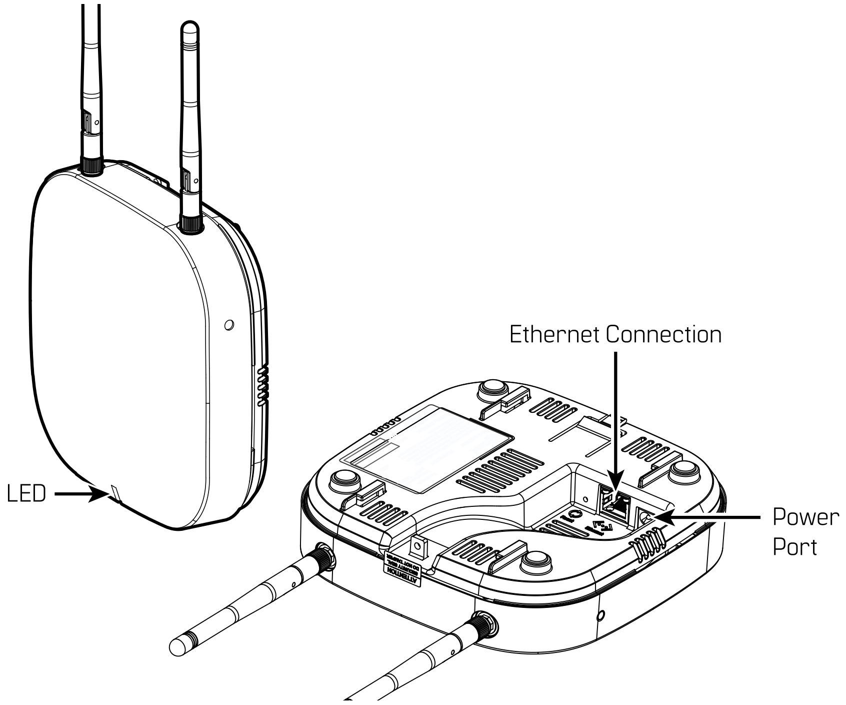
supply to the Wi-Q Gateway and plug in the AC adapter to the AC outlet. The indicator light on the top of the enclosure should come on and start flashing purple.

3 Wait for the indicator LED to turn solid red. This will take 4-5 minutes and indicates the Wi-Q Gateway is fully booted up. See the table below for a description of all the indicator light behaviors.

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.

4 After the Wi-Q Gateway is fully booted up the ethernet link indicator (See Fgure 9) light should come on and flash under normal operation.

Figure 9 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.

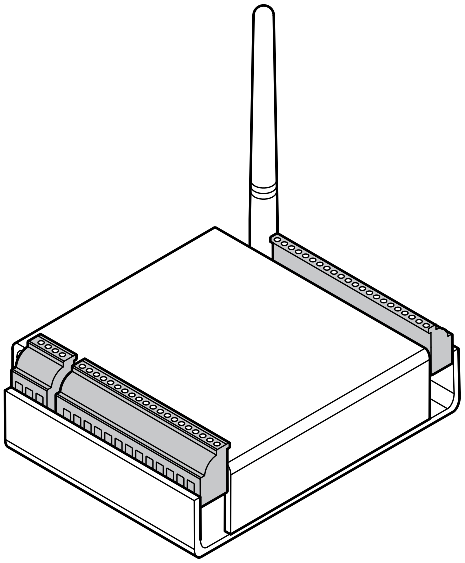
Installing a Wireless Access Controller

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 my be obsolete or unable to handle additional controller inputs. It supports Wiegand-compatible keypad Controllers and is configured and monitored in Wi-Q AMS the same as a standard controller.

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

Using the Wireless Access Controller (Figure 10), 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 10 Wireless Access Controller.



Installation

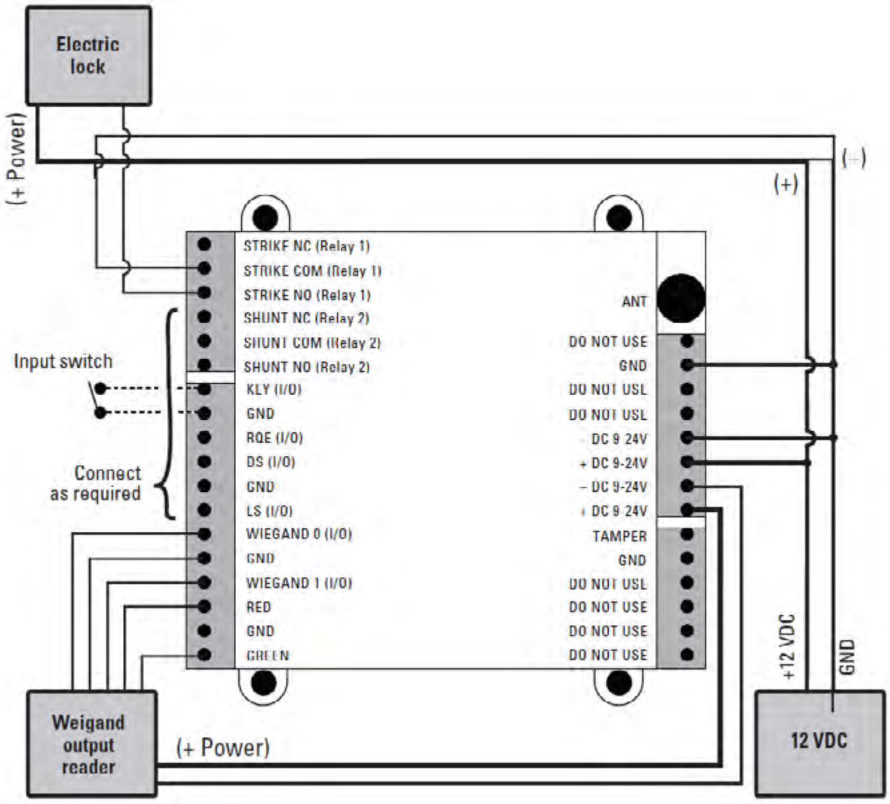
Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

WARNING: Wireless Access Controllers are intended for use in an 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 11 is a wiring diagram illustrating both configurations.

Figure 11 Connecting devices to a WAC



Once the WAC is installed and all points connected, it will be recognized by Wi-Q AMS as a 'Controller' in the system. For more information about configuring the WAC in the software, see "I/O" on page 132.

Install Door Hardware (Task 9)

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, BEST EXQ Trim, Omnilock 45KOM mortise locks, and Omnilock 9KOM cylindrical locks 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 the device. You will need this when configuring the controller in the 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 and Omnilock Controllers are designed for use on 1-3/4-inch doors. If you need to install on non-standard doors, contact dormakaba Technical Support for more information by calling 1-800-392-5209.
- 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 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 controller (mag card), default Programmer ID cards are supplied with the software. You will need these cards when you are ready to sign on the controllers.

To perform a magnetic stripe card verification:

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

6 Select the default Programmer ID card that matches the type for your magnetic card controller.

7 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 Controller will flash green once and unlock, then during the open delay time, it will flash green five times. Once this occurs, the card controller light will flash red and lock.

8 While unlocked, check for proper lock operation.

Keypad Check

If your Controller is a keypad type, perform the following steps:

9 At the keypad, enter the default Programmer ID, 1234#. The green light on top of the card controller will flash once and the lock will unlock, then during the open delay time, it will flash green five times. Once this occurs, the controller red light will flash and the lock will relock.

10 While unlocked, check for proper lock operation.

Proximity Reader check

1 Present the temporary operator card in front of the proximity reader.

2 The green light on top of the controller will flash once and 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.

3 While unlocked, check for proper lock operation.

Troubleshooting mortise and cylindrical locks

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

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:

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.

Once you have installed and tested your Controllers, you are ready to sign them on in your system. To do this, Wi-Q AMS 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. See "Add and Configure Wi-Q Gateways (Task 7)" on page 69. Once that is done you can return to the site and sign on the controllers. See "Sign on and Configure Controllers (Task 10)" on page 101.

Verify Signal Strength, Voltage and Packet Radio

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 Wi-Q Gateway built in Site Survey Mode or the Wi-Q AMS Statistics Monitor 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 Statistics Monitor application, see “Statistics Monitor” on page 208.

3 Software Installation

BEST Wi-Q AMS provides powerful suites of tools to manage your system: Configurator, Transactions and Statistics Monitor. View reports from all applications using Reports, and perform archivals and imports using Administrator.

Once the software is installed, you will find the Configurator shortcut on your desktop. You can access all applications from the Configurator main menu. You can also access these applications from the Windows Start Menu.

The following setup tasks are covered in this section:

Task 3 — Prepare your Computer

Task 4 — Gather and Organize Segment Data

Task 5 — Install Wi-Q AMS Software

Prepare Your Computer (Task 3)

To prepare your computer for the installation of the Wi-Q AMS software, you must ensure that your system is equipped with an appropriate operating system, database, and server and configure your Windows Firewall Ports.

Recommended System Limits

It is important to ensure your Host computer or computers are adequate to handle the system. The following table lists the recommended system limits for running Wi-Q AMS.

Hardware Configuration	**Parameter**		
	Config 1*	**Config 2***	**Config 3***
CPU Speed	2 cores @ 3GHz	4 cores @ 3GHz x 2 machines, Communication Servers	8 cores @ 3GHz x 4 machines (SQL Server & Communication Server)
RAM	4 GB, 8 GB	8 GB	16 GB
Hard Disk	40 GB	40 GB	100 GB
OS	Windows Server 2012 Windows 10 64Bit Standard and R2 x64, Server 2016	Windows Server Windows Server 2012 Windows Server 2016 Standard & R2 Standard x64	Windows Server 2012 Windows Server 2016 Standard & R2 Standard x64
SQL Version	SQL 2014 Express x64 SQL 2016 and 2017 SQL 2012 Express 64 Bit Only SQL 2012 R1 SP1 x64	SQL 2016, SQL 2017 SQL 2012 R1 SP1 x64	SQL 2016 and 2017 SQL 2012 R1 SP1 x64
Portal Gateways	25, 50	250	1000
Devices	300, 1000	3000	10000
Users	1000, 5000	10000	50000
Segments	1	1	1
Ethernet	1000 Base T	1000 Base T	1000 Base T

* — requires tuning of system parameters during installation by dormakaba Technical Support

Configure Windows Firewall Ports

Several ports must be enabled in your Windows firewall settings to allow proper communication with AMS. The following ports must be enabled:

- Port 23
- Port 80
- Port 443
- Port 1433
- Port 1434
- Port 8000
- Port 11000
- Port 5353

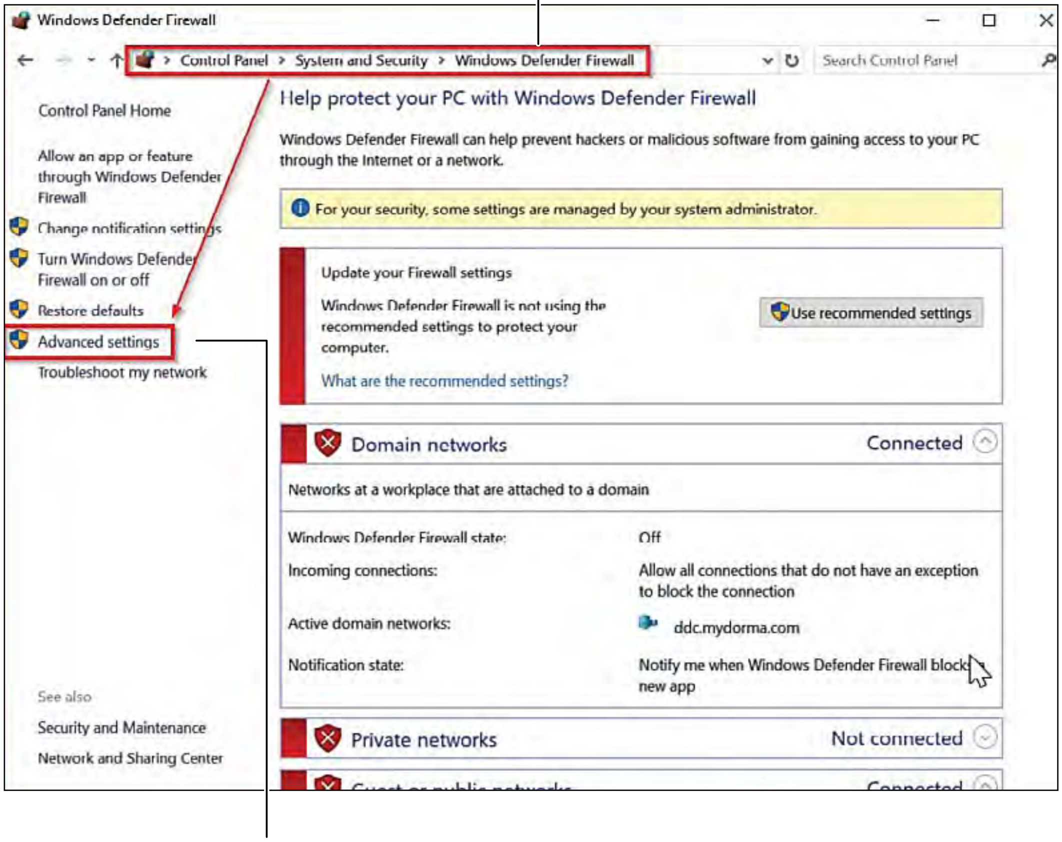
If your firewall is disabled, then all ports are open by default. If the firewall is on, perform the following steps in order to add the required ports listed above:

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

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.

What are the recommended settings?

Use recommended settings

Domain networks Connected

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

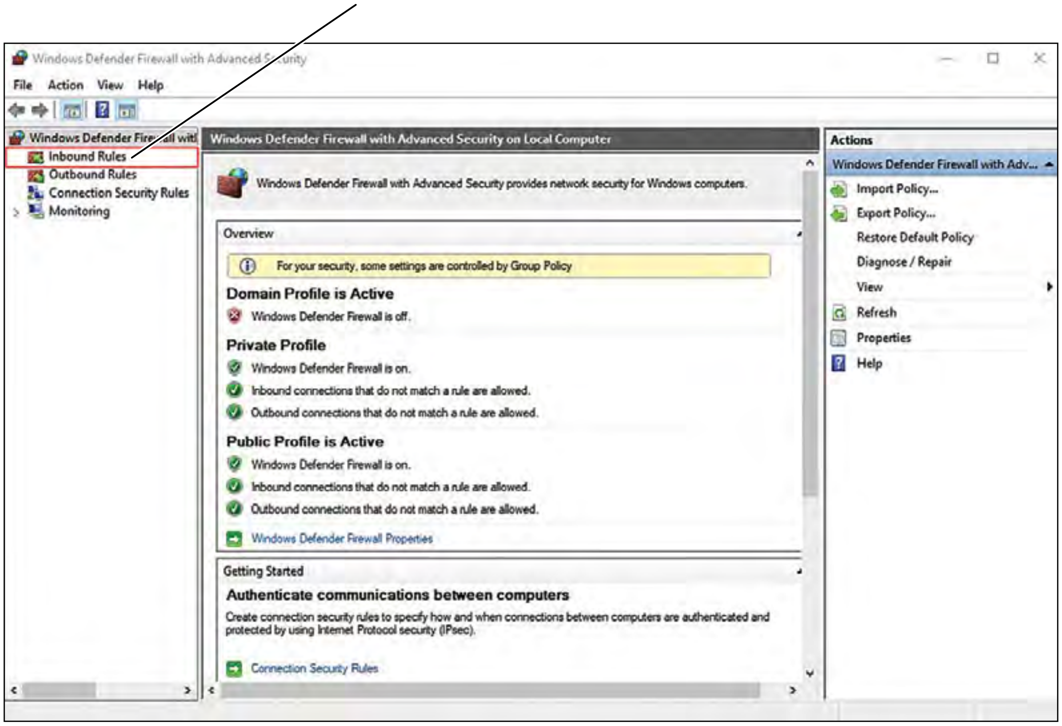
Private networks Not connected

Guest or public networks Connected

Click on Advanced settings

2 Select Inbound Rules.

Figure 13 Inbound Rules



Select Inbound Rules

Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring

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

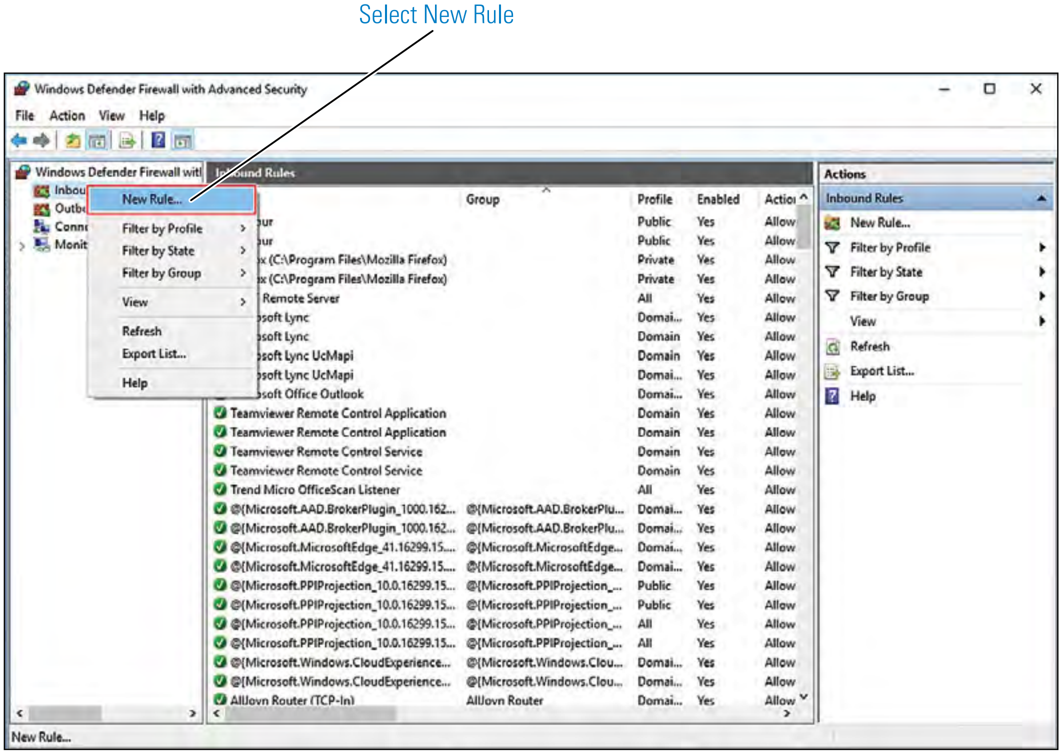
Authenticate communications between computers

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



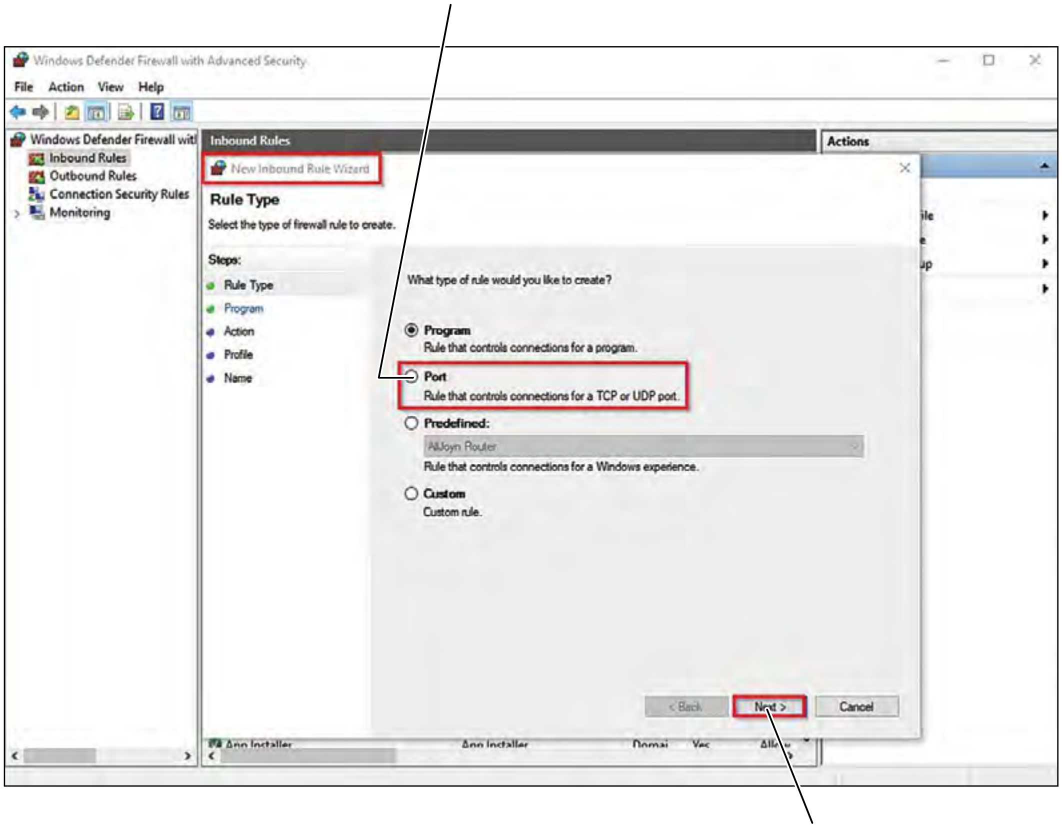
Select New Rule

	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

Select Port



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.

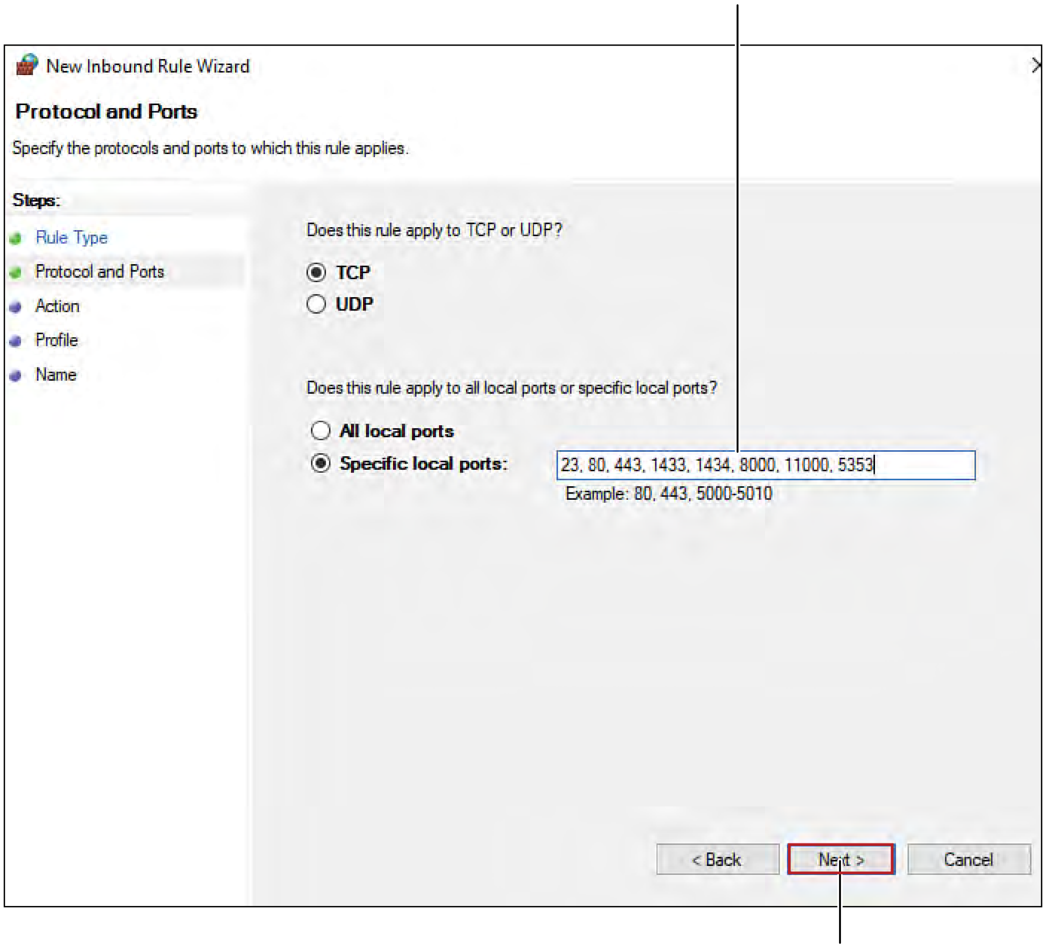
○ Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.

Click Next

5 Enter the following ports into the “Specific local posts” field: 23, 80, 443, 1433, 1434, 8000, 11000, 5353. Then, click Next to continue.

Figure 16 Enter Ports



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

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: 23, 80, 443, 1433, 1434, 8000, 11000, 5353

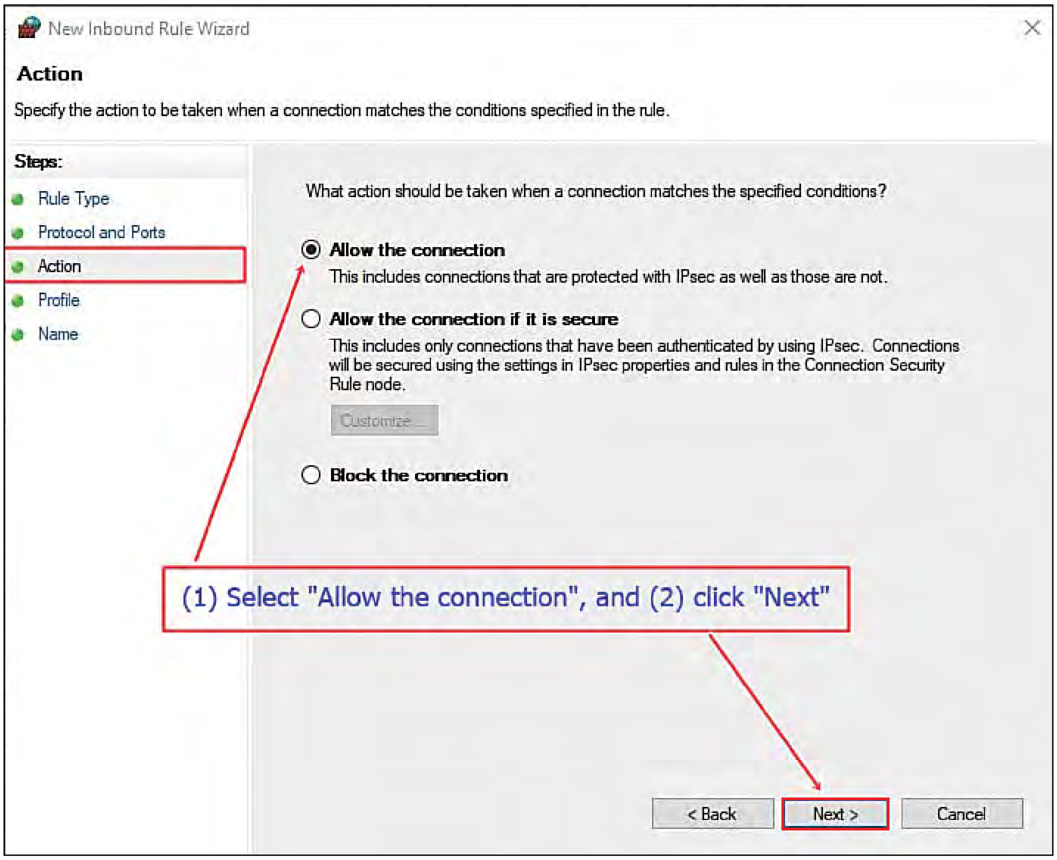
Example: 80, 443, 5000-5010

Ports: 23, 80, 443, 1433, 1434, 8000, 11000, 5353

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.

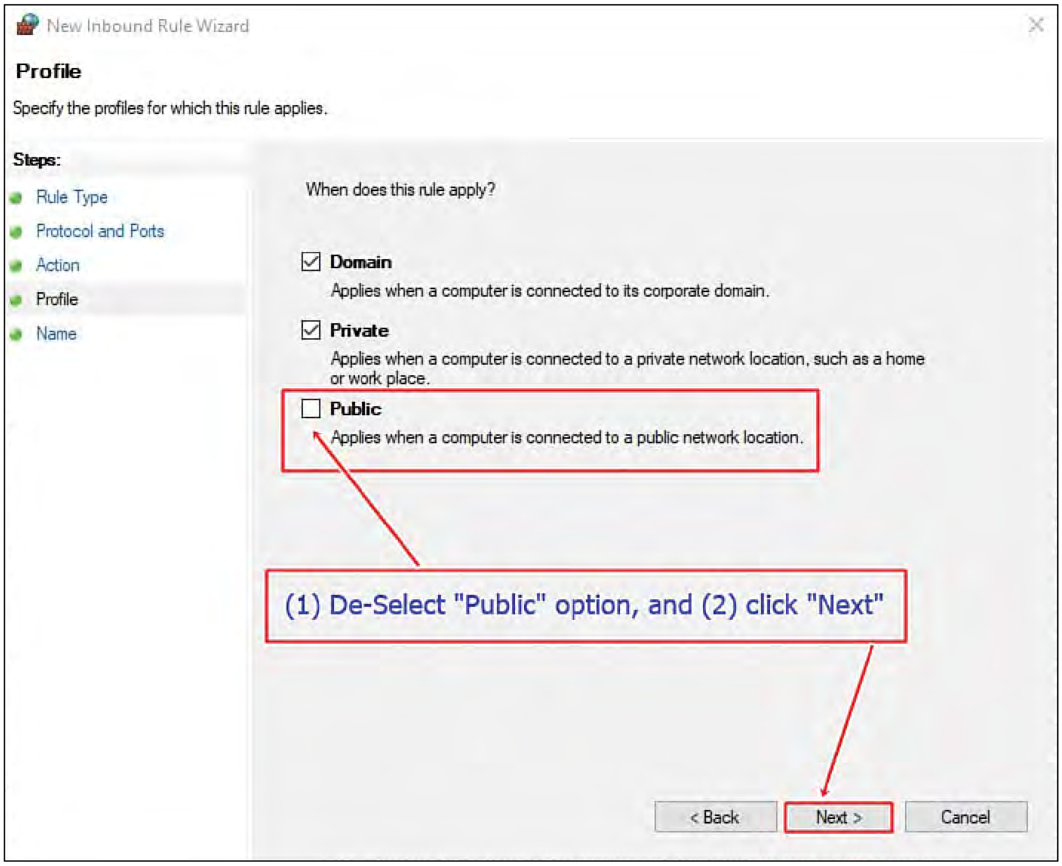
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **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



Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

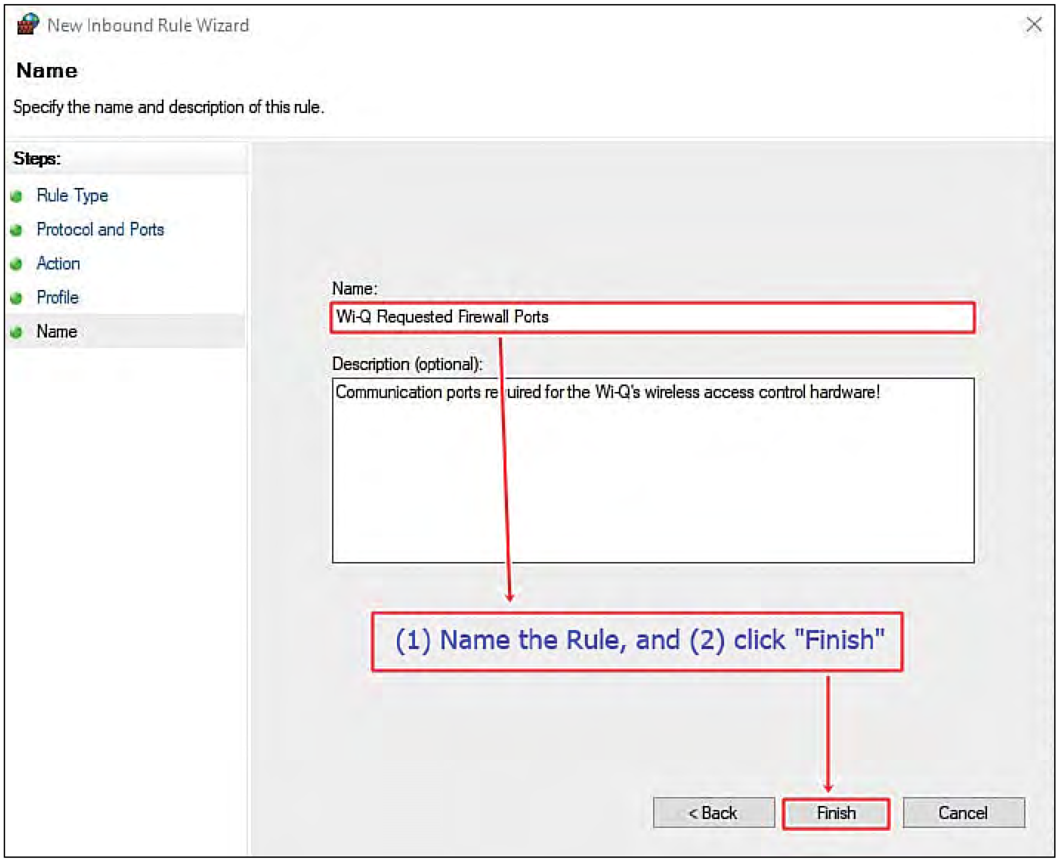
☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☐ **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.

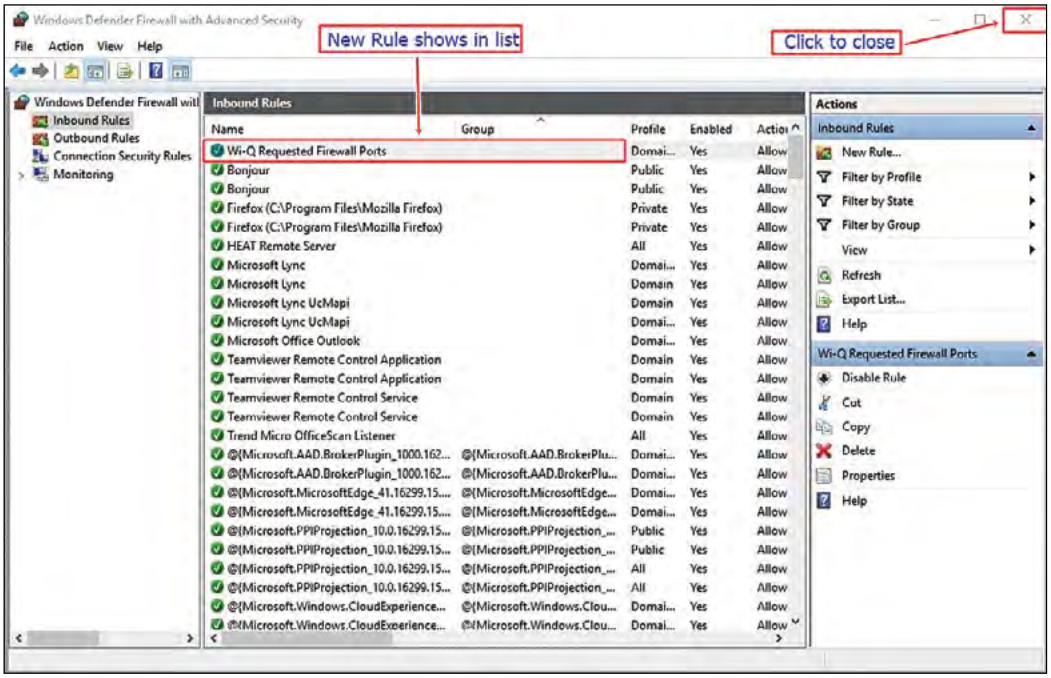
Name:
Wi-Q Requested Firewall Ports

Description (optional):
Communication ports re uired 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

Inbound Rules

Name	Group	Profile	Enabled	Actio
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

Gather and Organize Segment Data (Task 4)

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 Wi-Q AMS.

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 AMS Segment Tree. Ensure your site technical team will provide you this information as they work their way through the site.

User Information

You will also 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 AMS.

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:

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 wheelchair? 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 Wi-Q AMS using the program's System Administrator feature. If you have a large organization, this will save you time and reduce data entry error. See "Importing Data from a Legacy OFM Database" on page 187.

Install Software (Task 5)

The AMS software is installed in three steps: Install the Database Server component, Install Wi-Q AMS Web Services, Install Applications.

Note The installation may detect missing prerequisites during the installation process. Have your original Microsoft Windows installation files ready for use if prompted (Configuration #5 – Server PC (Pro and Enterprise Region Systems). In addition, be prepared to address the following conditions during the setup:

If...	Then
If you plan to use a secure socket layer (SSL) connection (connecting via the internet)	SSL Certificates must be issued by the Wi-Q Gateway and uploaded into the Wi-Q AMS Software. Certificates expire every 3 years for Wi-Q Gateways model WQX-PG and every 20 years for Wi-Q Gateways model WQXM-PG.
You plan to use a basic authentication	A local administrator user account, login, and password must be generated for the system to log into. (Instructions are presented in Wi-Q Gateway Setup, Setup tab, Host Access Settings. SQL Server permissions are also required on the WAMS database.)

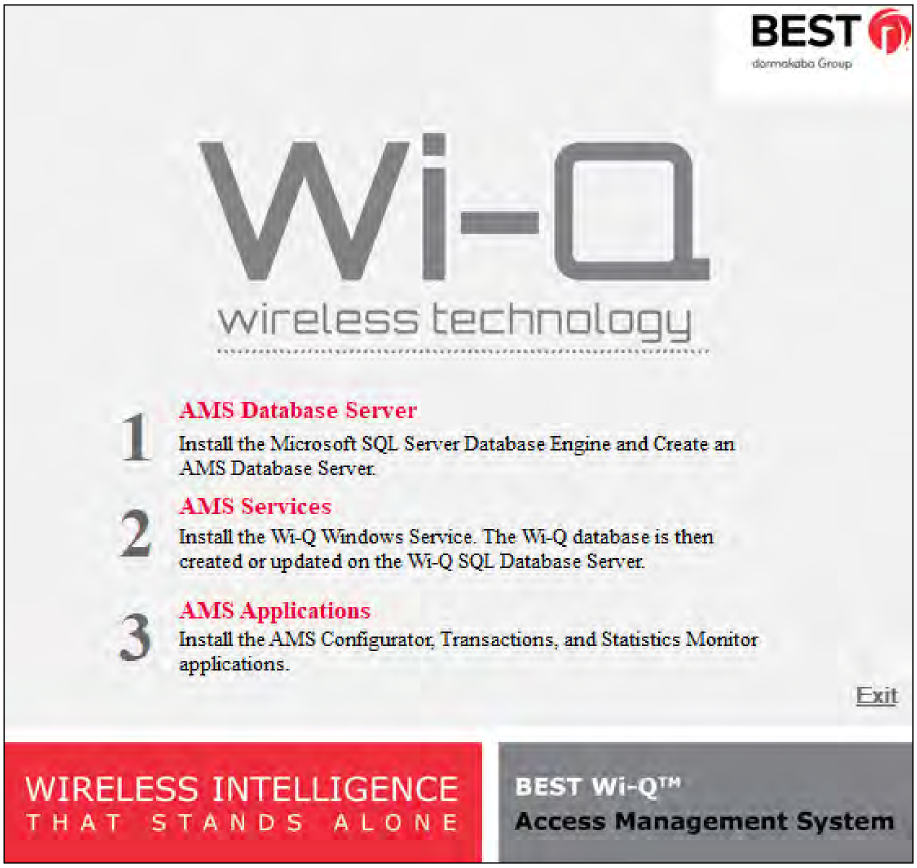
Beginning Installation

1 If you have not already done so, download the Wi-Q AMS Software from the dormakaba External Secure file share available to all Wi-Q Certified Technicians.

Note If you have downloaded the installation files to your machine, it is recommended that you save the folder directly on your local hard drive to keep the path to the files as short as possible such as C:\Temp.

2 To start the installation wizard, right-click on the WiQSetup.exe file and run as Administrator.

Figure 21 Wi-Q Launch



1 **AMS Database Server**
Install the Microsoft SQL Server Database Engine and Create an AMS Database Server.

2 **AMS Services**
Install the Wi-Q Windows Service. The Wi-Q database is then created or updated on the Wi-Q SQL Database Server.

3 **AMS Applications**
Install the AMS Configurator, Transactions, and Statistics Monitor applications.

3 Step 1 of the installation wizard is the SQL database server set up. This step will install the SQL Express Database Server as well as the SQL Server management Studio application.

4 Step 2, Wi-Q AMS Services Setup checks your workstation for any missing prerequisites, such as Microsoft.NET Framework.

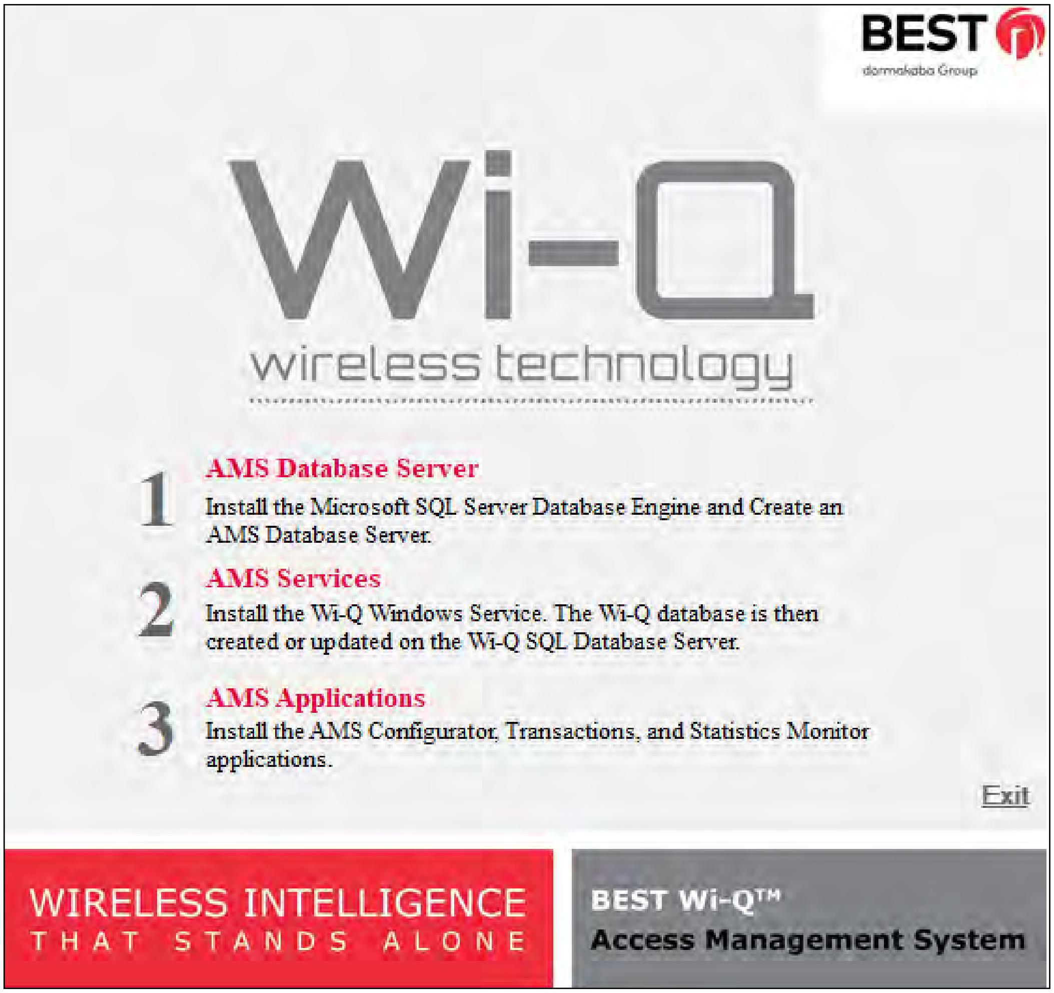
Note It is recommended that you reboot your machine after any missing prerequisites are installed before continuing on with the installation. After rebooting your machine, click the “Setup.exe” file again.

5 Step 3, Wi-Q AMS Applications for installing the Configurator, Transactions and Statistics Monitor.

Note You may wish to install the services and database on one machine (such as the Host) and the AMS Applications only at other machines. This can be done by only installing Step 3: AMS Applications on Client Machines.

Note The screenshots in this User Guide are from a BEST Wi-Q AMS system.

Figure 22 AMS Setup



1 AMS Database Server
Install the Microsoft SQL Server Database Engine and Create an AMS Database Server.

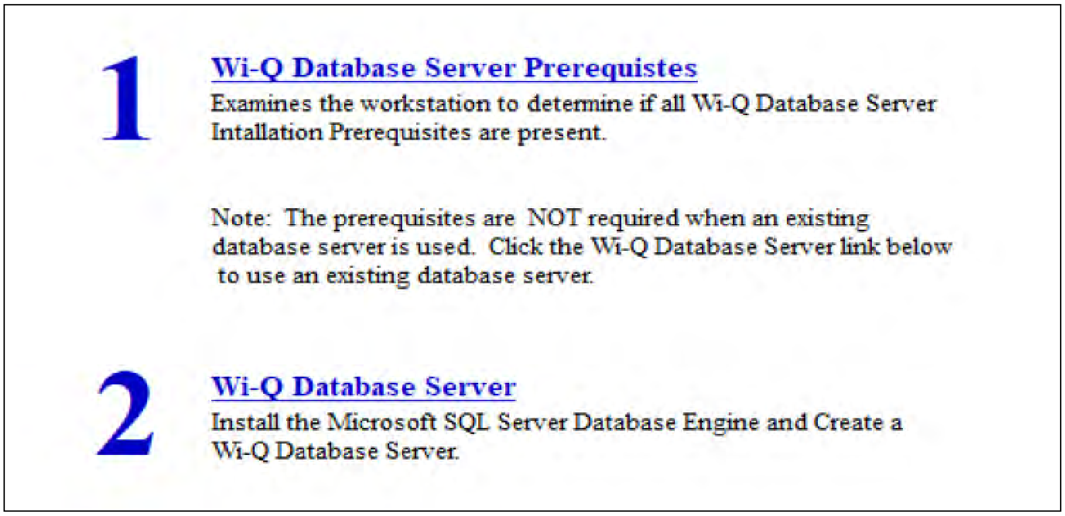
2 AMS Services
Install the Wi-Q Windows Service. The Wi-Q database is then created or updated on the Wi-Q SQL Database Server.

3 AMS Applications
Install the AMS Configurator, Transactions, and Statistics Monitor applications.

Step 1

1 Click the AMS Database Server link. If a similar dialog box opens with a link to install Prerequisites, click the link.

Figure 23 Database Server Prerequisites



1

Wi-Q Database Server Prerequistes

Examines the workstation to determine if all Wi-Q Database Server Intallation Prerequisites are present.

Note: The prerequisites are NOT required when an existing database server is used. Click the Wi-Q Database Server link below to use an existing database server.

2

Wi-Q Database Server

Install the Microsoft SQL Server Database Engine and Create a Wi-Q Database Server.

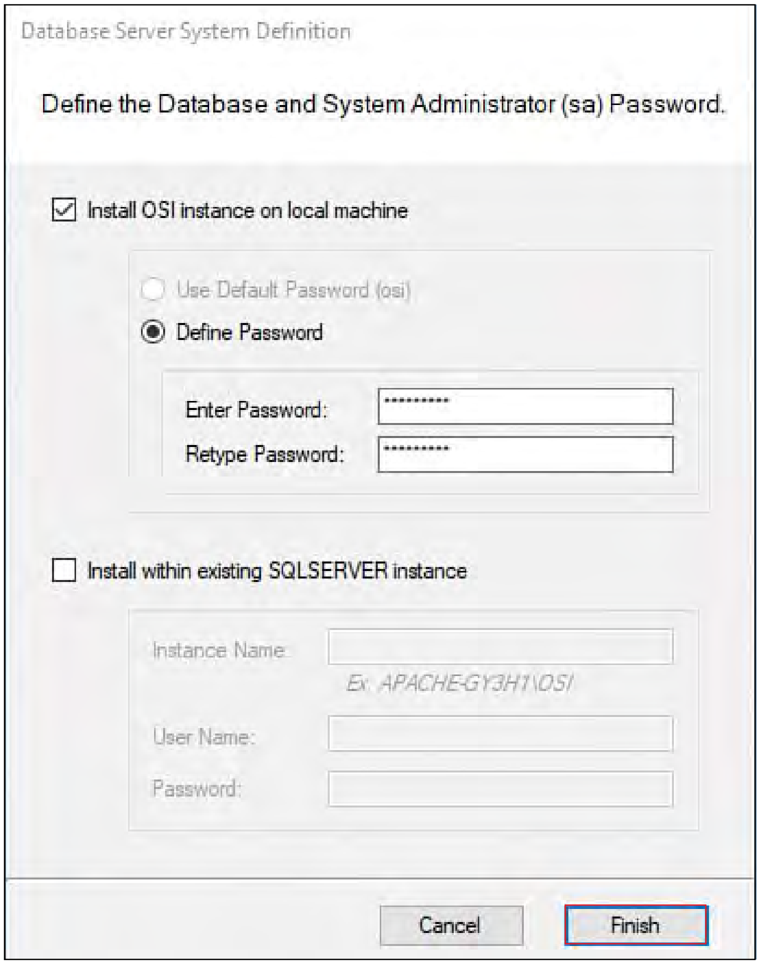
2 You may be prompted to install a number of prerequisites, including Microsoft Windows Installer and Windows PowerShell. To install the latest versions of these prerequisites, it is recommended that you click the website links provided and download directly from the Microsoft website. Once you've downloaded the setup files, follow the installation prompts provided.

Note It is recommended that you reboot your machine after any missing prerequisites are installed before continuing on with the installation.

3 Once all the prerequisites have been installed, click the link on the main setup screen to install the AMS Database Server.

4 The Database Server System Definition dialog box opens. Choose whether to install the server on a local machine or within an existing SQL Server instance. If you choose to install on a local machine, decide whether to use the default password or define a new password. If you choose to install within an existing server, enter the instance name and associated user name and password. Then click Finish.

Figure 24 Database Server System Definition



Database Server System Definition

Define the Database and System Administrator (sa) Password.

☑ Install OSI instance on local machine

○ Use Default Password (osi)

● Define Password

Enter Password: **********

Retype Password: **********

□ Install within existing SQLSERVER instance

Instance Name:

Ex: APACHE-GY3H1\OSI

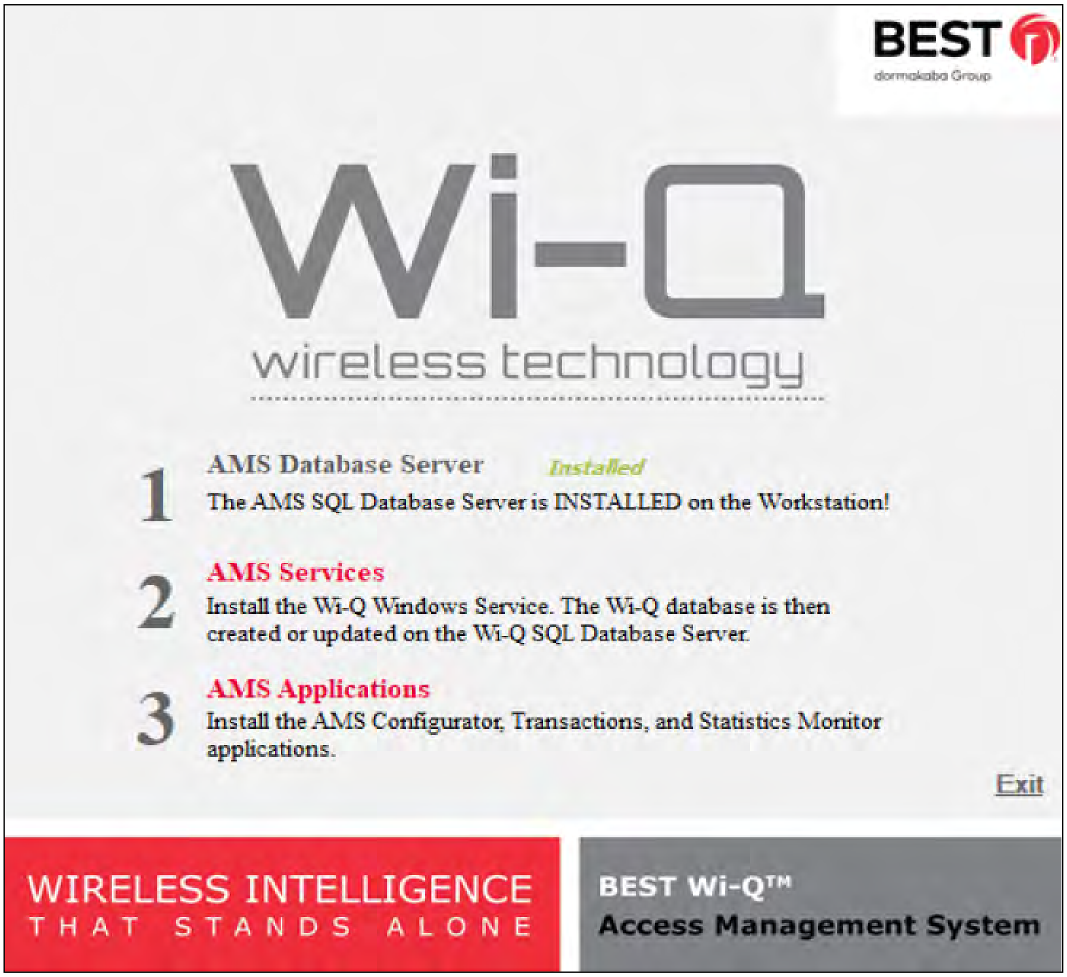
User Name:

Password:

5 The SQL Database Server will install now. This may take several minutes.

6 When the server is successfully installed, you will see “Installed” next to Step 1. As you work through the process, steps that have been completed or don’t need attention will no longer have clickable links.

Figure 25 AMS Database Server Successfully Installed



1 AMS Database Server *Installed*
The AMS SQL Database Server is INSTALLED on the Workstation!

2 AMS Services
Install the Wi-Q Windows Service. The Wi-Q database is then created or updated on the Wi-Q SQL Database Server.

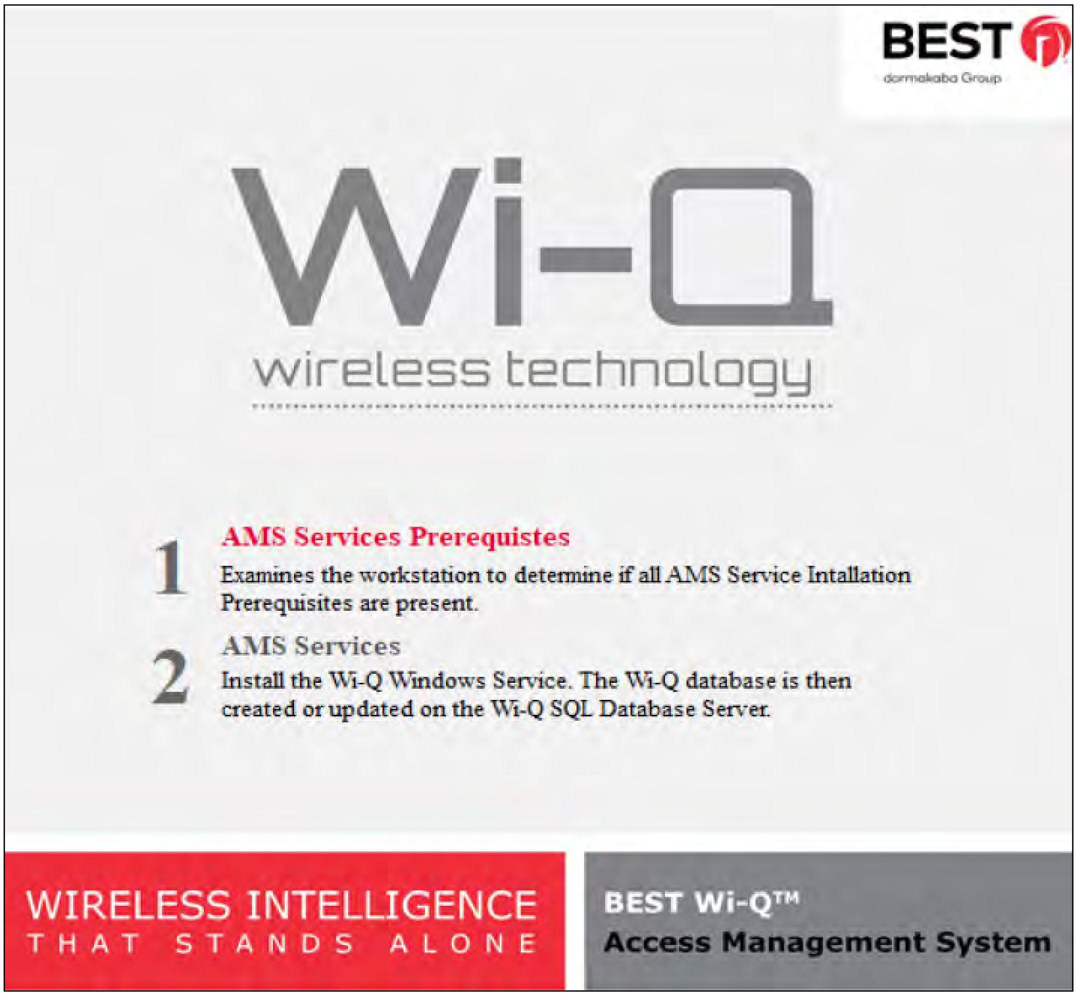
3 AMS Applications
Install the AMS Configurator, Transactions, and Statistics Monitor applications.

Step 2

1 On the Setup main page, click the AMS Services Prerequisites.

2 If a similar dialog box opens with a link to install Prerequisites, click the link. See Figure 26.

Figure 26 Install Prerequisites



1 **AMS Services Prerequistes**
Examines the workstation to determine if all AMS Service Intallation Prerequisites are present.

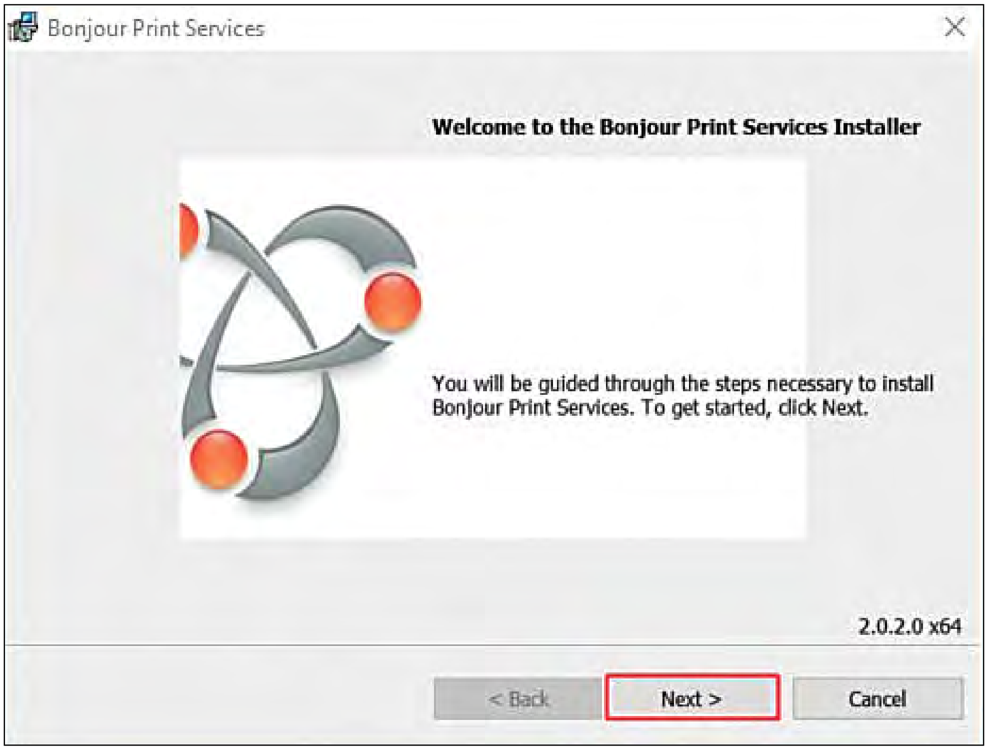
2 **AMS Services**
Install the Wi-Q Windows Service. The Wi-Q database is then created or updated on the Wi-Q SQL Database Server.

a You may be prompted to install Apple® Bonjour®. Bonjour networking technology is used by the Portal Configuration Tool to locate and list all Wi-Q Gateways on the network. Click the link to begin installing Bonjour.

b The Bonjour Print Services window opens. Click Next to continue.

Note Bonjour Print Services required to discover the Wi-Q Gateways on the network.

Figure 27 Bonjour Print Services Installer



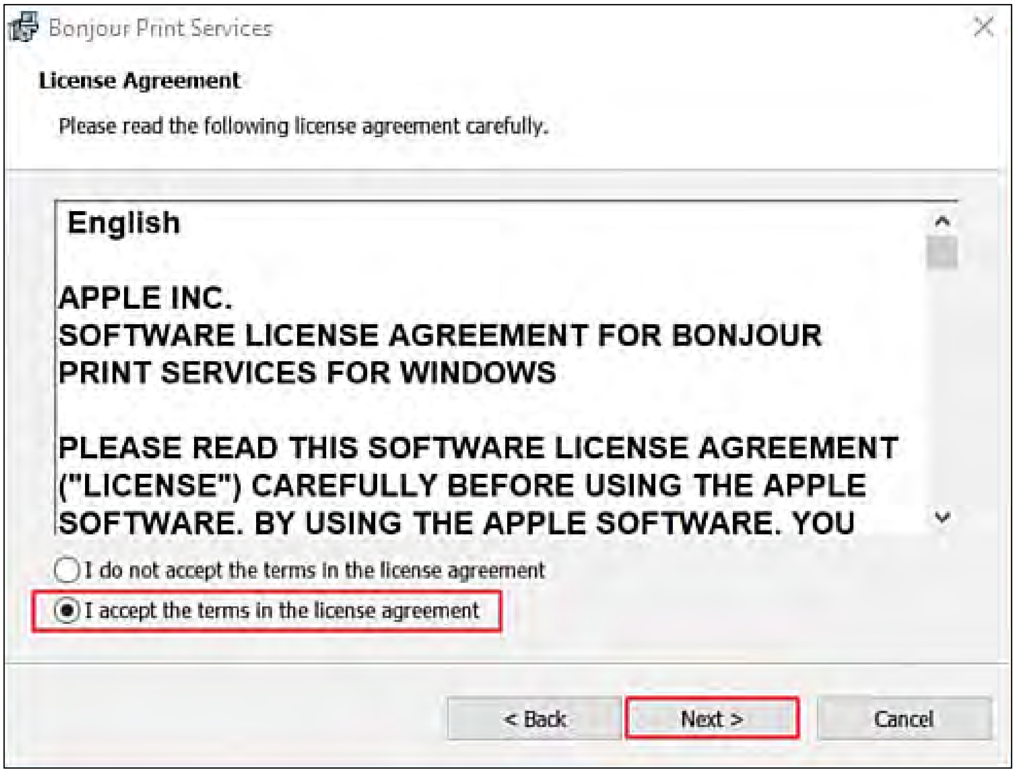
Welcome to the Bonjour Print Services Installer

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

2.0.2.0 x64

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

Figure 28 Bonjour Print Services License Agreement



License Agreement

Please read the following license agreement carefully.

English

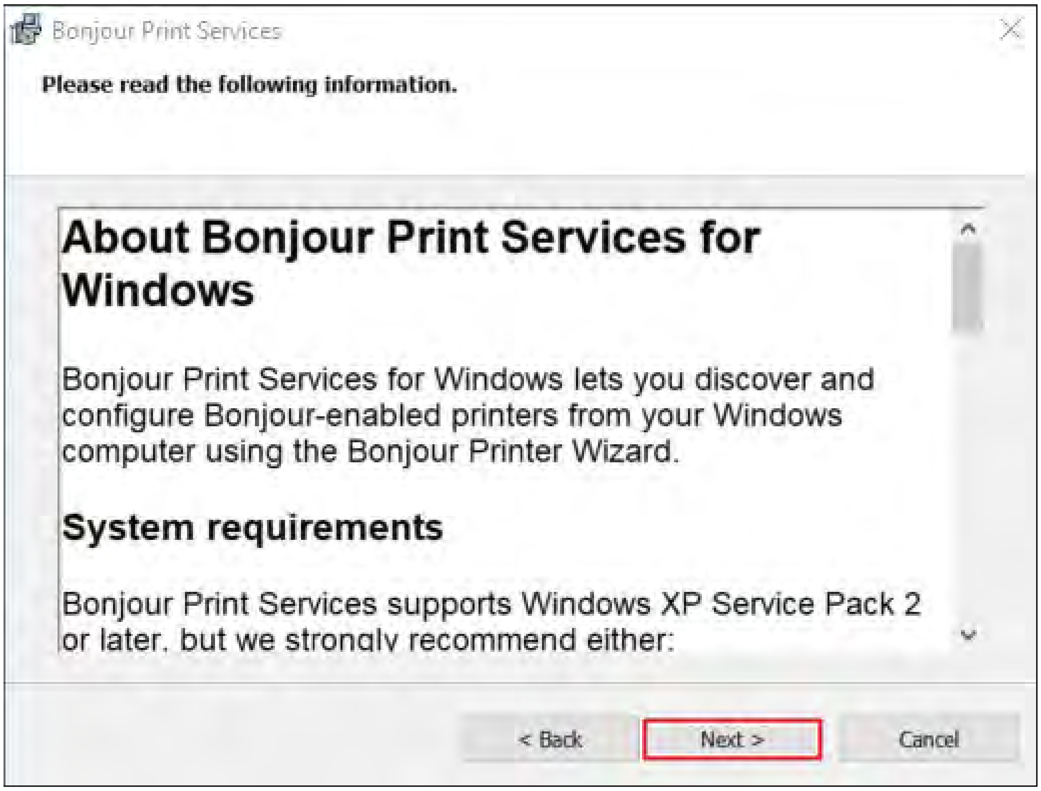
APPLE INC.
SOFTWARE LICENSE AGREEMENT FOR BONJOUR PRINT SERVICES FOR WINDOWS

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING THE APPLE SOFTWARE. BY USING THE APPLE SOFTWARE. YOU

○ I do not accept the terms in the license agreement
● I accept the terms in the license agreement

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

Figure 29 Bonjour Print Services Information



Bonjour Print Services

Please read the following information.

About Bonjour Print Services for Windows

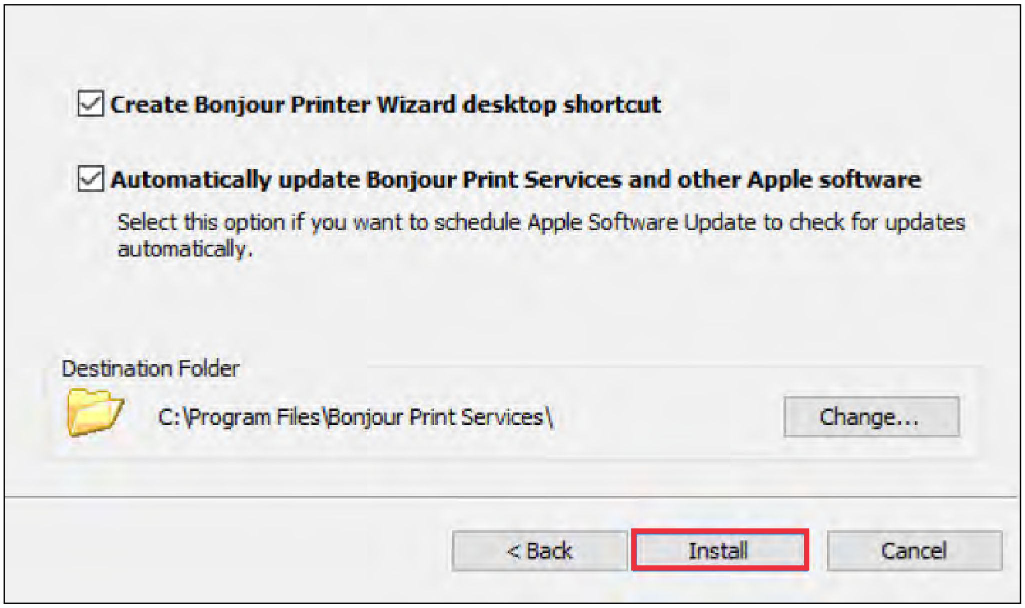
Bonjour Print Services for Windows lets you discover and configure Bonjour-enabled printers from your Windows computer using the Bonjour Printer Wizard.

System requirements

Bonjour Print Services supports Windows XP Service Pack 2 or later, but we strongly recommend either:

e 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 30 Bonjour Installation Options



☑ **Create Bonjour Printer Wizard desktop shortcut**

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

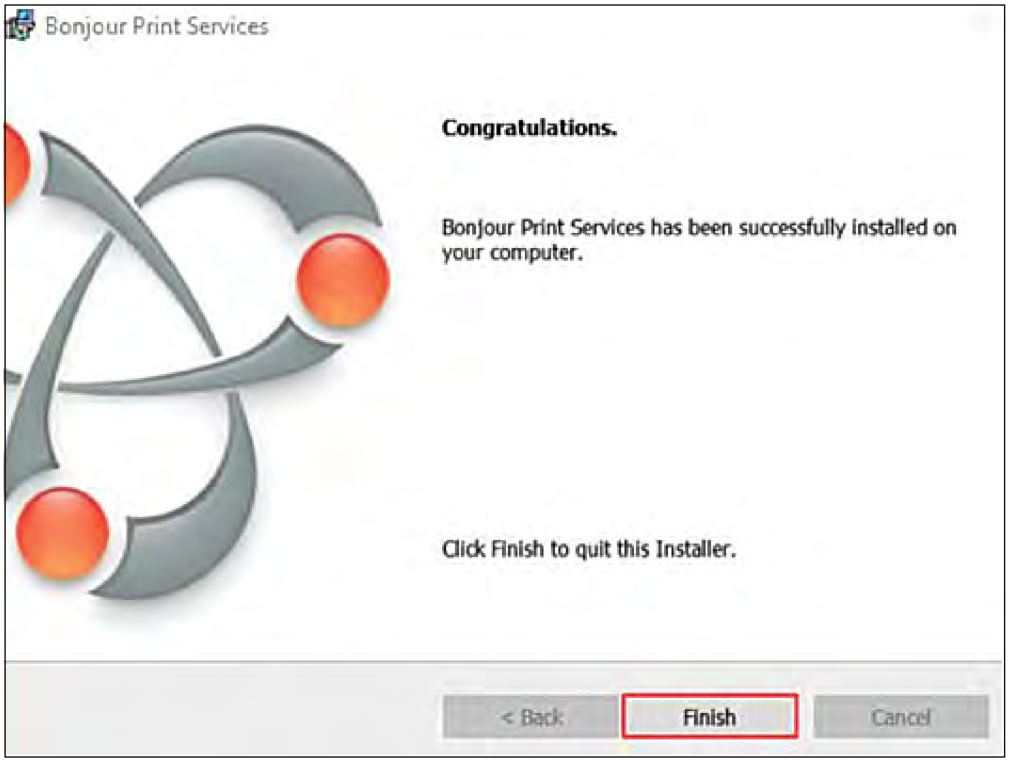
Select this option if you want to schedule Apple Software Update to check for updates automatically.

Destination Folder

C:\Program Files\Bonjour Print Services\

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

Figure 31 Bonjour Print Services Installation Complete



Congratulations.

Bonjour Print Services has been successfully installed on your computer.

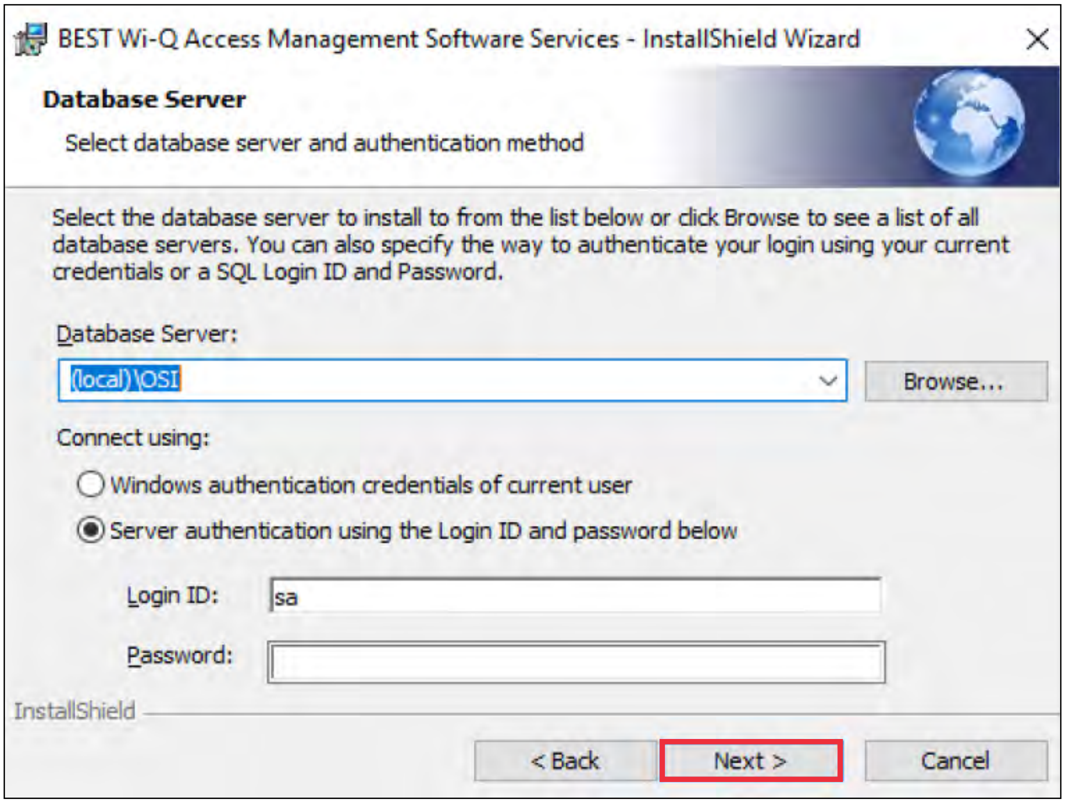
Click Finish to quit this Installer.

3 Click on AMS Services to install the Wi-Q/Omnilock Windows Service and create a database.

4 Click Next to continue past the Welcome page.

5 On the Database Server dialog box, browse to your database server and select your connection method. In the Connect Using section, choose your connection method. If you choose Server authentication, provide the Login ID and Password for the server. See Figure 32.

Figure 32 InstallShield Wizard Database Server



BEST Wi-Q Access Management Software Services - InstallShield Wizard

Database Server

Select database server and authentication method

Select the database server to install to from the list below or click Browse to see a list of all database servers. You can also specify the way to authenticate your login using your current credentials or a SQL Login ID and Password.

Database Server: (local)\OSI

Connect using:

○ Windows authentication credentials of current user

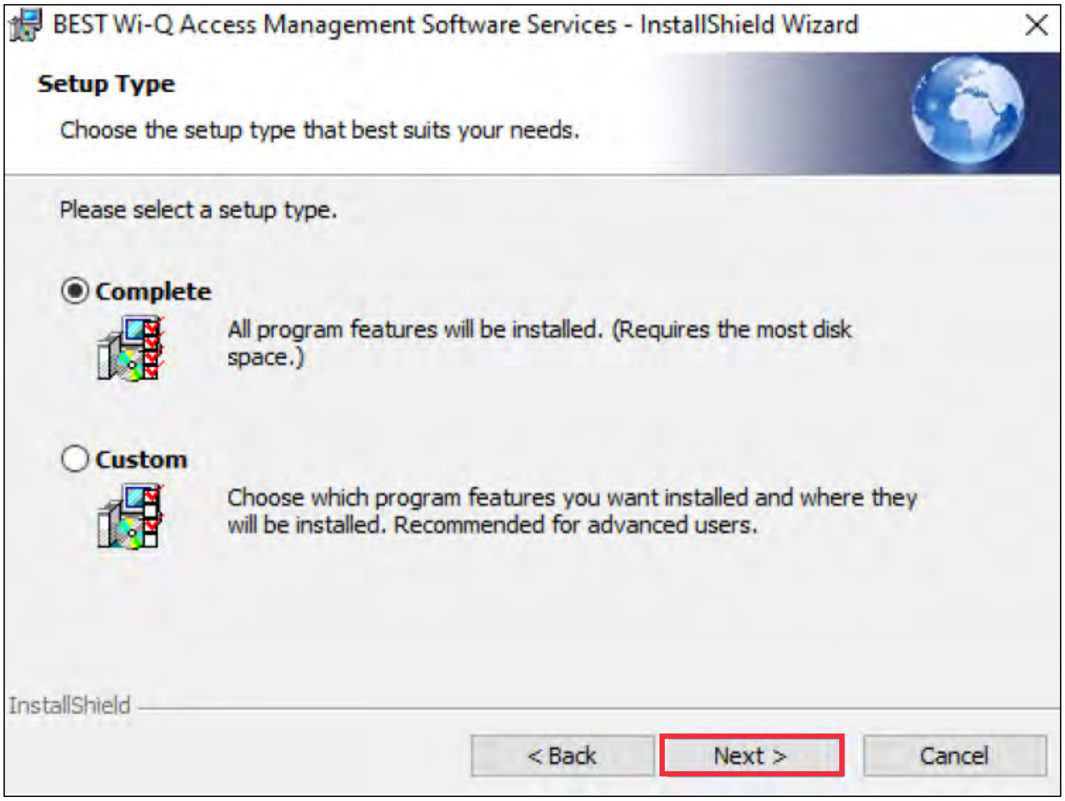
● Server authentication using the Login ID and password below

Login ID: sa

Password:

6 In the Setup Type dialog box (Figure 33), select a Complete or Custom install. Selecting Complete will run installations for the Database, Communication Service, Portal Config App, and Wi-Q/Omnilock Service. Selecting Custom will allow you to choose which components to install. Once you've made your selection, press Next to continue.

Figure 33 Setup Type



BEST Wi-Q Access Management Software Services - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Complete**

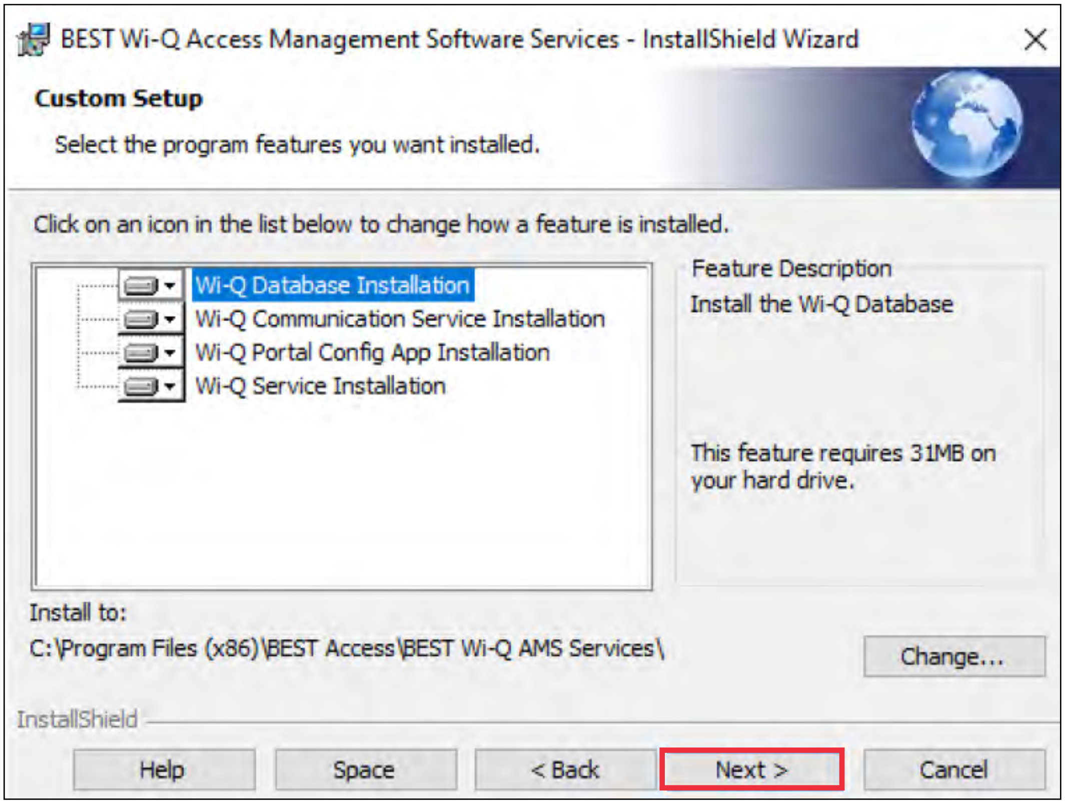
All program features will be installed. (Requires the most disk space.)

○ **Custom**

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

Figure 34 shows the installation components available in a Custom Setup.

Figure 34 Custom Setup



BEST Wi-Q Access Management Software Services - 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.

- Wi-Q Database Installation
- Wi-Q Communication Service Installation
- Wi-Q Portal Config App Installation
- Wi-Q Service Installation

Feature Description

Install the Wi-Q Database

This feature requires 31MB on your hard drive.

Install to:

C:\Program Files (x86)\BEST Access\BEST Wi-Q AMS Services\

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

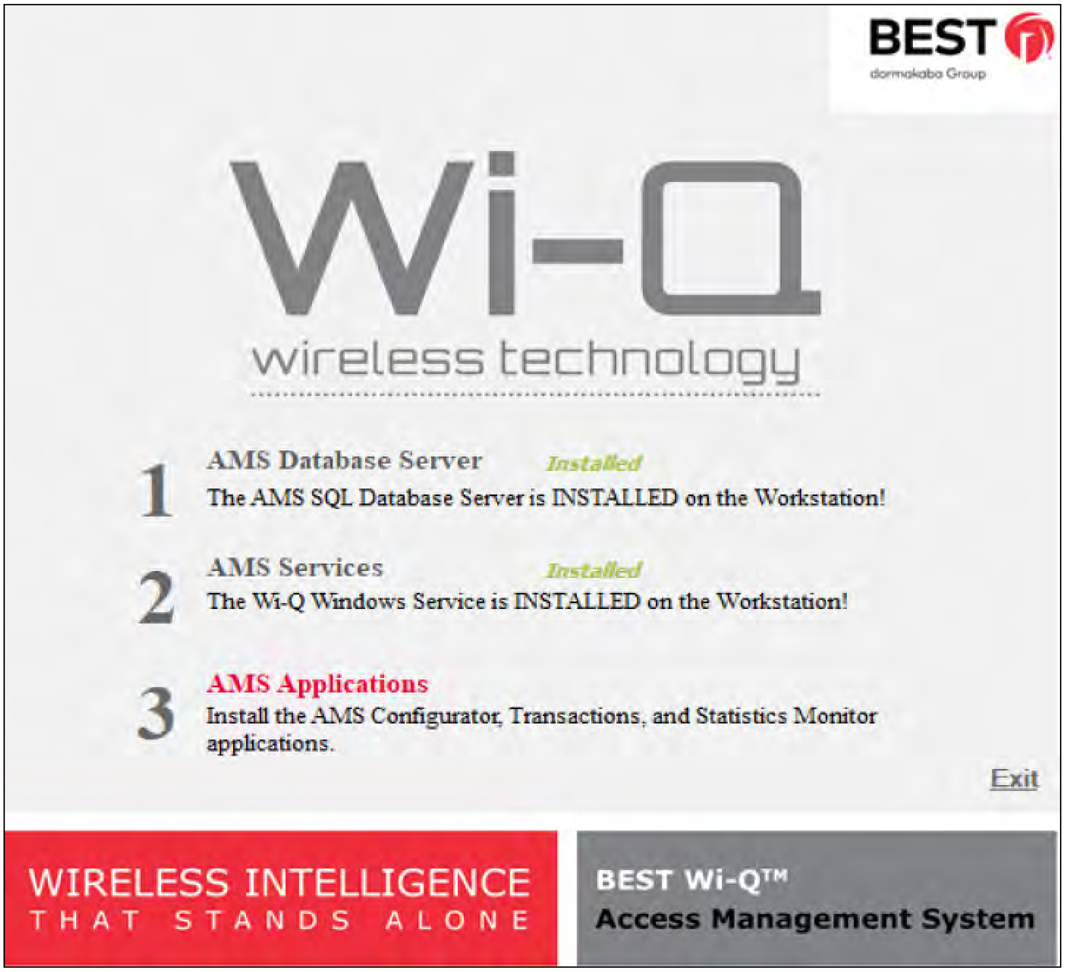
7 The wizard is now ready to begin the installation. Click Install.

8 Once the installation is complete, click Finish.

Step 3

1 On the Setup main page, click the AMS Applications link.

Figure 35 Install AMS Applications



1 AMS Database Server *Installed*
The AMS SQL Database Server is INSTALLED on the Workstation!

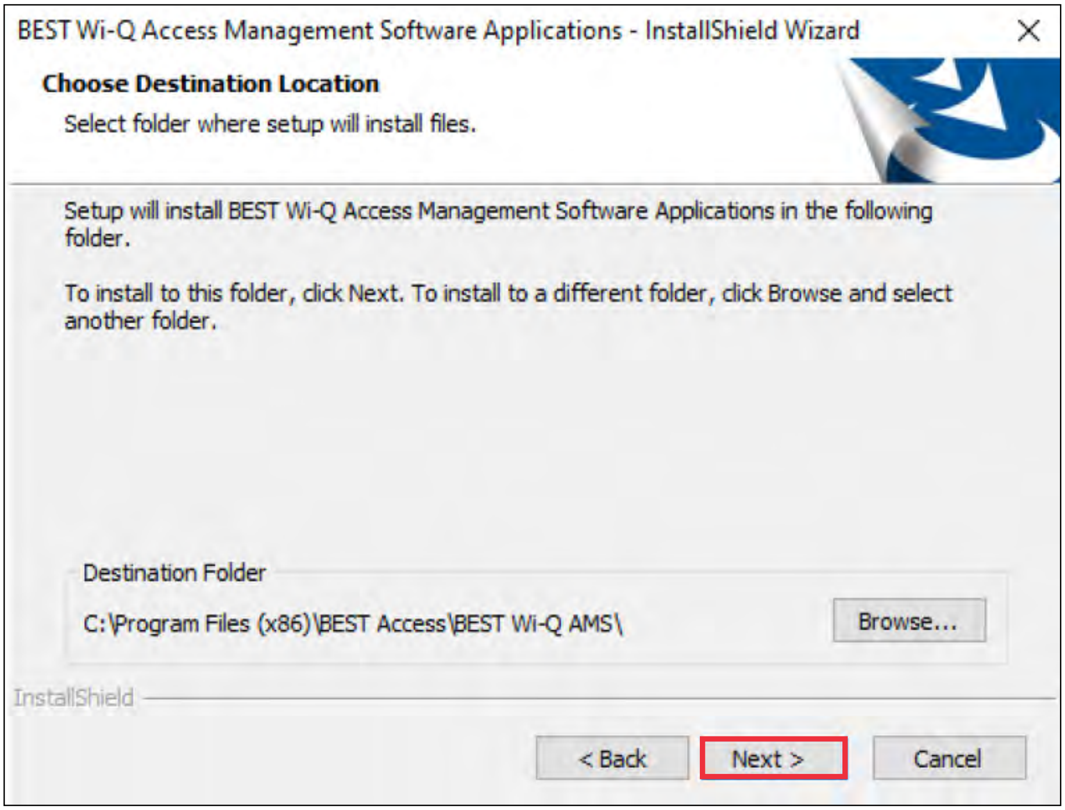
2 AMS Services *Installed*
The Wi-Q Windows Service is INSTALLED on the Workstation!

3 AMS Applications
Install the AMS Configurator, Transactions, and Statistics Monitor applications.

2 On the InstallShield Wizard Welcome screen, click Next to continue.

3 On the Destination Folder screen, click Change if you would like to change the install folder location and browse to the desired location. Then, click Next.

Figure 36 Destination Folder



BEST Wi-Q Access Management Software Applications - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install BEST Wi-Q Access Management Software Applications in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

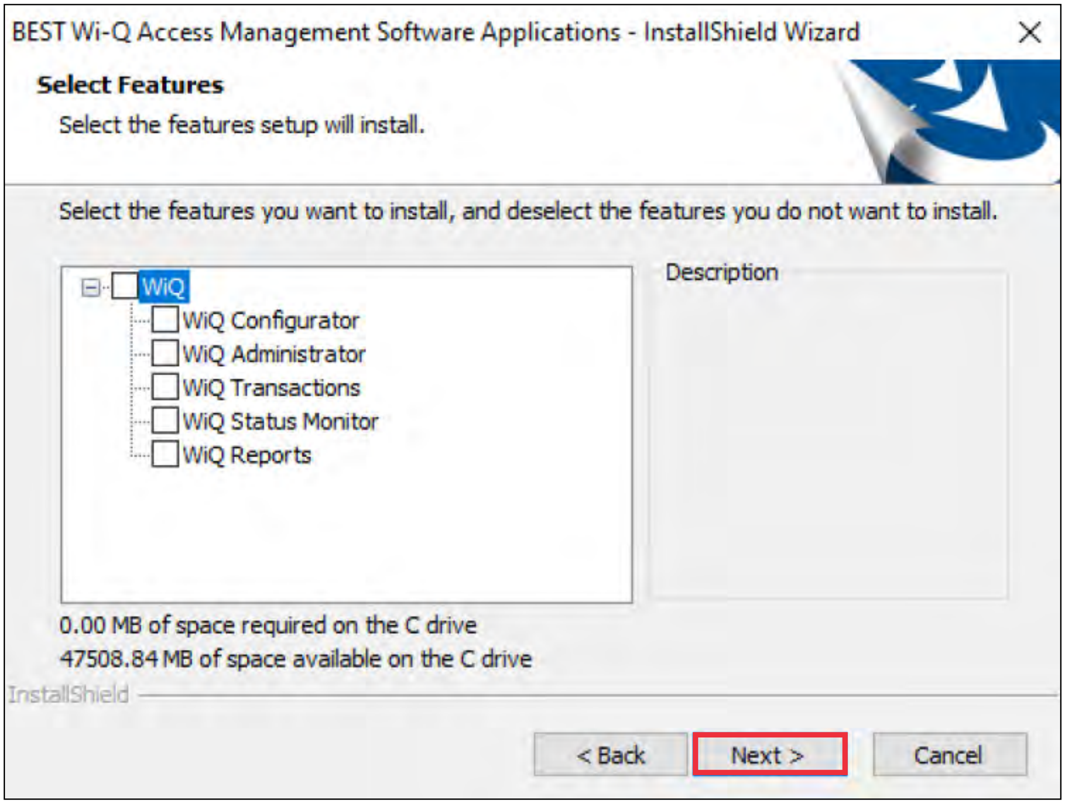
Destination Folder

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

4 In the Setup Type dialog box, select a Complete or Custom install. Selecting Complete will run installations for the Configurator, Transactions, Administrator, Status Monitor and Reports applications. Selecting Custom will allow you to choose which components to install. Once you've made your selection, press Next to continue.

Figure 37 shows the installation components available in a Custom Setup.

Figure 37 Custom Setup



BEST Wi-Q Access Management Software Applications - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

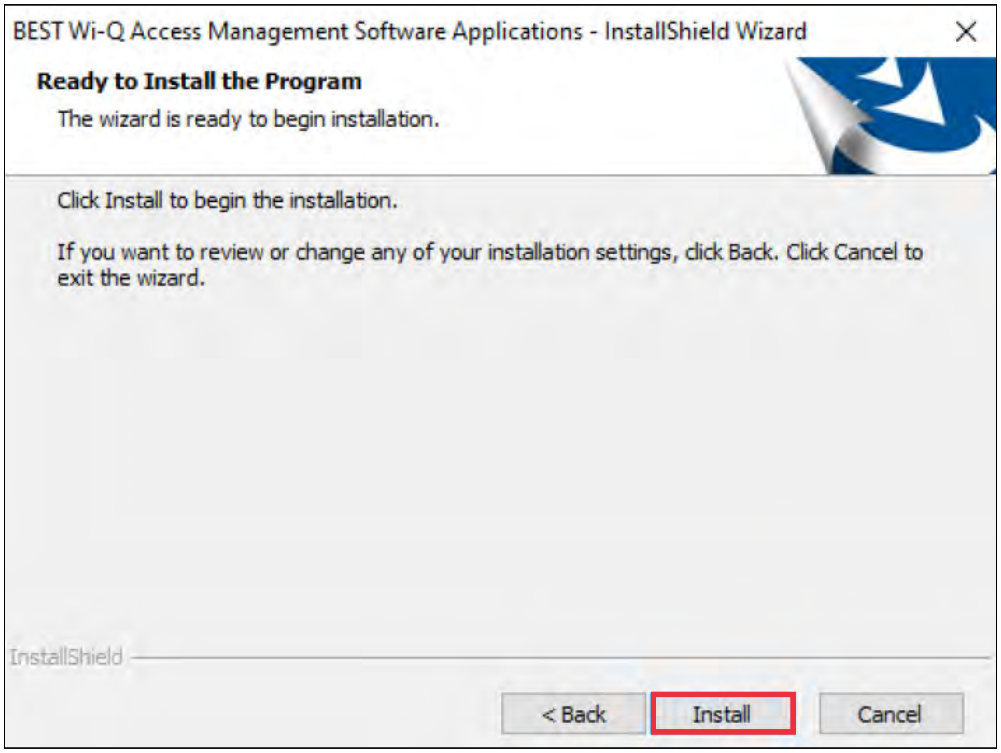
- □ WiQ
  - □ WiQ Configurator
  - □ WiQ Administrator
  - □ WiQ Transactions
  - □ WiQ Status Monitor
  - □ WiQ Reports

Description

0.00 MB of space required on the C drive
47508.84 MB of space available on the C drive

Checking the boxes to the left of each component will bring up installation options. If you decide on a Custom Setup, you must select an installation option for each component. Then click Next to continue.

Figure 38 Ready to Install



BEST Wi-Q Access Management Software Applications - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

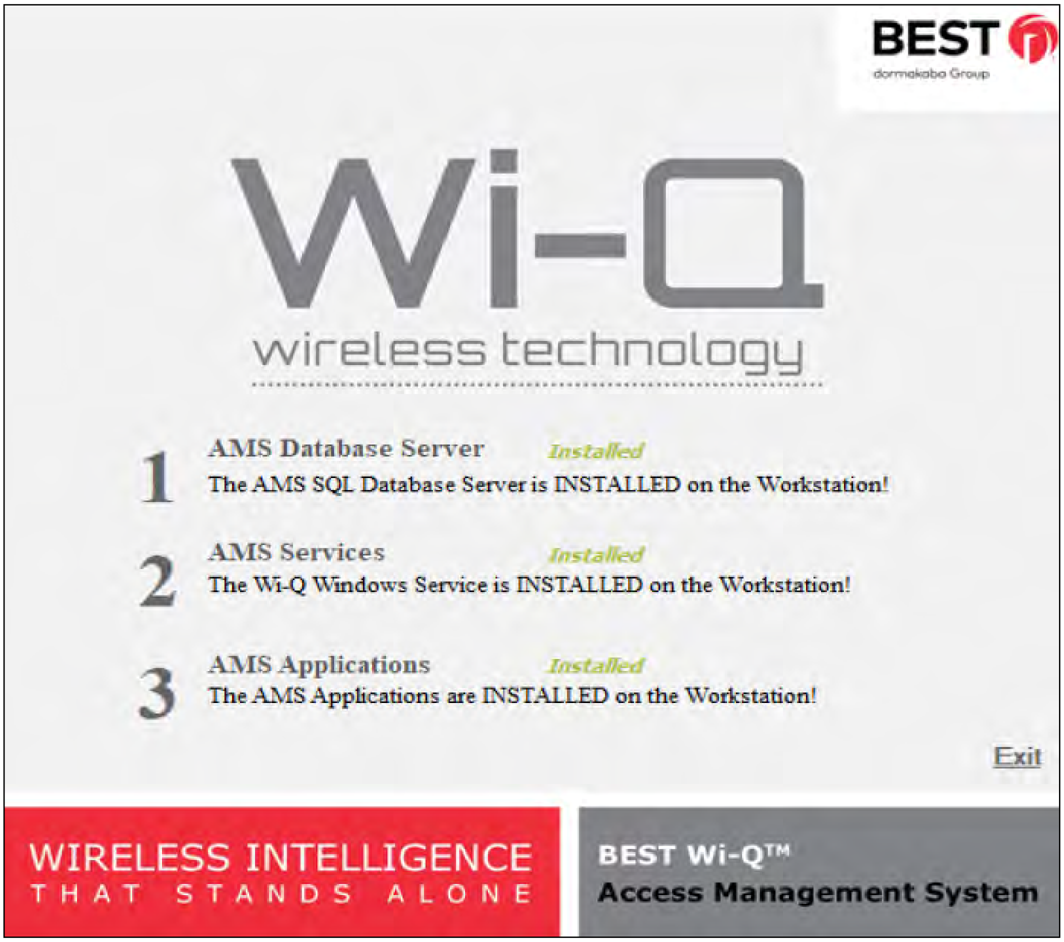
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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

6 Once the installation is complete, click Finish.

The installation of all three components is now complete.

Figure 39 Successful System Setup



1 AMS Database Server *Installed*
The AMS SQL Database Server is INSTALLED on the Workstation!

2 AMS Services *Installed*
The Wi-Q Windows Service is INSTALLED on the Workstation!

3 AMS Applications *Installed*
The AMS Applications are INSTALLED on the Workstation!

Click Exit on the Setup window. Wi-Q AMS will be accessible through your Start Menu.

Note It is recommended that you reboot your machine after installation is complete. If you chose a non-standard database server location in Step 1, you must reboot your machine now.

4 Configuring Segments, Wi-Q Gateways and Controllers

This chapter contains detailed steps to perform the following tasks:

- Task 6: Create your Segment
- Task 7: Add and Configure Wi-Q Gateways
- Task 10: Sign on and Configure Controllers

After segment creation, this chapter discusses Wi-Q Gateway and Controller configuration. However, it is perfectly acceptable to add Users, User Groups and any special Timezones you will need before configuring Wi-Q Gateways and Controllers. An advantage to adding Users and User Groups before you add Wi-Q Gateways and Controllers is that they will be available as you configure each new Wi-Q Gateway and Controller in the system. You can also add Wi-Q Gateways, Controllers, users, and user groups as you go, building the system in any way that makes it efficient with the data that you have available.

Note The terms “Controller” and “Reader” are used synonymously throughout this chapter.

Create Your Segment (Task 6)

It is important to give some thought to how you will go about configuring a segment in Wi-Q AMS.

Logging in to Configurator

To get started, open your Configurator module. You can access it via the icon on your desktop or from the Windows Start Menu (Programs>BEST Access).

The Wi-Q AMS splash screen appears briefly, then the Login dialog box opens.

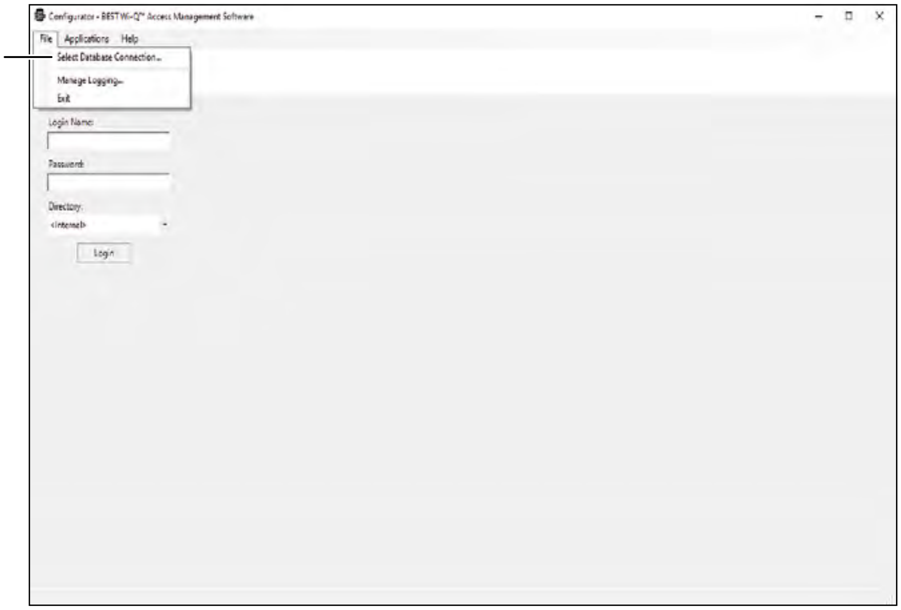
Selecting the Database Connection

When you start up Wi-Q AMS, the system defaults to the database installed on the Host computer. If for some reason your database resides on a computer other than the one running AMS, you must select the database before you login.

To select a database on a different computer

1 From the File menu, select Select database connection from the drop-down list.

Figure 40 Select Database Connection

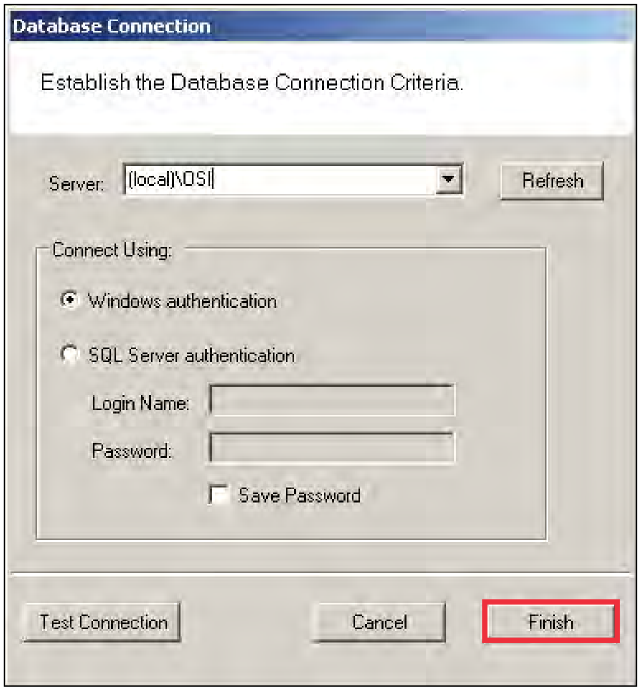

Configurator - BEST Wi-Q™ Access Management Software
File
Applications
Help
Select Database Connection...
Manage Logging...
Exit
Login Name:
Password:
Login

Directory: <Internal>

Click on Select Database Connection

The Database Connection dialog box opens.
See Figure 41.

Figure 41 Database Connection Window



Database Connection

Establish the Database Connection Criteria.

Server: (local)\OSI

Connect Using:

● Windows authentication

○ SQL Server authentication

Login Name:

Password:

□ Save Password

2 In the Server field, select the server location from the drop-down list.

3 Under Connect Using, select either Windows authentication or SQL Server authentication. If you select SQL Server, enter the login name and password for that server.

4 Click Test Connection.

5 Click Finish. You are ready to login to AMS using your desired database.

Login Information

When you enter the system for the first time, the default, case-sensitive, User Name and Password are:

Login: Admin

Password: Admin

1 Enter the Login Name and Password.

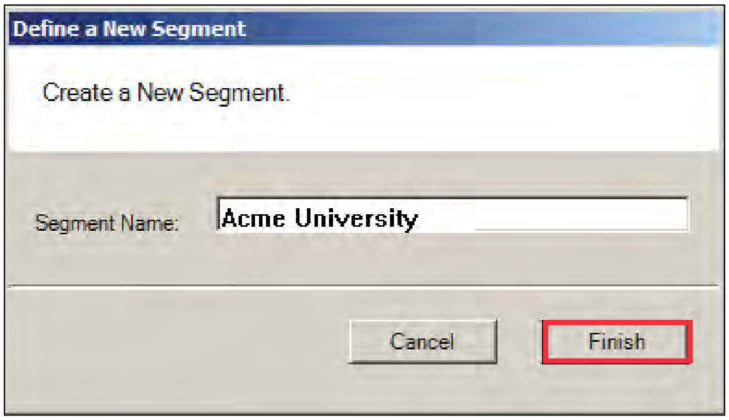
2 Select Login. You are ready to start setting up your new segment.

When you select Login, the Define a New Segment dialog box opens.

Define a New Segment

1 In the Segment Name box, enter a unique name for your segment.

Figure 42 Define a New Segment



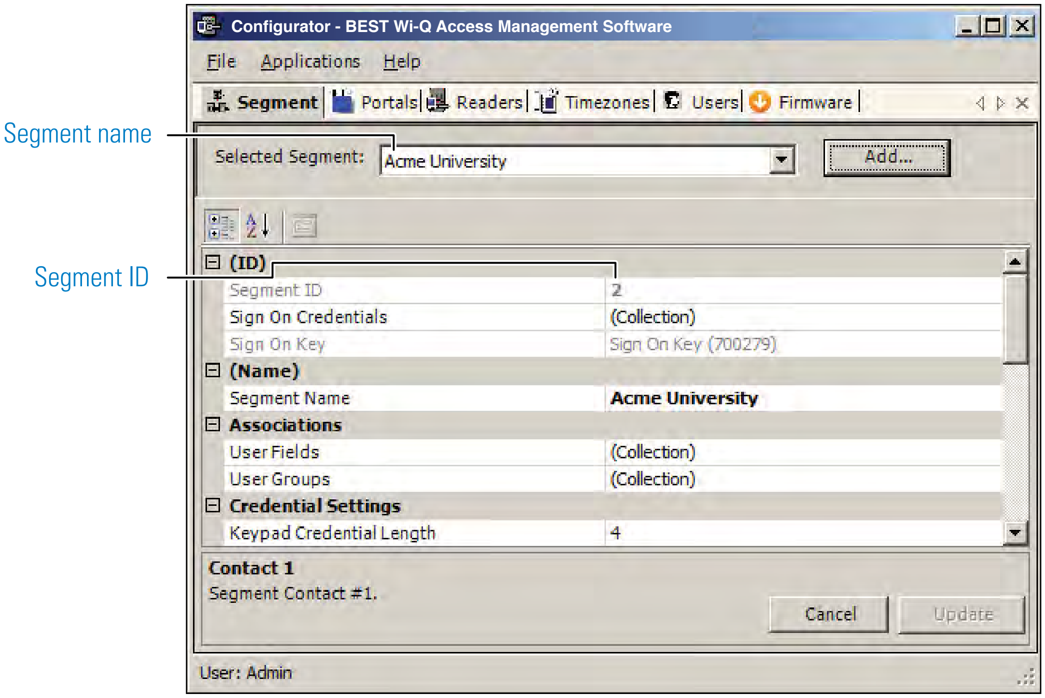
Define a New Segment

Create a New Segment.

Segment Name: Acme University

2 Select Finish. The Configurator dialog box opens on the Segment Tab. The new segment name appears in the Selected Segment box and AMS assigns it a unique Segment ID.

Figure 43 Identifying the Segment name and ID



Segment name

Segment ID

Configurator - BEST Wi-Q Access Management Software

Selected Segment: Acme University

(ID)	
Segment ID	2
Sign On Credentials	(Collection)
Sign On Key	Sign On Key (700279)
(Name)	
Segment Name	**Acme University**
Associations	
User Fields	(Collection)
User Groups	(Collection)
Credential Settings	
Keypad Credential Length	4

Contact 1
Segment Contact #1.

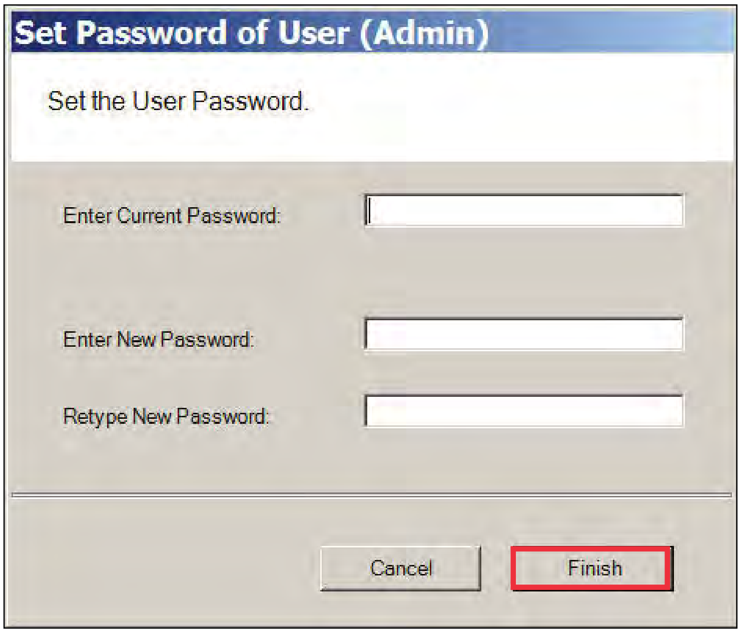
User: Admin

Note Once you have successfully logged in, it is recommended that you change the default User Name and Password to ensure system security.

To change the Password

1 At the top left corner of the Configurator dialog box, select File>Change Password. The Set Password of User dialog box opens.

Figure 44 Set Password of User



Set Password of User (Admin)

Set the User Password.

2 Enter the new password

3 Retype the new password.

4 Select Finish.

WARNING: Be sure to keep a record of your new password in a locked safe that is available to your senior management team!

Add and Configure Wi-Q Gateways (Task 7)

Wi-Q Gateways can now be added and configured within the software. Wi-Q Gateways are configured from the factory with a LAN IP address of 192.168.1.200. When configuring a Wi-Q Gateway, it is best to connect directly to the Portal before placing it on the network. This removes the possibility of duplicate IP addresses on the network.

You can change the IP address of your Wi-Q Gateways with the Portal Configuration Module.

Note All Wi-Q Gateway IP address must be unique across the entire system.

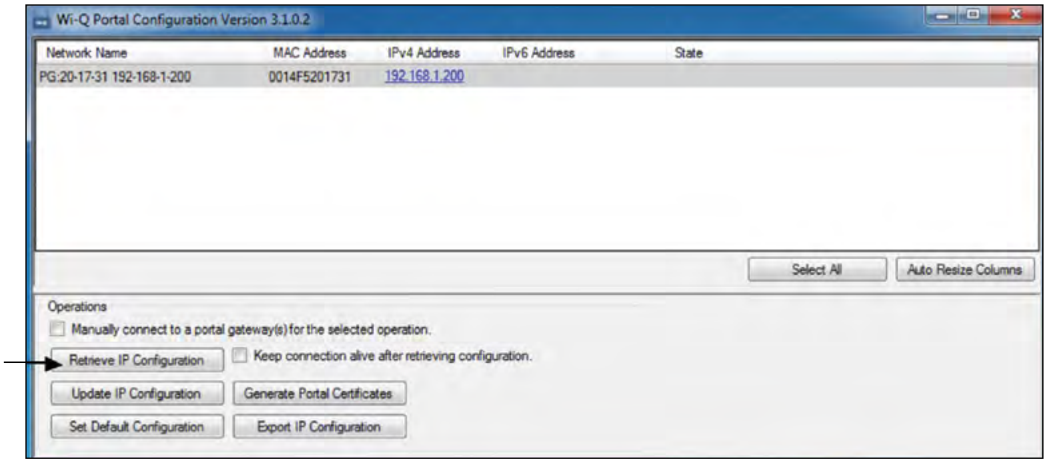
Configuring a Wi-Q Gateway with the Portal Configuration Module

Perform the following steps to change your Wi-Q Gateway's IP address.

1. Connect the Wi-Q Gateway to the Host either over the network or directly via crossover Ethernet cable (recommended). For more information on connecting a Wi-Q Gateway, see "Connecting the Wi-Q Gateway and Verifying Operation" on page 25.
2. Open the Portal Configuration module (Start>Best Access>Wi-Q Portal Config Tool).
3. Wi-Q Gateways available on the network will automatically be listed in the Portal Configuration module.

Note This tool is password protected and must run as administrator. The password expires every 3 months and requires 8 characters, 1 capital letter, 1 special character, and a number.

Figure 45 Wi-Q Gateways Available on the Network



Wi-Q Portal Configuration Version 3.1.0.2

Network Name	MAC Address	IPv4 Address	IPv6 Address	State
PG:20-17-31 192-168-1-200	0014F5201731	192.168.1.200		

Operations

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

□ Keep connection alive after retrieving configuration.

Select All
Auto Resize Columns
Retrieve IP Configuration
Update IP Configuration
Generate Portal Certificates
Set Default Configuration
Export IP Configuration

4 Select a Wi-Q Gateway from the list.

5 At this point, you may change the IP address from the factory setting to one from the range you've created. Click on Update IP Configuration to update the selected Wi-Q Gateway.

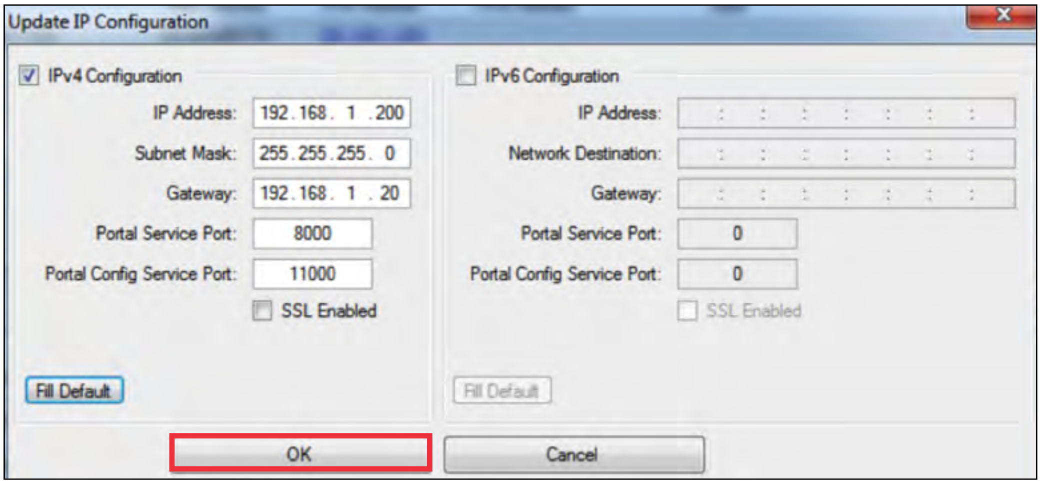
6 Select IPv4 and/or IPv6 and enter the IP address.

7 You may need to adjust the SubNet Mask/Network Destination and Gateway to match your network. Consult your network administrator for details.

8 If you wish to generate a SSL certificate for a more secure connection, click on the SSL Enabled checkbox, then click OK.

Note If you enable SSL, you must create a certificate and load the certificate into your system.

Figure 46 Update IP Configuration



Update IP Configuration

☑ IPv4 Configuration

IP Address: 192 . 168 . 1 . 200
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 192 . 168 . 1 . 20
Portal Service Port: 8000
Portal Config Service Port: 11000
☐ SSL Enabled

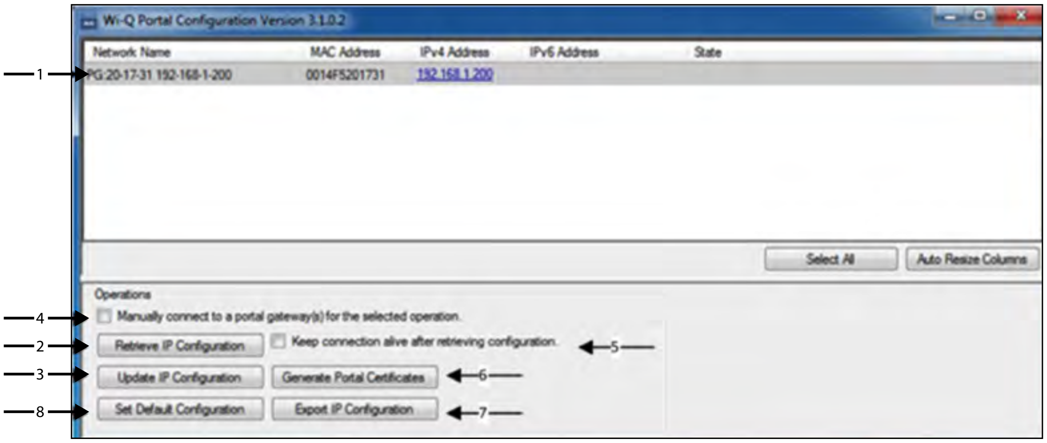
☐ IPv6 Configuration

IP Address:
Network Destination:
Gateway:
Portal Service Port: 0
Portal Config Service Port: 0
☐ SSL Enabled

Wi-Q Gateway Configuration Features and Functions

Review this section for additional information regarding the Wi-Q Gateway Configuration window. See Figure 47.

Figure 47 Wi-Q Gateway Configuration Window



Wi-Q Portal Configuration Version 3.1.0.2

Network Name	MAC Address	IPv4 Address	IPv6 Address	State
PG-20-17-31 192-168-1-200	0014F5201731	192.168.1.200		

Operations

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

□ Keep connection alive after retrieving configuration.

1 **Portals on the Network Grid**
Provides a list of Wi-Q Gateways on the network. It shows the status of the last operation performed, the portal network name, a hyperlink that opens the corresponding status page, portal MAC address, and portal IP configuration data.

2. **Retrieve IP Configuration**
When checked, attempts to retrieve the current IP Configuration for the corresponding portal. This requires direct communication with the portal configuration service, which only runs for one hour after a reboot. If the service is not running, the IP Configuration data will return unknown data.

3. **Update IP Configuration**
Updates the IP Configuration of the selected portal. This requires direct communication with the portal configuration service. The “New Portal IP Configuration” fields are used for the new IP Configuration data.

Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

4. **Manual Connection**
   When checked, allows a portal to be configured by IP address. Some networks do not allow port 5353 to be open, which is required by the application when scanning for portals. This allows manual connection to the portal so the portal can be configured. You must click on Update IP Configuration after selecting this box.

Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

5. **Keep Connection Alive Checkbox**
   Allows the connection with the portal to continue, otherwise, a reboot will occur after the action selected.

6. **Generate Portal Certificates**
   Generates a portal certificate that is sent to the portal and stored to the file system. Enable this box when data encryption is required. Multiple portals can be selected when generating certificates.

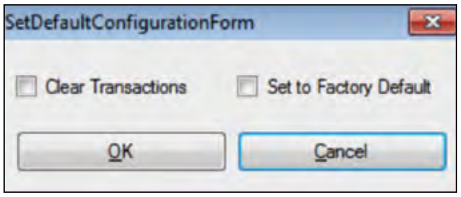
Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

7. **Export Portal IP Configuration**
   Exports the portal IP configuration for the selected portals.

Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

8. **Set Default Configuration**

Figure 48 Set Default Configuration



SetDefaultConfigurationForm

□ Clear Transactions □ Set to Factory Default

9. **Clear Transactions**
   When checked, allows you to clear all transactions from portals you select in the list above. This may be selected in combination with the Set Back to Factory Default checkbox.

Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

10. **Set Back to Factory Default**
    When checked, allows you to set change the IP address(es) of the portal(s) you select in the list above back to factory default (192.168.1.200). This may be selected in combination with the Clear Transactions checkbox.

Once you've configured your Wi-Q Gateways with the Portal Configuration module, you can add them into your Wi-Q AMS Software.

Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

Configure Gateways

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

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

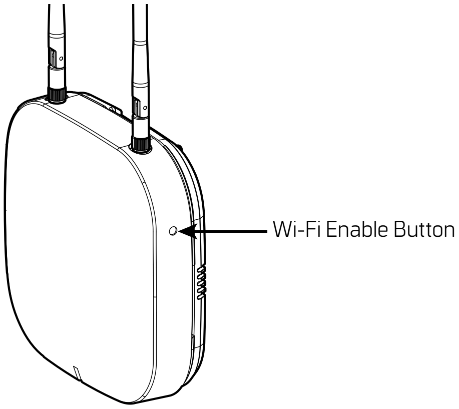
For example: Use 192.168.2.100, where 2 instead of 3 is used in the address's 3rd octet, when assigning an IP address to the Ethernet adapter on the Gateway if a Class C IPv4 network is in use.

Access the Gateway's Wireless Network

The WQXM-PG Gateway is equipped with a wireless network used to access the Gateway and configure it. The portal default IP address on this network is 192.168.1.200. To temporarily enable the portal's wireless network for configuration, do the following:

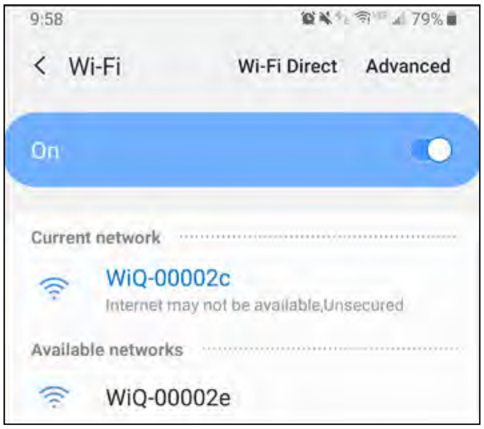
- Push the Wi-Fi enable button on the side of the WQXM-PG Wi-Q Gateway. See figure 49.

Figure 49 Wi-Fi Enable Button



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

Figure 50 Wi-Fi Networks



Current network

WiQ-00002c

Internet may not be available,Unsecured

Available networks

WiQ-00002e

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

Example ---> Mac address of new Gateway: 0014F500002E

Wi-Fi SSID to use: WiQ-00002E

Click on the network for the portal that is to be configured.

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

1 Press Wi-Fi button on the side of the Wi-Q Gateway.

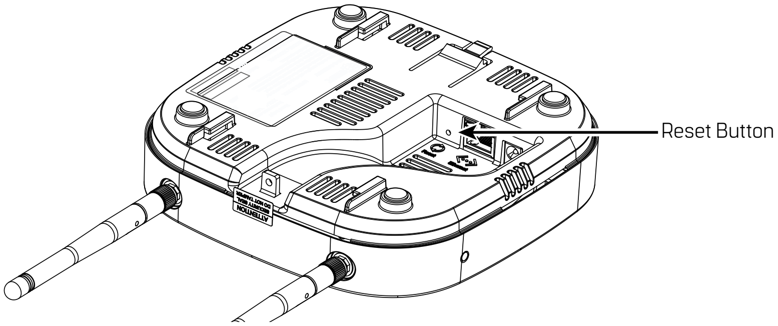
2 Reconnect to the Gateway's unique wireless network connection.

3 Try to log in again.
The Wi-Fi SSID Password = password for first time login and will be updated each time the user login password for the gateway web UI is updated.

4 Power cycle the Gateway and attempt to log in again once it is powered back up.

5 If the power cycle is not successful and connection to the to the Gateway's webpage is still inaccessible, then perform a "Deep-Reset" by taking a pin and depressing the reset button on the Gateway for 10+ seconds at which time the LED will begin to flicker purple. See figure 51.

Figure 51 Wi-Fi Reset Button



6 A purple light will flash confirming the deep reset.

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

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

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

Configure the WQXM-PG Gateway

Open the device's browser window and navigate to the Gateway's web UI pages.

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

Login Screen

Log in to the Gateway.

- The default Username is admin.
- The default Password is password.

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

Manage Profile

The first time a Gateway is logged in to, the manage profile screen will appear prompting to change the Username or Password. The user will be prompted to change the Password every time the Gateway is logged in to until it has been changed to something other than the default. To update the Username and Password after the initial configuration, click on the Username link in the upper right corner of the screen. In the following image, it is labeled:

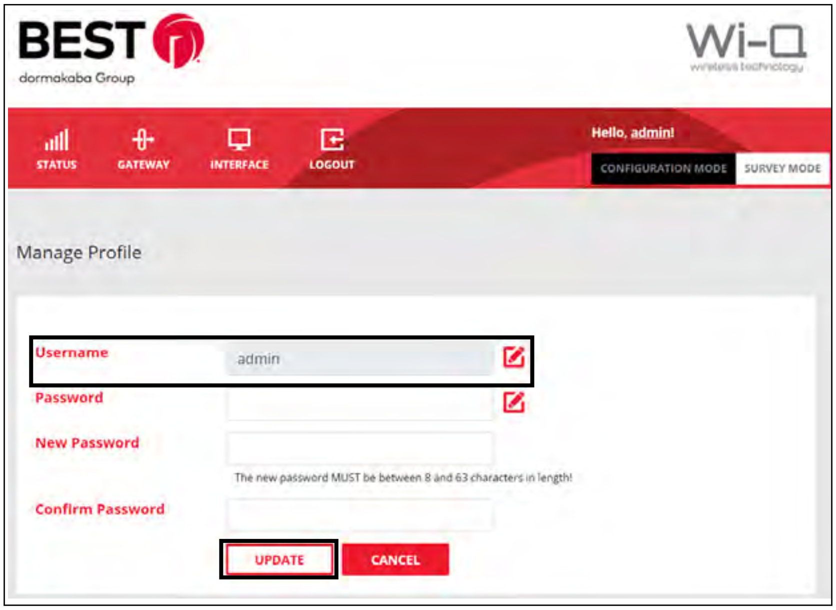
Hello, admin!

Change the Default Username.

1. Click on the Edit icon next to the Username field.
2. Enter the new Username into the New Username and Confirm Username fields.
3. Click the Update button to save the changes.
4. Click on the Update button to confirm the changes in the pop-up notification.
5. Click the Close button to close the pop-up notification.

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

Figure 52 Manage Profile



Manage Profile

Username: admin

Password:

New Password:

The new password MUST be between 8 and 63 characters in length!

Confirm Password:

Change the Default Password.

1 Click on the Edit icon to the right of the Password field.

2 Enter the current Password in the Password field.

3 Enter the new Password in the New Password field.

4 Enter the new Password again in the Confirm Password field.

5 Click the Update button to save the changes.

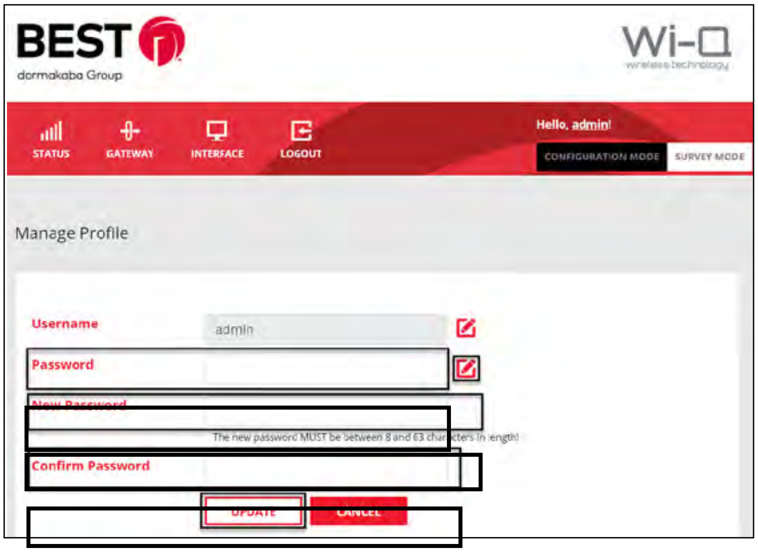
6 Click the Update button in the pop-up notification window to confirm the changes.

7 Click the Close button to close the notification window.

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

Once changes are updated, a pop-up window appears with the status of the changes being made. Click the Close button to close the pop-up window.

Figure 53 Manage Profile



Manage Profile

Username admin

Password

New Password

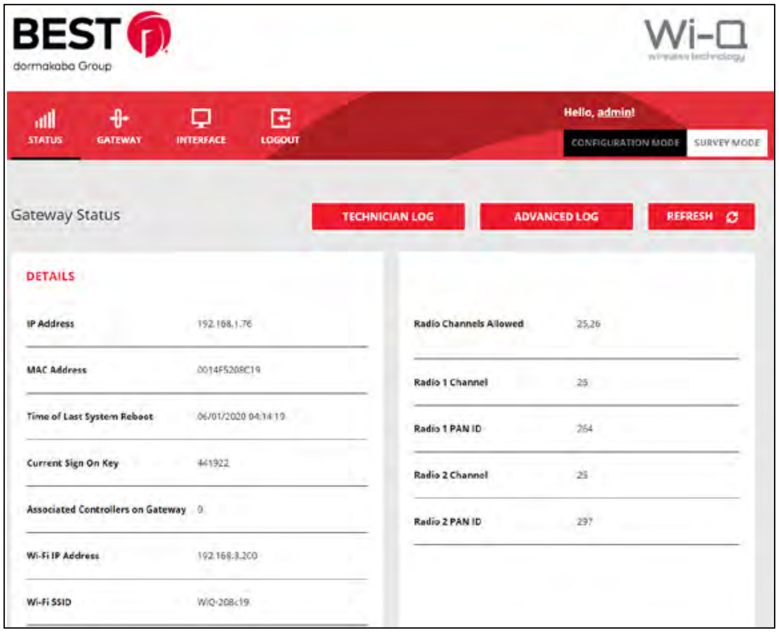
The new password MUST be between 8 and 63 characters in length!

Confirm Password

Gateway Status Window

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

Figure 54 Gateway Status



Gateway Status

DETAILS

IP Address	192.168.1.76
MAC Address	0014F5208C19
Time of Last System Reboot	06/01/2020 04:14:19
Current Sign On Key	441922
Associated Controllers on Gateway	0
Wi-Fi IP Address	192.168.3.200
Wi-Fi SSID	WiQ-208c19

Radio Channels Allowed	25,26
Radio 1 Channel	25
Radio 1 PAN ID	264
Radio 2 Channel	25
Radio 2 PAN ID	297

Details

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

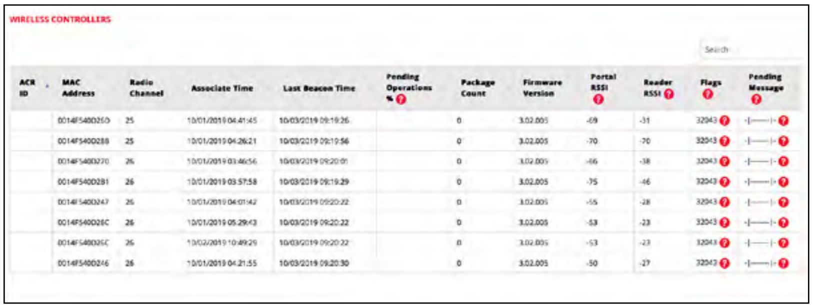
Note: Radio 1 PAN ID can be edited when in Mercury Mode. PAN IDs only need to be changed if there is a conflict with multiple Gateways within RF range of each other. Editing Radio 1 PAN ID will also change Radio 2 PAN ID. Each Gateway uses up to 66 PAN IDs.

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

Wireless Controllers

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

Figure 55 Associated 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 ?
	0014F540D250	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 ?	-|——|- ?
	0014F540D25C	26	10/02/2019 10:49:29	10/03/2019 09:20:22		0	3.02.005	-53	-23	32043 ?	-|——|- ?
	0014F540D246	26	10/01/2019 04:21:55	10/03/2019 09:20:30		0	3.02.005	-50	-27	32043 ?	-|——|- ?

- **ACR ID** – The Reader ID when the portal is in Mercury Mode with the LP4502 Access Control Board. This field will be blank when Mercury Mode is not in use.
- **MAC Address** – The Reader's unique Media Access Control address that uniquely addresses the device on the network.
- **Radio Channel** – The channel the door controller is communicating on with the Gateway.
- **Associate Time** – The date and time the Wi-Q Door Controller associated with the Gateway.
- **Last Beacon Time** – The last date and time the Wi-Q Door Controller beaconed information up to the Gateway.
- **Pending Operations** – Progress percentage of pending messages from the door controller to the Gateway.
- **Package Count** – The number of pending messages in the current queue that the Gateway has received from the Wi-Q Door Controller.
- **Firmware Version** – The current version of door controller firmware on the Wi-Q Device.
- **Portal RSSI** – Portal RSSI is the how well the Gateway received a signal from the Wi-Q Door Controller. The signal strength ranges from -18 (highest/best) to -91 (lowest/worst). Ideally, this value should be -75dB or better.
- **Reader RSSI** – Reader RSSI is the how well the Wi-Q Door Controller receives a signal from the Gateway. The signal strength ranges from -18 (highest/best) to -91 (lowest/worst). Ideally, this should be -65dB or better.
- **Flags** – The Flags indicate the device status. Common device statuses for Wi-Q Controllers when they are connected to a Gateway are below:
  - 010001 – Controller initial connection to the Gateway.

- **30207** – Controller connected to the Gateway and is waiting for segment updates.
- **30063** – Controller has a deep reset command pending.
- **30017** – Controller waiting to be pulled into the segment and has not received segment updates.
- **30007** – Controller has received segment updates and is waiting in the “New Segment Items” folder in Wi-Q AMS Configuration software.
- **30043** – Controller is signed in to the ACS, connected, configured, and not locked to the Gateway.
- **30053** – Controller is taking configuration updates.
- **32043** – Controller is signed in to the ACS, connected, configured, and locked to the Gateway.
- **32243** – Controller is locked to portal but has not been added to an access level or a direct assignment to a User. No user credentials are assigned to the controller in the software.
- **38053** – Controller has a firmware update pending.
- **38043** – Controller is receiving a firmware update.
- **32207** – Controller completed the firmware update and is waiting for updates from the portal.

- Pending Messages – The letters in the pending messages column are update messages that are being sent to the controller.
  - **S** – Segment information (pin length, DST Times)
  - **C** – Card formats
  - **L** – Controller configuration (beacon time settings, channels, transaction masks, etc.)
  - **U** – User credentials and properties
  - **T** – Timezone intervals
  - **I** – WAC I/O
  - **F** – Firmware
  - **P** – Ping (missing LIF data after association or updates)

Generate Logs

Click on the Generate Logs button in the upper right corner of the Gateway status screen.

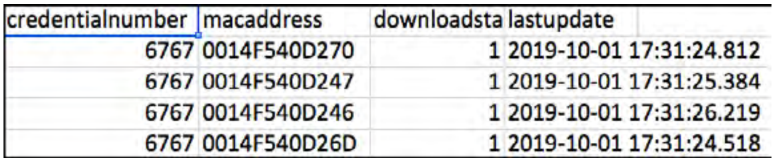
The Technician and Advanced log buttons allows the installer/technician to assist dormakaba BEST software support in troubleshooting an issue. These logs may be used by the local installer to troubleshoot or verify the credentials are all making it to the controllers or requested during a troubleshooting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

To generate logs, do the following:

Technician Log

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

The Technician Log looks like the following table.



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

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

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

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

Advanced Log

Advanced logs are used by engineering to perform advanced troubleshooting. These logs are encrypted and can only be decrypted by our engineering group. These logs may occasionally be requested by Software Technical Support during a troubleshooting session. Clicking on the Advanced Log button will download the log file to the browser's download location and should be forwarded to Technical Support via email at bas.support.best.us@

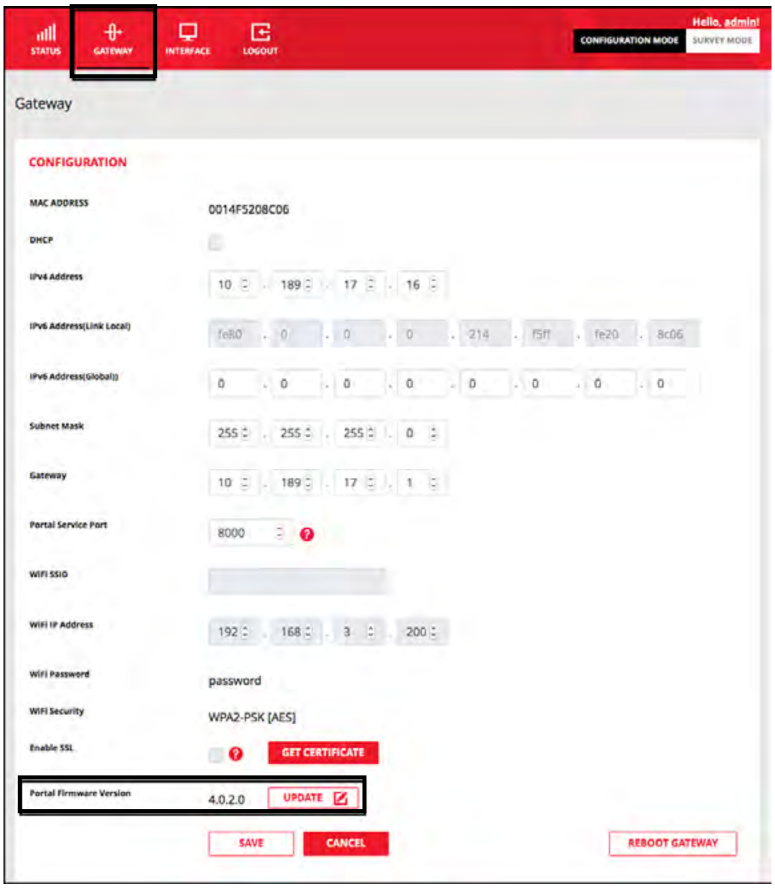
dormakaba.com. The file will be named with the following naming convention:

Portal_0014fmacaddress_201907datetime.tar.gz.enc

Gateway Menu

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

Figure 56 Gateway Configuration Page



Gateway

CONFIGURATION

MAC ADDRESS	0014F5208C06
DHCP	□
IPv4 Address	10 . 189 . 17 . 16
IPv6 Address(Link Local)	fe80 . 0 . 0 . 0 . 214 . f5ff . fe20 . 8c06
IPv6 Address(Global))	0 . 0 . 0 . 0 . 0 . 0 . 0 . 0
Subnet Mask	255 . 255 . 255 . 0
Gateway	10 . 189 . 17 . 1
Portal Service Port	8000
WiFi SSID	
WiFi IP Address	192 . 168 . 3 . 200
WiFi Password	password
WiFi Security	WPA2-PSK [AES]
Enable SSL	□
Portal Firmware Version	4.0.2.0

Assigning an IP Address

Configuration changes on the Gateway are only available via the portal's wireless network after the Enable Wi-Fi button has been pushed. The WLAN IP address for the WQXM-PG wireless network is a static 192.168.3.200 and cannot be changed. Once the LAN IP address has been updated, the Enable Wi-Fi button can be depressed for a second time to disable the Wi-Fi on the WQXM-PG. Additionally, if nothing has been connected to WQXM-PG wireless network for 30 minutes, the internal Wi-Fi network will automatically disable.

DHCP

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

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

Static IP Assignment

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

To assign a static IP address configure the following fields:

- IPv4 address or IPv6 address
- Subnet mask (for IPv4 addresses only)
- Gateway (for IPv4 addresses only)

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

Portal Service Port

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

Enabling SSL

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

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

1 Click on the Enable SSL checkbox in the Gateway configuration page.

2 Click on the Get Certificate button to download the portal's SSL certificate. This portal certificate will download to the predetermined location on the local browser.

3 Click on the Save button to save the SSL setting.

4 Locate the SSL certificate on the PC where the certificate was downloaded and upload the SSL certificate into the ACS.

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