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_L, December 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.

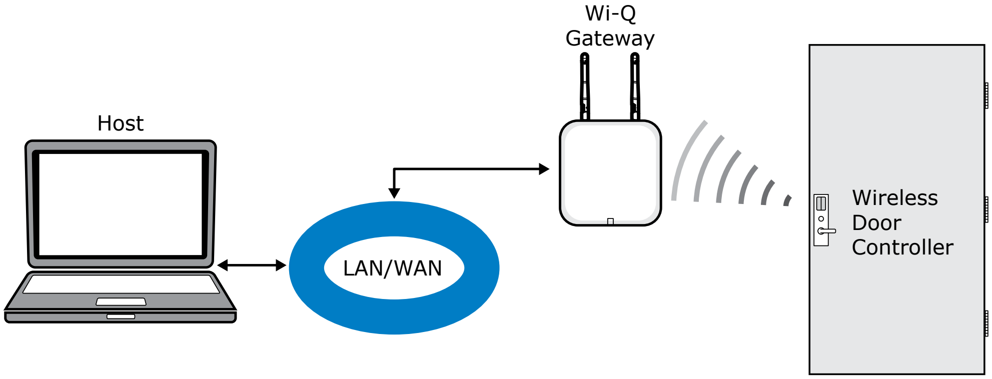
System Overview

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.

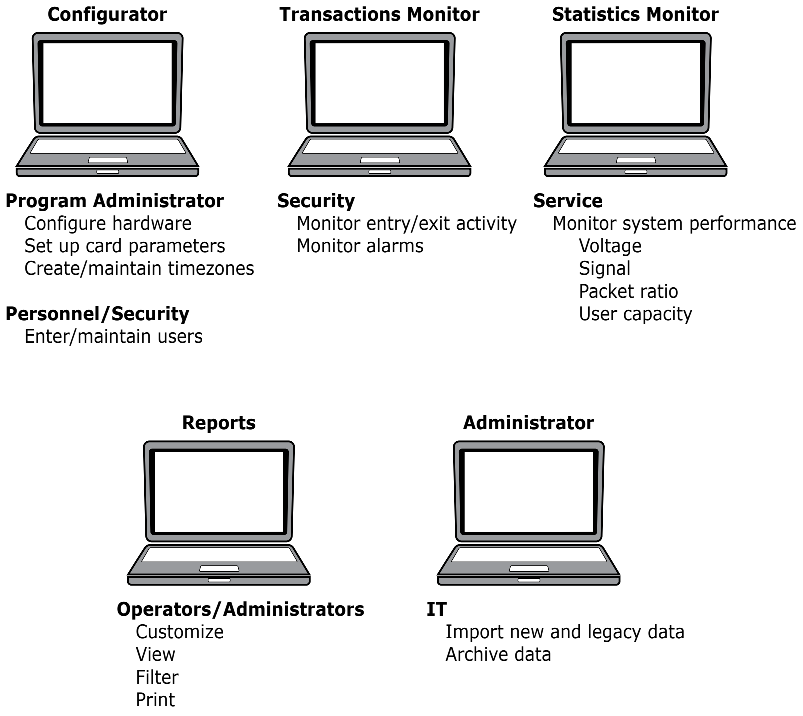
For more information about various applications, you can adapt for use with Wi-Q AMS, see "Hardware Overview" on page 13.

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

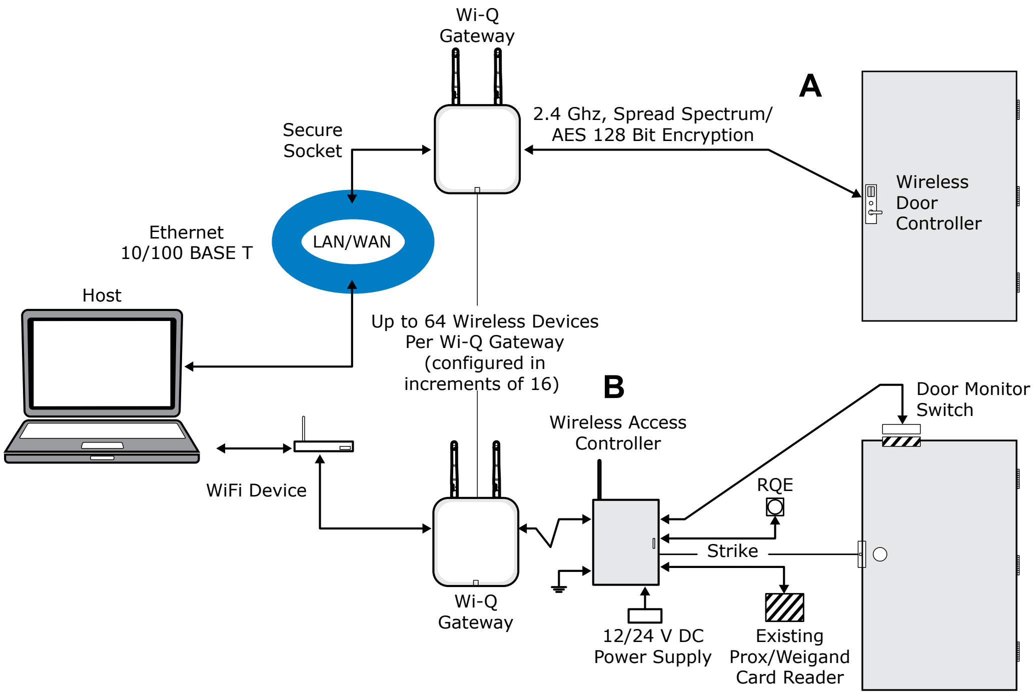
Hardware Overview

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
WiFi Device
RQE
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:

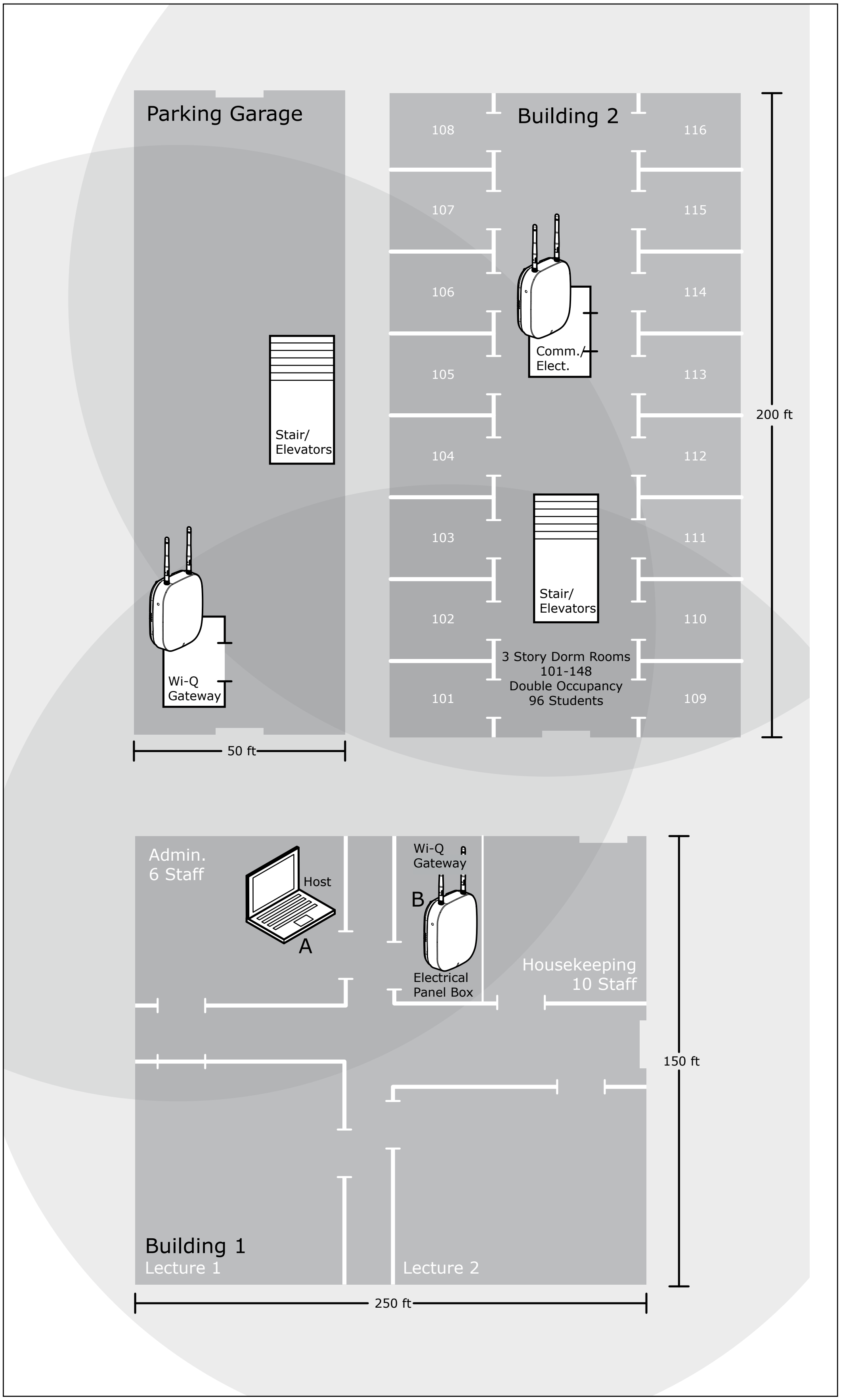
Transmit range from Wi-Q Gateway to controller varies based on building construction. Site characteristics such as reinforced concrete walls could interfere or weaken the signal; open spaces and low interference can increase signal strength.

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:

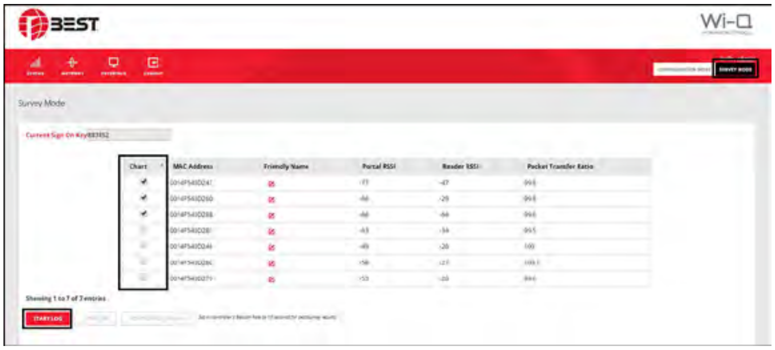
1 Log in to the WQXM-PG by navigating to the IPv4 address using an Internet browser.

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	✎	-46	-29	99.8
✓	0014F540D288	✎	-46	-44	99.6
☐	0014F540D281	✎	-43	-34	99.5
☐	0014F540D244	✎	-49	-20	100
☐	0014F540D28C	✎	-58	-27	[illegible]
☐	0014F540D271	✎	-53	-20	99.6

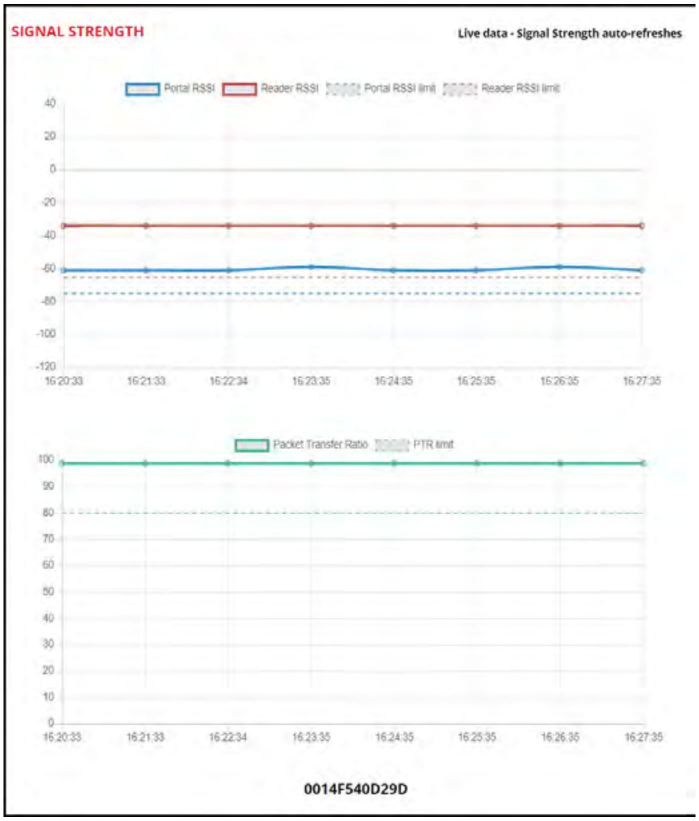
Showing 1 to 7 of 7 entries

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.

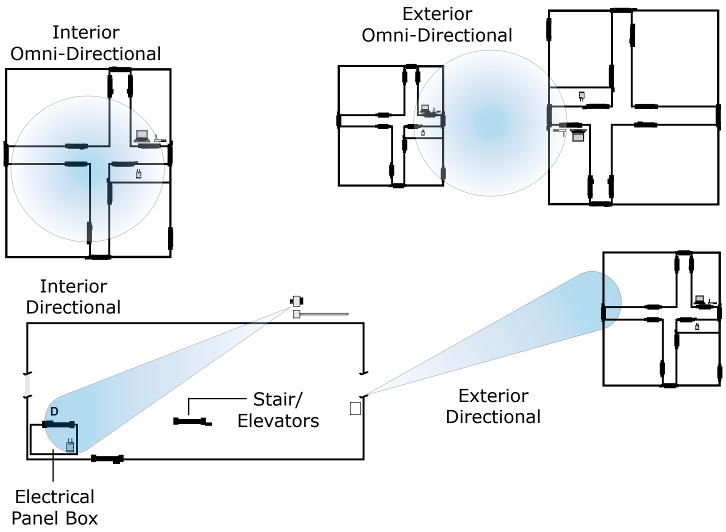
Note OnGuard 7.4 and higher with Wi-Q Interfaced installations using the WQXM-PG, require global statistics update poll rates to be made during troubleshooting. Please contact dormakaba Technical Support for direction at 800-392-5209 or via email at bas.support.best.us@dormakaba.com.

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.

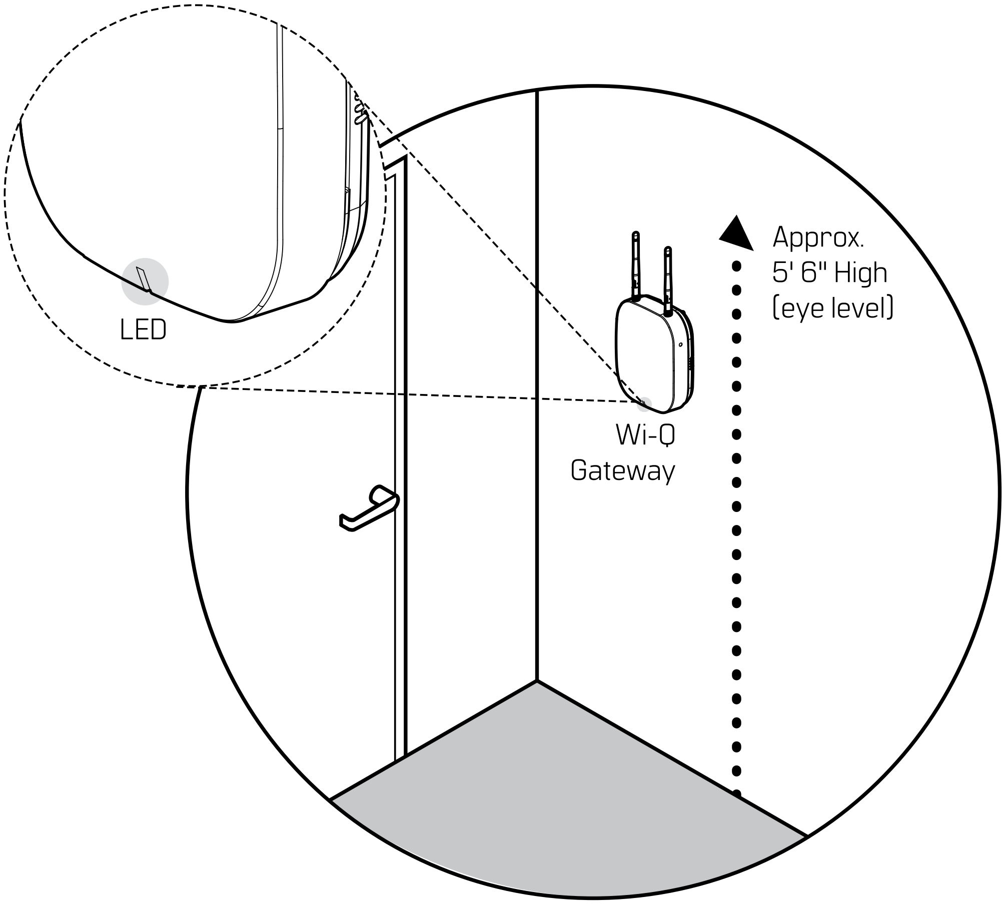
Next steps

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

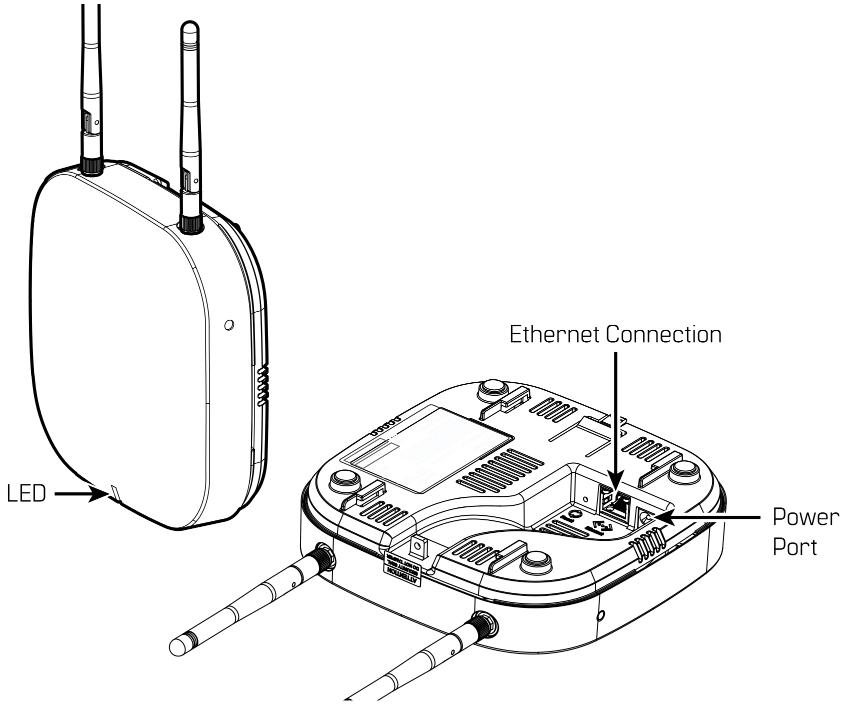
supply to the Wi-Q Gateway and plug in the AC adapter to the AC outlet. The indicator light on the top of the enclosure should come on and start flashing purple.

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.

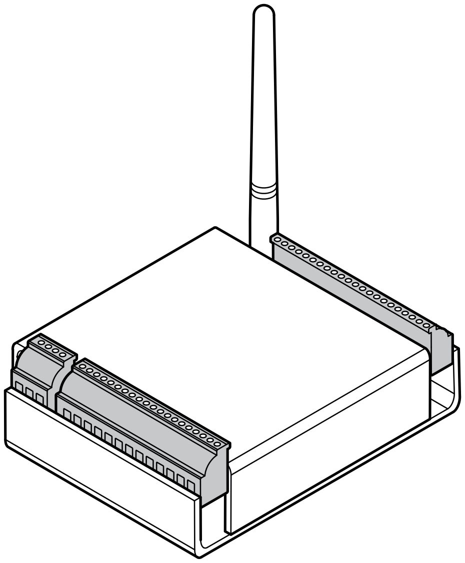
Installing a Wireless Access Controller

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

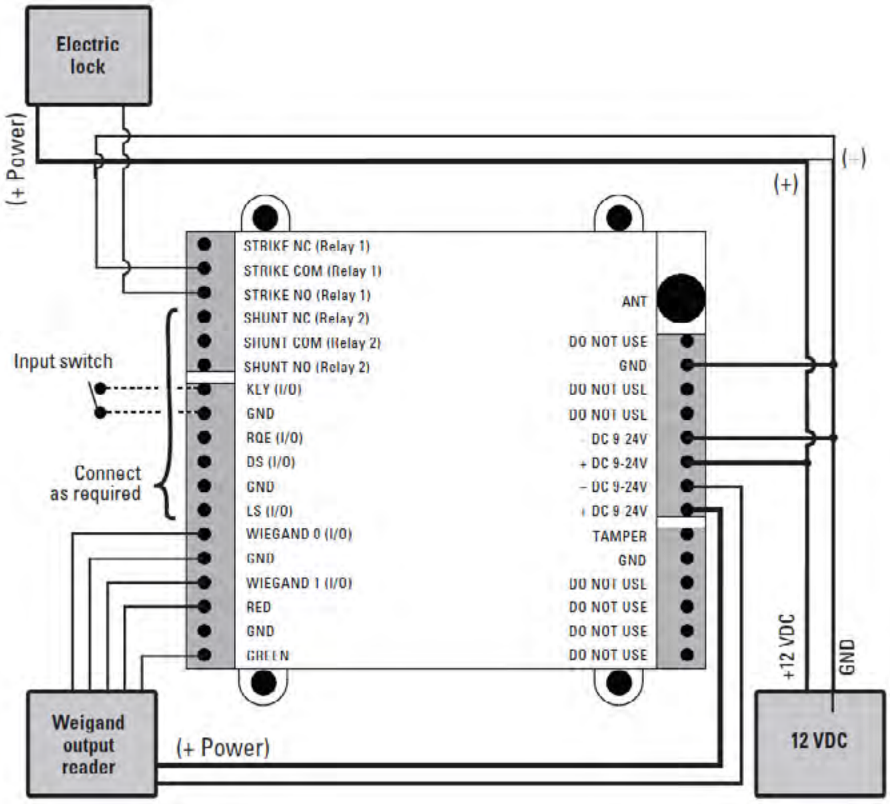
Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

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

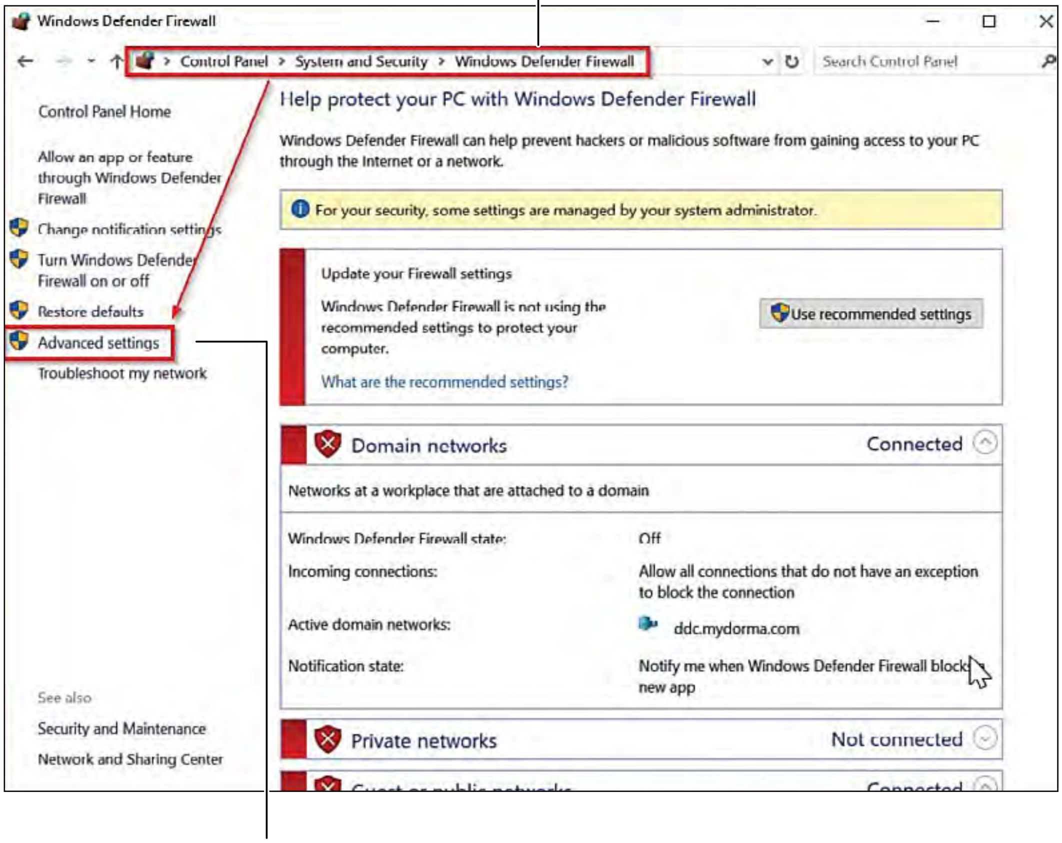
If your firewall is disabled, then all ports are open by default. If the firewall is on, perform the following steps in order to add the required ports listed above:

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

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?

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

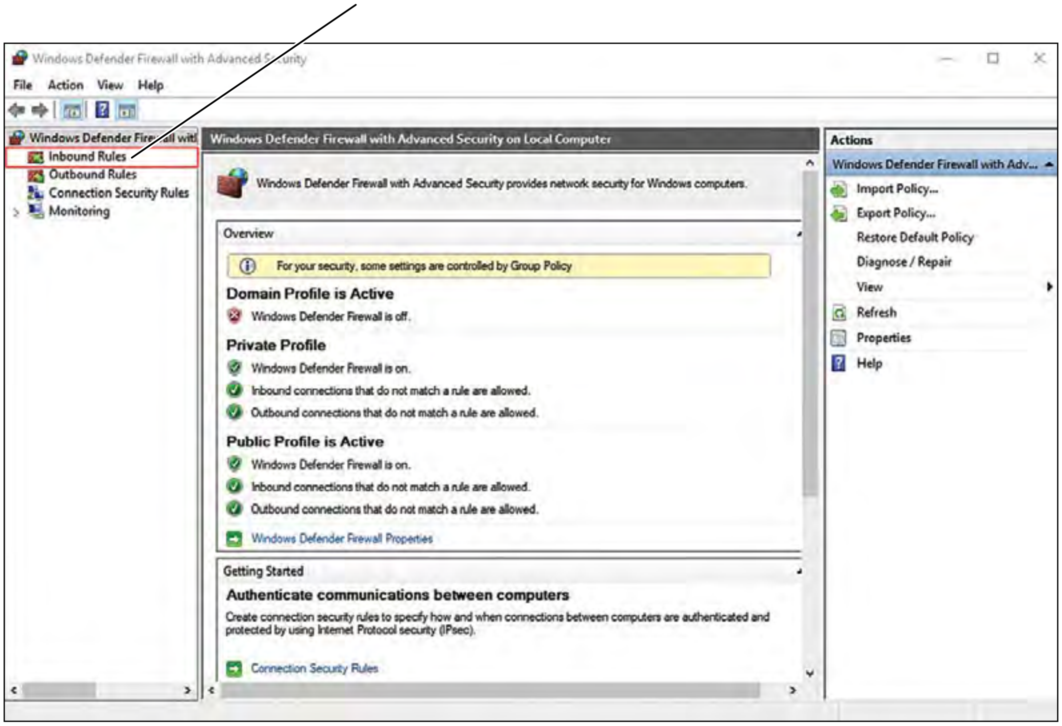
Guest or public networks Connected

Search Control Panel
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center
Use recommended settings

Click on Advanced settings

2 Select Inbound Rules.

Figure 13 Inbound Rules



Select Inbound Rules

Windows Defender Firewall with Advanced Security on Local Computer

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

Overview

For your security, some settings are controlled by Group Policy

Domain Profile is Active

Windows Defender Firewall is off.

Private Profile

Windows Defender Firewall is on.

Inbound connections that do not match a rule are allowed.

Outbound connections that do not match a rule are allowed.

Public Profile is Active

Windows Defender Firewall is on.

Inbound connections that do not match a rule are allowed.

Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

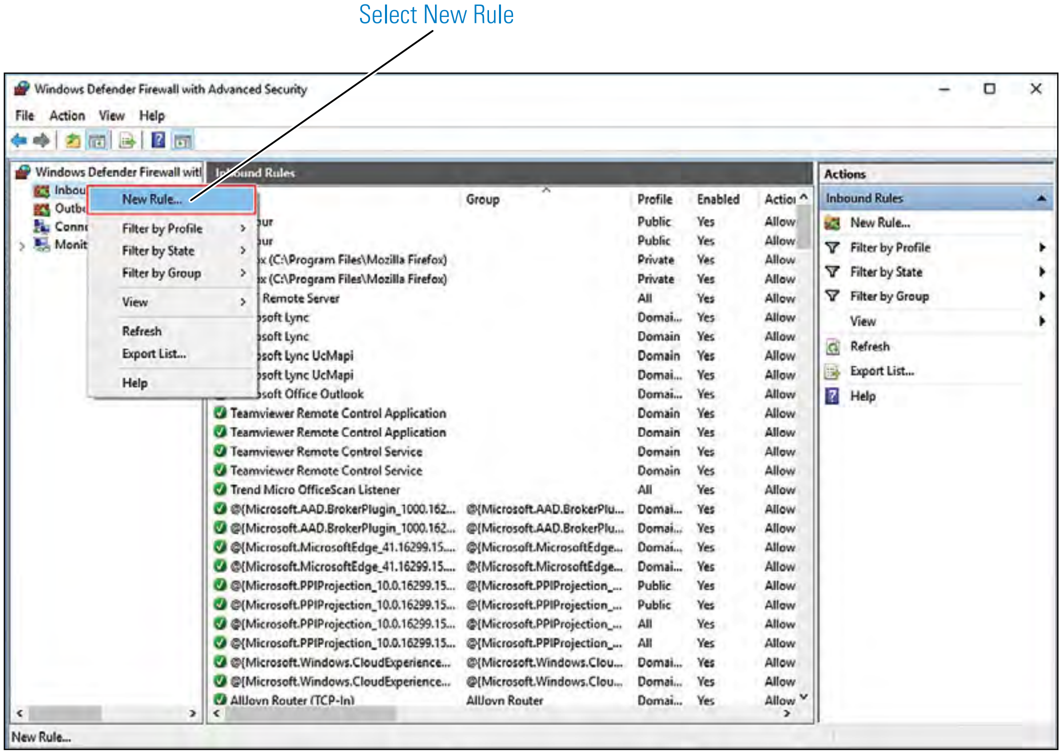
Authenticate communications between computers

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

Connection Security Rules

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

Figure 14 New Rule



Select New Rule

Windows Defender Firewall with Advanced Security

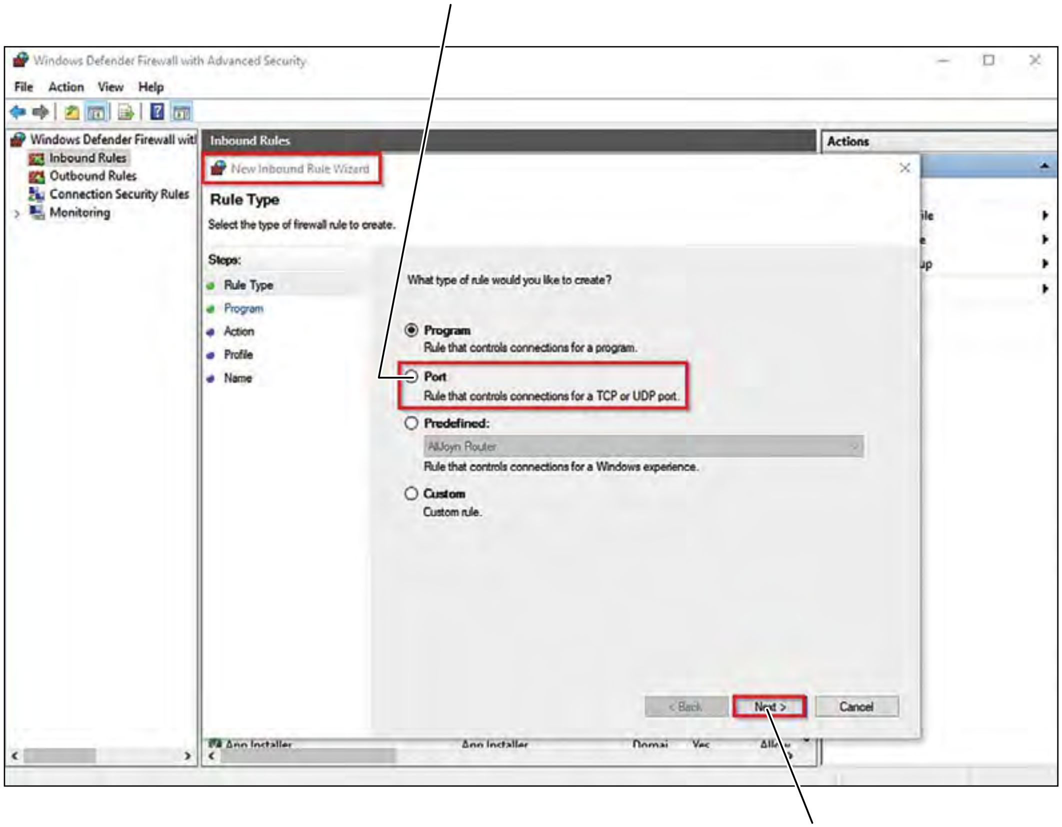
Inbound Rules

	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

New Rule...

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.

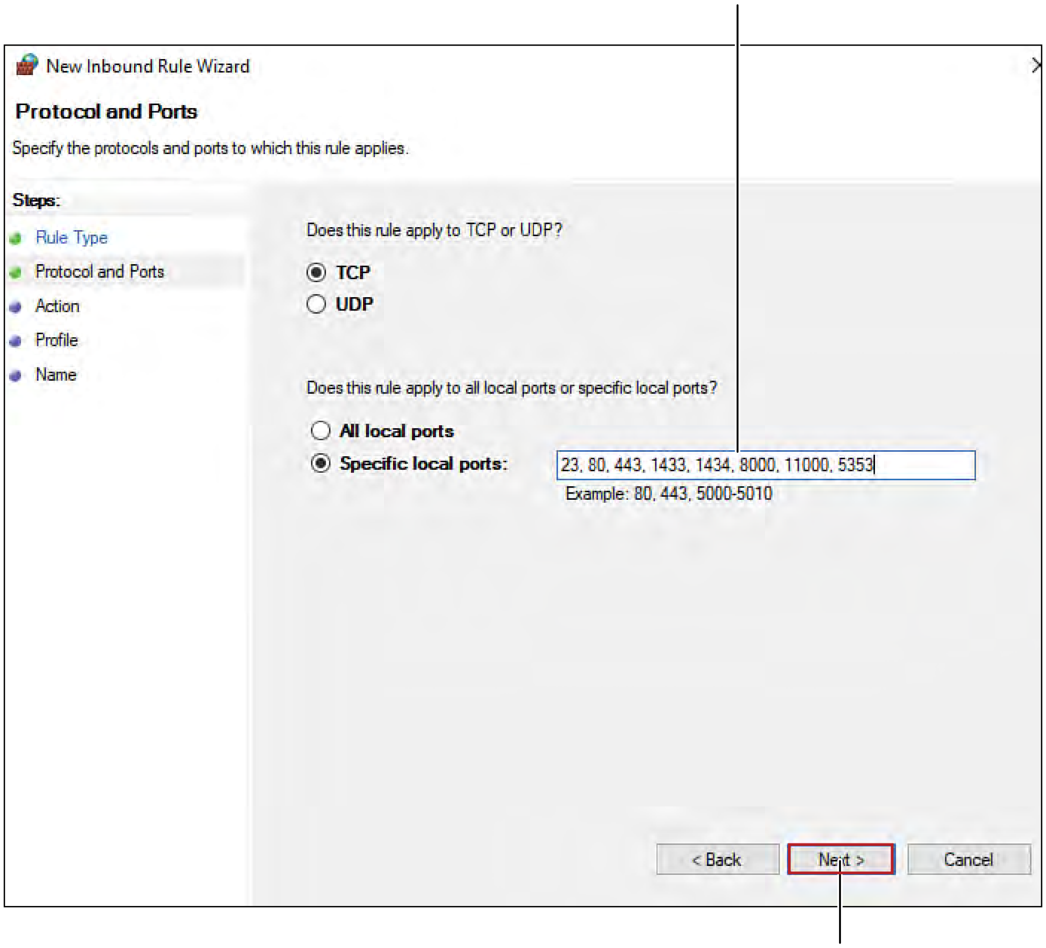
○ Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.

○ 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.

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

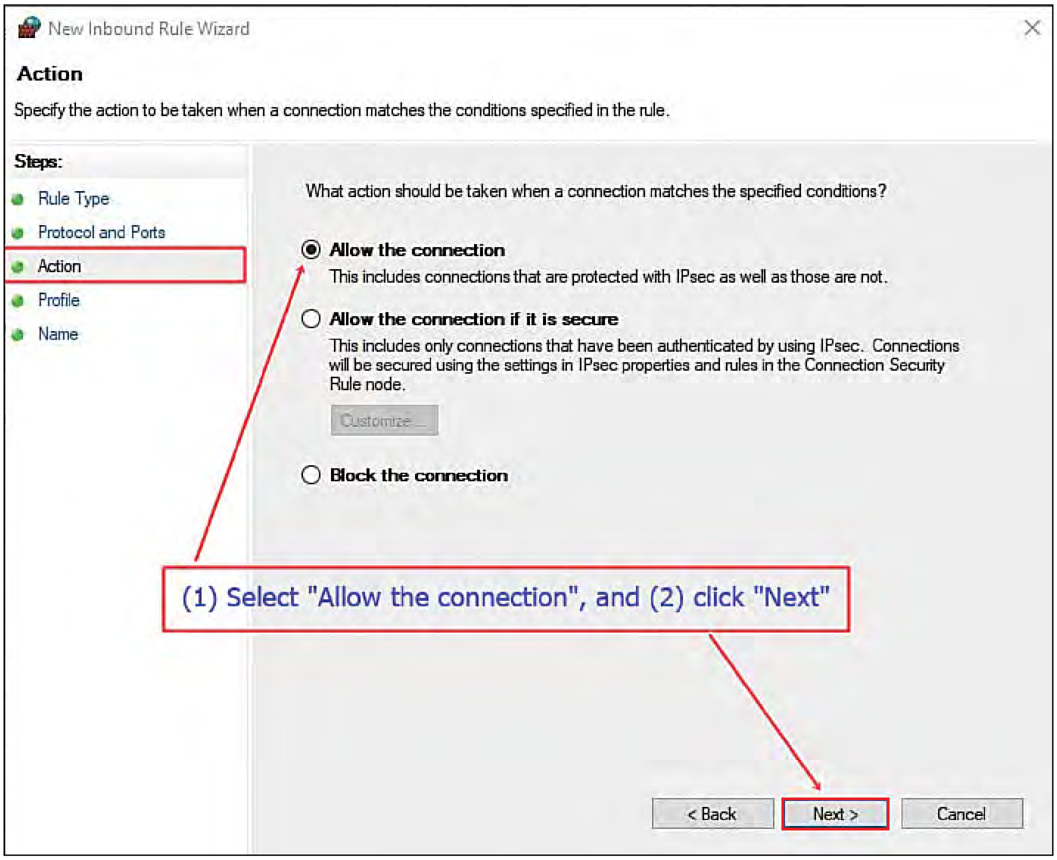
Example: 80, 443, 5000-5010

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.

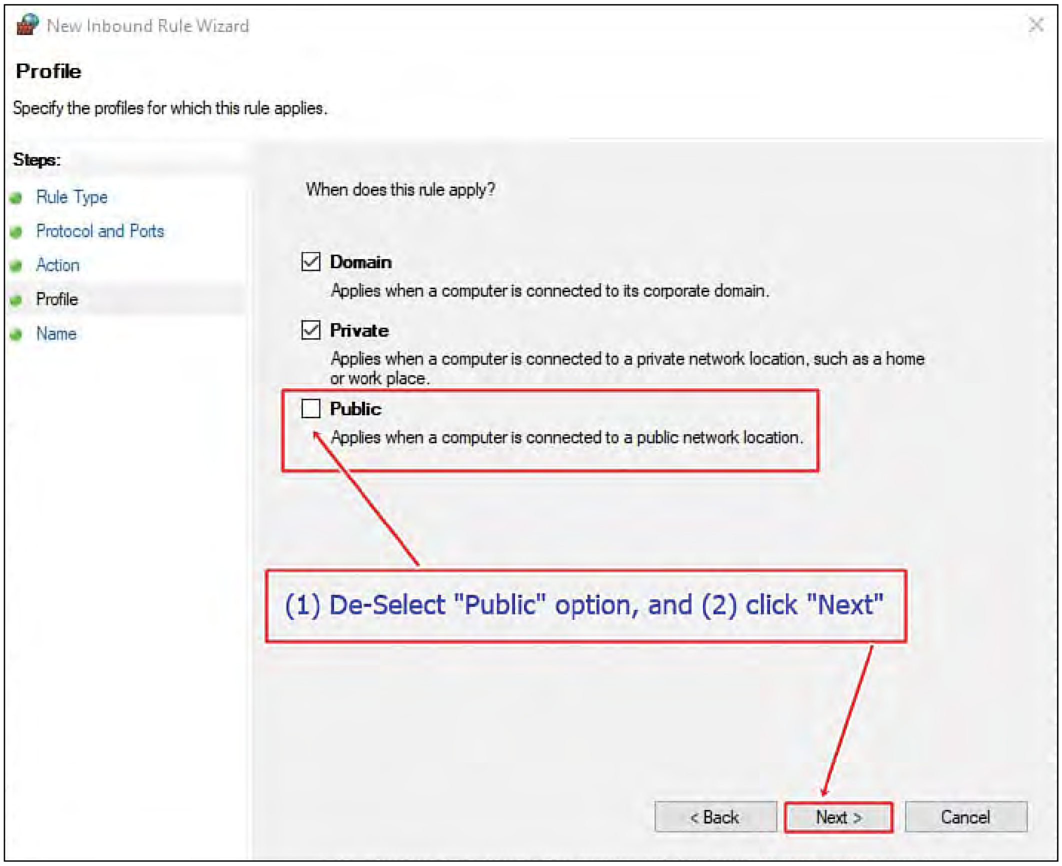
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **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



New Inbound Rule Wizard

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.

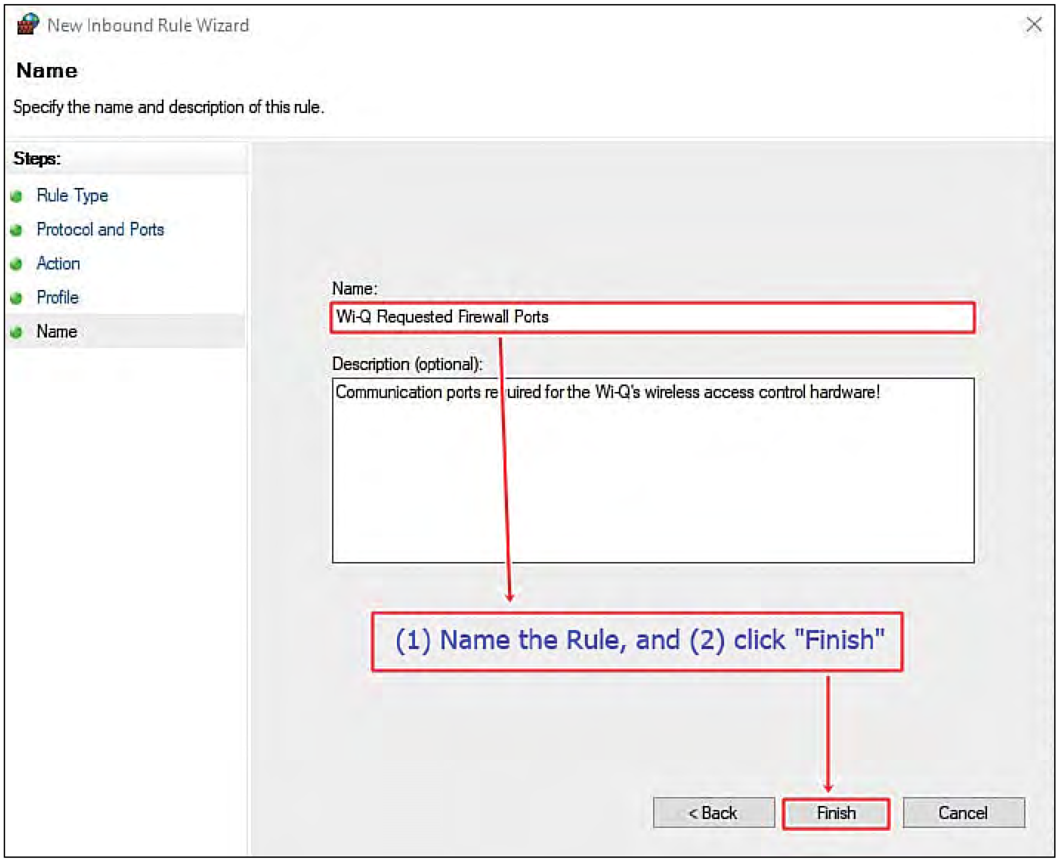
□ **Public**

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



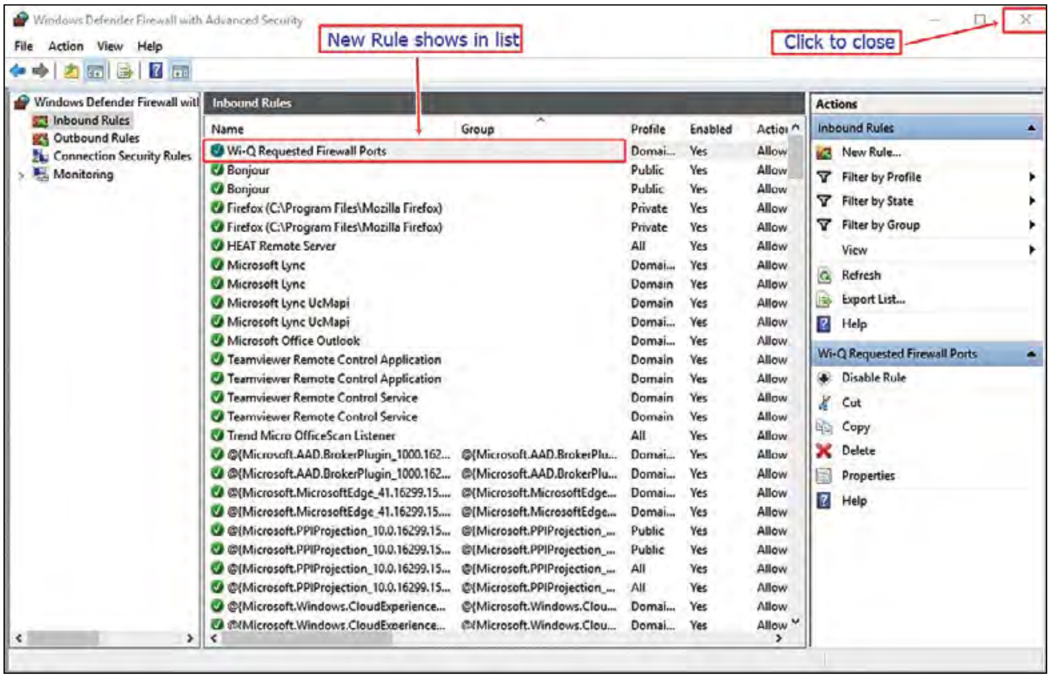
Name: Wi-Q Requested Firewall Ports

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.)

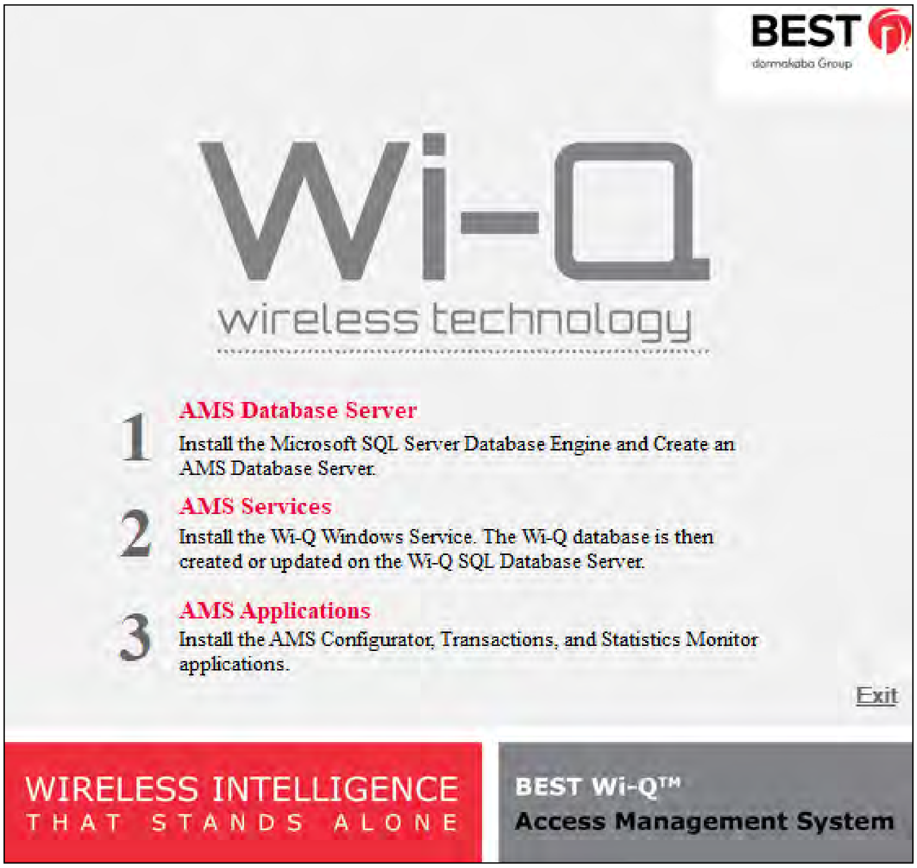
Beginning Installation

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



BEST dormakaba Group

Wi-Q wireless technology

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.

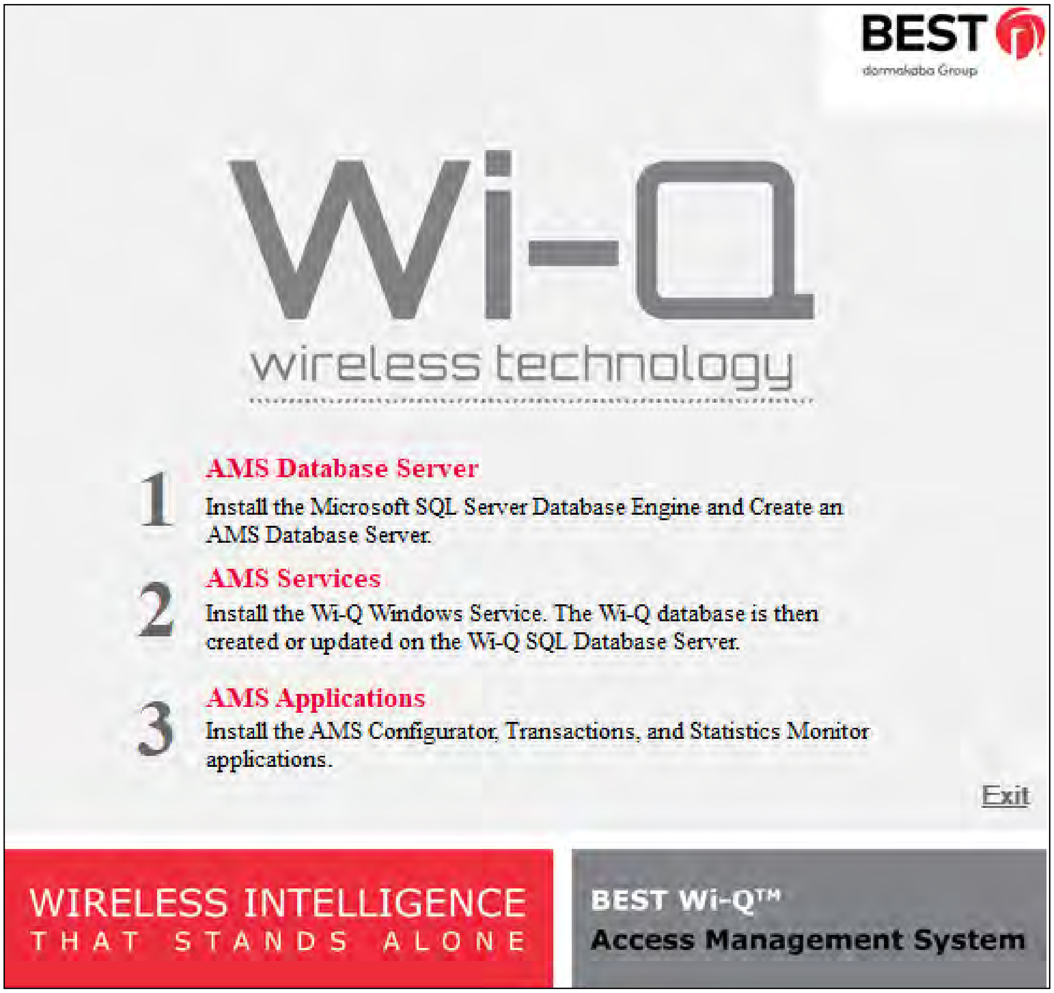
Note It is recommended that you reboot your machine after any missing prerequisites are installed before continuing on with the installation. After rebooting your machine, click the “Setup.exe” file again.

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.

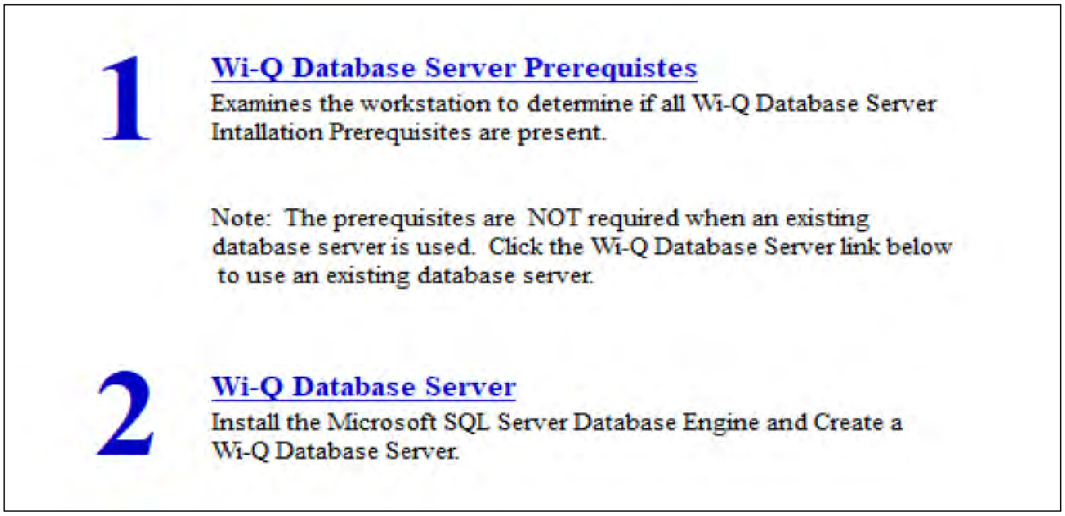
3 **AMS Applications**

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.

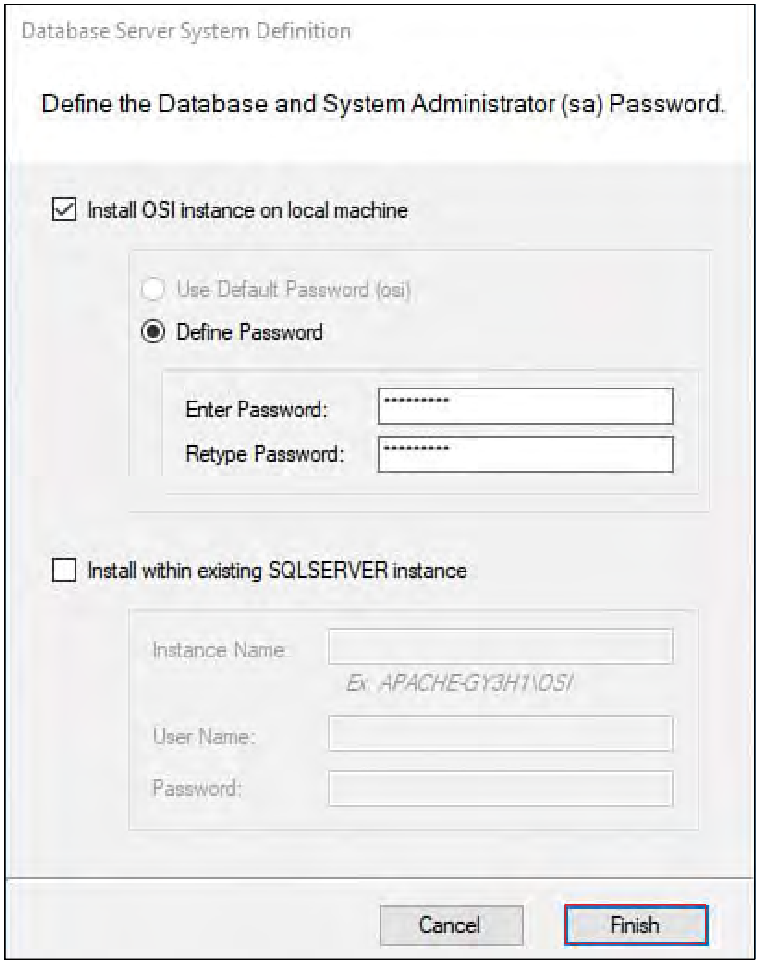
2 You may be prompted to install a number of prerequisites, including Microsoft Windows Installer and Windows PowerShell. To install the latest versions of these prerequisites, it is recommended that you click the website links provided and download directly from the Microsoft website. Once you've downloaded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

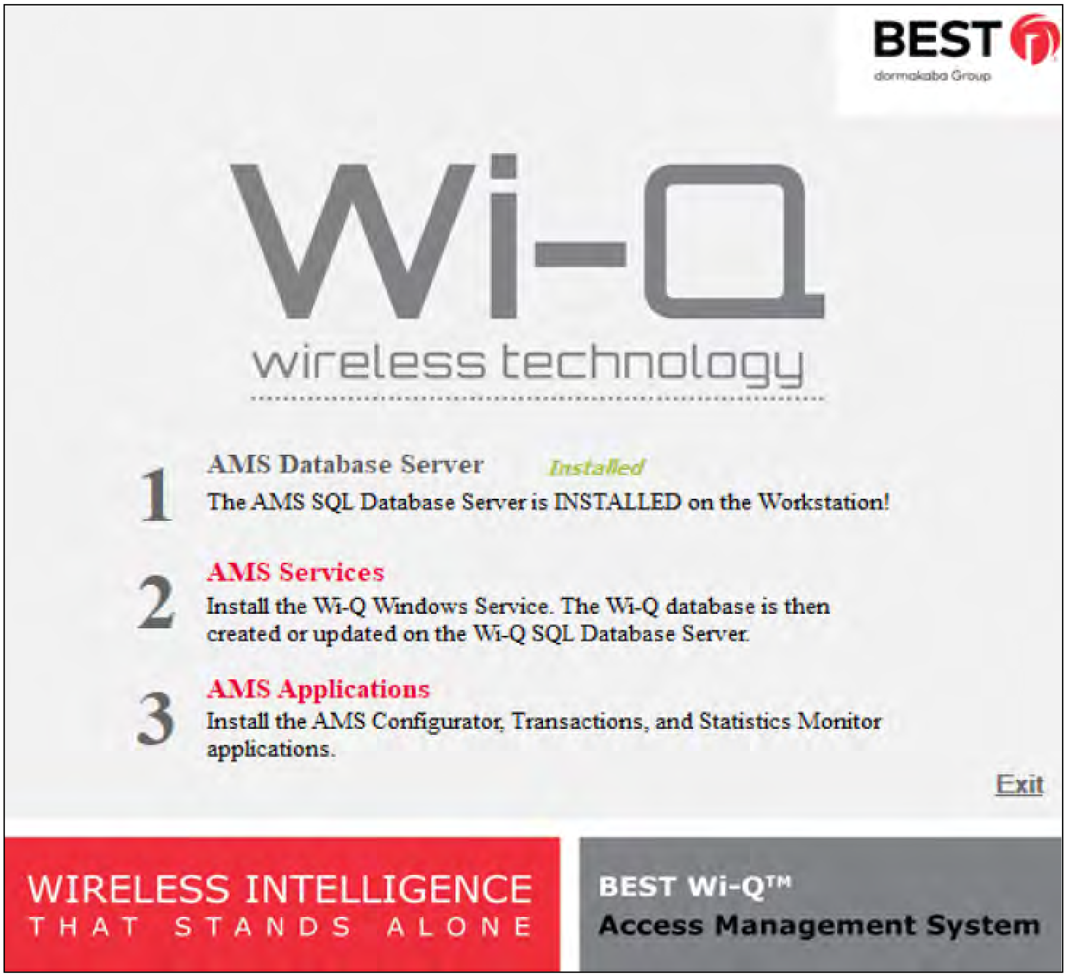
User Name:

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.

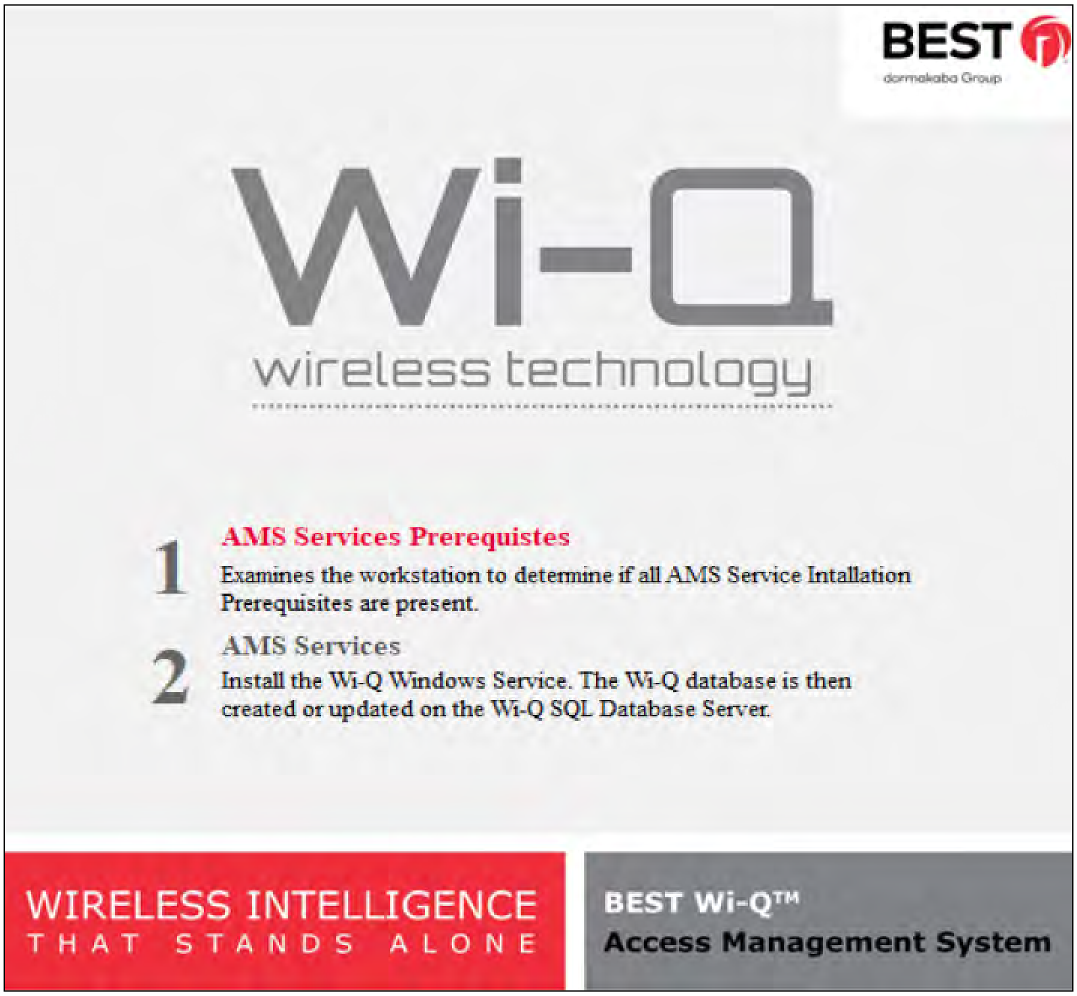
3 AMS Applications
Install the AMS Configurator, Transactions, and Statistics Monitor applications.

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.

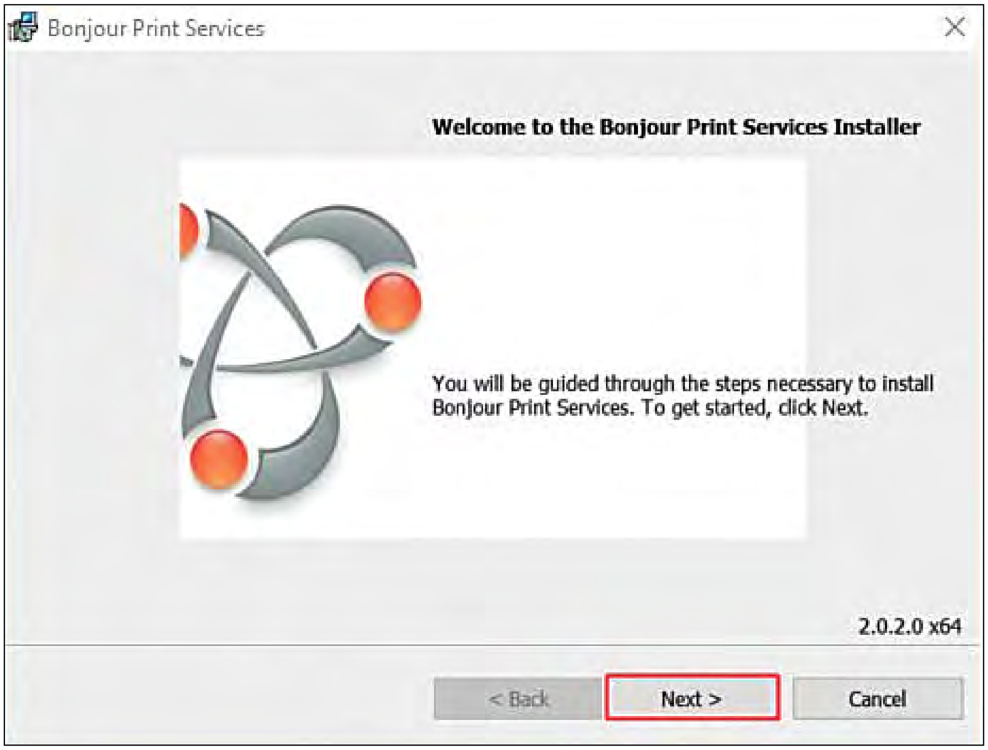
2 AMS Services
Install the Wi-Q Windows Service. The Wi-Q database is then created or updated on the Wi-Q SQL Database Server.

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



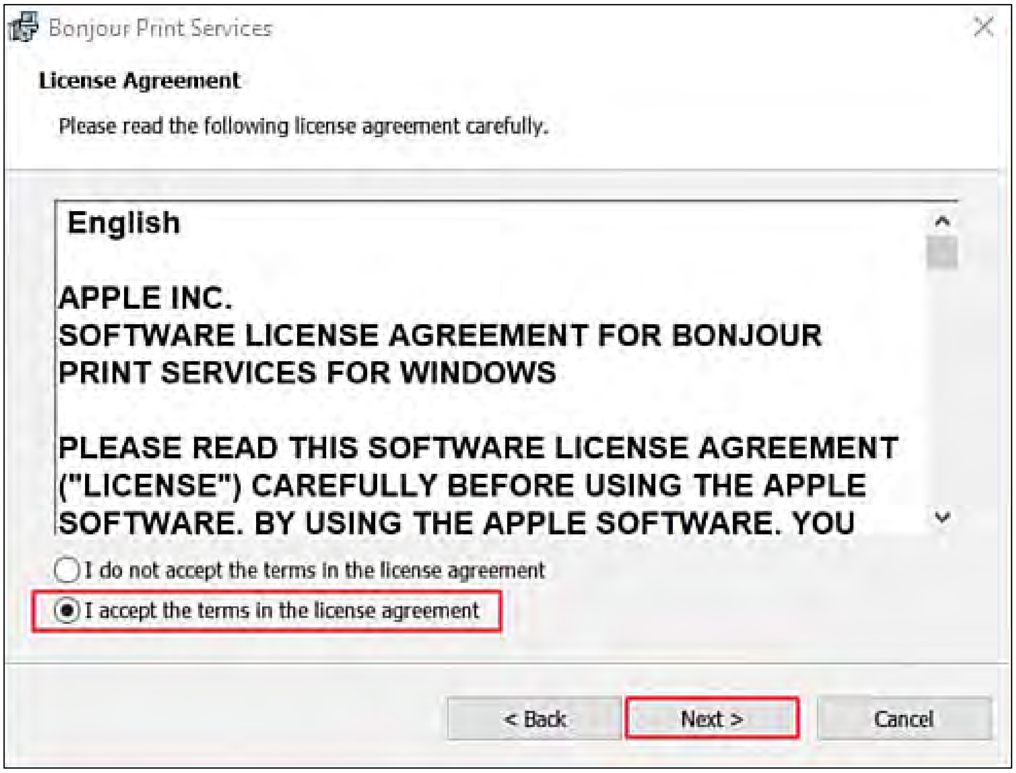
Welcome to the Bonjour Print Services Installer

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

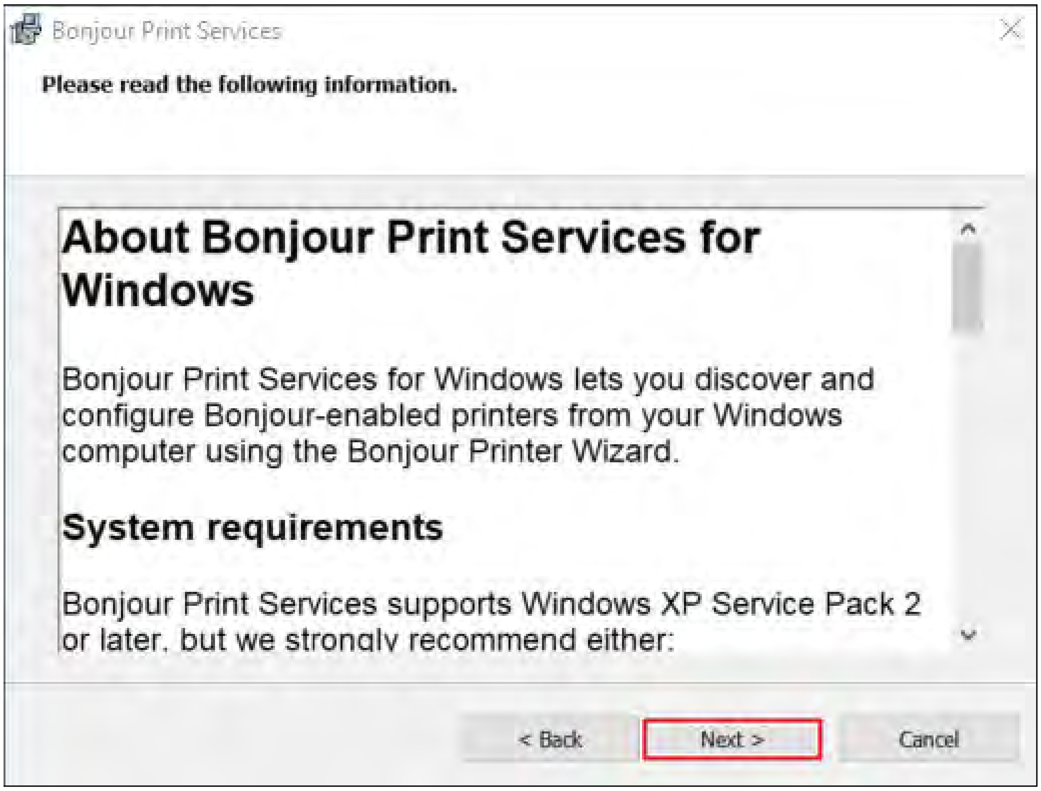
APPLE INC.
SOFTWARE LICENSE AGREEMENT FOR BONJOUR PRINT SERVICES FOR WINDOWS

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



Please read the following information.

About Bonjour Print Services for Windows

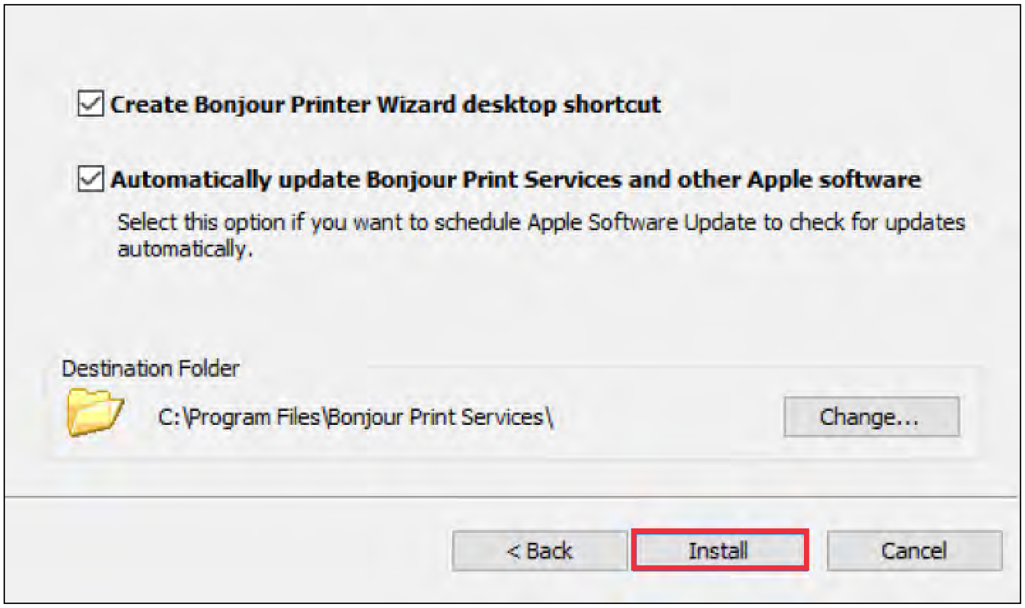
Bonjour Print Services for Windows lets you discover and configure Bonjour-enabled printers from your Windows computer using the Bonjour Printer Wizard.

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**

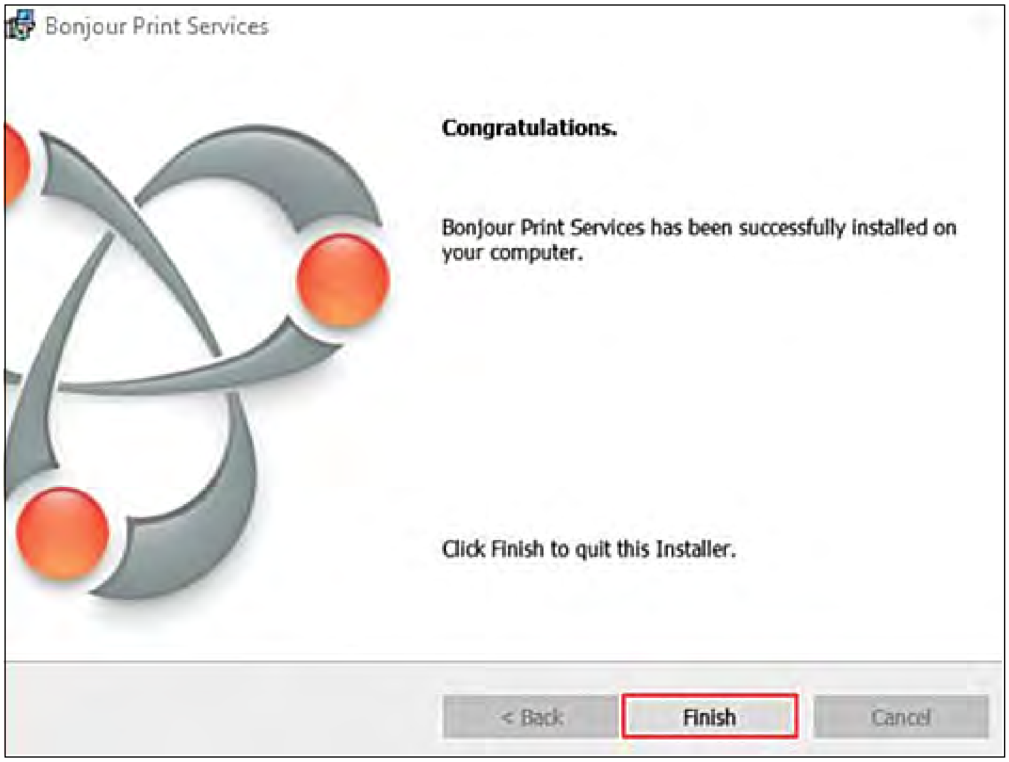
Select this option if you want to schedule Apple Software Update to check for updates automatically.

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.

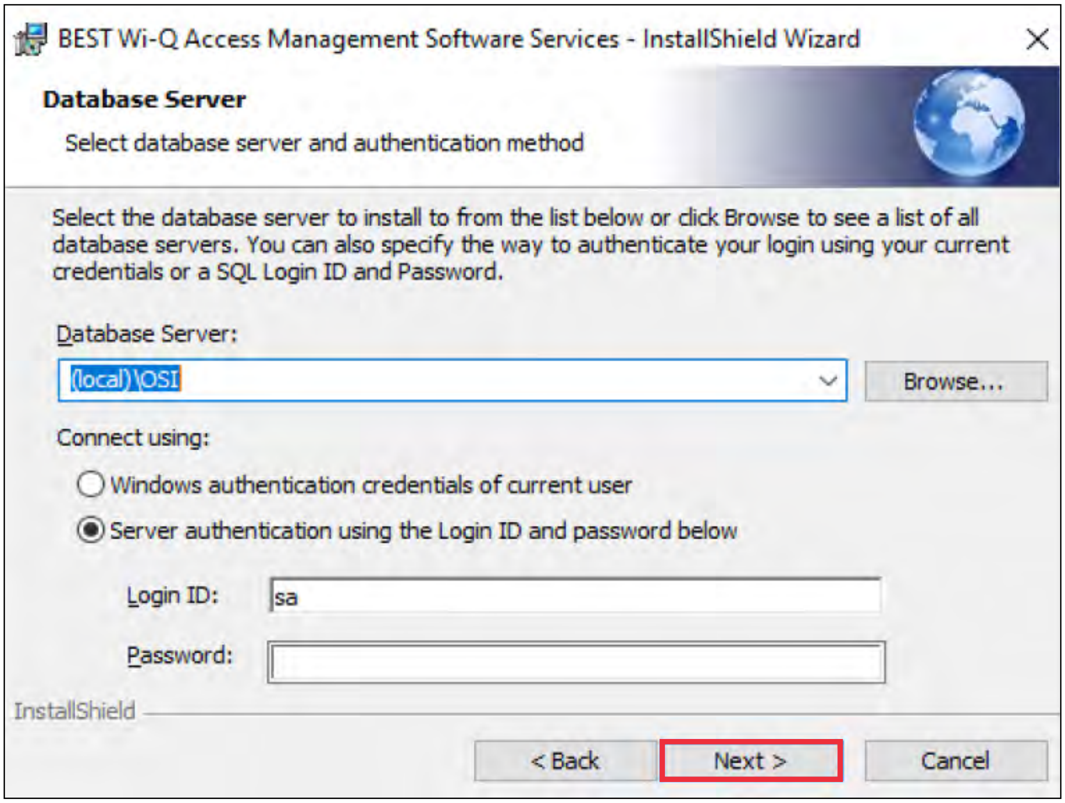
Click Finish to quit this Installer.

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

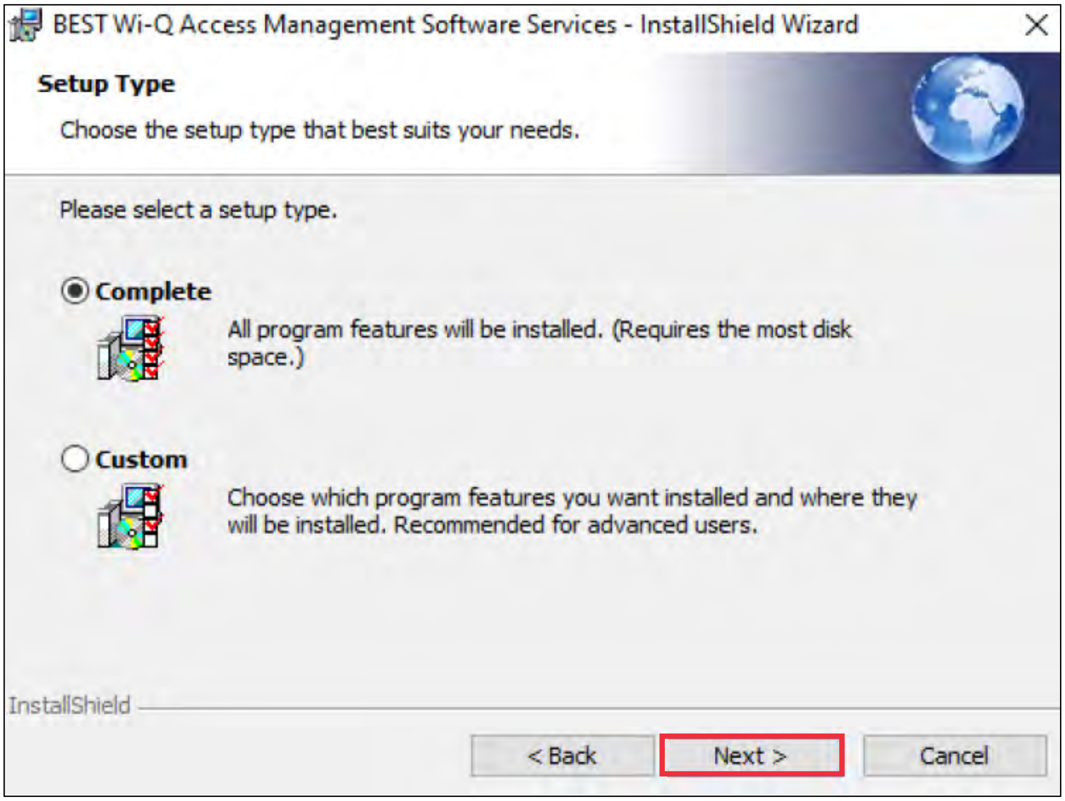
● Server authentication using the Login ID and password below

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**

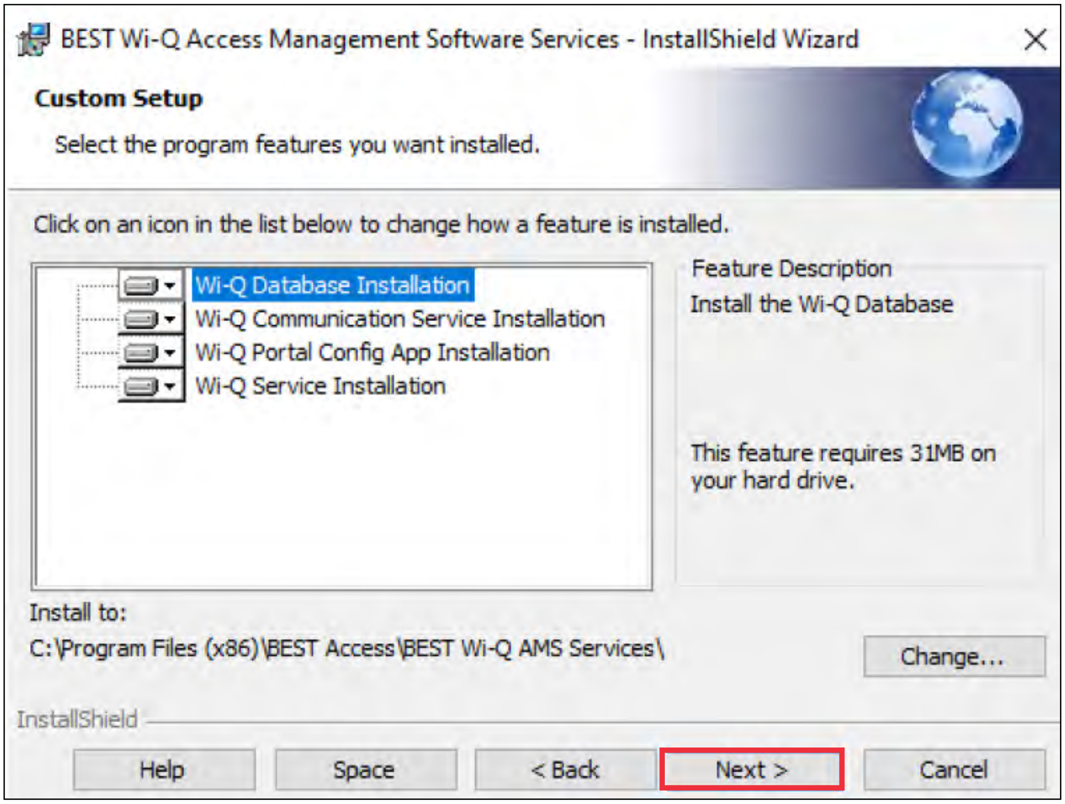
All program features will be installed. (Requires the most disk space.)

○ **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.

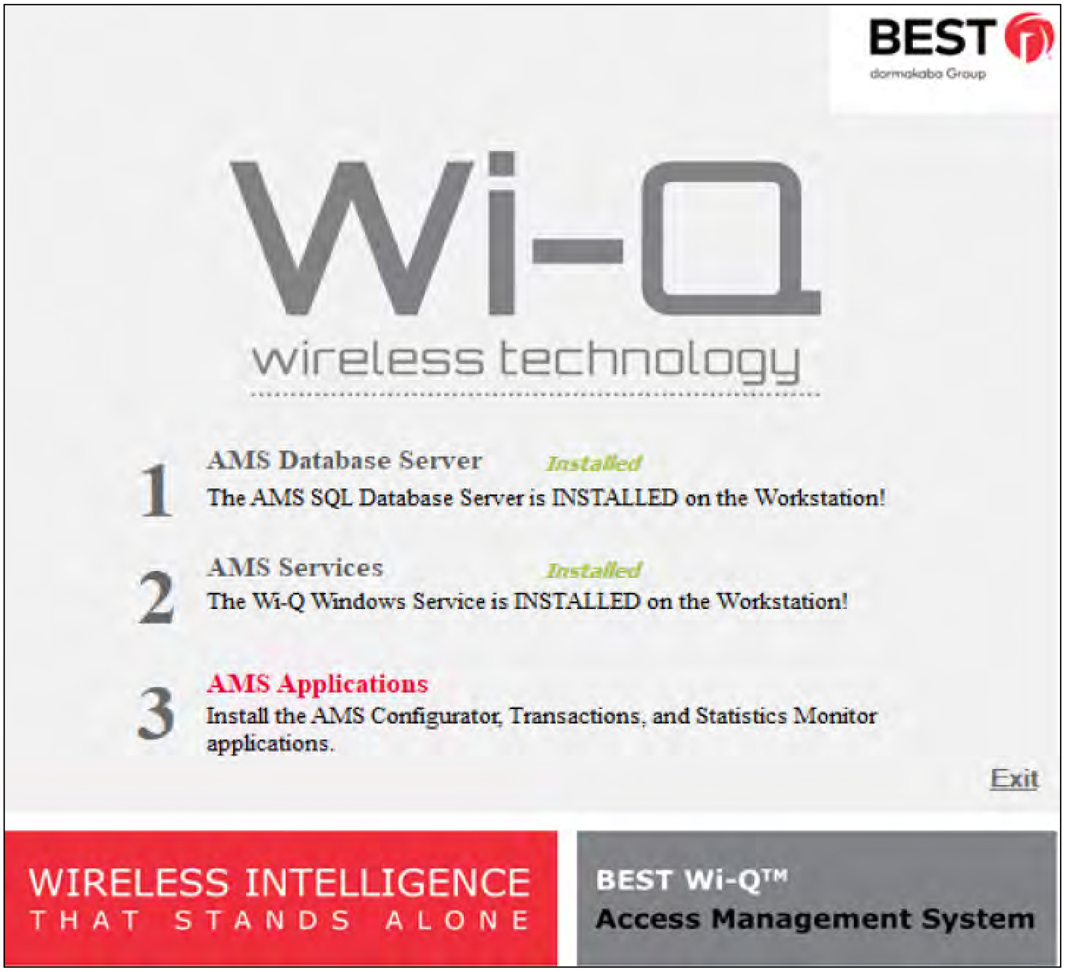
7 The wizard is now ready to begin the installation. Click Install.

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!

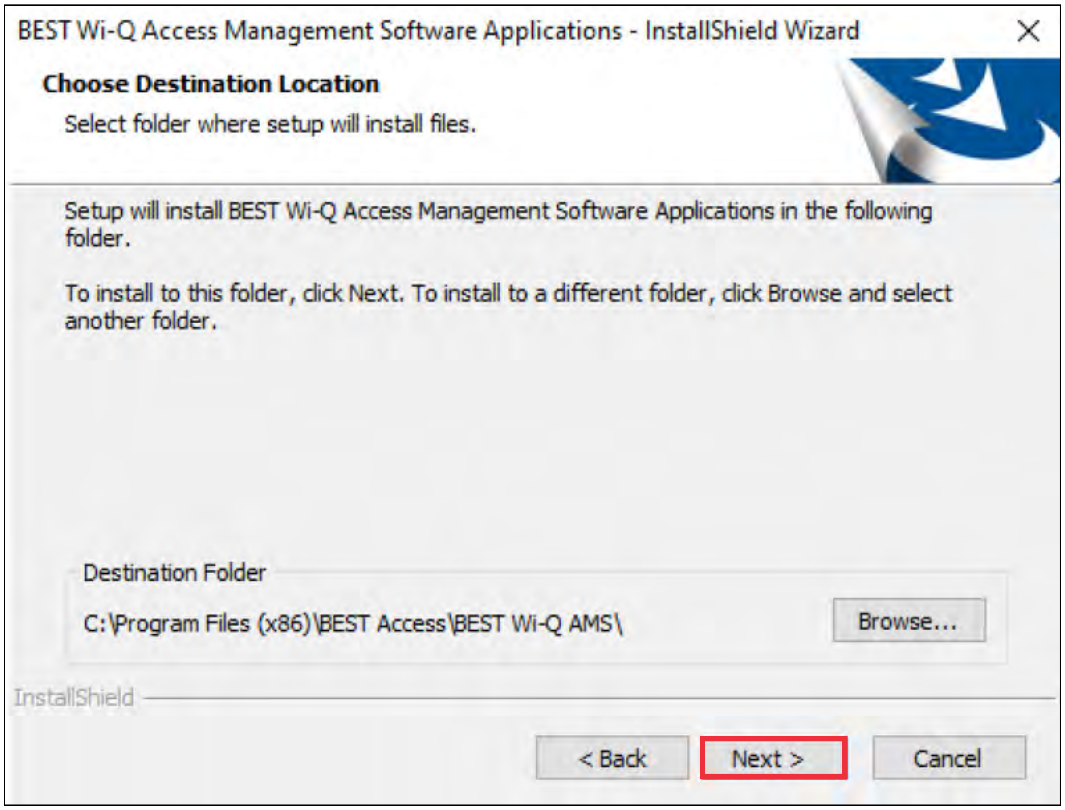
2 AMS Services Installed
The Wi-Q Windows Service is INSTALLED on the Workstation!

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.

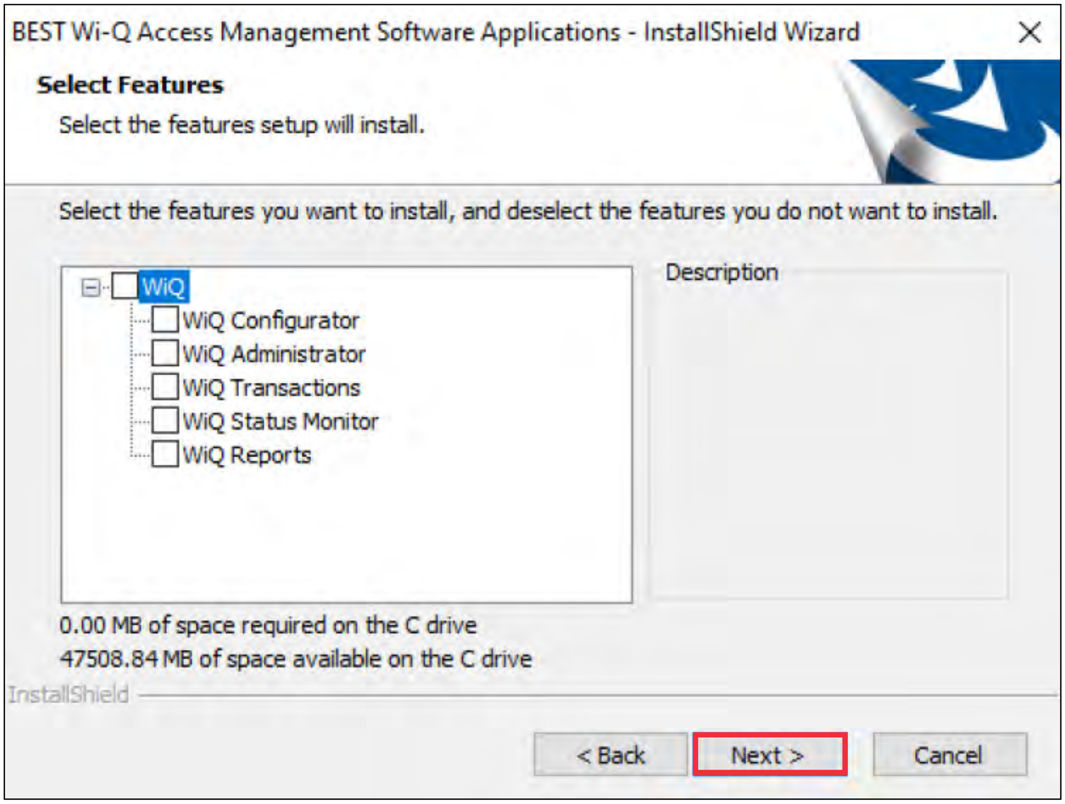
Destination Folder

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

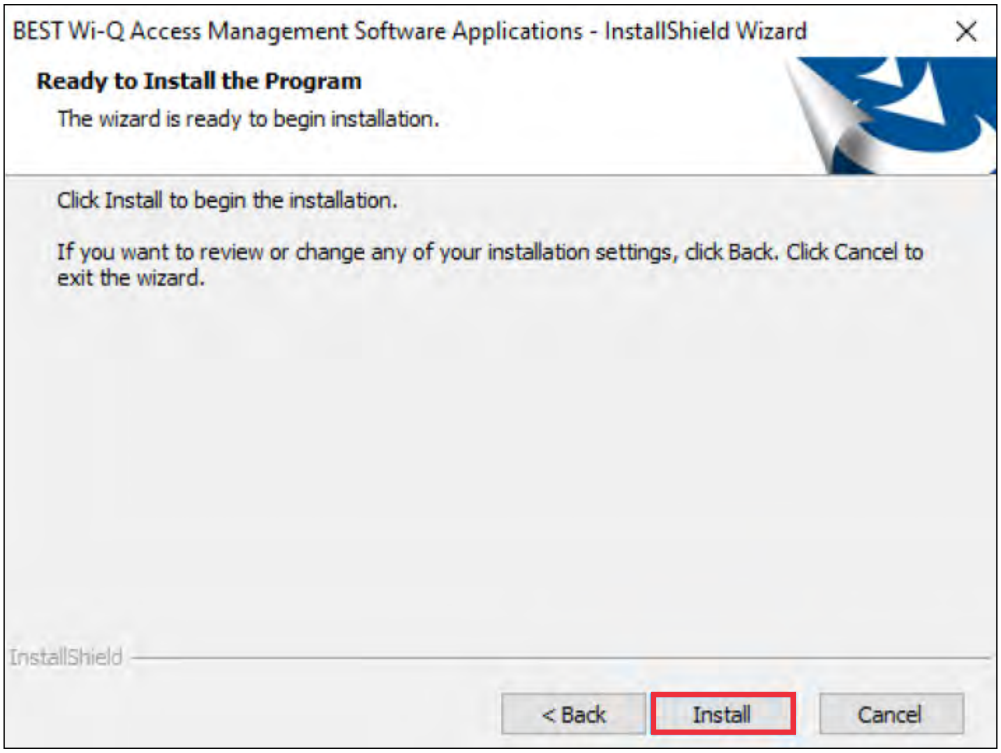
Description

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.

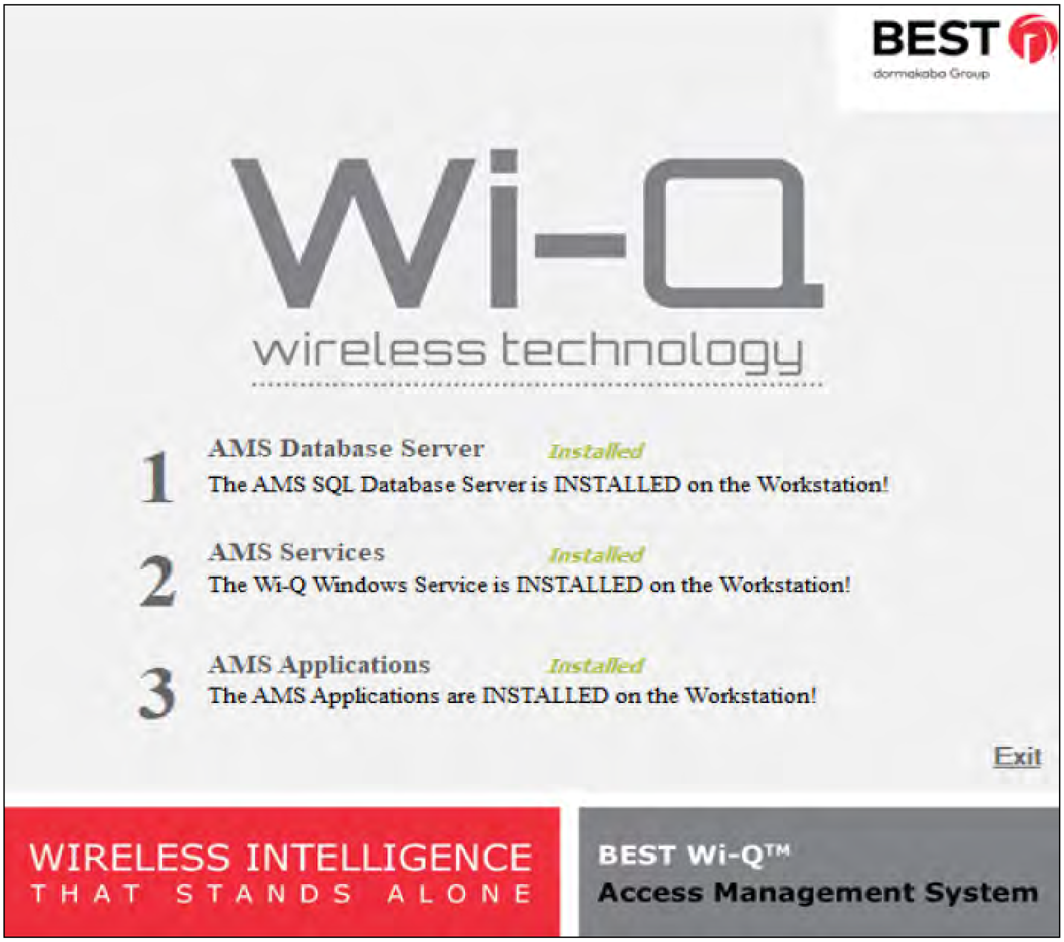
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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.

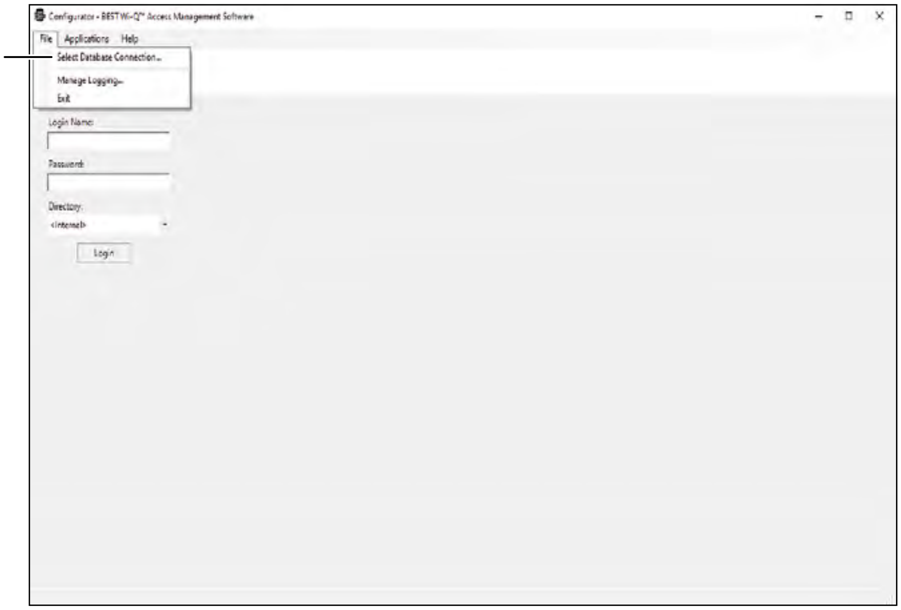
Selecting the Database Connection

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.

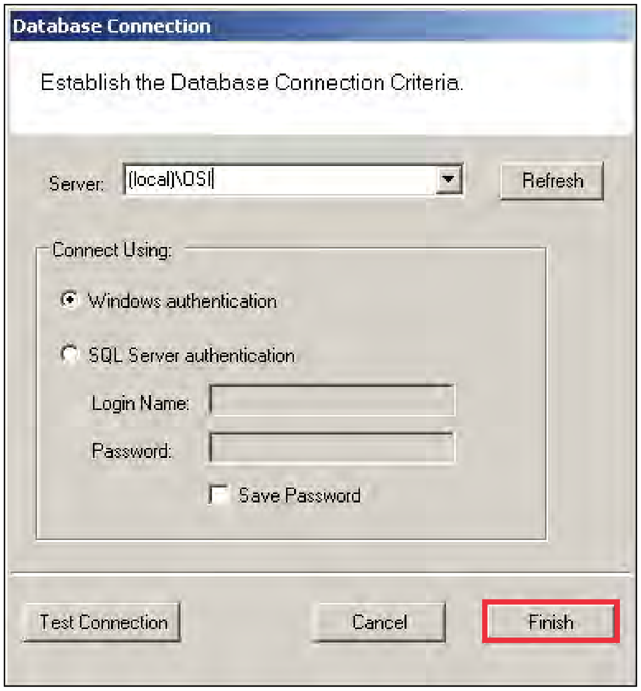
Figure 40 Select Database Connection



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.

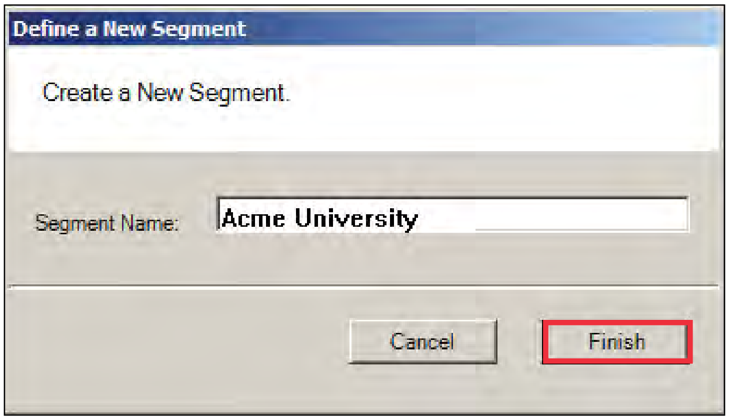
2 Select Login. You are ready to start setting up your new segment.

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



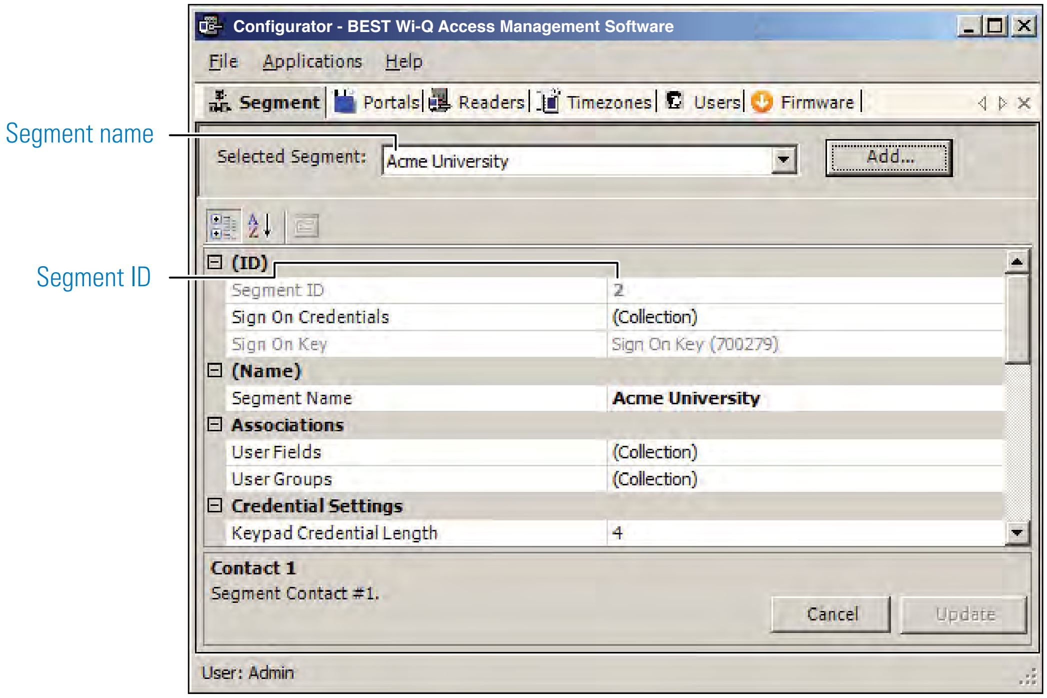
Define a New Segment

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.

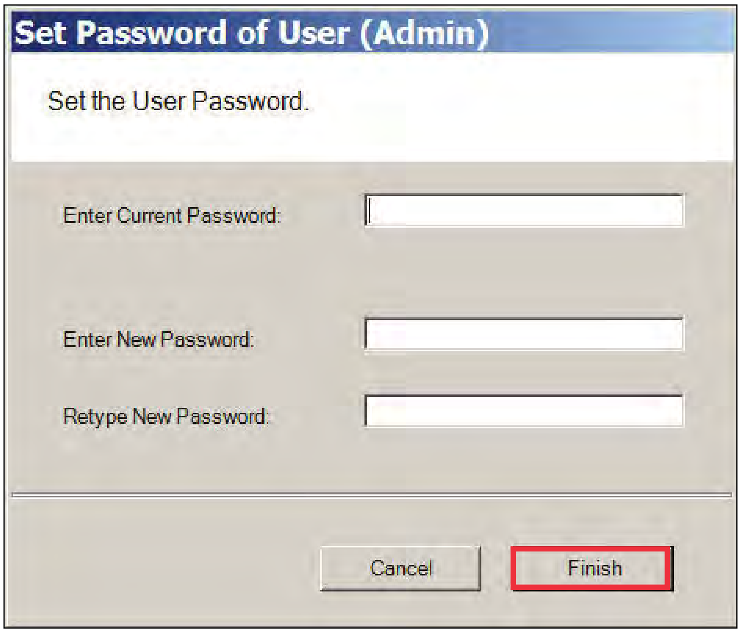
User: Admin

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.

Enter Current Password:

Enter New Password:

Retype New 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.

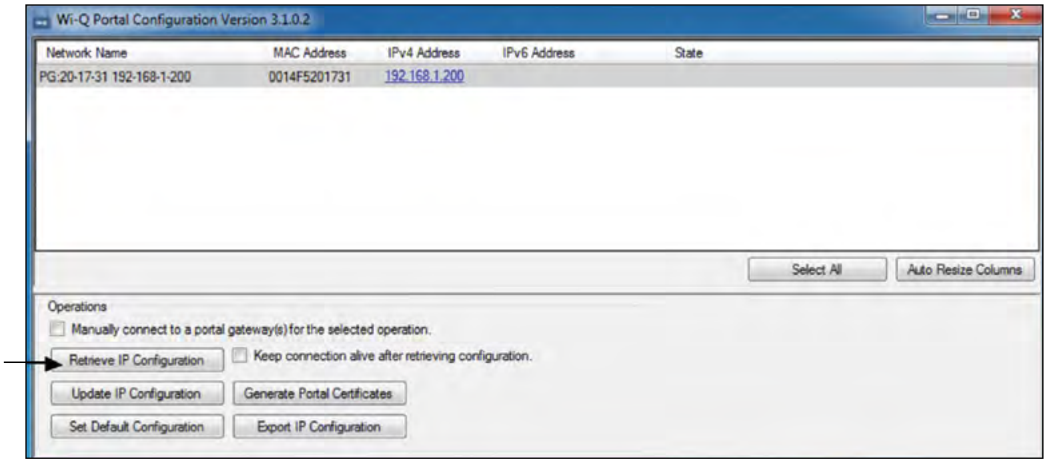
1 Connect the Wi-Q Gateway to the Host either over the network or directly via crossover Ethernet cable (recommended). For more information on connecting a Wi-Q Gateway, see "Connecting the Wi-Q Gateway and Verifying Operation" on page 25.

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

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

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

☐ Keep connection alive after retrieving configuration.

4 Select a Wi-Q Gateway from the list.

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.

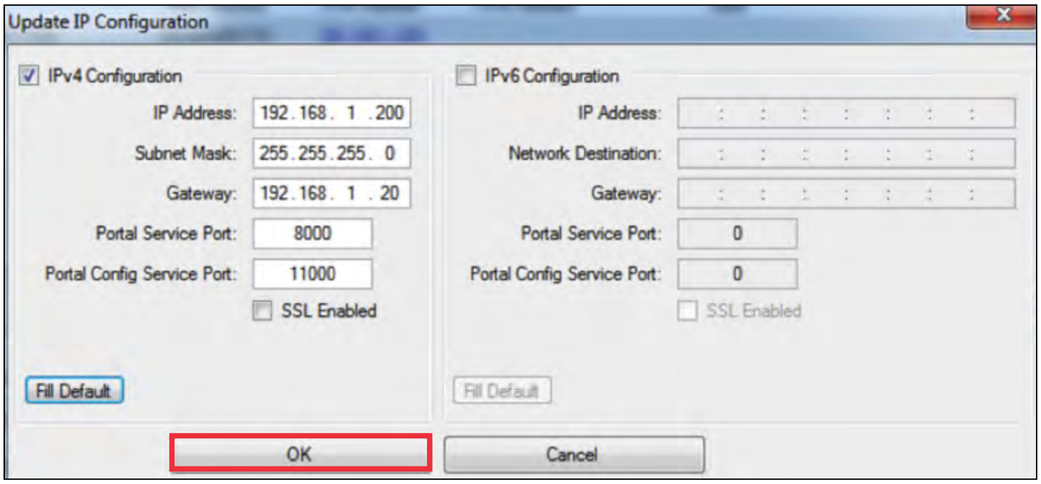
6 Select IPv4 and/or IPv6 and enter the IP address.

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

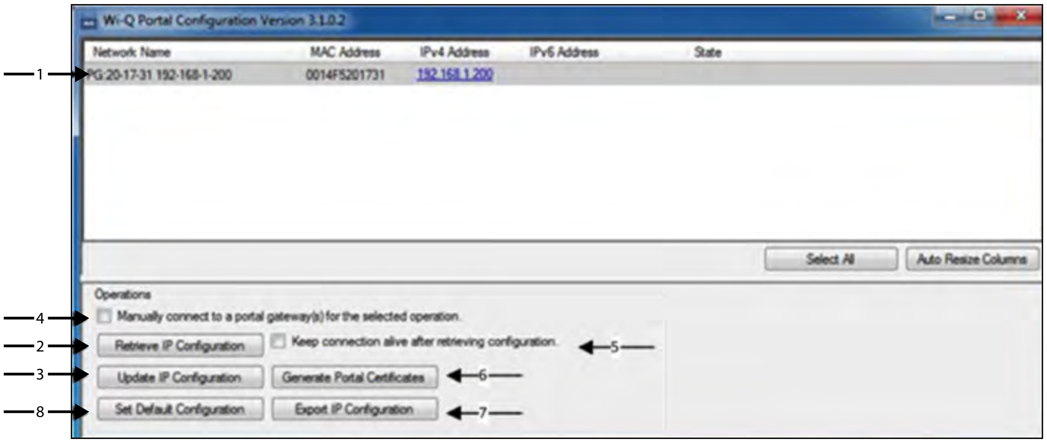
Portal Config Service Port: 0

☐ 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



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

Wi-Q Portal Configuration Version 3.1.0.2
Select All
Auto Resize Columns
Operations
□ Manually connect to a portal gateway(s) for the selected operation.
Retrieve IP Configuration
□ Keep connection alive after retrieving configuration.
Update IP Configuration
Generate Portal Certificates
Set Default Configuration
Export IP Configuration
1
4
2
3
8
5
6
7

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.

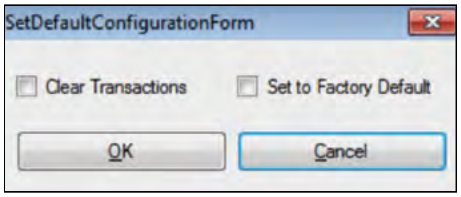
Note This feature does not work with the Wi-Q Gateway model WQXM-PG.

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



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.

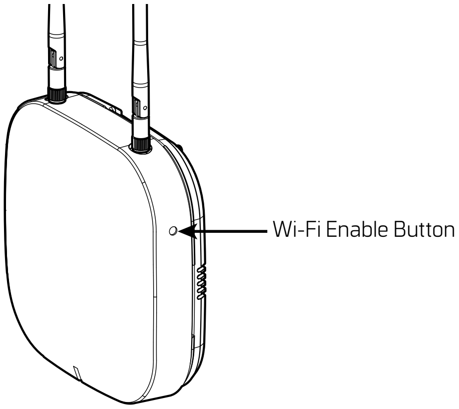
For example: Use 192.168.2.100, where 2 instead of 3 is used in the address's 3rd octet, when assigning an IP address to the Ethernet adapter on the Gateway if a Class C IPv4 network is in use.

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:

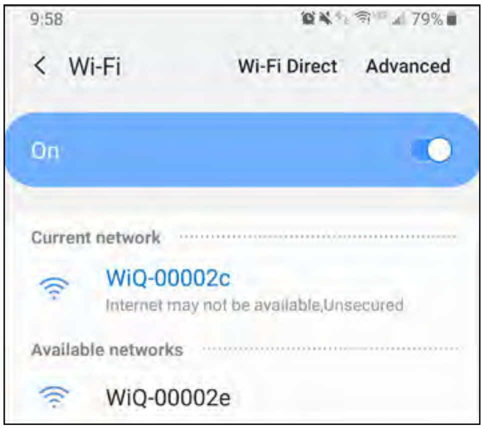
- Push the Wi-Fi enable button on the side of the WQXM-PG Wi-Q Gateway. See figure 49.

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.

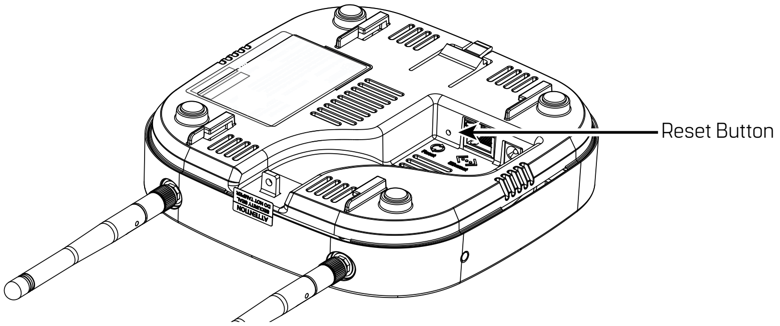
2 Reconnect to the Gateway's unique wireless network connection.

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.

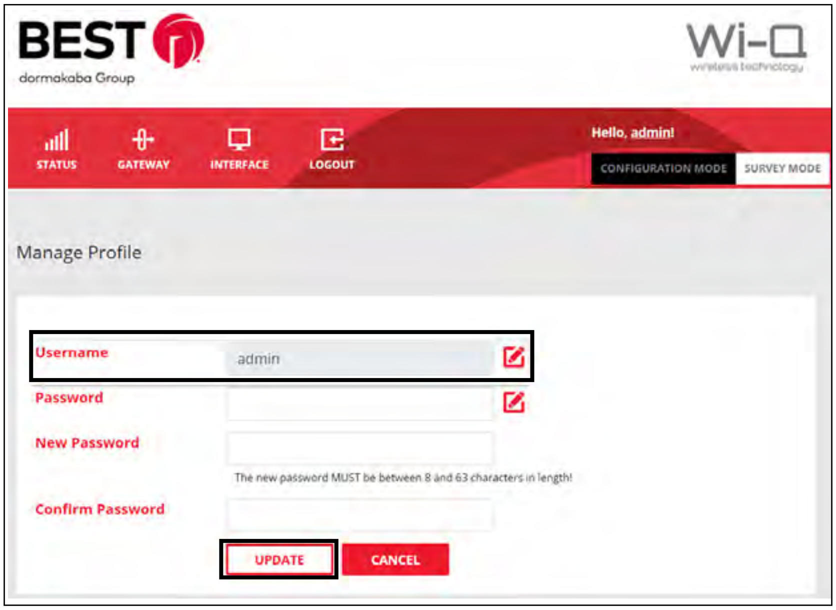
3 Click the Update button to save the changes.

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.

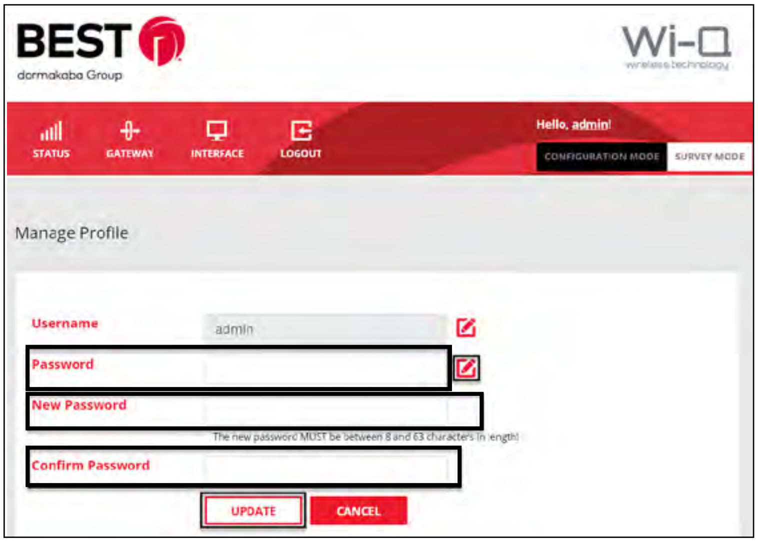
6 Click the Update button in the pop-up notification window to confirm the changes.

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

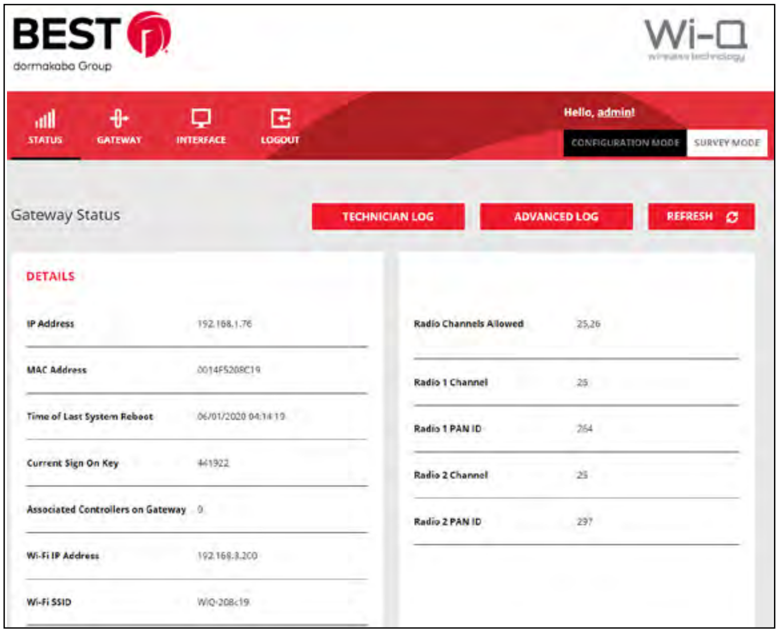
The new password MUST be between 8 and 63 characters in length!

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.

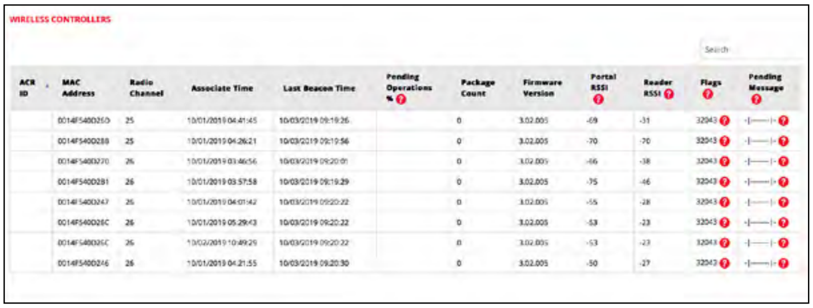
Note: Radio 1 PAN ID can be edited when in Mercury Mode. PAN IDs only need to be changed if there is a conflict with multiple Gateways within RF range of each other. Editing Radio 1 PAN ID will also change Radio 2 PAN ID. Each Gateway uses up to 66 PAN IDs.

- **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.

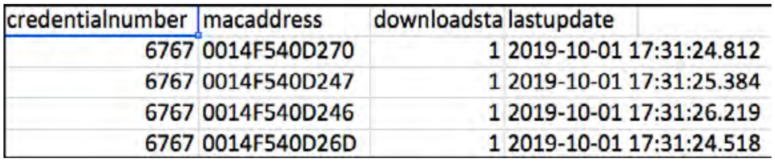
The Technician and Advanced log buttons allows the installer/technician to assist dormakaba BEST software support in troubleshooting an issue. These logs may be used by the local installer to troubleshoot or verify the credentials are all making it to the controllers or requested during a troubleshooting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

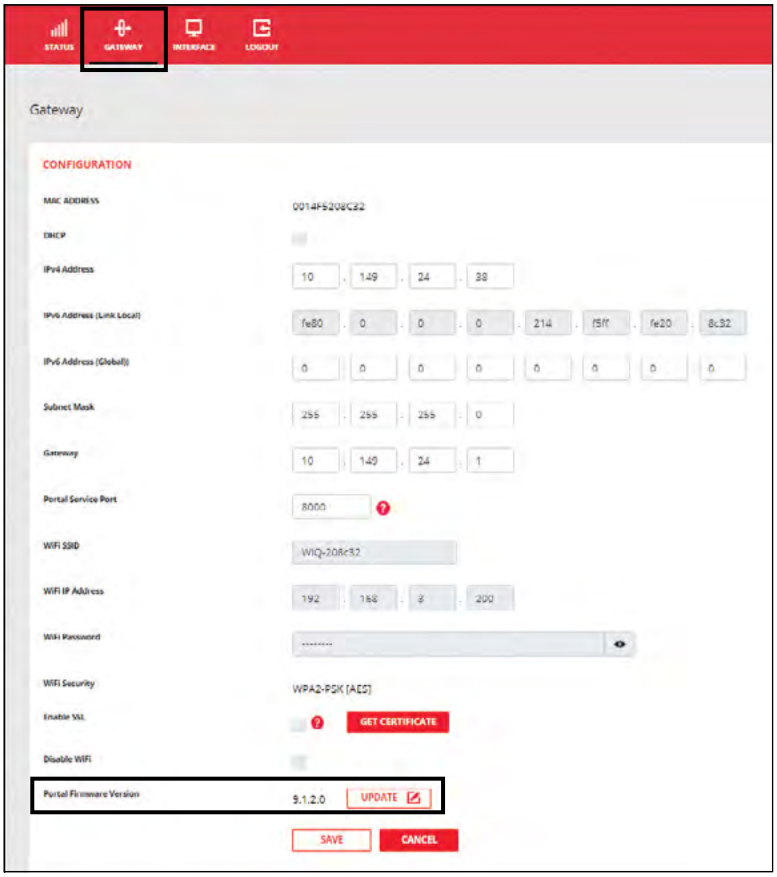
dormakaba.com. The file will be named with the following naming convention:

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 0014F5208C32

DHCP □

IPv4 Address 10 . 149 . 24 . 38

IPv6 Address (Link Local) fe80 . 0 . 0 . 0 . 214 . f5ff . fe20 . 8c32

IPv6 Address (Global) 0 0 0 0 0 0 0 0

Subnet Mask 255 . 255 . 255 . 0

Gateway 10 . 149 . 24 . 1

Portal Service Port 8000

WiFi SSID WIQ-208c32

WiFi IP Address 192 . 168 . 3 . 200

WiFi Password ---------

WiFi Security WPA2-PSK [AES]

Enable SSL □

Disable WiFi □

Portal Firmware Version 9.1.2.0

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.

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

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

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.

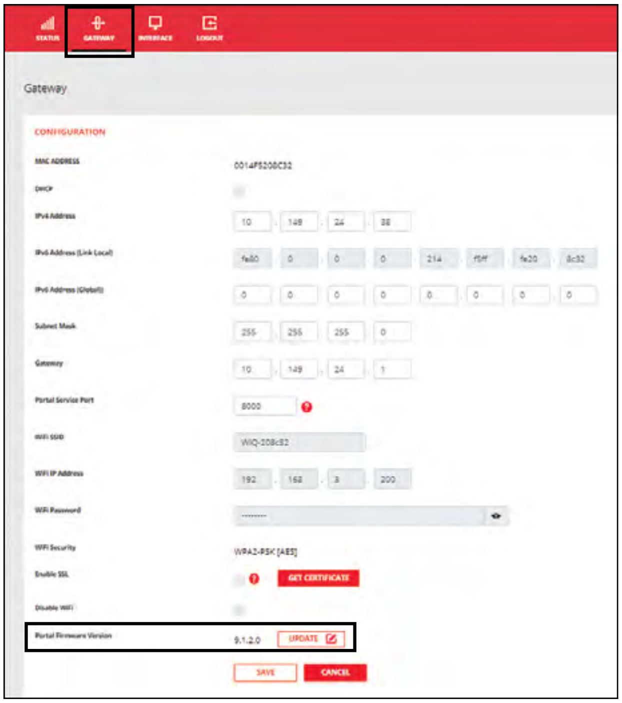
Update Portal Firmware

Occasionally it is necessary to upgrade the portal firmware. To upgrade the portal firmware, do the following:

1 Navigate to the Gateway menu option in the WQXM-PG webpage.

2 Click on the Update button towards the bottom of the Gateway page.

Figure 57 Gateway Configuration Page



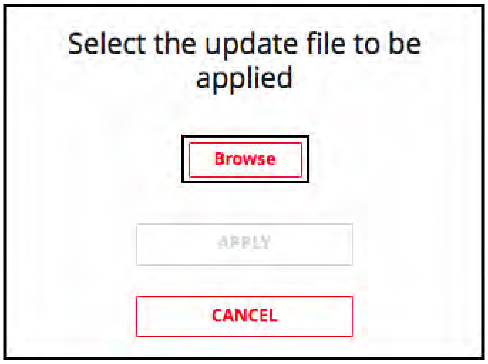
Gateway

CONFIGURATION

MAC ADDRESS	0014F5208C32
DHCP	□
IPv4 Address	10 . 149 . 24 . 38
IPv6 Address (Link Local)	fe80 : 0 : 0 : 0 : 214 : f5ff : fe20 : 8c32
IPv6 Address (Global)	0 : 0 : 0 : 0 : 0 : 0 : 0 : 0
Subnet Mask	255 . 255 . 255 . 0
Gateway	10 . 149 . 24 . 1
Portal Service Port	8000
WiFi SSID	WIQ-208c32
WiFi IP Address	192 . 168 . 3 . 200
WiFi Password	··········
WiFi Security	WPA2-PSK [AES]
Enable SSL	□ GET CERTIFICATE
Disable WiFi	□
Portal Firmware Version	9.1.2.0 UPDATE

3 In the firmware upgrade pop-up screen, click on the Browse button to browse to the firmware file.

Figure 58 Gateway Configuration Page



Select the update file to be applied

4 Browse to the previously extracted .gzhe portal firmware file and click the Open button to upload the file.

5 The selected file will be listed in the pop-up window. Verify it is correct and click the Apply button.

6 The firmware will be applied to the Gateway. The Gateway's LED will flash aqua when it downloads the firmware.

Reboot Gateway

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

1 Navigate to the Gateway menu option of the Gateway.

2 Scroll to the bottom of the screen.

3 Click the Reboot Gateway button.

4 A pop-up window will appear asking if you are sure you want to reboot the Gateway. Any changes made and that have not been saved will be lost. Click the Reset button to continue.

5 The Gateway will reboot immediately. During a reboot, the Gateway will flash purple. Once it reconnects to the ACS, the LED will display a solid green light.

Factory Reset the Gateway

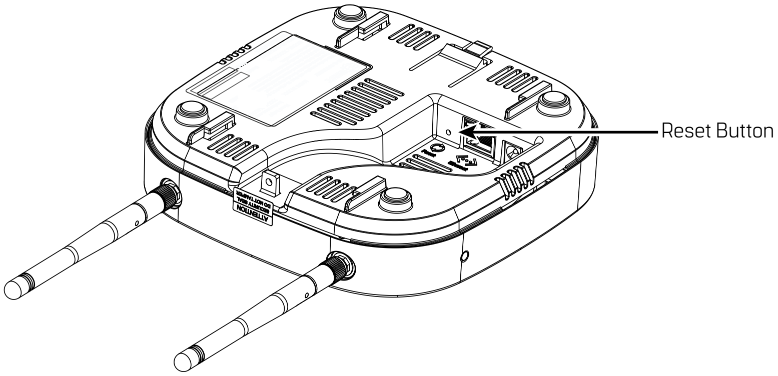
Occasionally, situations arise that require the Gateway to be reset back to factory default settings. To perform a factory reset, do the following:

1 Remove Gateway from enclosure or from the mounted location.

2 On the back of the Gateway locate the Deep Reset button next to the Ethernet inlet. The Deep Reset button
is a recessed button accessible from a pin hole. See
Figure 60.

3 Push and hold the Deep Reset button using a small implement such as a paper clip for more than 10 seconds.

Figure 59 Wi-Fi Reset Button



Interface Menu

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

Adding Wi-Q Gateways to AMS

Portals can be added to your system in two ways:

- Adding — normally use this method if the number of Wi-Q Gateways is manageable. This is a manual method that requires manual entry of the IP address of each Wi-Q Gateway.
- Bulk Importing — normally use this method for large systems. This is done through the System Administrator application through the Import Portals selection.

Adding Wi-Q Gateways One at a Time

1 In the Configurator application, click the Portals Tab.

2 Click Add and the Configure New Wi-Q Gateway screen opens.

3 In the Workstation field, select the location of your server.

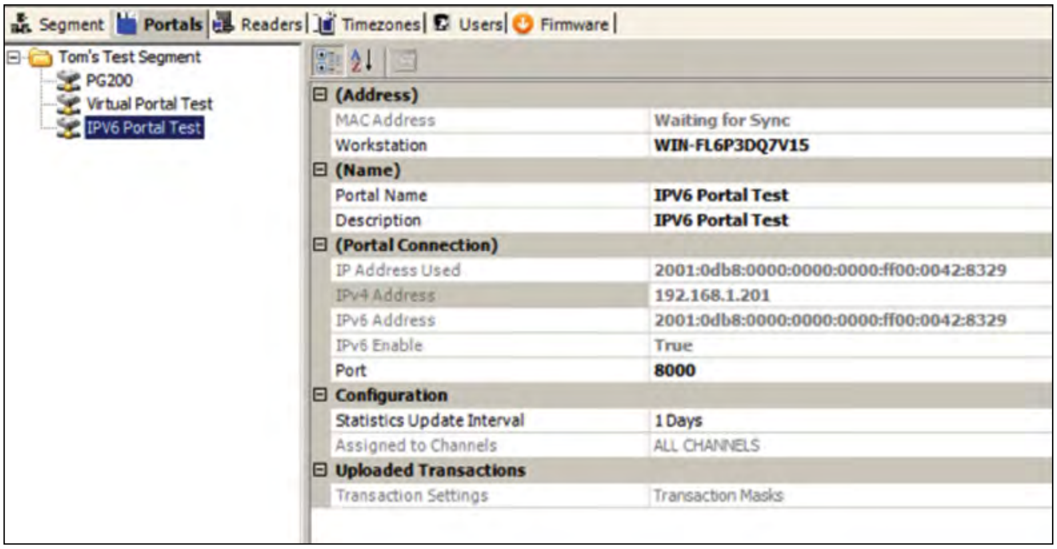
4 Enter the name and description of the Wi-Q Gateway.

Note Normally name Wi-Q Gateways by their location. For large systems, work out a naming scheme that makes it easy to locate the Wi-Q Gateway in your segment.

5 Enter the IP address of the Wi-Q Gateway. You will need to get IP addresses from your network administrator.

6 Enter the port.

Figure 60 Configure New Wi-Q Gateway screen



(Address)	
MAC Address	Waiting for Sync
Workstation	WIN-FL6P3DQ7V15
(Name)	
Portal Name	IPV6 Portal Test
Description	IPV6 Portal Test
(Portal Connection)	
IP Address Used	2001:0db8:0000:0000:0000:ff00:0042:8329
IPv4 Address	192.168.1.201
IPv6 Address	2001:0db8:0000:0000:0000:ff00:0042:8329
IPv6 Enable	True
Port	8000
Configuration	
Statistics Update Interval	1 Days
Assigned to Channels	ALL CHANNELS
Uploaded Transactions	
Transaction Settings	Transaction Masks

7 Click the ellipsis button next to the Channels field and select at least two channels that the Wi-Q Gateway will use to communicate. Check with your network administrator to make sure the channels are available.Click the ellipsis button next to the Update Interval field. Here you can set how often the system will update the Wi-Q Gateway with changes you've made to users, readers, timezones, and other functional changes to the database.

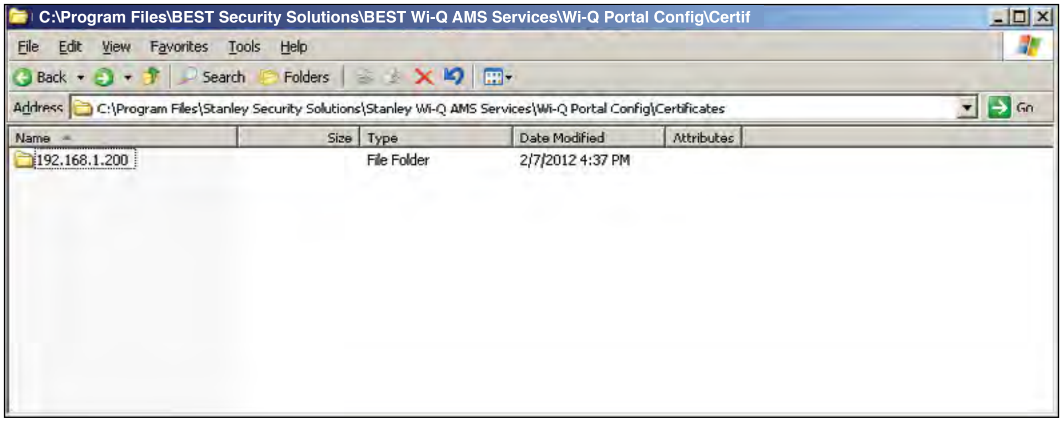
8 Click the ellipsis button next to the Transactions field to select which, if any, Wi-Q Gateway transactions you want to enable and which you want to make a priority. Priority transactions will be uploaded immediately rather than waiting for the next update interval that was set in the field above. Two transactions are available:

- Portal Firmware Update
- Portal Radio Start Failed

If you click on Select All, a dialog box window will ask you to confirm your choice and it will also ask if you would like to enable priorities as well.

9 If you generated SSL certificates within the Portal Configuration module, you may browse to your Wi-Q Gateway's certificate by clicking on the ellipsis button next to the SSL Certificate field. The Certificate can be found in your Program Files in the following location: C:\Program Files X68>Best Access>Wi-Q Portal Config>Certificates. The file is located within a folder named for the Wi-Q Gateway's IP address. Select the file with the .pfx extension, and click Open.

Figure 61 Path to Certificate File



C:\Program Files\BEST Security Solutions\BEST Wi-Q AMS Services\Wi-Q Portal Config\Certif

Address: C:\Program Files\Stanley Security Solutions\Stanley Wi-Q AMS Services\Wi-Q Portal Config\Certificates

Name	Size	Type	Date Modified	Attributes
192.168.1.200		File Folder	2/7/2012 4:37 PM	

10 Click Finish.

The Portal(s) you have added will now be visible in the Segment Tree. See "Viewing the Segment Tree" on page 96. You can check the operational status of your Portal(s) by clicking on the top folder within your Segment Tree.

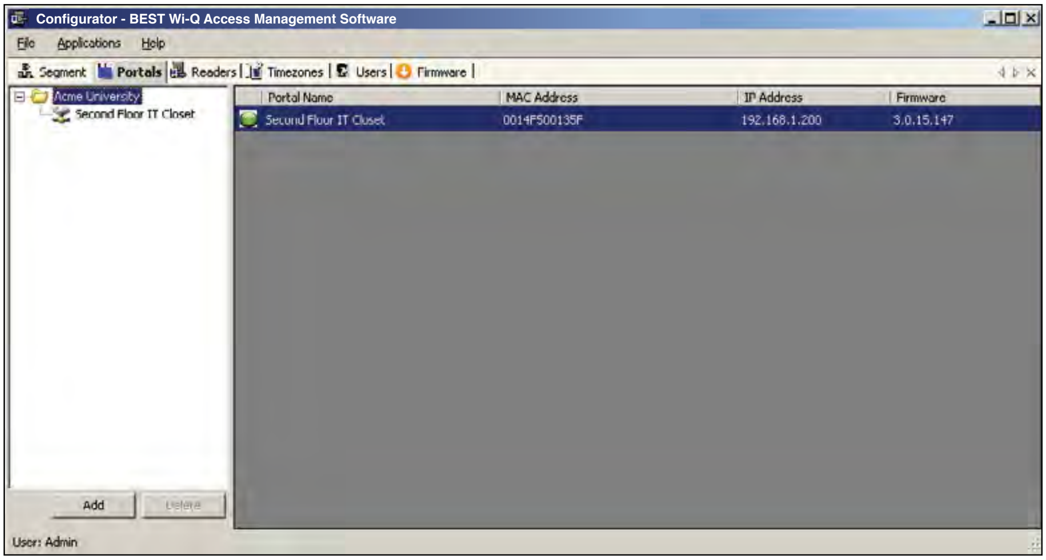
Wi-Q Gateway Operational Status

When you are on the Portals tab within the Configurator module, you can click on the top folder within your Segment Tree, and the right side of the screen will change to a list of Portals in your system. The icon next to each Portal will give you the Portal's operational status. Five different status icons are present in the system for Wi-Q Gateways:

Icon	Name	Description
?	Question Mark	Device is loading.
●	Green Circle	Device is online.
❌	Red X	Device is offline.
⬇	Blue Down Arrow	Wi-Q Gateway or Controller is not assigned to a workstation or the workstation is not running.
🚫	Out-of-Date Firmware	Incompatible or Out-of-Date Firmware, all features may not be supported

If your Wi-Q Gateways have blue down arrow icons, restart your Communication Server. See “Restarting your Communication Server”. After you restart your Communication Server, your Wi-Q Gateway status icons should change to green circles, indicating that the devices are online. See Figure 62.

Figure 62 Wi-Q Gateway with Green Circle Icon

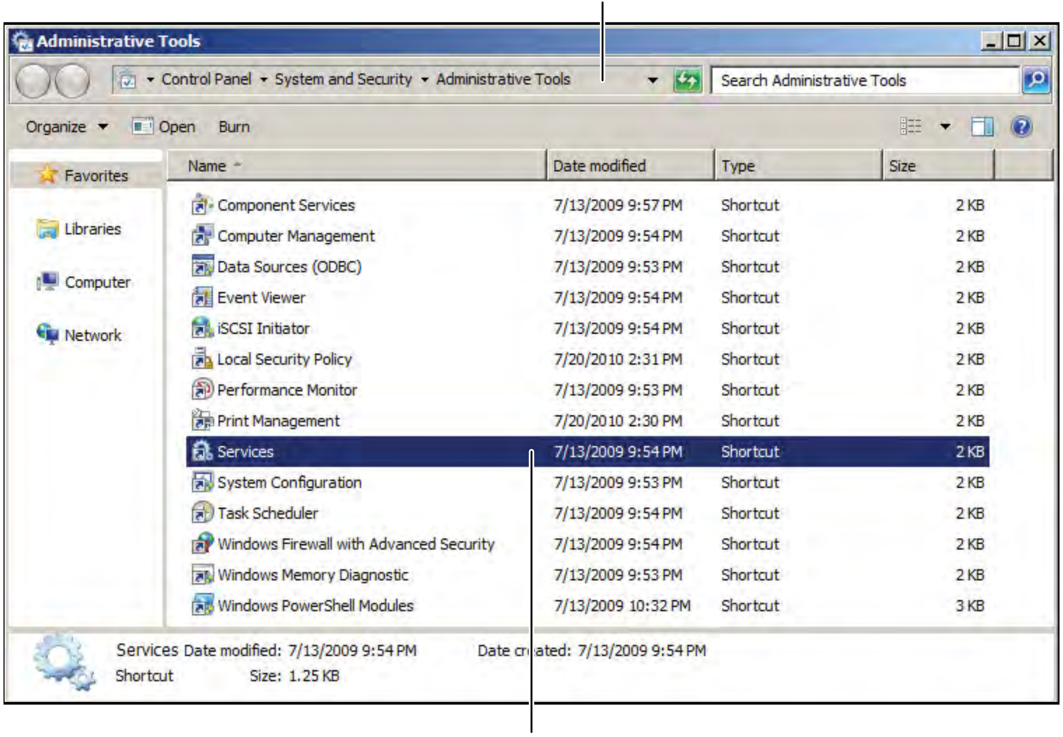


Portal Name	MAC Address	IP Address	Firmware
🟩 Second Floor IT Closet	0014F500135F	192.168.1.200	3.0.15.147

Restarting your Communication Server

If you need to restart your Communication Server, navigate to your system's Services via Administration Tools. See Figure 63.

Figure 63 Navigate to Services


Administrative Tools
Control Panel ▸ System and Security ▸ Administrative Tools
Search Administrative Tools
Organize
Open
Burn
Favorites
Libraries
Computer
Network

Name	Date modified	Type	Size
Component Services	7/13/2009 9:57 PM	Shortcut	2 KB
Computer Management	7/13/2009 9:54 PM	Shortcut	2 KB
Data Sources (ODBC)	7/13/2009 9:53 PM	Shortcut	2 KB
Event Viewer	7/13/2009 9:54 PM	Shortcut	2 KB
iSCSI Initiator	7/13/2009 9:54 PM	Shortcut	2 KB
Local Security Policy	7/20/2010 2:31 PM	Shortcut	2 KB
Performance Monitor	7/13/2009 9:53 PM	Shortcut	2 KB
Print Management	7/20/2010 2:30 PM	Shortcut	2 KB
Services	7/13/2009 9:54 PM	Shortcut	2 KB
System Configuration	7/13/2009 9:53 PM	Shortcut	2 KB
Task Scheduler	7/13/2009 9:54 PM	Shortcut	2 KB
Windows Firewall with Advanced Security	7/13/2009 9:54 PM	Shortcut	2 KB
Windows Memory Diagnostic	7/13/2009 9:53 PM	Shortcut	2 KB
Windows PowerShell Modules	7/13/2009 10:32 PM	Shortcut	3 KB

Services Date modified: 7/13/2009 9:54 PM Date created: 7/13/2009 9:54 PM
Shortcut Size: 1.25 KB

Navigate to Administrative Tools

Click to Open Services

Next, locate "Wi-Q Communication Service" in the list of services. Right-click on the line and select Restart.

Importing Wi-Q Gateways in Bulk

Before you can import Wi-Q Gateways in bulk, you must generate an XML bulk import file using the Portal Configuration module.

Generating an XML Bulk Import File

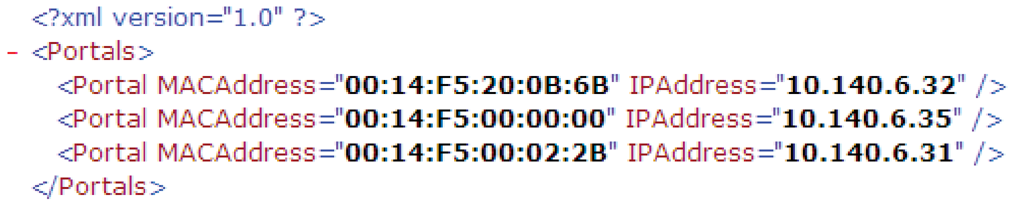
The XML file you will generate documents and cross-references Wi-Q Gateways' Mac addresses and IP addresses. Perform the following steps inside the Portal Configuration module.

1 Select all the Portals you wish to add to your AMS software using Select All button.

2 Click on Export Portal IP Configurations (See Figure 47).

3 Choose a location to save your XML file, and click Save. Figure 64 shows a sample XML file.

Figure 64 Sample XML file



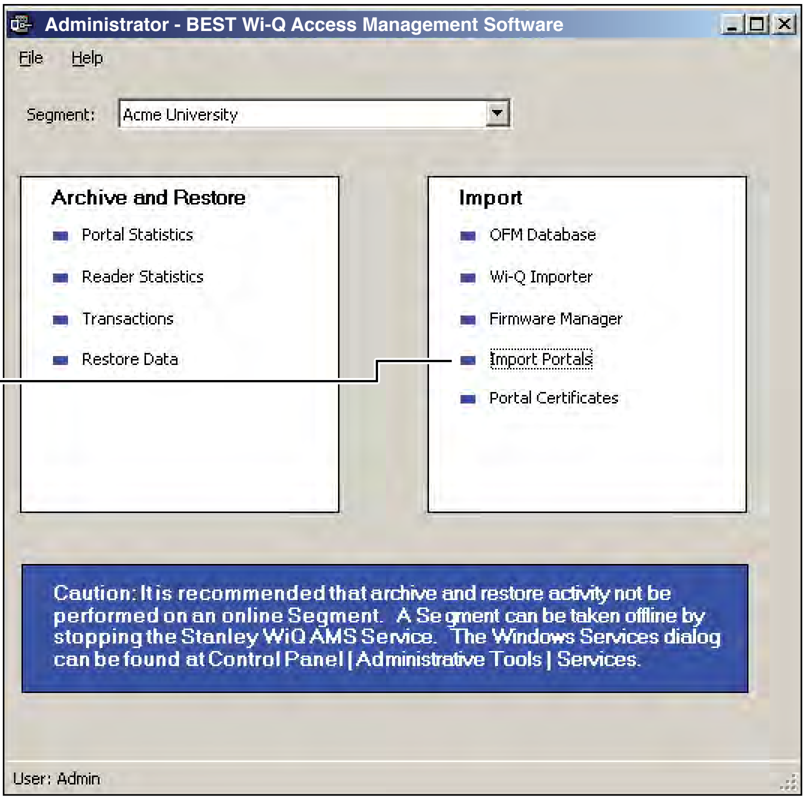
```
  <?xml version="1.0" ?>
- <Portals>
    <Portal MACAddress="00:14:F5:20:0B:6B" IPAddress="10.140.6.32" />
    <Portal MACAddress="00:14:F5:00:00:00" IPAddress="10.140.6.35" />
    <Portal MACAddress="00:14:F5:00:02:2B" IPAddress="10.140.6.31" />
  </Portals>
```

Once you have generated your XML bulk import file, perform the following steps.

1 Start the System Administrator module (Applications dropdown menu inside Configurator).

2 Click the Import Portals link from the Import pane. See Figure 65.

Figure 65 System Administrator Wi-Q Gateway Import



Caution: It is recommended that archive and restore activity not be performed on an online Segment. A Segment can be taken offline by stopping the Stanley WiQ AMS Service. The Windows Services dialog can be found at Control Panel | Administrative Tools | Services.

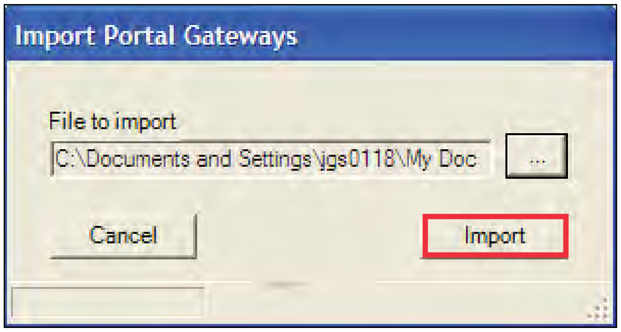
Click the Import Portals Link

3 The Import Wi-Q Gateways dialog displays.

4 Click the ellipsis button and locate the bulk import XML file.

5 Click Open.

Figure 66 Import Wi-Q Gateways



File to import: C:\Documents and Settings\jgs0118\My Doc

6 Click Import.

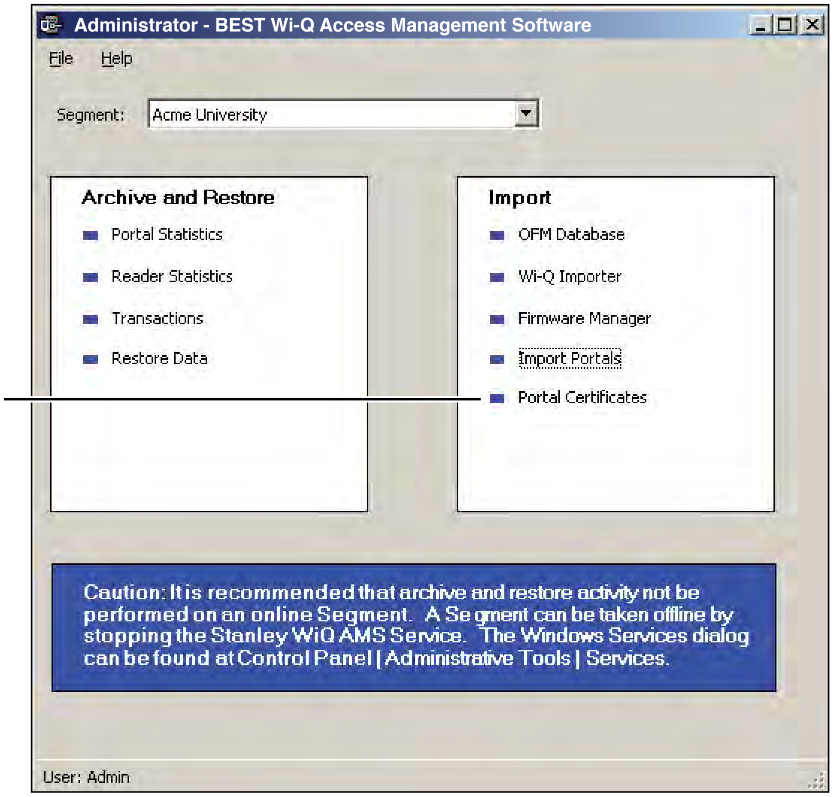
Note The Portals are imported (or updated) and a results box details the import. Workstation needs to be allocated and the MAC addresses should automatically show up in Wi-Q Gateways' properties.

Importing Portal SSL Certificates

If you previously generated SSL certificates for your Wi-Q Gateways, you may import them now. Perform the following steps.

1 From the System Administrator application, click the Portal Certificates link under the Import pane. See Figure 67.

Figure 67 System Administrator Portal Certificates link



Caution: It is recommended that archive and restore activity not be performed on an online Segment. A Segment can be taken offline by stopping the Stanley WiQ AMS Service. The Windows Services dialog can be found at Control Panel | Administrative Tools | Services.

Click the Portal Certificates Link

2 Choose the Wi-Q Gateway that you want to import an SSL certificate to and click the ellipsis button next to it. Then find the certificate file in the the Certificates folder in the following location C:\Program Files X86>Best Access >Wi-Q Portal Config.

3 When finished with importing all the Wi-Q Gateway SSL certificates, click Finish.

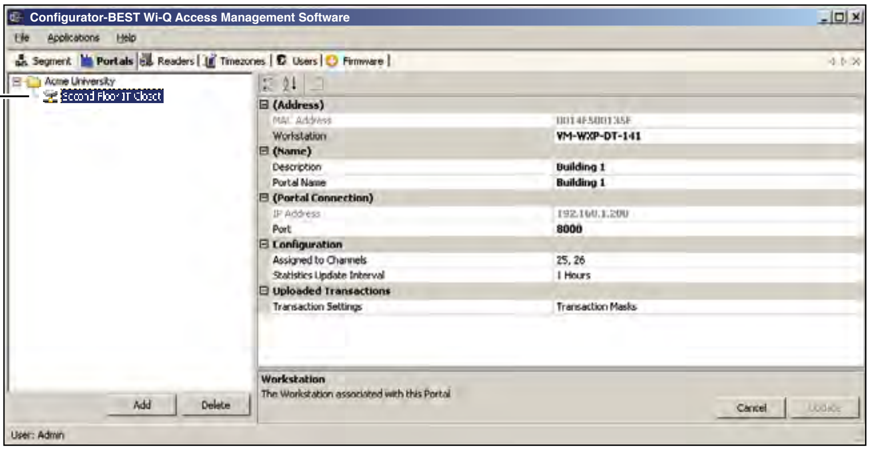
The Portals you have added will now be visible in the Segment Tree. See “Viewing the Segment Tree”. You may now check the operational status of your Wi-Q Gateways. See “The Portal(s) you have added will now be visible in the Segment Tree. See “Viewing the Segment Tree” on . You can check the operational status of your Portal(s) by clicking on the top folder within your Segment Tree.

Viewing the Segment Tree

The Segment Tree is a visual representation of the locations and associations of the Wi-Q Gateways, associated Controllers and I/O devices in your segment. As you configure your Wi-Q Gateways, sign on Controllers and configure additional hardware in your system, you can drag them to the folders and subfolders you create in the Segment Tree.

Figure 68 shows an example Wi-Q Gateway in the Segment Tree.

Figure 68 Wi-Q Gateway visible in Segment Tree



Portal Gateway in Segment Tree

(Address)	
MAC Address	0014F500135F
Workstation	VM-WXP-DT-141
(Name)	
Description	Building 1
Portal Name	Building 1
(Portal Connection)	
IP Address	192.160.1.200
Port	8000
Configuration	
Assigned to Channels	25, 26
Statistics Update Interval	1 Hours
Uploaded Transactions	
Transaction Settings	Transaction Masks

Workstation
The Workstation associated with this Portal

To view the Segment Tree

1 In the Segment tab, select the segment you wish to work with.

2 Click on the Portals tab. The Segment Tree pane displays on the left, and a list of all prepared devices displays on the right. The first item in the Segment Tree is the folder for the selected segment, in this case, Acme University.

The Segment Tree is also viewable from within the Readers tab. See "Adding Controllers to the Segment Tree".

Organizing your Segment Tree

You can organize your Segment Tree by Portals and Controllers, or by building locations, or by any other method you prefer. Remember, the Segment Tree is provided as a visual aid and does not affect the actual hardware or communication to the devices.

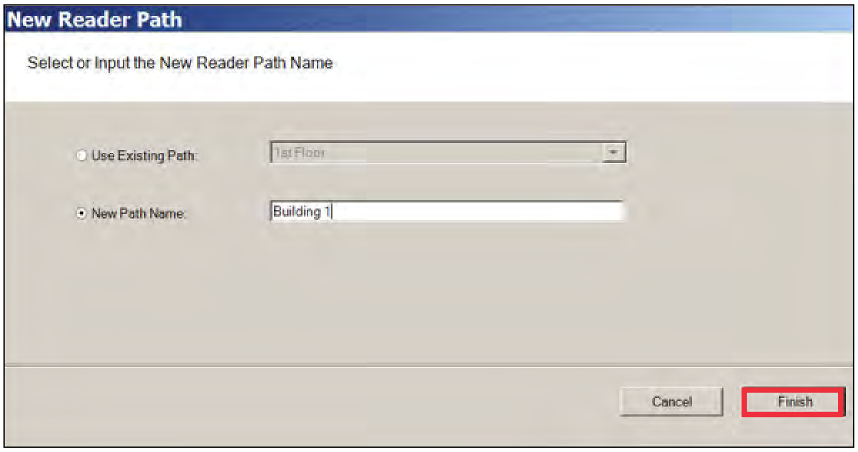
The first level below the Segment level in the tree might contain, for example, folders for Portals and Controllers, or folders for building locations. You can create sub-items in each folder as needed, for example, First Floor, Second Floor, offices, laboratories, and so on. There is no specific protocol for creating the hierarchy; only that it makes sense to your operation so that when you add other elements to the system, you can easily locate the Controllers to be assigned. Once you create Segment folders of your own, you can move your Portals to the appropriate folders.

Note To delete a folder, you must already have moved any devices in that folder to a different location.

To create a new segment item folder

1 Right-click on the parent folder and select New Path from the drop-down list. The New Reader Path dialog box opens.

Figure 69 Defining a New Reader Path



New Reader Path

Select or Input the New Reader Path Name

○ Use Existing Path: 1st Floor

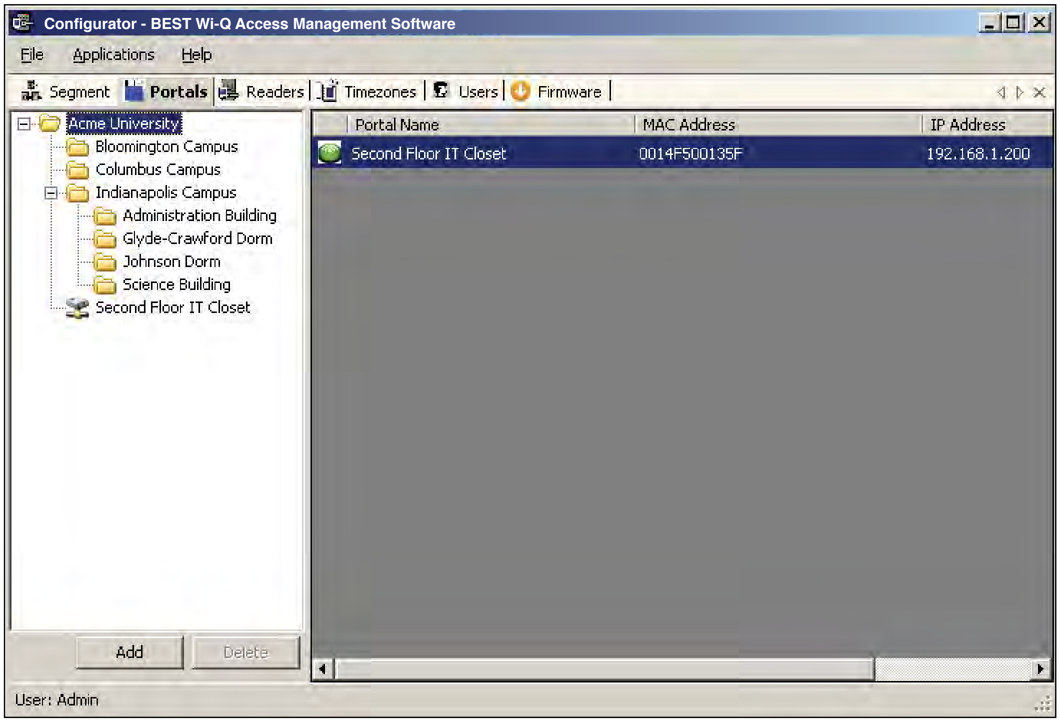
● New Path Name: Building 1

Select New Path Name and enter a name

2 Select New Path Name and enter the name.

3 Select Finish. The new path folder is added to the Segment Tree. Repeat the process to create the folders needed to define your Segment Tree. Figure 70 shows a Segment Tree with several added folders and sub-folders.

Figure 70 Folders and Sub-Folders in the Segment Tree



- Acme University
  - Bloomington Campus
  - Columbus Campus
  - Indianapolis Campus
    - Administration Building
    - Glyde-Crawford Dorm
    - Johnson Dorm
    - Science Building
  - Second Floor IT Closet

Portal Name	MAC Address	IP Address
Second Floor IT Closet	0014F500135F	192.168.1.200

Moving Wi-Q Gateways within the Segment Tree

Once you have created the Segment Tree with folders and sub-folders, you can move Wi-Q Gateways into the appropriate folders.

Click on the Portals tab. Select the desired Wi-Q Gateway from within the Segment Tree and drag it to the desired folder.

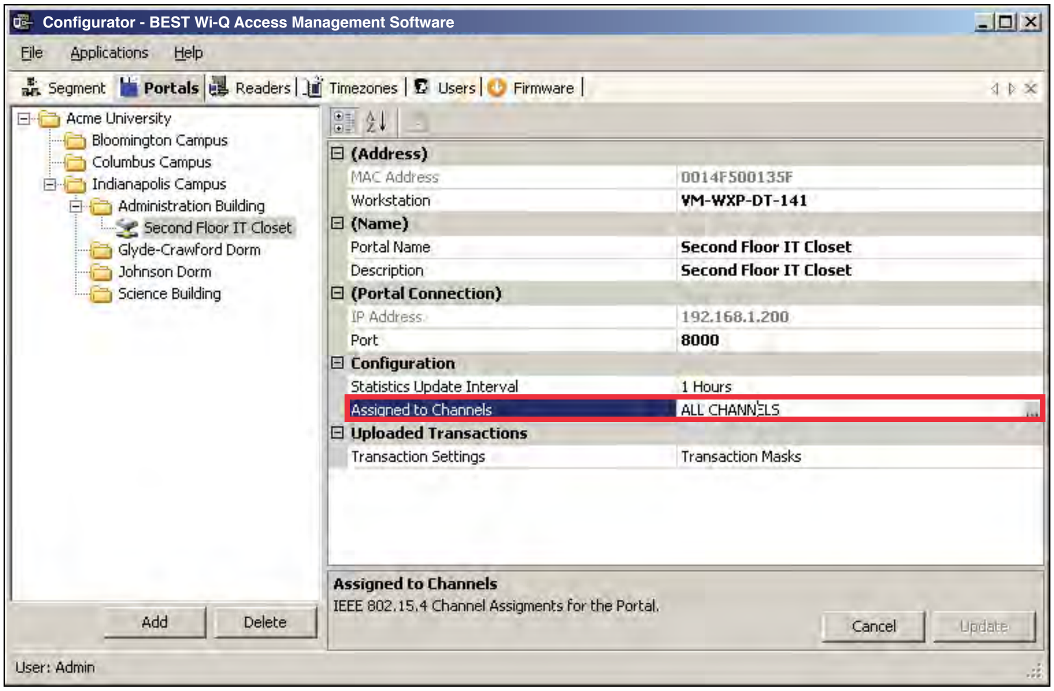
Assign Portal Channels

Wi-Q Gateways default to All Channels; however, you can assign specific channels if needed. For example, if you have configured a new wireless component to operate on channel 17, you will want to disable channel 17 in the Portal channel configuration.

To assign Portal channels

1 Click on the Portal tab, and select the desired Portal from the Segment Tree. Clicking on a Portal will display Portal properties on the left.

Figure 71 Portal Properties



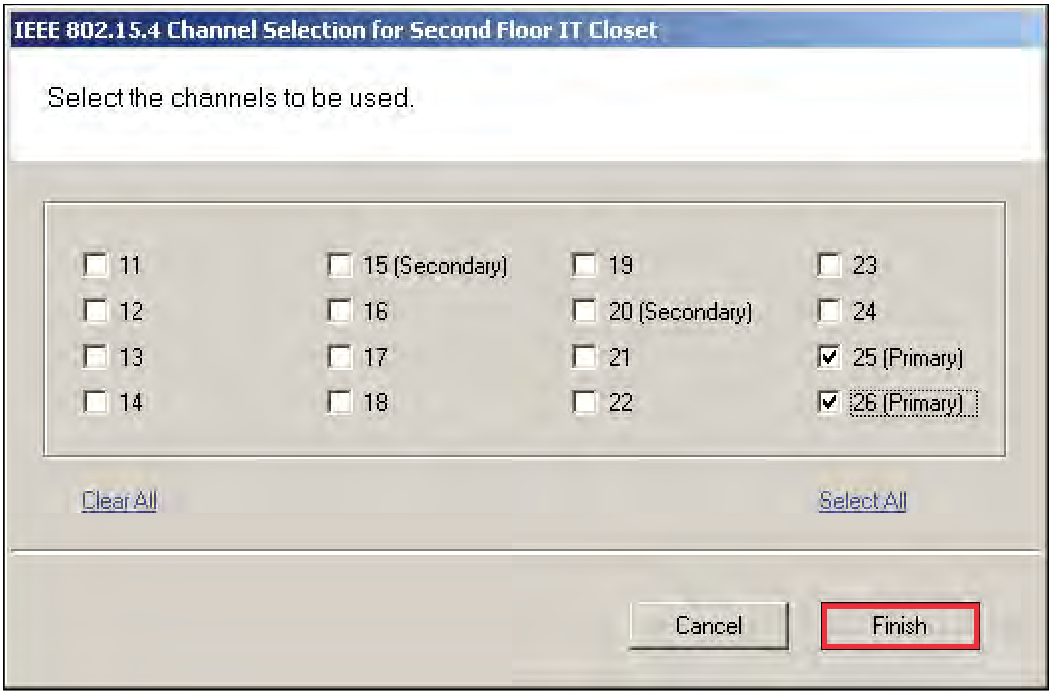
- Acme University
  - Bloomington Campus
  - Columbus Campus
  - Indianapolis Campus
    - Administration Building
      - Second Floor IT Closet
    - Glyde-Crawford Dorm
    - Johnson Dorm
    - Science Building

(Address)	
MAC Address	0014F500135F
Workstation	VM-WXP-DT-141
(Name)	
Portal Name	Second Floor IT Closet
Description	Second Floor IT Closet
(Portal Connection)	
IP Address	192.168.1.200
Port	8000
Configuration	
Statistics Update Interval	1 Hours
Assigned to Channels	ALL CHANNELS
Uploaded Transactions	
Transaction Settings	Transaction Masks

Assigned to Channels
IEEE 802.15.4 Channel Assigments for the Portal.

2 Under the Configuration category, click in the Assigned to Channels field. The ellipsis button appears at the far right of the field. Click the ellipsis button to open the Channel Selection window.

Figure 72 Portal Channel Selection



IEEE 802.15.4 Channel Selection for Second Floor IT Closet

Select the channels to be used.

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

3 Enable or disable channels as needed (at least one channel must be selected).

4 Click Finish to save your settings.

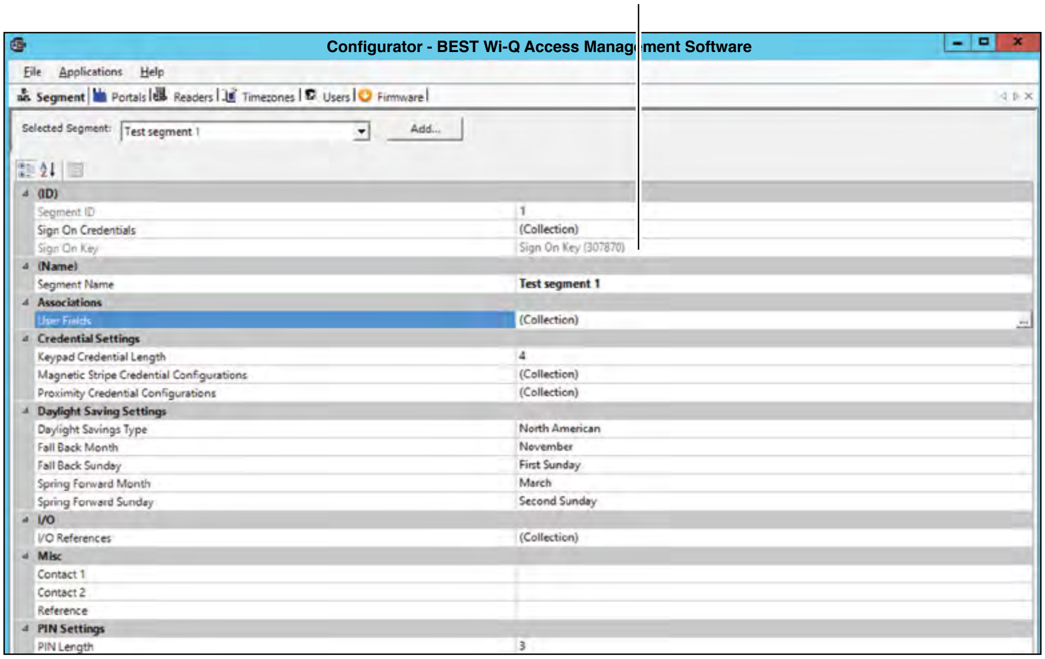
Note Wi-Q devices are designed to coexist with Wi-Fi, but for optimal operation you may want to use non-overlapping channels for Wi-Q and your corporate Wi-Fi. Recommended channels are 15 and 20 if your Wi-Fi is only using CH1, CH6, or CH11. If Wi-Fi channels are unknown, then Wi-Q CH25 and CH26 are the only channels that do not overlap with Wi-Fi.

Sign on and Configure Controllers (Task 10)

Each segment created in AMS is assigned a discrete Sign On Key number. Select a segment and you will find this number in the ID Category of the Configurator module's Segment Tab.

Figure 73 Signing on readers from the Segment tab

Sign On Key



Selected Segment: Test segment 1

(ID)	
Segment ID	1
Sign On Credentials	(Collection)
Sign On Key	Sign On Key (307870)
(Name)	
Segment Name	**Test segment 1**
Associations	
User Fields	(Collection)
Credential Settings	
Keypad Credential Length	4
Magnetic Stripe Credential Configurations	(Collection)
Proximity Credential Configurations	(Collection)
Daylight Saving Settings	
Daylight Savings Type	North American
Fall Back Month	November
Fall Back Sunday	First Sunday
Spring Forward Month	March
Spring Forward Sunday	Second Sunday
I/O	
I/O References	(Collection)
Misc	
Contact 1	
Contact 2	
Reference	
PIN Settings	
PIN Length	3

If your segment uses Controllers with keypads, you must enter this number at each Controller to establish connection between the Controllers and the Portals, and ultimately to a segment in the software. If you use card readers, you can create a sign-on card to use at each reader. Either way, you must sign on each Controller in the system to register them in the database and ultimately establish communication with the software.

Note Readers associated with Single Door Controllers are configured, signed on, and monitored in Wi-Q AMS exactly like any other networked keypad Controller in the system.

Signing on Keypad Controllers

If your segment uses keypad Controllers, use the following steps, in sequence, to register each Controller in the system. Once this is done, the readers will appear in the <New Segment Items> folder, viewable in the Readers tab Segment Tree.

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

1. At a keypad Controller, press the following number sequence on the keypad: 5678# (Wi-Q) or 5678 (Omnilock and WAC). The green light will flash three times.
2. Within five or six seconds, begin to enter the six-digit segment sign on key number, followed by #. You will have about five seconds to enter each number. The sequence will time out if more than five seconds elapses between numbers.
3. Once the key number is completed, the reader begins to alternately flash green and red to signify that it is searching for Wi-Q Gateways in range. If the sequence was completed successfully, three green flashes indicate the Controller has accepted the sign on key.
4. If you see three red flashes, the Controller has not accepted the number or you have exceeded the time limit. Begin again at step two, and continue until you receive three green flashes.

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

Signing on Card Readers

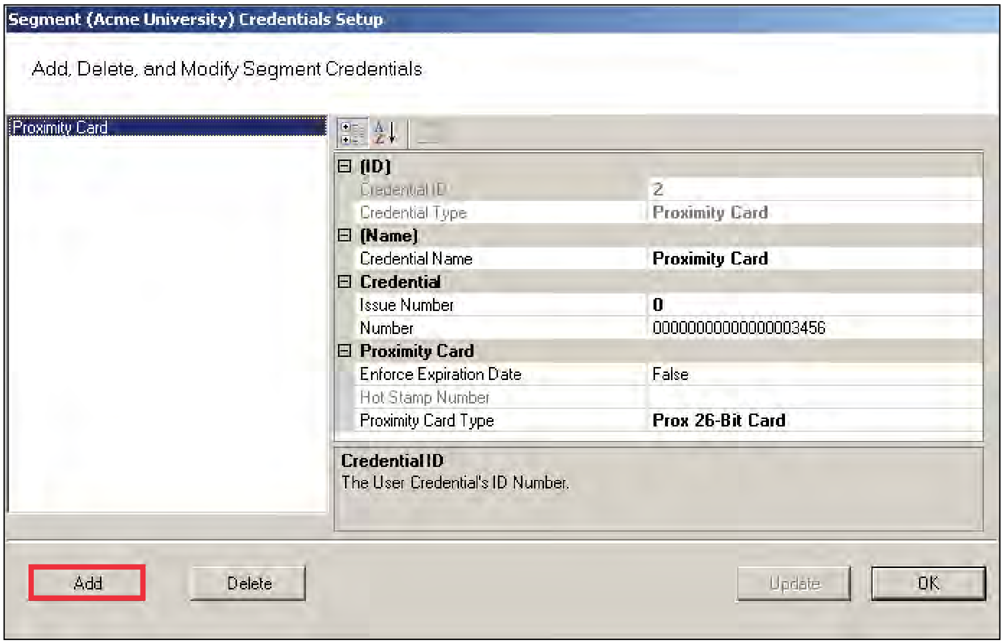
If your segment uses card readers, you may want to register one of your cards with a segment credential number. This card will be used to sign on card readers to the system. You can register a separate card and hold it specifically for this purpose, or register one that belongs to a user such as the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

To register a card with a segment credential

1 In the Configurator's Segment tab, select the segment to which the readers belong.

2 In the ID Category, click in the Sign On Credentials field and select the ellipsis button at the far right of the field. The Segment Credentials Setup property sheet opens.

Figure 74 Segment Credentials Setup



Segment (Acme University) Credentials Setup

Add, Delete, and Modify Segment Credentials

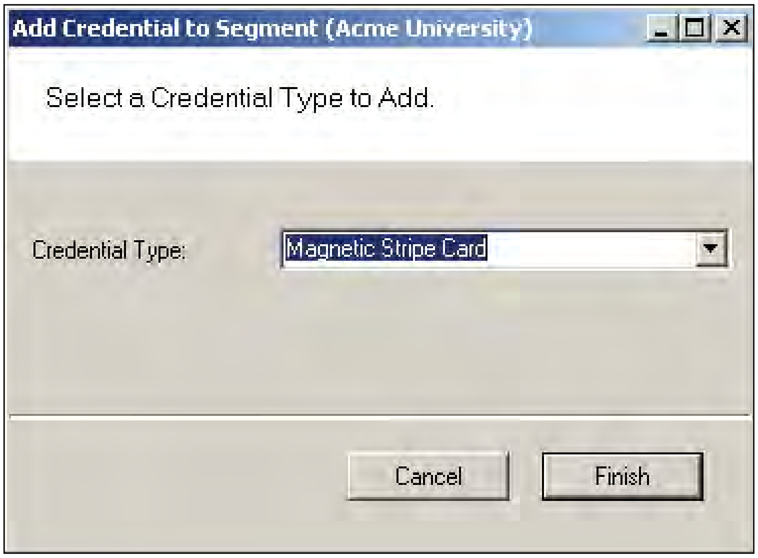
Proximity Card

(ID)	
Credential ID	2
Credential Type	Proximity Card
(Name)	
Credential Name	**Proximity Card**
Credential	
Issue Number	**0**
Number	00000000000000003456
Proximity Card	
Enforce Expiration Date	False
Hot Stamp Number	
Proximity Card Type	**Prox 26-Bit Card**

Credential ID
The User Credential's ID Number.

3 Select the type of card you will use. If your card type is not listed, select Add. The Add Credential to Segment dialog box opens.

Figure 75 Add Credential to Segment



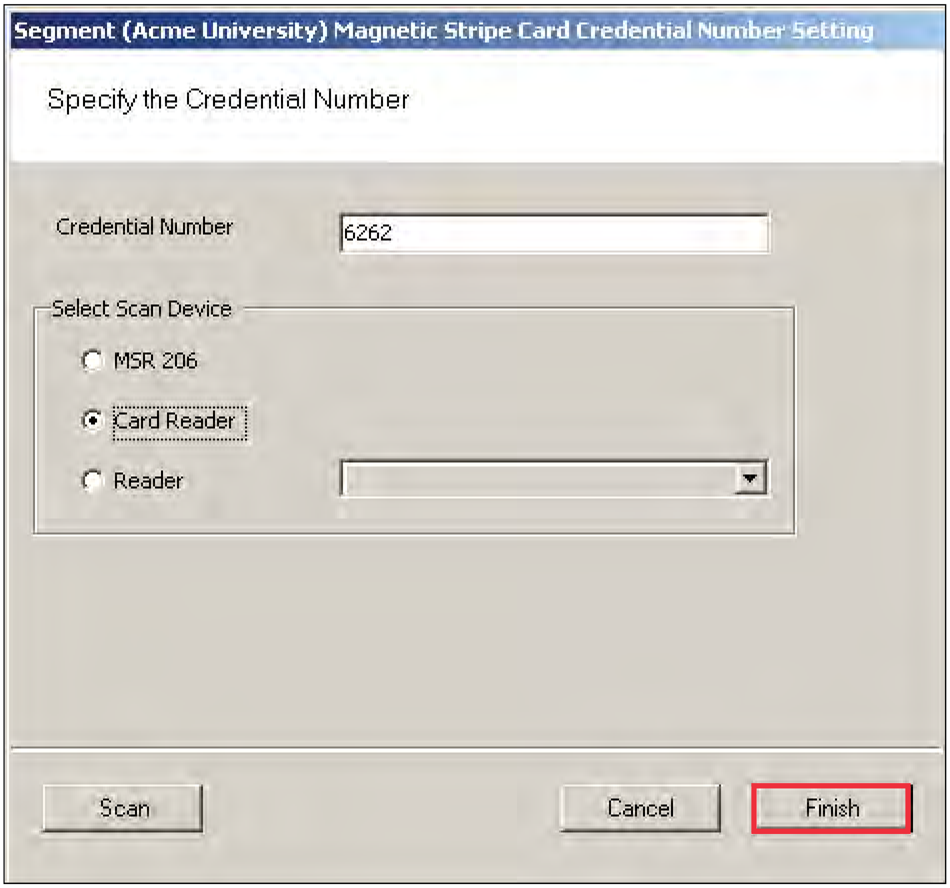
Add Credential to Segment (Acme University)

Select a Credential Type to Add.

Credential Type: Magnetic Stripe Card

4 Select the card type from the drop-down list, in this case, Magnetic Card. The Segment (Magnetic) Card Credential Number Setting dialog box opens.

Figure 76 MAG Card Settings



Segment (Acme University) Magnetic Stripe Card Credential Number Setting

Specify the Credential Number

Credential Number: 6262

Select Scan Device

○ MSR 206

● Card Reader

○ Reader

5 You can enter the card's 16-digit credential number manually; or, you can scan the card at a local scanning wedge, or select a reader where the card will be scanned.

To Scan a card locally, select Card Reader and Select Scan. You will have about 30 seconds from the time you select Scan to actually scan the card through a reader.

To Scan at a reader, select Reader and select the reader from the drop-down list to scan at from the drop-down list, then select Scan. You will have about 30 seconds from the time you select Scan to actually scan the card through a reader (this option is available only if the reader has been signed on).

6 Select Finish to save your settings and return to the Segment Credentials Setup dialog box, or Cancel if you decide not to create the number. The number appears in the Credential Number category and the card is now registered. If you will use a Prox card, see the following additional steps to complete registration.

Completing the Credential for a Prox card

1 Under the Proximity Card category, Enforce Expiration Date, select True or False, depending on your preference. If you select true, you will need to register a new card when the expiration date occurs. If False, the card will not expire.

2 Under Proximity Card Type, select the type of encryption the card uses from the dropdown menu.

3 Select Finish. Once this is done, you can use this card to sign on card readers.

To sign on card readers

1 At each card reader, scan the card you registered with the segment credential.

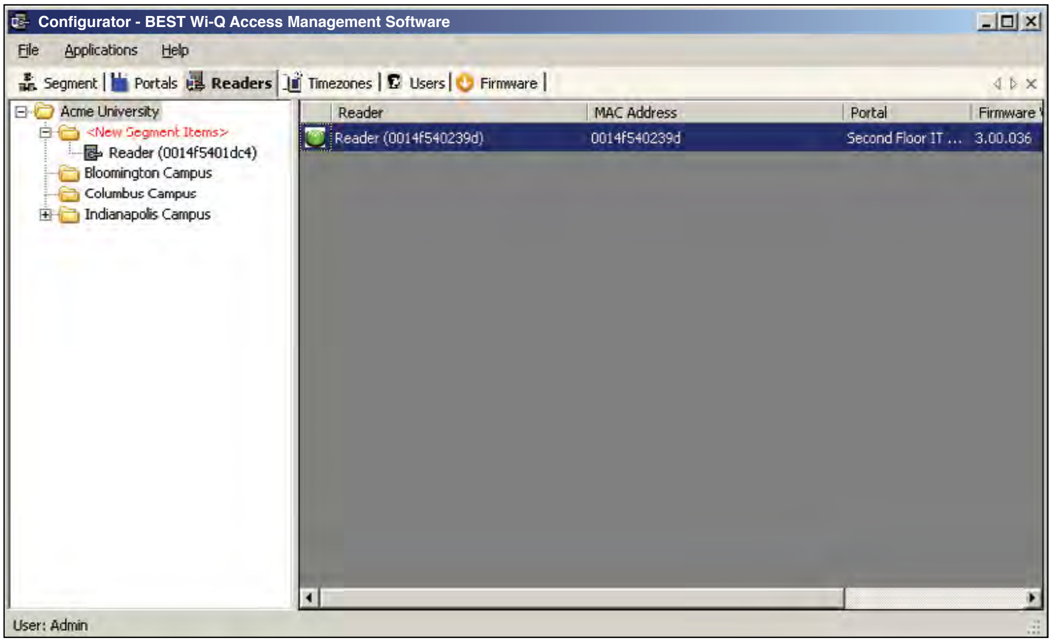
2 Once this is done, the readers will appear in the <New Segment Items> folder, viewable in the Readers tab Segment Tree.

Note Once a reader has been signed on, all sign-on functionality is disabled, that is, removed from the database. If you wish to use the reader in a different capacity, that will require a new sign on. You will need to perform a reset to restore its sign on capability.

Adding Controllers to the Segment Tree

Within 1 to 2 minutes after you sign on a controller, it will appear in the Configurator <New Segment Items> folder, viewable in the Readers tab. The folder will appear in red to indicate that it has received new Controllers. See Figure 77.

Figure 77 <New Segment Items>



Reader	MAC Address	Portal	Firmware
Reader (0014f540239d)	0014f540239d	Second Floor IT ...	3.00.036

User: Admin

You can move new Controllers into sub-folders within the Segment Tree by dragging them to the desired location. When all new Controllers have been assigned to segment folders, the <New Segment Items> folder will be empty and the display color will change from red to black. You can move segment sub-folders to different locations in the tree and the Controllers within will move with them.

If you expand your segment by adding new Controllers, the new Controllers will appear again in the red <New Segment Items> folder so that they can be assigned a location in the Segment Tree.

When you first configure a Controller, you will have the option to configure a new Controller or copy parameters from one that has already been configured.

Copying Reader Parameters

The Copy Reader Parameters feature is useful when you have more than one reader that serves the same users and user groups or will be assigned a special Timezone Group. This feature is available when you first bring a Controller from the <New Segment Items> folder to the Segment Tree, and as a right-mouse-click copy function. It makes sense then that if you are going to use this feature you will want to configure the Users and User Groups before configuring the readers. See "User Groups" on page 119 and "Adding Users to the Segment" on page 137 for steps to create these parameters.

Configuring New Controllers

When you create a new Controller, its name is displayed in the Reader Properties section on the right, and it is automatically assigned to the Master Timezone. Users, User Groups, and Timezone Groups will be available to the Controllers only if they have already been configured. If not, you can configure the Controllers first with default parameters and return to assign Users, User Groups and any Timezone Groups after they are created.

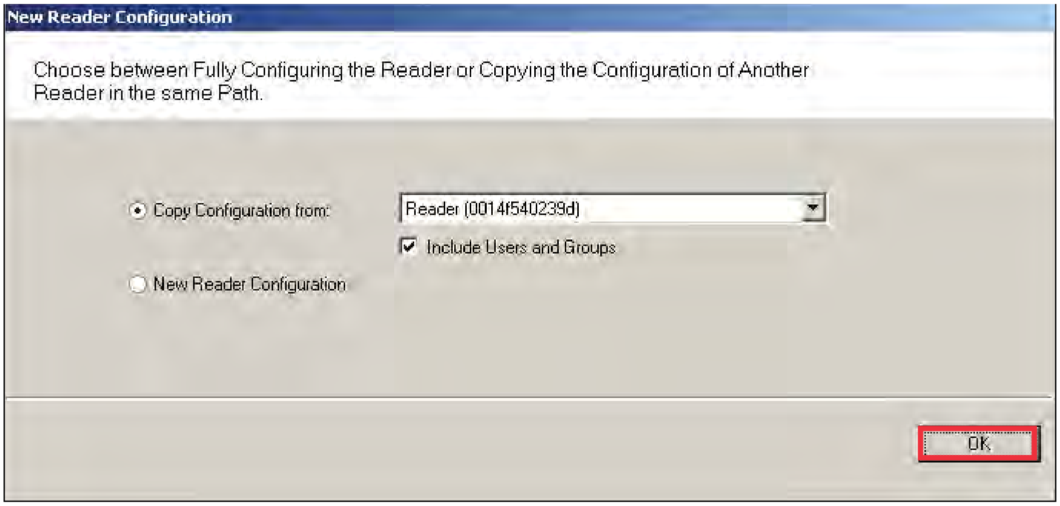
To configure a new Controller

1. Drag your Controller out of the <New Segment Items> folder and into your desired subfolder in the Segment Tree.
2. If you are configuring your first controller, select the Controller within the tree, and the Reader Properties sheet will show on the right.

   If you have signed on more than one Controller into your segment, a window will open to ask if you would like to copy a configuration from another reader or create a new configuration. See Figure 78.

   If you select Copy Configuration from, you can choose a reader in the dropdown list from which to copy configuration settings.

Figure 78 New Reader Configuration



New Reader Configuration

Choose between Fully Configuring the Reader or Copying the Configuration of Another Reader in the same Path.

● Copy Configuration from: Reader (0014f540239d)

☑ Include Users and Groups

○ New Reader Configuration

When you have made your selection, click OK. If you are copying reader properties, a window will open asking if you would like to proceed. Click Yes to proceed.

Field Category Definitions

The following is a list of Reader property field categories and their functions.

Reader Name —The Reader name displays automatically. You may change it by typing over the default name.

Associations —If you have already configured User Groups and Users, you can assign them to the readers now. If you have not yet configured these parameters, or don’t wish to do it now, you can come back later to add these settings.

Configuration —Under the Configuration category, you can configure various reader settings, such as default settings for Channels, Beacon Time, Operate and Shunt times, and add delays depending on how the reader will be used.

Assigned to Channels — New readers default to All Channels; however, you can assign specific channels if needed. For example, if an existing wireless component operates on Channel 17, you will want to disable Channel 17 in the reader channel configuration. See “Assigning Reader Channels”.

Beacon Time — The default Beacon Time for a reader is one minute; however, you can manually input a different value anywhere from 10 seconds to 1 day. Keep in mind, the more frequent the beacon time, the more battery power used.

Note For best results, it is recommended that beacon time be set to no lower than 1 minute.

Default Operate Time — The Default Operate time is three seconds. You can manually enter a different value as needed.

Default Shunt Time — The Default Shunt Time is three seconds. You can manually enter a different value as needed. This feature is useful for readers that will be used to accommodate wheelchairs or other equipment that may need additional time to get through the door before the alarm is triggered.

Operate Delay — This feature is useful during situations where, for example, a guard may want a chance to visually confirm the identity of the user before access is granted.

Shunt Delay — This feature is useful when the users accessing this reader typically need more time to pass through the door after it unlocks; such as, someone in a wheelchair or someone who will move equipment through the doorway.

Statistics Update Interval — Manually enter the desired reader polling time.

Wiegand Device — Define if applicable.

First Card Unlock Authority — The reader requires authority to leave the door unlocked when in an unlock with ID access mode.

Card Formats Assignments — Assign card formats to the reader.

Assigning Reader Channels

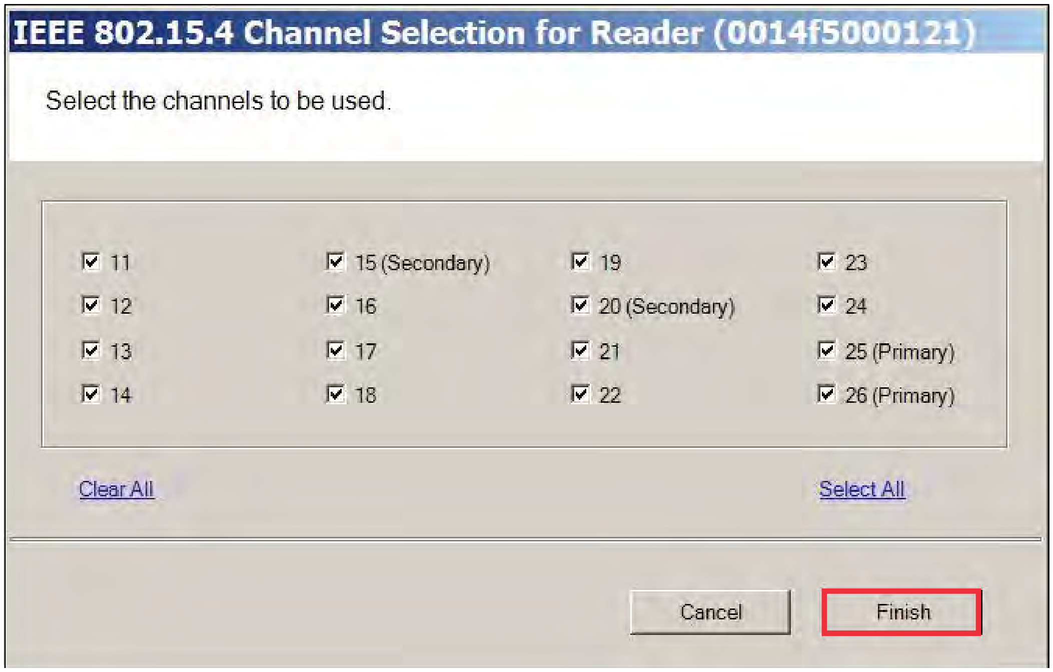
Perform the following steps to assign reader channels.

1 In the Reader tab, select the desired reader within the Segment Tree.

2 In the Reader Properties sheet, under the Configuration category, click in the Assigned to Channels field. The ellipsis button appears at the far right of the field.

3 Click the ellipsis button to display the Channel Selection for the Reader.

Figure 79 Reader Channel Selection



IEEE 802.15.4 Channel Selection for Reader (0014f5000121)

Select the channels to be used.

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

4 Select your desired channels.

5 Click Finish to save your settings.

Note When changing a reader's channels, ensure that it can connect to a Wi-Q Gateway on the same channel. For example: if a reader is changed to use only Channel 17, the Portal's channels must include Channel 17.

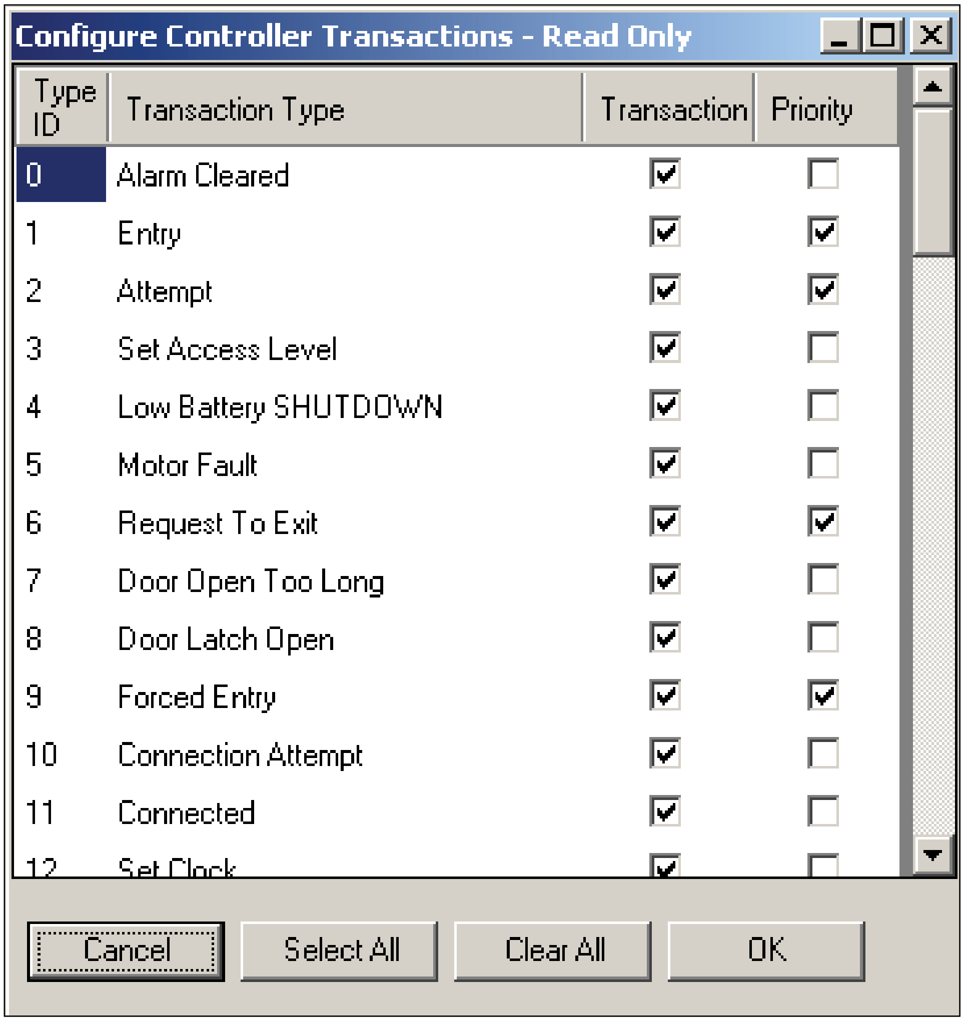
Reader Control

The Reader Control dropdown list corresponds to settings configured under the Reader Control sub tab in the Timezones tab. See "Configuring Timezones" on page 154 for more information.

Uploaded Transactions

Click on the Transaction Masks ellipsis button, the Configure Controller Transactions dialog box will open.

Figure 80 Configure Controller Transactions



Type ID	Transaction Type	Transaction	Priority
0	Alarm Cleared	☑	□
1	Entry	☑	☑
2	Attempt	☑	☑
3	Set Access Level	☑	□
4	Low Battery SHUTDOWN	☑	□
5	Motor Fault	☑	□
6	Request To Exit	☑	☑
7	Door Open Too Long	☑	□
8	Door Latch Open	☑	□
9	Forced Entry	☑	☑
10	Connection Attempt	☑	□
11	Connected	☑	□
12	Set Clock	☑	□

Here, you can determine what transaction types will show up in the Transactions application. If you make a transaction a priority by checking the Priority checkbox, it will come through immediately instead of waiting until the next beacon. If you click on the Select All or Clear All buttons, a dialog box will open to ask if you want to include Priorities as well. Select Yes or No.

5 Configure AMS Software (Task 11)

This chapter will provide detailed information on configuring the AMS Software.

Now that Wi-Q Gateways and Controllers have been added to and configured within the software, you are ready to configure your segment even further. The first part of this chapter will discuss the configurable items within the different categories of the Segment tab.

Associations

In the Associations category of the Segment tab, you can select from a set of supplied User Fields or add your own and create User Groups for your segment.

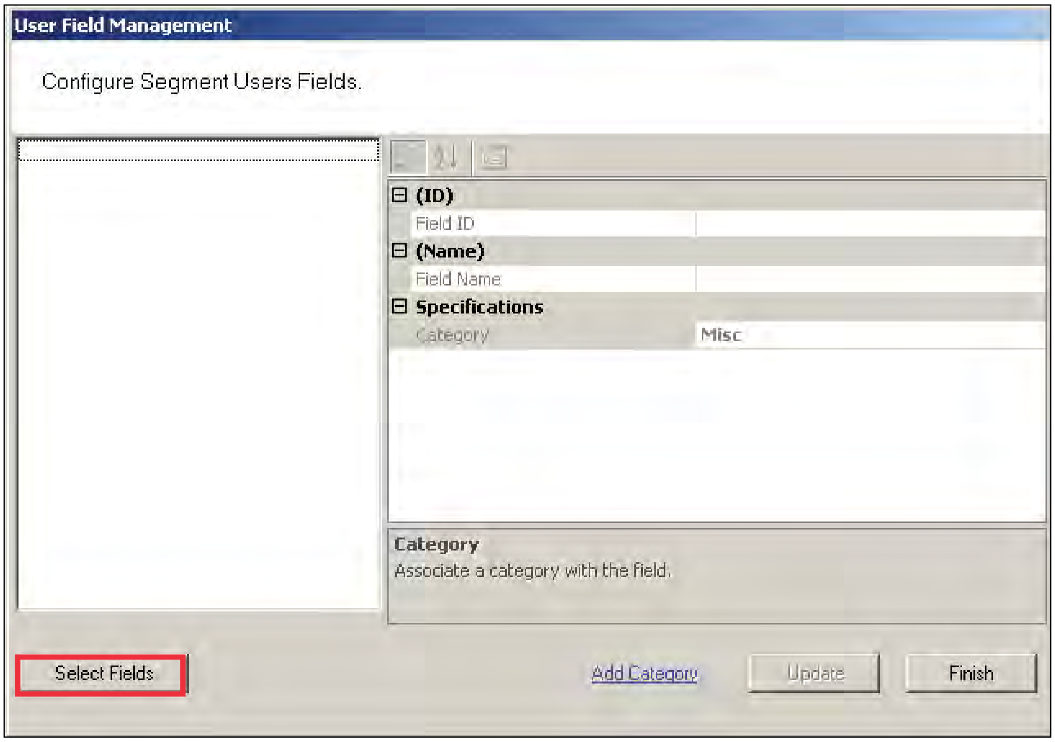
User Fields

Wi-Q AMS supplies you with a set of common User Fields which are available in the User Tab when you start adding users. You are also supplied with a set of additional User Fields and Categories that you can add to the system if needed. If you do not find the fields and categories you need to fully define your user parameters, you can create your own and they will be available from the User Tab. When you add and remove User Fields, the changes affect all segments in the system.

Adding Additional User Fields

1 In the Segment tab, click on User Fields and select the ellipsis button at the far right of the field. The User Field Management dialog box opens.

Figure 81 User Field Management

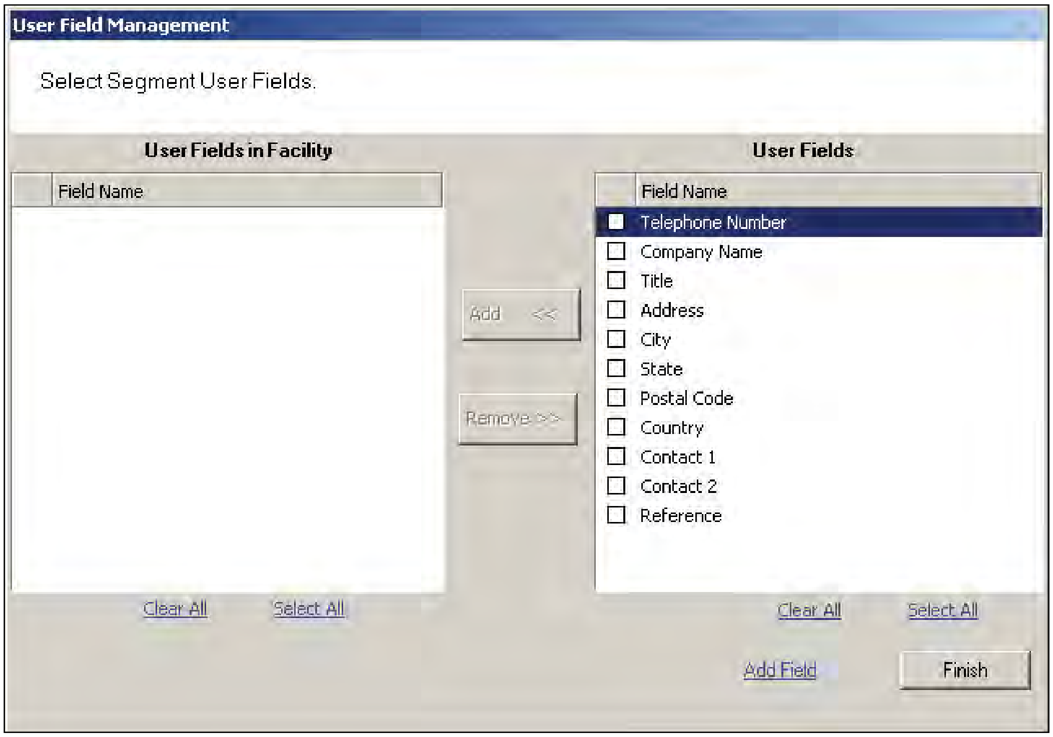


User Field Management

Configure Segment Users Fields.

2 Click the Select Fields button at the bottom of the dialog box. The Select Segment User Fields dialog box opens. Additional pre-defined User Fields are listed on the right.

Figure 82 Select Segment User Fields


User Field Management

Select Segment User Fields.

User Fields in Facility

Field Name

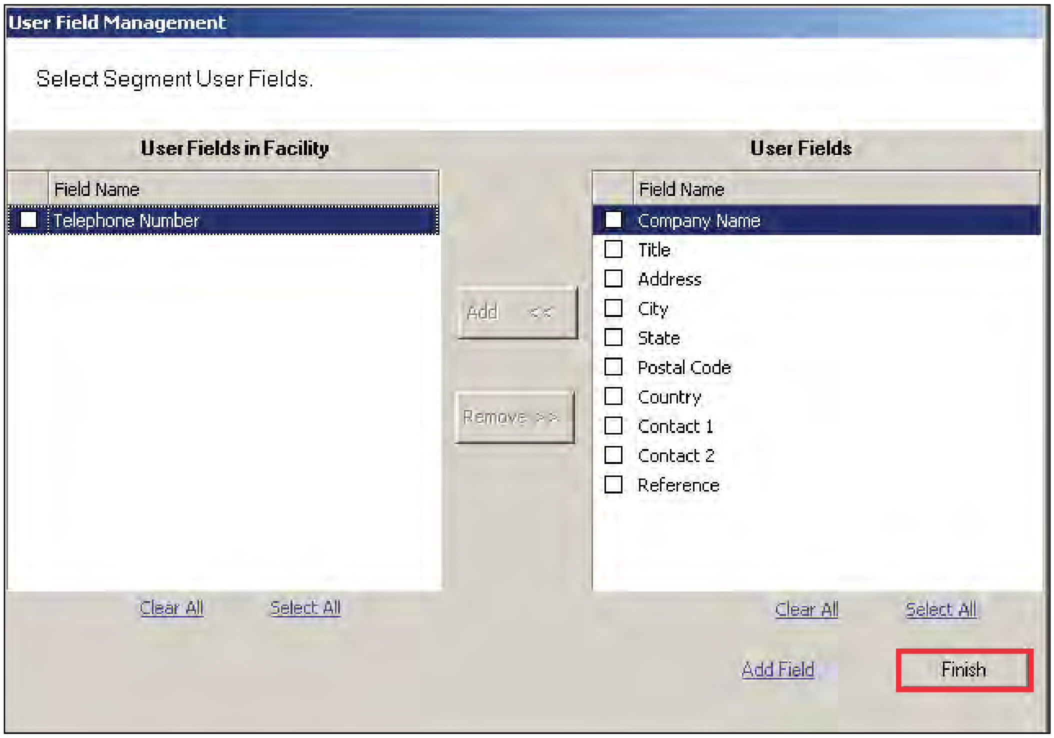
User Fields

Field Name

- ☐ Telephone Number
- ☐ Company Name
- ☐ Title
- ☐ Address
- ☐ City
- ☐ State
- ☐ Postal Code
- ☐ Country
- ☐ Contact 1
- ☐ Contact 2
- ☐ Reference

3 To add one of these fields, select the checkbox next to the field and select <<Add. The field is transferred to the User Fields in Facility box on the left.

Figure 83 User Fields in Facility


User Field Management

Select Segment User Fields.

User Fields in Facility

Field Name

- ☐ Telephone Number

User Fields

Field Name

- ☐ Company Name
- ☐ Title
- ☐ Address
- ☐ City
- ☐ State
- ☐ Postal Code
- ☐ Country
- ☐ Contact 1
- ☐ Contact 2
- ☐ Reference

4 Select Finish. Once you add the field to a Segment, it will appear on the Users Tab in the Configurator module. See the next few sections for steps to complete this process.

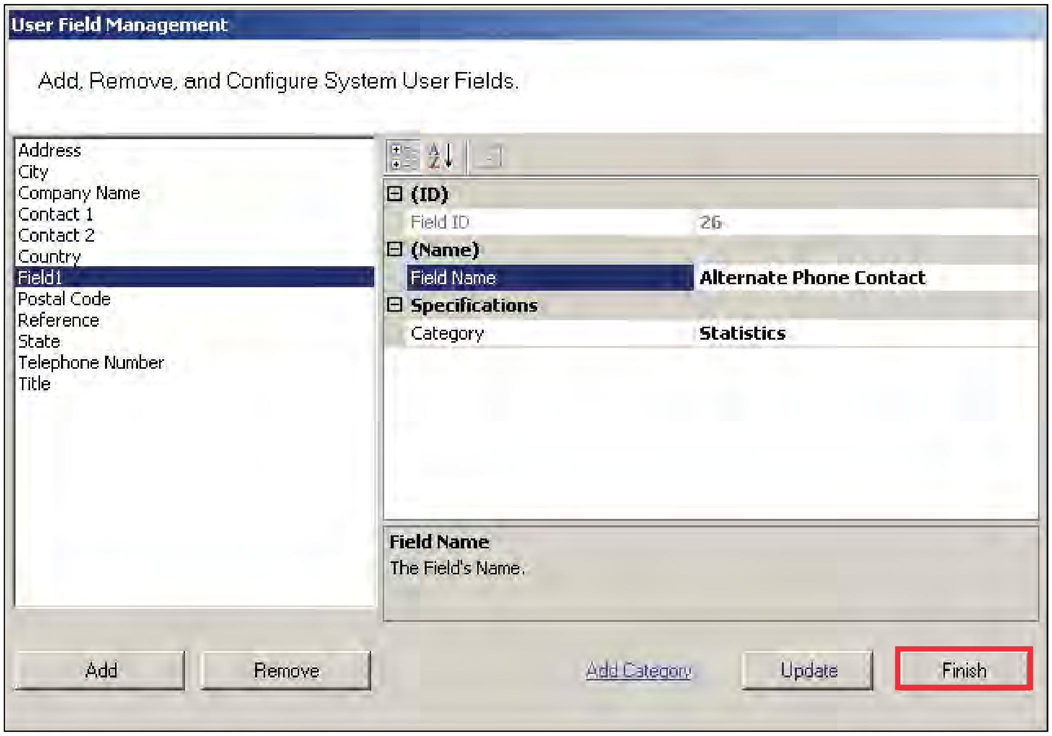
Creating New User Fields

If the field you wish to add does not appear in the User Fields list on the right, you can add one of your own. Once this is done, you can add it to an existing Category, or create a new Category for the field. You can add any number of new fields and new categories.

Perform the following steps to To create a New User Field.

1 In the Select Segment User Fields dialog box, select Add Field at the bottom of the box. The Add, Remove, and Configure System User Fields dialog box opens.

Figure 84 Add, Remove and Configure System User Fields



User Field Management

Add, Remove, and Configure System User Fields.

Address
City
Company Name
Contact 1
Contact 2
Country
Field1
Postal Code
Reference
State
Telephone Number
Title

⊟ (ID)

Field ID	26

⊟ (Name)

Field Name	Alternate Phone Contact

⊟ Specifications

Category	Statistics

Field Name
The Field's Name.

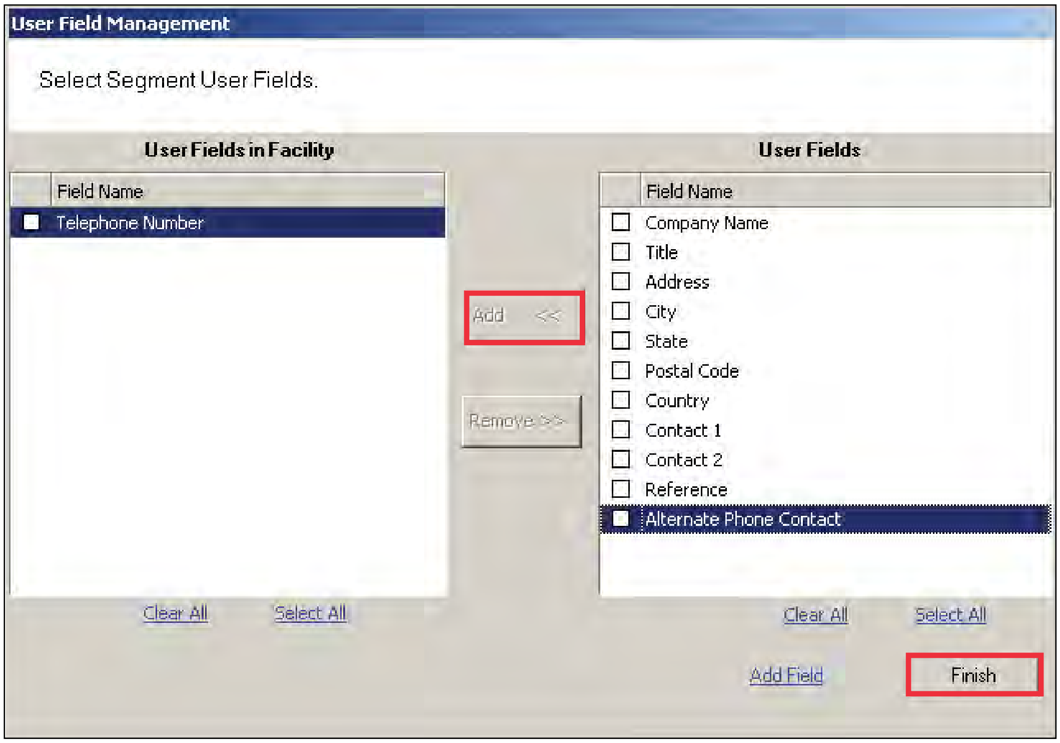
2 Under Specifications, Category, select the category under which you wish the new field to appear from the drop-down list, for example, Statistics.

Note If the category you want is not available, you can also create your own category. See “Adding a New User Fields Category” on page 117.

3 In the Field Name category on the right, type in a new name for the new field. In the example, we used Alternate Phone Contact.

4 Select Update. When you click Finish, the Select Segment User Fields dialog box shows that your new field is now available for selection.

Figure 85 User Field added to list



User Field Management

Select Segment User Fields.

User Fields in Facility

	Field Name
□	Telephone Number

User Fields

	Field Name
□	Company Name
□	Title
□	Address
□	City
□	State
□	Postal Code
□	Country
□	Contact 1
□	Contact 2
□	Reference
□	Alternate Phone Contact

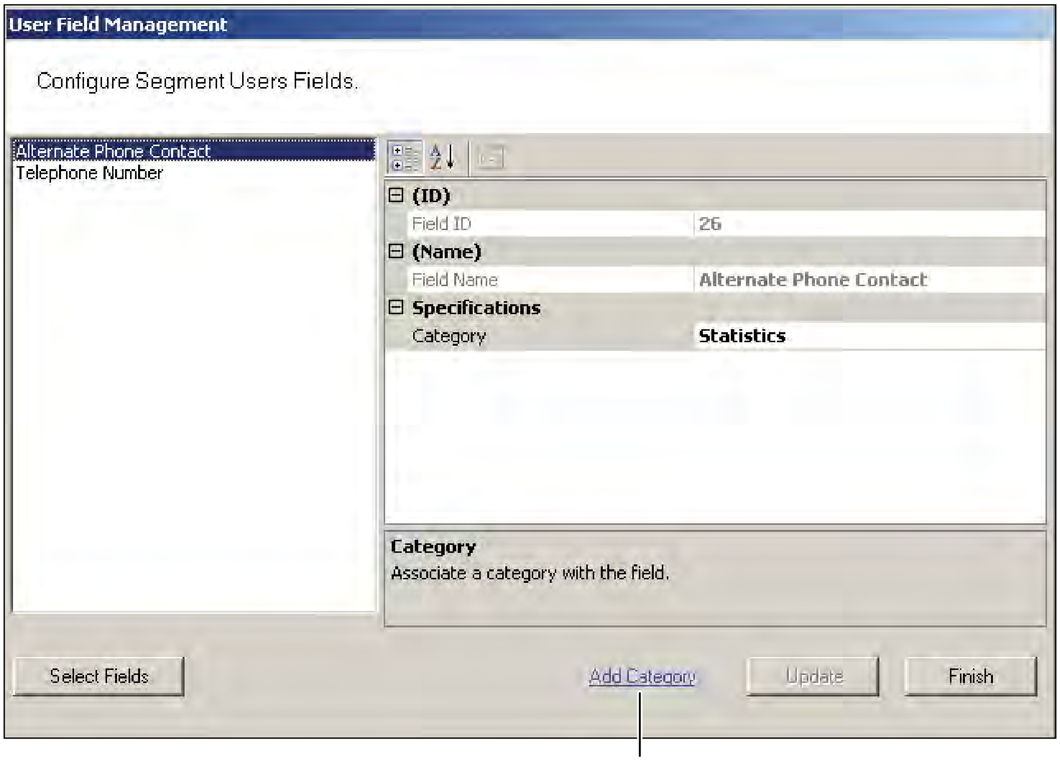
5 Select the Checkbox next to the field and click <<Add. The field is transferred to the User Fields in Segment box on the left.

6 Select Finish. The new field is now added to the User Field Management dialog box.

Adding a New User Fields Category

1 In the User Field Management of Segment dialog box, click the Add Category Link at the bottom of the dialog box.

Figure 86 Add Category



User Field Management

Configure Segment Users Fields.

Alternate Phone Contact
Telephone Number

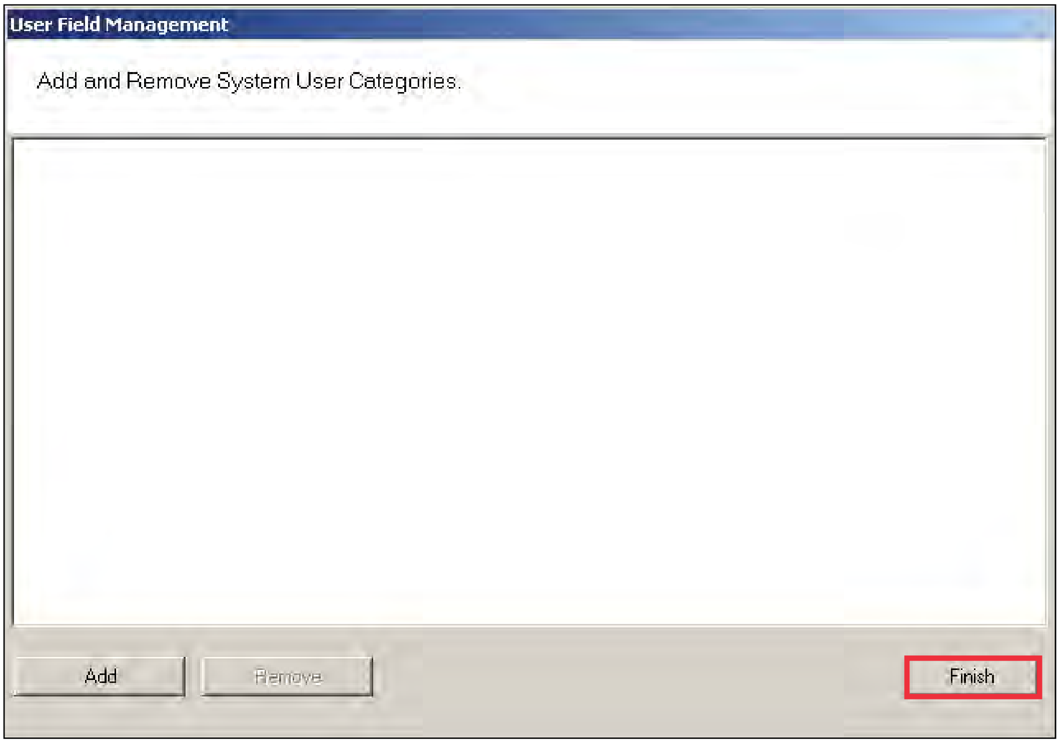
(ID)	
Field ID	26
(Name)	
Field Name	Alternate Phone Contact
Specifications	
Category	**Statistics**

Category
Associate a category with the field.

Add Category

2 The Add and Remove System User Categories window opens.

Figure 87 Adding and Remove System User Categories



User Field Management

Add and Remove System User Categories.

3 Click the Add button. “Category 1” appears in the text box.

4 Double-click on “Category 1” to rename it.

5 Click Finish. In the Configure Segment Users Fields dialog box, the new category is now available for selection from the Category drop-down list. Now you can select this category when defining a new User Field.

Removing User Fields and Categories

You can also remove added User Fields and Categories from the system. The system will not allow you to do this, however, if the field or category is in use. Before you remove the field or category, ensure there are no records assigned to them, then perform the following steps.

To remove User Fields from the system

1. In the User Fields Management dialog box, click the Select Fields button at the bottom of the dialog box.
2. From the User Fields in Facility list on the left, select the fields you wish to remove and click Remove>>. The field is moved to the User Fields list on the right, and remains inactive unless you add it back to the list.
3. Click Finish. The field is no longer available in the User Fields list.

To remove added Categories from the system

1. In the User Field Management window, select Add Category.
2. The Add and Remove System User Category window opens.
3. Select the category you wish to remove, and click Remove. Click Finish when you are done.

User Groups

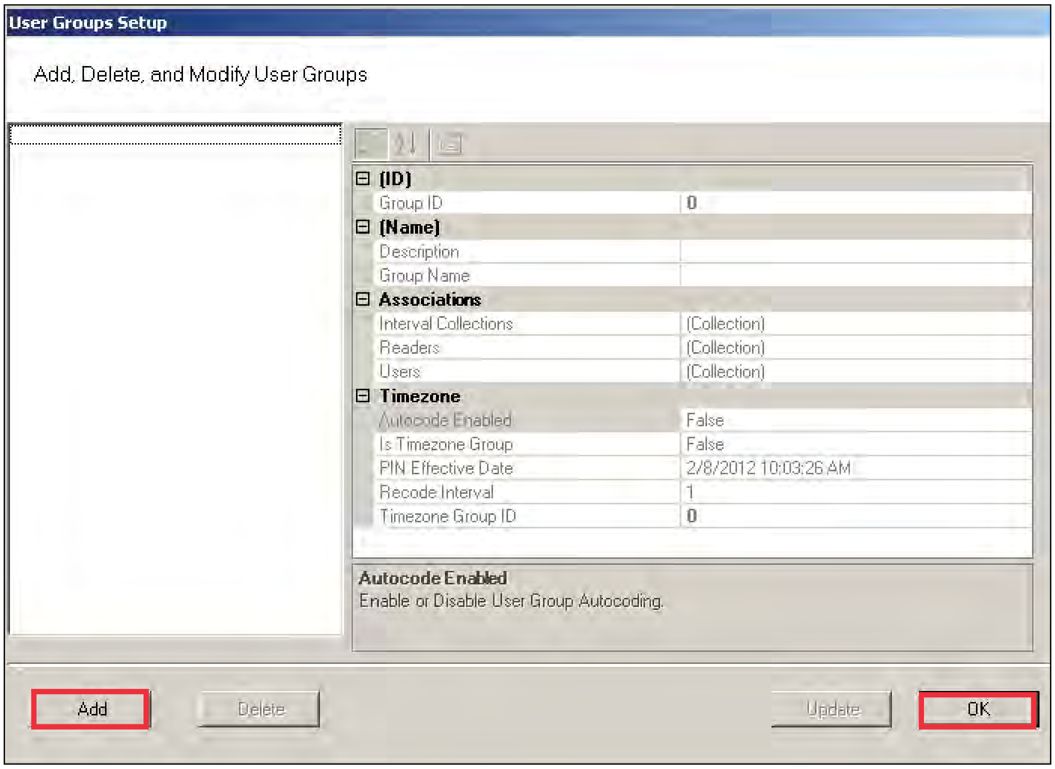
User Groups are a convenient way to define properties that will affect certain groups of individuals in your system. For example, if your Administrative personnel have different hours or entry parameters, you can create an Administrative group, make that group a Timezone Group and assign administrative personnel to that group.

You can define any number of User Groups, such as Administrative, General, Laboratories, Dormitories, Night Shift, Contractors, and so on.

Adding User Groups

1. In the Users Tab, Associations category, click the User Groups field. Select the ellipsis button at the far right of the field. The User Group Setup dialog box opens.

Figure 88 User Groups Setup



Add, Delete, and Modify User Groups

[ID]	
Group ID	0
[Name]	
Description	
Group Name	
Associations	
Interval Collections	(Collection)
Readers	(Collection)
Users	(Collection)
Timezone	
Autocode Enabled	False
Is Timezone Group	False
PIN Effective Date	2/8/2012 10:03:26 AM
Recode Interval	1
Timezone Group ID	0

Autocode Enabled
Enable or Disable User Group Autocoding.

2 The groups you create display on the left. The group's ID, Name, Associations and Timezone appear on the right.

3 Select Add. A new Group (Group1) is created and displays on the left.

4 In the Group Name box, replace the name Group1 with a name for the new group (for example, Administrative).

5 Select OK.

Note Once you have added users to the system via the Users Tab, you can assign them to these User Groups.

Removing User Groups

In the User Group Setup dialog box, select the group you wish to remove and select the Delete button. The group is immediately removed from the list, along with its associations.

Associating Users with User Groups

1 In the Segment Tab, Associations category, click the User Groups field.

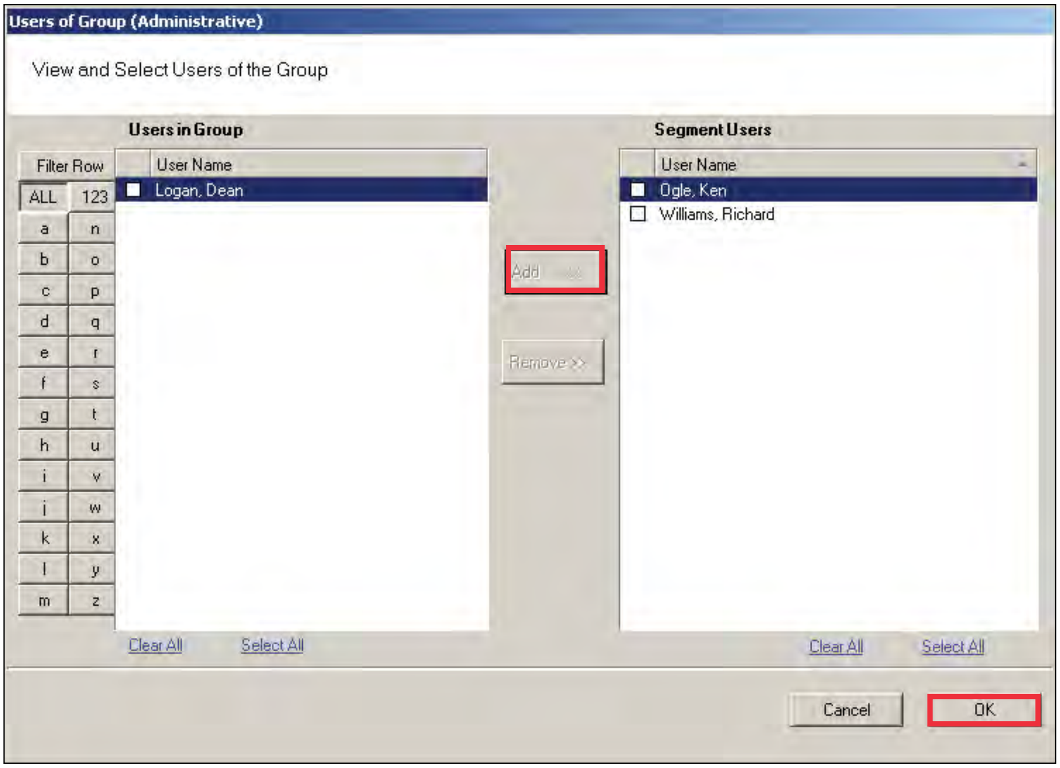
2 Select the ellipsis button at the far right of the field.

3 In the User Groups Setup dialog box, select the group you wish to associate with users.

4 In the Associations category, click in the Users field and select the ellipsis button. The Users of Group dialog box opens.

5 All users in the segment not already assigned to the group are displayed under Segment Users list on the right.

Figure 89 Users of Group



Users of Group (Administrative)

View and Select Users of the Group

Users in Group

User Name
□ Logan, Dean

Segment Users

User Name
□ Ogle, Ken
□ Williams, Richard

Note Users will not appear in the Segment Users list until they have been added to the system. If you have a large number of users, you can use the Alphabetic sorter buttons on the left of the list to more quickly find a specific user.

6 Select the checkbox next to the users you wish to associate with the User Group.

7 Select <<Add. The User names will be removed from the Segment Users list on the right and display under Users in Group list on the left.

8 Select OK to close the Users of Group dialog box.

Removing Users from User Group

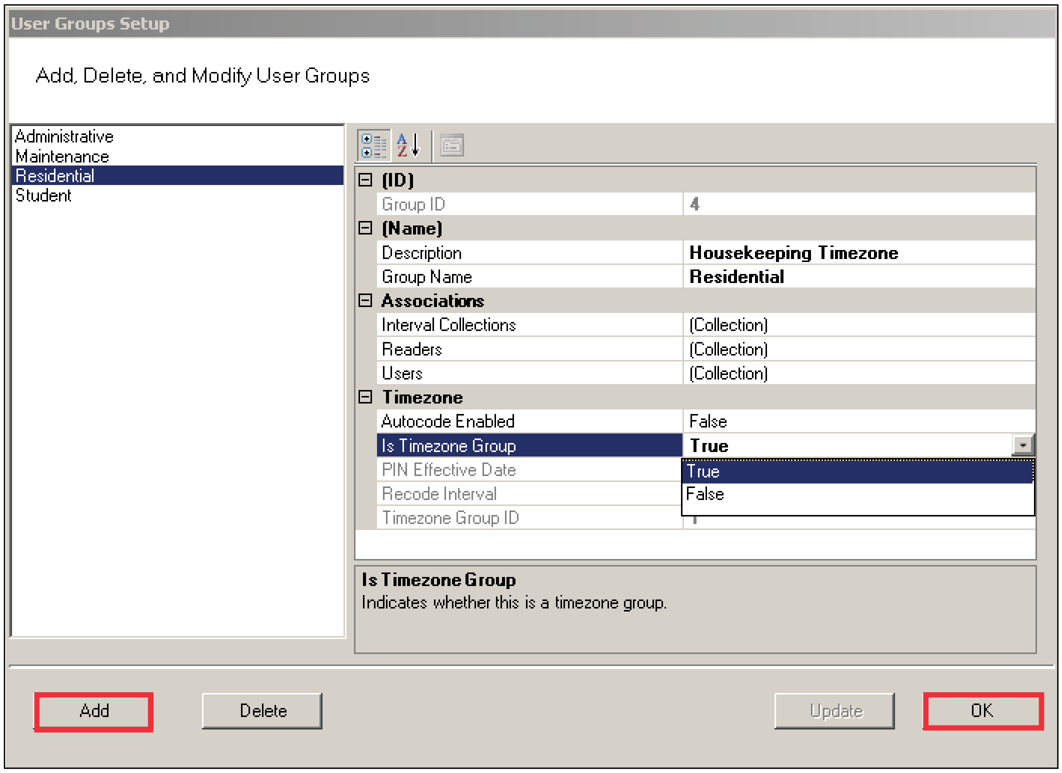
1. In the User Groups Setup dialog box, select the group in which the user currently resides.
2. In the Associations category, click on the Users field, and select the ellipsis button. The Users of Group dialog box opens.
3. From the Users in Group list on the left, select the checkbox next to the user you wish to remove from the group.
4. Select Remove. The user name will be removed from Users in Group list on the left and moved back to the Segment Users list on the right. Select OK to close the Users of Group dialog box.

Timezone User Groups

You can create up to 512 Timezone User Groups to further define access levels for the Master Timezone. These can restrict access of a certain group of employees to a specific time period. Perform the following steps to create a timezone user group.

1. In the Segment Tab, select the Segment to which you wish to add a new Timezone User Group.
2. In the Associations Category, select User Groups and click the ellipsis button at the far right of the field. The User Groups Setup dialog box opens.

Figure 90   Creating a Timezone User Group



(ID)	
Group ID	4
(Name)	
Description	**Housekeeping Timezone**
Group Name	**Residential**
Associations	
Interval Collections	(Collection)
Readers	(Collection)
Users	(Collection)
Timezone	
Autocode Enabled	False
Is Timezone Group	**True**
PIN Effective Date	
Recode Interval	
Timezone Group ID	1

Is Timezone Group
Indicates whether this is a timezone group.

3 Select Add. Group1 is created.

4 In the Name Category, Description, enter a description for the group, for example, Housekeeping Timezone.

5 In the Group Name, replace Group1 with the name of your new user group, for example, Residential.

6 Under Timezone, change the Is Timezone Group default setting from False to True. Select Update to continue creating groups.

7 Select OK to save the new Timezone group.

Once you have created a Timezone group, you will need to set up access times to apply to that group. For more information about Timezones and Timezone User Groups, see "Configuring Timezones" on page 154.

Credential Settings

Keypad credentials, magnetic card settings, and proximity card settings are all set in this category. Detailed steps are presented in the following sections.

Keypad Credential Length

If your access system will have or currently has cards encoded with keypad credentials, you may set the number of digits required here.

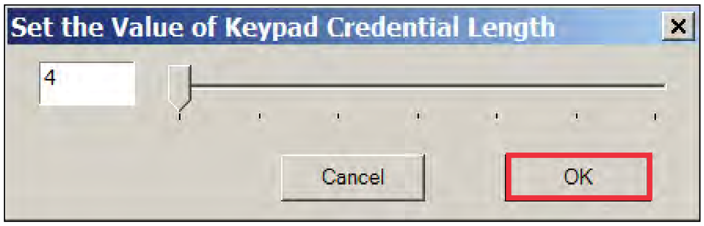
Note Keypad credential length must be set before you add users to the system.

Perform the following steps to set the Keypad Credential Length.

1 In the Segment Tab, under the Credential Settings category, click in the Keypad Credential Length field.

2 Click the ellipsis button at the far right of the field. The Set value of Keypad Credential Length dialog box opens.

Figure 91 Setting the Credential Length



4

3 Enter the length or slide the bar to select the position of the Keypad Credential length you will use on segment cards.

4 Select OK to save your settings and exit the box.

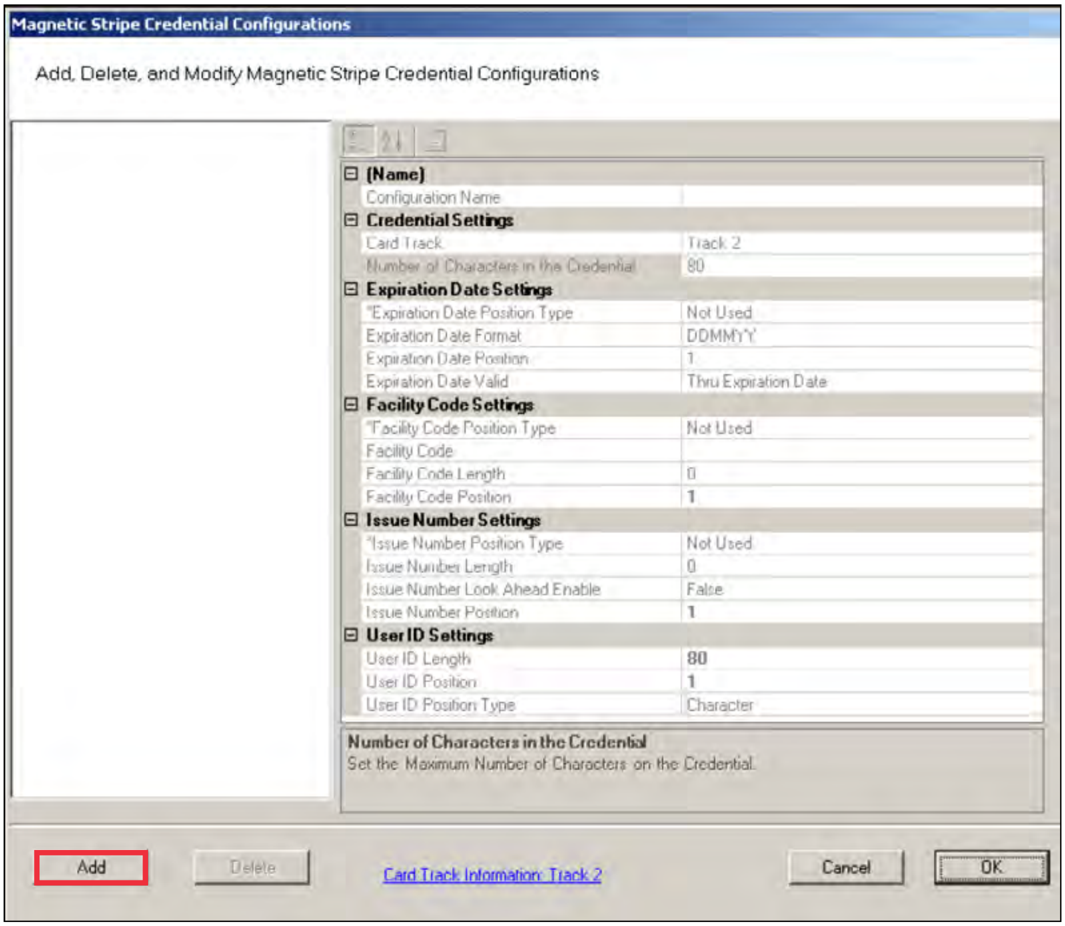
Magnetic Stripe Credential Configurations

Before Magnetic cards can be used in the system, you must configure AMS to accept the card types and settings. Figure 92 shows the Magnetic Stripe Credential Configurations Window. Default settings will be sufficient for most systems.

Most users will use Track 2 cards and will not need to set up any type of advanced card parameters. Wi-Q AMS default Expiration Date, Segment Code, and Issue Number settings to Not Used, and no other changes need to be made.

dormakaba currently stocks and provides Track 2 or Track 3 magnetic cards. These cards conform to ISO standards and can be ordered pre-encoded or blank. The
system can be used with either Track 1, Track 2, or 3 cards, however, you can only encode 1 type within the same segment.

Figure 92 Magnetic Stripe Credential Configurations



Magnetic Stripe Credential Configurations

Add, Delete, and Modify Magnetic Stripe Credential Configurations

(Name)	
Configuration Name	
Credential Settings	
Card Track	Track 2
Number of Characters in the Credential	80
Expiration Date Settings	
*Expiration Date Position Type	Not Used
Expiration Date Format	DDMMYY
Expiration Date Position	1
Expiration Date Valid	Thru Expiration Date
Facility Code Settings	
*Facility Code Position Type	Not Used
Facility Code	
Facility Code Length	0
Facility Code Position	1
Issue Number Settings	
*Issue Number Position Type	Not Used
Issue Number Length	0
Issue Number Look Ahead Enable	False
Issue Number Position	1
User ID Settings	
User ID Length	80
User ID Position	1
User ID Position Type	Character

Number of Characters in the Credential
Set the Maximum Number of Characters on the Credential.

If you must make changes to the default settings, click Add to create a new Magnetic Stripe card configuration, and give a name to your configuration in the Configuration name field.

Credential Settings

Wi-Q AMS can be configured to accept coding from existing Track 1(210 BPI), Track 2 (75 BPI) or Track 3 (210 BPI) cards as long as the code does not exceed the maximum number of characters for that track and/or controller. Magnetic cards are configured as Track 2 by default. Perform the following steps to change to change the segment track setting for encoding cards:

1 In the Magnetic Stripe Credential Configurations window, click the Card Track Information link at the bottom of the window.

2 The Define Magnetic Stripe Card Track Information window opens. Specify the desired track from the dropdown menu. Then click Finish.

3 Click OK to exit the Magnetic Stripe Credential Configurations window.

4 In the Segment tab, click Update at the bottom right to update your segment.

Card Track Limits

Wi-Q AMS is flexible and may accept coding from existing Track 2 or Track 3 cards as long as they do not exceed the maximum number of characters for that track and/or controller. These characters include any digits and field separators, however, they exclude the starting and ending sentinels. Refer to the BEST Knowledge Base or contact dormakaba Technical Support for controller hardware track limits.

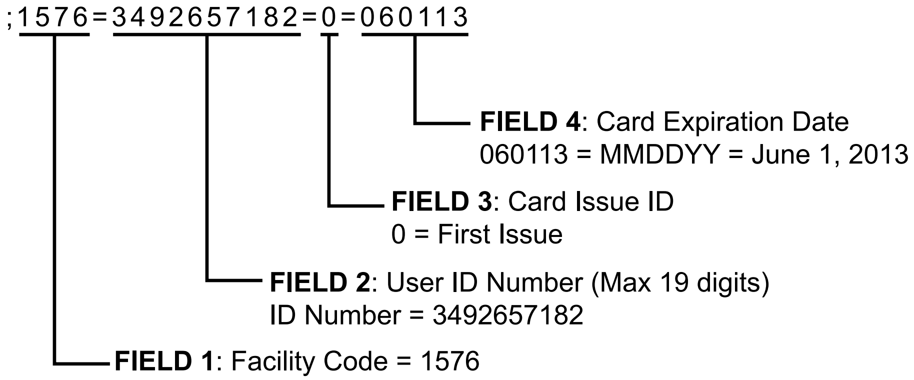
Character codes and counts

The software recognizes data on a magnetic card stripe using ANSI standard codes formatted to either a field separator or character count. Following is a brief description of each type.

Field Separator — Field Separator (FS) character, generally represented as an equal sign (=) to separate two independent data fields. A card using this method might have the owner's individual ID encoded at the beginning of the stripe followed by the FS character then the global segment ID. The fields can be in either order, or there can be more than two fields, which could be required for compatibility with pre-existing systems, and any one of them can be set up as User ID, Segment ID, Card Issue ID, or Expiration Date.

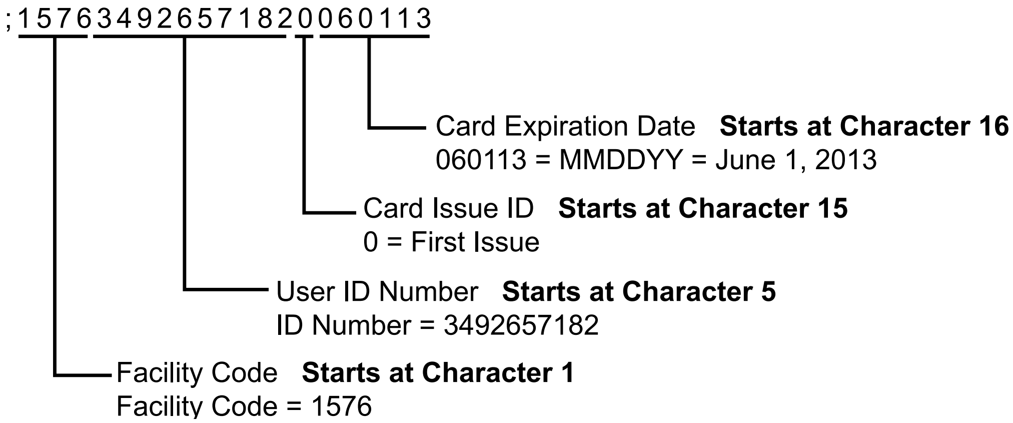
Following is an example of encoded data using field separators on Track 2.

Figure 93 Data Fields


;1576=3492657182=0=060113
FIELD 4: Card Expiration Date
060113 = MMDDYY = June 1, 2013
FIELD 3: Card Issue ID
0 = First Issue
FIELD 2: User ID Number (Max 19 digits)
ID Number = 3492657182
FIELD 1: Facility Code = 1576

Character Count — You can set up a character count from the beginning of each ID. For example, the Segment ID could start at the beginning of the data stripe, digit count of 1. If the Segment ID has eight digits, the User ID would be set to start at digit count of 9. This method requires all data groups with exception of the last one, to have a fixed number of digits. Following is an example of encoded data using character counts on Track 2.

Figure 94 Character count fields



;15763492657182006011 3
Card Expiration Date **Starts at Character 16**
060113 = MMDDYY = June 1, 2013
Card Issue ID **Starts at Character 15**
0 = First Issue
User ID Number **Starts at Character 5**
ID Number = 3492657182
Facility Code **Starts at Character 1**
Facility Code = 1576

Note If you are not using the default settings for Magnetic Stripe Credential Configurations, make sure that Expiration Date Position Type, Facility Code Position Type, Issue Number Position Type, and User ID Position Type are all set to either must be set to “Field” (Field Separator) or “Character” (Character Count); you cannot mix types.

Expiration Date Settings

Perform the following steps to define a card expiration date.

1 In the Magnetic Stripe Credential Configurations window, under the Expiration Date Settings category, click in the Expiration Date Position Type field.

2 Select either Character or Field from the drop-down list. The Expiration Date Format, Position, and Valid list boxes activate.

3 In the field next to Expiration Date Format, select the date format you need from the drop-down list (MMDDYY, etc.).

4 In the field next to Expiration Date Position, enter the value to represent either the field position or the character number where the expiration date appears on the card stripe.

5 In the field next to Expiration Date Valid, select either To or Thru Expiration date.

6 Select OK to save your settings and exit the box.

Note If you use the character code format and select the six-digit expiration date format,the value of your next setting (Facility Code Settings) must start with character position 7. If you enter an incorrect value, the system will report an error message. Review the “Character codes and counts” on page 127 if you need clarification.

Facility Code Settings

Perform the following steps to define a facility code type, position, and length.

1 Under the Facility Code Settings category, click in the Facility Code Position Type field.

2 Select either Character or Field from the drop-down list. The Facility Code fields below activate.

3 In the field next to Facility Code, enter your Facility Code number.

4 In the field next to the Facility Code Length, enter the length.

5 In the field next to Facility Code Position, enter the facility code position.

6 Select OK to save your settings and exit the box.

Issue Number Settings

You can issue a replacement card to a user in lieu of issuing a new User ID. The Card Issue ID consists of one or two digits from 0 through 99. After using the card with an incremented (higher number) Card Issue ID in a reader, that lock will no longer accept cards with the same User ID that have a lower Card Issue ID.

Perform the following steps to define an issue number position.

1. In the Issue Number Settings category, click in the Issue Number Position Type field.
2. Select either Character or Field from the drop-down list. The Issue Number fields below activate.
3. Enter the Issue Number length.
4. Click the Issue Number Look Ahead Enable field, and select true or false from the dropdown menu.
5. Enter the Issue Number position.
6. Select OK to save your settings and exit the box.

User ID Settings

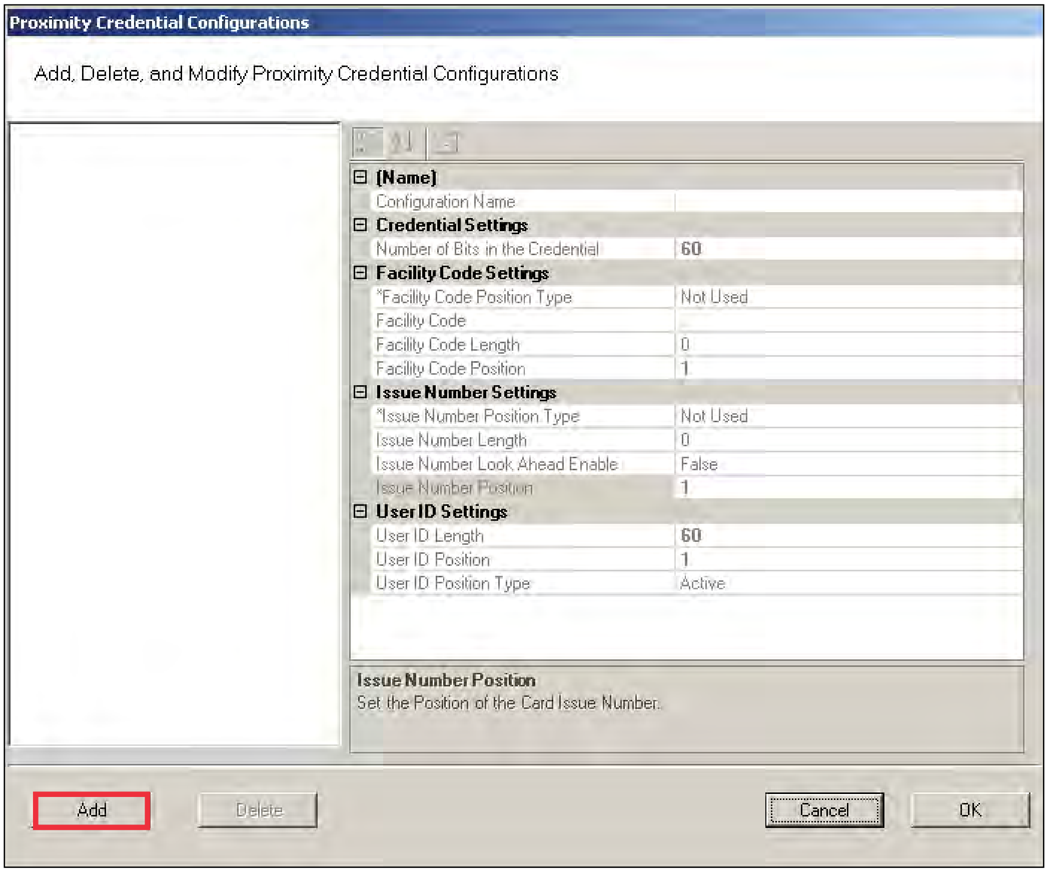
You can specify the position of the User ID code in the credential number either by character or field position. Perform the following steps to modify the User ID Settings.

1. Enter the User ID Length.
2. In the User ID Position field, enter the position number.
3. In the User ID Position Type field, specify Character or Field.
4. Select OK to save your settings and exit the box.
5. Select Finish to save all your settings.

Proximity Credential Configurations

If you are using proximity cards in your system, you can add card configurations by clicking on the Proximity Credential Configurations field and selecting the ellipsis button at the far right. Figure 95 shows the Proximity Credential Configurations window.

Figure 95 Proximity Credential Configurations



Proximity Credential Configurations

Add, Delete, and Modify Proximity Credential Configurations

[Name]	
Configuration Name	
Credential Settings	
Number of Bits in the Credential	60
Facility Code Settings	
*Facility Code Position Type	Not Used
Facility Code	
Facility Code Length	0
Facility Code Position	1
Issue Number Settings	
*Issue Number Position Type	Not Used
Issue Number Length	0
Issue Number Look Ahead Enable	False
Issue Number Position	1
User ID Settings	
User ID Length	60
User ID Position	1
User ID Position Type	Active

Issue Number Position
Set the Position of the Card Issue Number.

To add a card configuration, perform the following steps.

1 Click Add. Give your new configuration a name in the Configuration Name field.

2 Under Credential Settings, select Number of Bits in the Credential. Change the number to the right (default 60) to match the number of bits on your card.

3 If your card is configured to include the facility code, change Facility Code Position type to Active. The facility code fields below will activate.

   a Enter your facility code in the Facility Code field.

   b Change the Facility Code Length to match the number of bits in your facility code.

   c Change the Facility Code Position to match your card.

Note Issue Number Settings are not configurable for proximity cards. Proceed to User ID Settings.

4 Under the User ID Settings category, change the User ID Length to the number of bits used for User IDs on your card. Set the User ID Position.

5 When finished, click OK.

Daylight Saving Settings

You can set Wi-Q AMS to automatically respond to Daylight Saving Time settings. When you select North American as the Daylight Saving Type, the system defaults to standard Daylight Saving Time settings. When you select Europe as the Daylight Saving Type, the system defaults to the settings for Europe. When you select Southern Hemisphere, the system defaults to the settings for the Southern Hemisphere. Once the settings are selected, the system will adjust to Daylight Saving Time automatically.

To change Daylight Savings Settings, place the cursor in the field next to Daylight Saving Type and select the type you wish to use. The settings below change to the defaults for that setting.

I/O

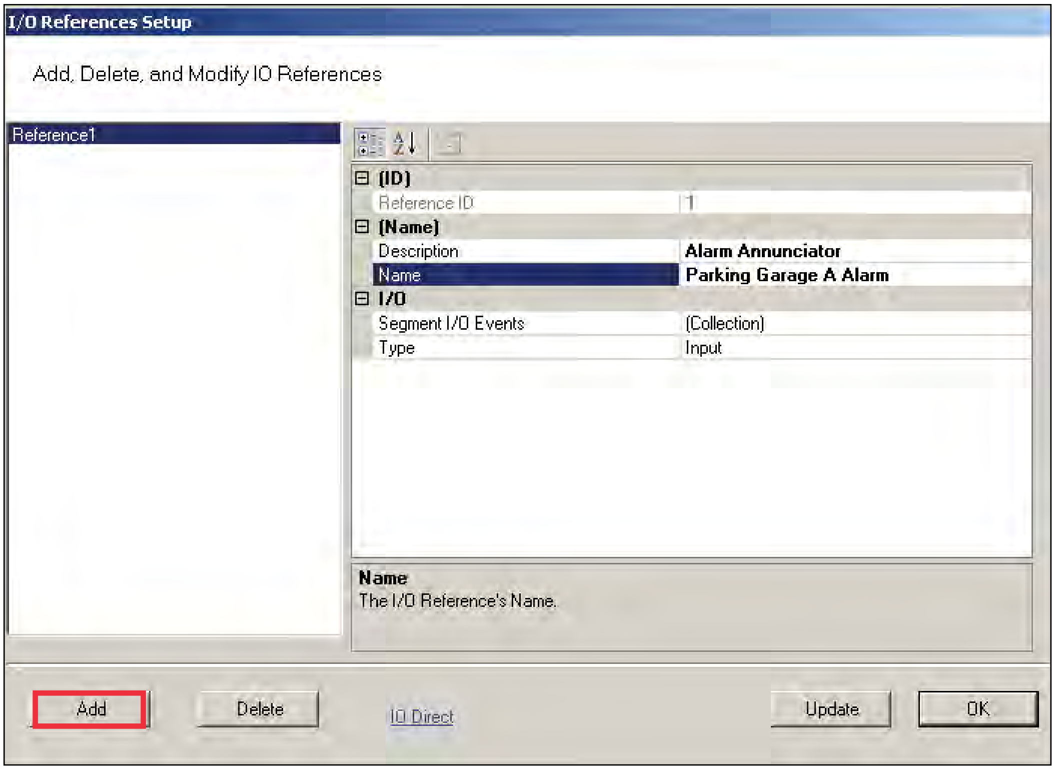
If you are using input/output devices in your system, they are recognized and defined similar to a Controller.

For example, if you are using a WAC to collect transactions from an alarm, you will see it in your Segment Tree as a “Reader” when its associated Wi-Q Gateway is brought online. You can define and modify I/O events for the controller under I/O References.

Adding and Modifying I/O References

1 In the Segment tab, click the I/O References field, and click the ellipsis button at the far right. The I/O References Setup dialog box opens.

Figure 96 I/O References Setup



I/O References Setup

Add, Delete, and Modify IO References

Reference1

(ID)

Reference ID: 1

(Name)

Description: Alarm Annunciator

Name: Parking Garage A Alarm

I/O

Segment I/O Events: (Collection)

Type: Input

Name

The I/O Reference's Name.

Here, you define an event and type for the reference. The system creates an I/O reference point in the left column of the dialog box and assigns it a reference ID number.

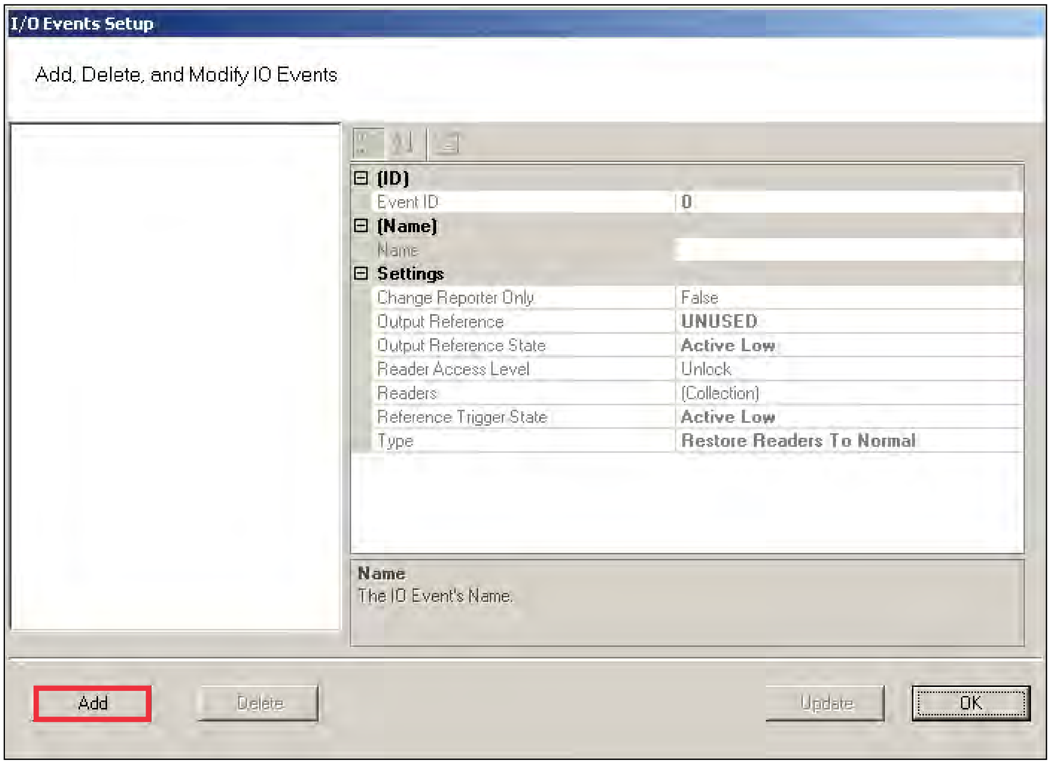
2 Click Add.

3 Under Description, replace the default description “Reference1’ with a description that will have meaning for your segment, such as Alarm Annunciator.

4 Under Name, replace the default name “Reference1” with a name that will have meaning for your segment, such as Parking Garage A Alarm.

5 Under the I/O category, click the Segment I/O Events field and select the ellipsis button at the far right. This will open the I/O Events Setup window.

Figure 97 I/O Events Setup



I/O Events Setup

Add, Delete, and Modify IO Events

⊟ (ID)

Event ID	0

⊟ (Name)

Name	

⊟ Settings

Change Reporter Only	False
Output Reference	UNUSED
Output Reference State	Active Low
Reader Access Level	Unlock
Readers	(Collection)
Reference Trigger State	Active Low
Type	Restore Readers To Normal

Name
The IO Event's Name.

From here you can create an event, check the device's current state of operation, define an access level, associate it with a reader in the system, define a trigger state (high or low), and define the type of event to be triggered.

Note: The system recognizes the WAC as any other "reader" in the system. It will appear in the referenced dialog boxes as a reader; however, you will recognize it by its MAC address.

6 Click the Add button. The system creates an Event ID and adds it to the list in the left hand column.

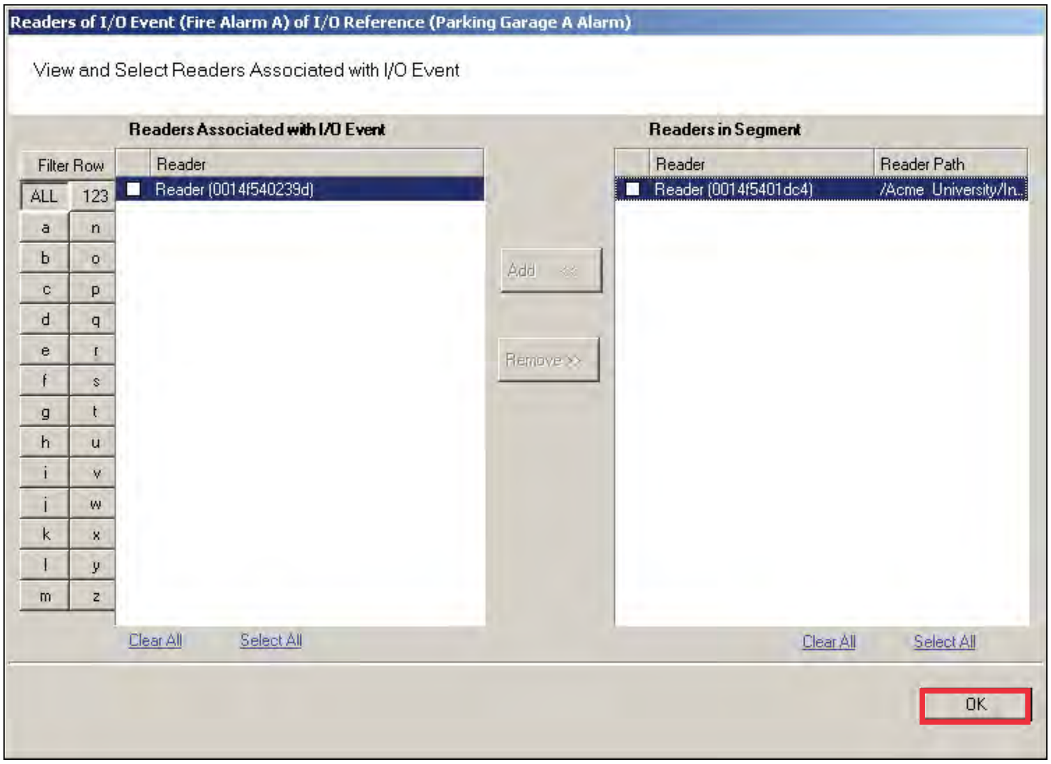
7 Enter a name for the event, such as Fire Alarm A.

8 Under the Settings Category, click the Readers field and click the ellipsis button.

9 This will open up a new window. See Figure 98. Select a device from the Readers in Segment section that will be associated with the event.

10 Click Add << to add it to the list of Readers Associated with I/O Event list.

Figure 98 Associating an I/O event with a Reader


Readers of I/O Event (Fire Alarm A) of I/O Reference (Parking Garage A Alarm)

View and Select Readers Associated with I/O Event

Readers Associated with I/O Event

	Reader
□	Reader (0014f540239d)

Readers in Segment

	Reader	Reader Path
□	Reader (0014f5401dc4)	/Acme University/In...

11 Click OK to save the association and return to the Setup dialog.

12 In the Reader Access level field, select either Unlock or Lockout from the drop-down list.

13 In the Reference Trigger State field, select either Active High or Active Low from the drop-down list (this reference will act as a toggle from one state to the other).

14 Under Type, select the event type from the drop-down list.

- Restore Readers To Normal
- Change Output Reference
- Override Reader Access Level
- Override Timezone User Group Access
- Restore Output Reference To Normal.

15 Click Update and continue defining devices then click Finish to save your settings and exit the dialog box.

Misc

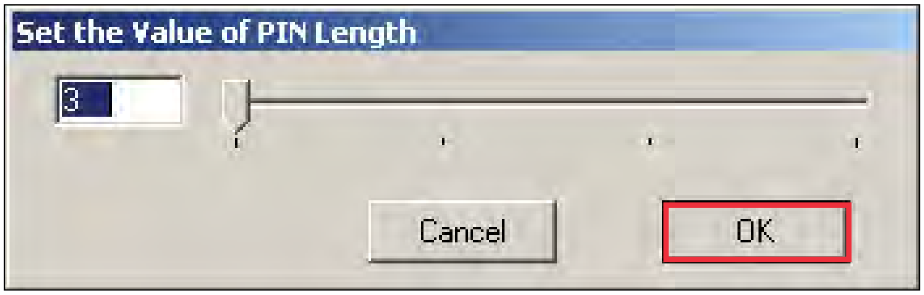
This category contains three fields (Contact 1, Contact 2, and Reference) that you can use to store any miscellaneous information you that will be helpful to you and your system. For example, you may decide to enter the phone number or email address for dormakaba Technical Support in case you experience technical difficulties.

PIN Settings

If your system will require user PINs, you may set the PIN length here. Perform the following steps.

1 Click in the PIN Length field, and select the ellipsis button at the far right. The PIN Length window opens.

Figure 99 Set the Value of PIN Length



2 Set the value to a number between 3 and 6 by typing it in or sliding the bar to select the position of the PIN length you will use on segment cards. Then, press OK.

Adding Users to the Segment

The system is now ready for you to add users. Follow the steps in this section the first time you enter users, and each time you add a new user to the system. To get started, navigate to the Users tab within the Configurator module.

Before You Begin

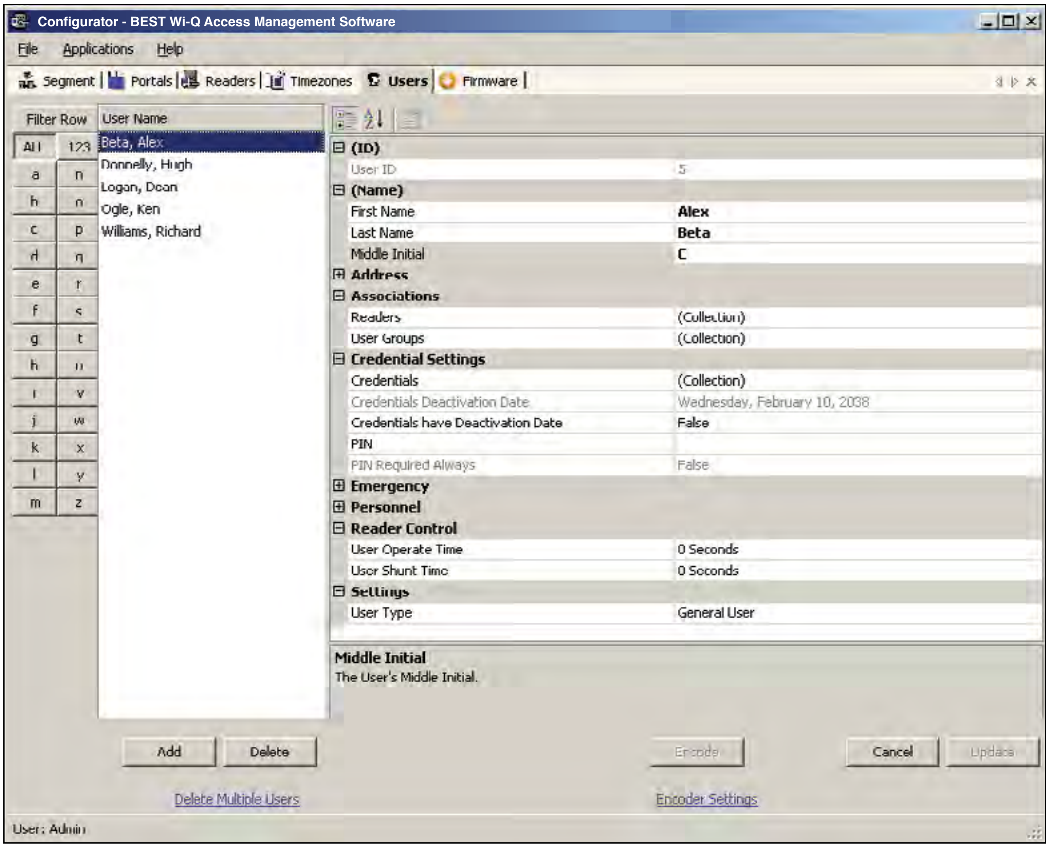
Before you begin adding users to the system for the first time, be prepared to address the following items:

If...	**Then...**
You plan to use only keypad Controllers	AMS assigns a unique keypad credential to each new user and automatically registers it with the system.
You plan to use card readers	You must know the card type and settings required for that type.
You plan to use a serial scanning device at your computer to register user credentials	The scanning device must be attached to the computer com port and you must be able to identify that port (Com1, Com 2) when you register the credential.
You plan to use local readers to register credentials	Know the reader name and locations to be used.
You plan to manually enter the credential numbers	Have a credential number list or creating conventions ready to enter.

Note If you do not have this information, contact your System Administrator before you begin.

Users Tab Overview

Figure 100 Users Tab



User Name
Beta, Alex
Donnelly, Hugh
Logan, Dean
Ogle, Ken
Williams, Richard

(ID)	
User ID	5
(Name)	
First Name	Alex
Last Name	Beta
Middle Initial	C
Address	
Associations	
Readers	(Collection)
User Groups	(Collection)
Credential Settings	
Credentials	(Collection)
Credentials Deactivation Date	Wednesday, February 10, 2038
Credentials have Deactivation Date	False
PIN	
PIN Required Always	False
Emergency	
Personnel	
Reader Control	
User Operate Time	0 Seconds
User Shunt Time	0 Seconds
Settings	
User Type	General User

Middle Initial
The User's Middle Initial.

User: Admin

In the Users Tab, all users currently in the system display in the list on the left. If you have a large number of users, you can use the alphabet buttons on the far left to quickly sort through the list. Users Categories display on the right. By default, these categories display as shown; however, you can click the A-Z sort button to display categories alphabetically. Here you can add or remove users from the system, set their credentials, and include any personal information needed to identify that person in the system.

If an ellipsis button displays when you select a field, additional parameters are available for selection. From here you will define user name and address information and access parameters such as readers, user groups, credentials, PIN, and so on.

Note If you see a need for additional fields to define for your Users, contact your System Administrator. They can add more fields to the Users Tab, or create additional User Fields unique to your organization.

The following sections describe each category in the Users Tab, and present steps for adding and configuring users in the system.

ID — When you add a user, the system automatically assigns them a unique ID and displays the number in the User ID field.

Name — Provides entry fields for Users' first and last name and middle initial.

Adding a User Name

1 In the Users Tab, select the Add User button. In the ID category, the system will display a new unique User ID.

2 In the First Name line, highlight and replace the default text (example: User1) with a first name.

3 In the Last Name field, highlight and replace the default text ("_New") with a last name. Add a Middle Initial if needed.

Note The Update button will flash to remind you to update your settings. You can update each time you add a user, or wait until all user information is added. The software will automatically update your settings when you exit the Users tab.

User Defined Categories and Fields— If your segment has been configured with user defined categories and fields, such as Address, City, Zip Code, enter the information as configured.

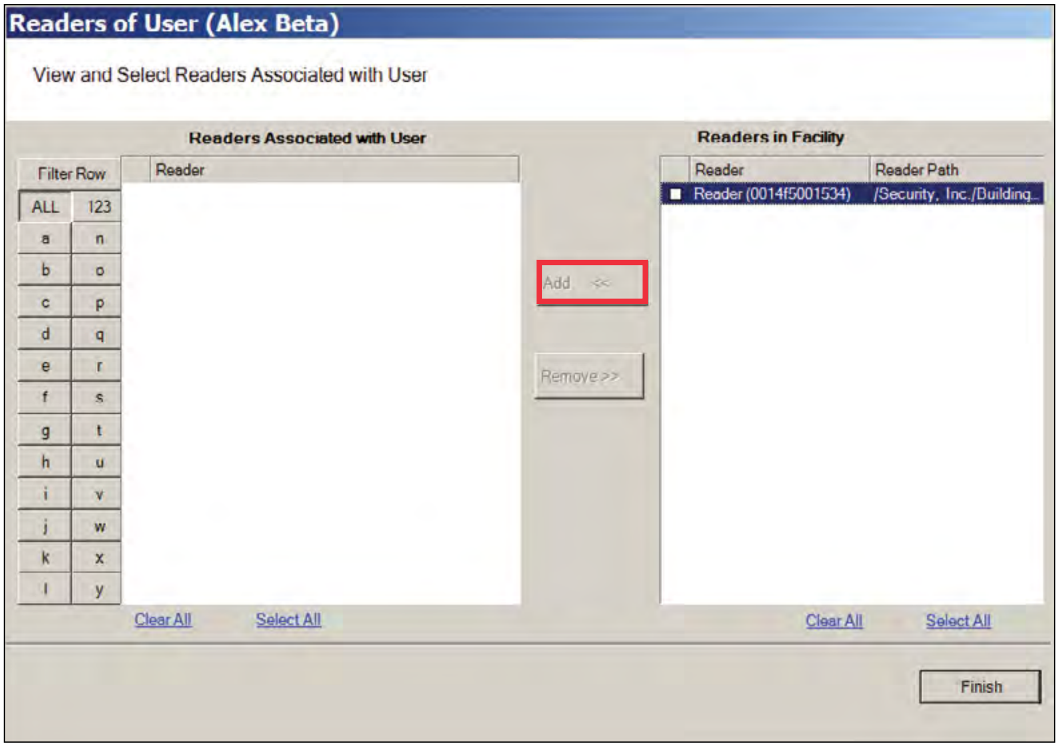
Associations — In this category, you associate Users with Readers and User Groups. This task defines which readers will recognize the User's requests for entry and exit. If User Groups have been created for your organization, these will also be available for selection from the Associations category.

To associate a user with readers

1 In the Associations category, click inside the Readers field, and select the ellipsis button at the far right.

2 The Readers of User dialog box opens and displays a list of readers available to the User.

Figure 101 Readers of User



Readers of User (Alex Beta)

View and Select Readers Associated with User

Readers Associated with User

Reader

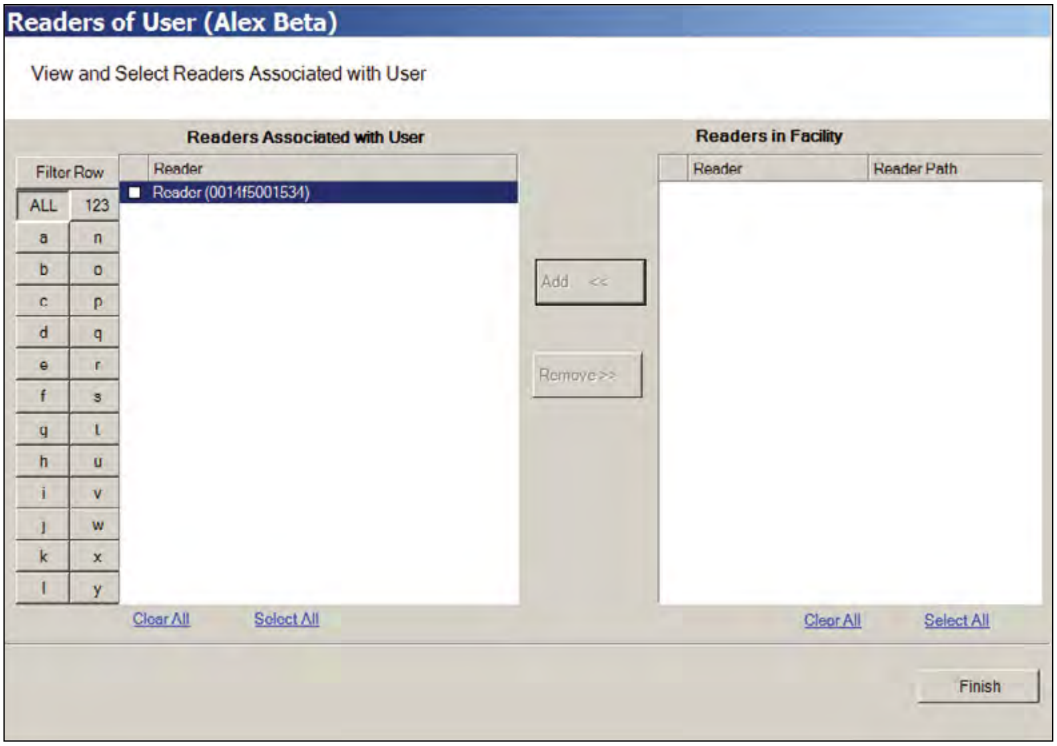
Readers in Facility

	Reader	Reader Path
■	Reader (0014f5001534)	/Security, Inc./Building...

3 Select the reader(s) from Readers in Segment.

4 Select Add <<. The selected readers are moved from the Readers in Segment list to the Readers Associated with User list on the left. You can associate a user with any number of readers.

Figure 102 Selecting a reader to associate with a user



Readers of User (Alex Beta)

View and Select Readers Associated with User

Readers Associated with User

	Reader
□	Reader (0014f5001534)

Readers in Facility

	Reader	Reader Path

5 Select OK to save your settings and return to the Users Tab.

User Groups

If User Groups have been created for your segment, these will already be associated with readers. For example, a User Group may have been defined for Laboratory Building 1. Laboratory Building1 might have six readers. By assigning the User to the Laboratory Building 1 Users Group, they will automatically be associated with all the readers in that group.

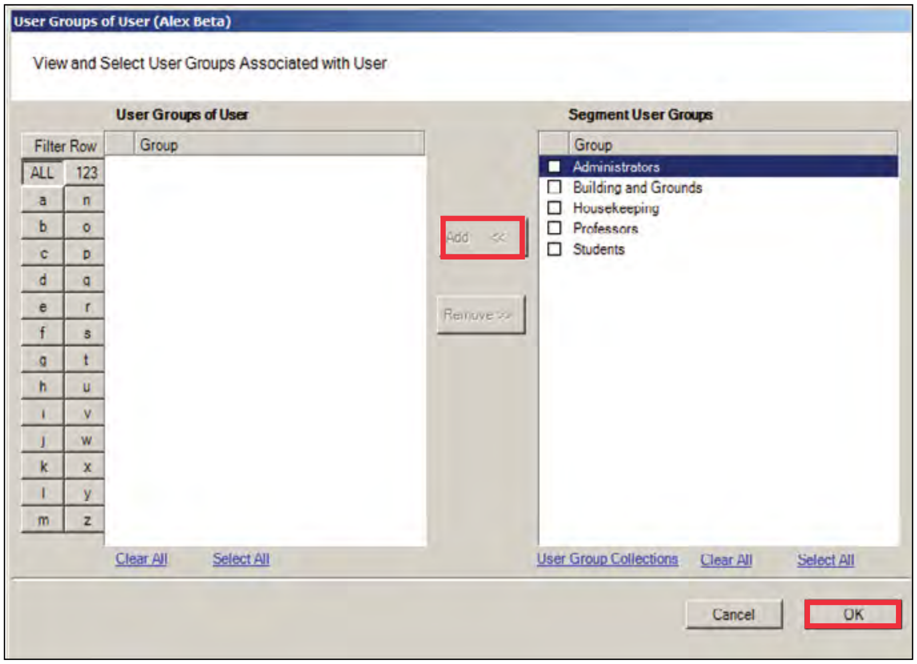
A User Group may also be defined as a Timezone Group. Timezone User Groups further define access levels for the Master Timezone. You can restrict access of certain groups of employees to a specific time period. For example, you may have a housekeeping group designated as a Timezone Group with restricted access to dormitories from 8:00 a.m. to 4:00 p.m., weekdays only. You would then assign Users from the housekeeping department to this group. Steps to add users to User Groups are presented in the following section. For more information about creating Timezone Groups, see “Timezone User Group Collections” on page 159.

Perform the following steps to add a user to a User Group.

To add a user to a User Group

1 When adding or editing a User, in the Associations Category, click in the User Groups field and click the ellipsis button. The User Groups of User dialog box opens.

Figure 103 User Groups of User



User Groups of User (Alex Beta)

View and Select User Groups Associated with User

2 Select the group(s) to associate with this user and click the Add << button. The groups are added to the User of Groups list.

3 Select OK to save your selections and return to the Users Tab. You can add or change User Groups for a user any time by returning to this list.

Credential Settings

Wi-Q AMS tracks individual requests for access or exit from the segment by their unique credentials, and each request is recorded as a transaction in the database for reference. Whether your organization uses keypad Controllers or card readers, each user will be assigned a unique credential number. Under Credential Settings, you will enter the credential ID and number, select a credential type, and set additional parameters related to the credential type. You can add another level of security by combining an individual's credential with a personal ID number (PIN). If your organization requires a PIN, you will enter them here. Credential setup is a two-step process: First, you will select the credential type to be used, then you will register the credential.

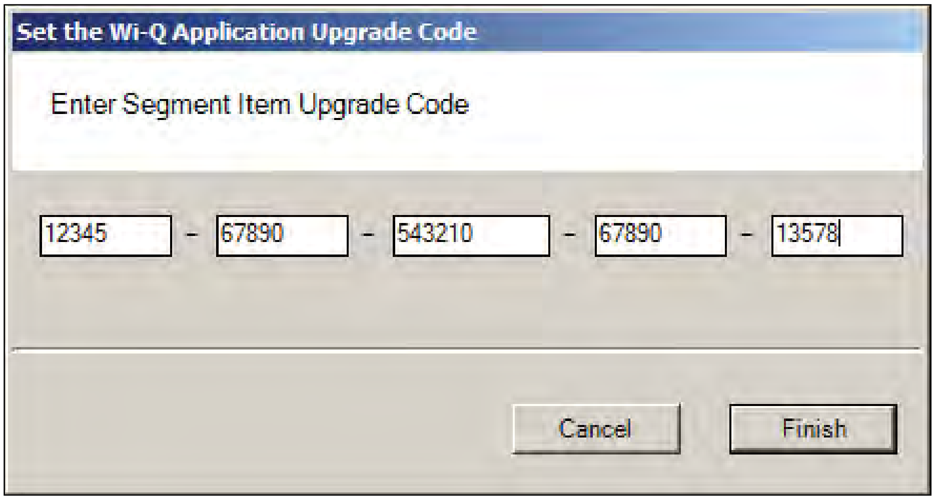
Keypad Type — The default credential type in AMS is Keypad. When you add a user to the system, the software assigns them a unique keypad credential number, then automatically registers it with the system. If your segment uses only keypads, once you add the new user name, you can skip to Adding PINs and Expirations Dates.

Card Type — If your segment uses card type credentials, you must select the card type, enter the appropriate settings, and then register the credential number with the system.

To select the card type

1 In the Users Tab, Credentials line, select the ellipsis button. The User Credentials Setup dialog box opens. The credential types are listed on the left and the categories available for each type are listed on the right.

Figure 104 Selecting a User Credential type



Set the Wi-Q Application Upgrade Code

Enter Segment Item Upgrade Code

12345 - 67890 - 543210 - 67890 - 13578

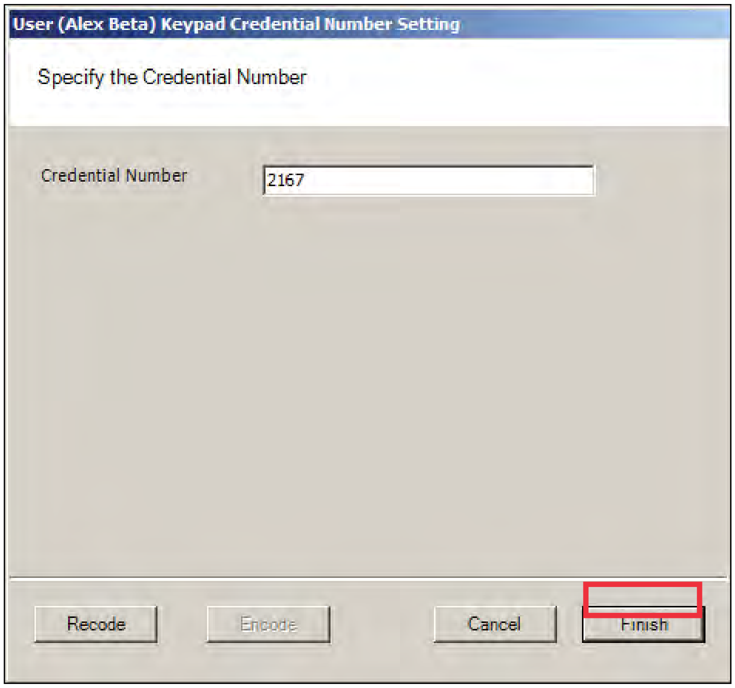
2 Select the type of credential the reader will use, for example, Keypad. The credential options in the categories on the right will change, depending on the type selected.

Passage Mode Authority — User credential has the authority to activate passage mode with 2 entries.

1st Card Unlock Authority — User credential has the authority to leave the door unlocked when in an 'unlock with ID' access mode.

3 Under the credential category, click the Number field and click the ellipsis button. The Specify the Credential Number dialog box opens.

Figure 105 Enter a user credential number



User (Alex Beta) Keypad Credential Number Setting

Specify the Credential Number

Credential Number: 2167

4 If you wish to have the software generate a new number, select Recode. Or, you may type in the user's credential number. Click Finish. You can change the credential number at a later date if needed.

5 Now you are ready to register the credential.

Note If the credential type you need is not in the list of card types on the left, you can add one. See "Adding a Credential Type" on page 148.

Credentials Deactivation Date — You can define whether a user's credentials can be automatically de-activated based on an expiration date. This is useful, for example, when entering credentials for a temporary employee or contractor. If the credential can expire, select True from the drop-down list next to the Credentials have Deactivation Date field, and then enter the de-activation date in the Credentials Deactivation Date field. If the credential cannot be de-activated, select False from the drop-down list. The default deactivation date is 26 years to ensure a user's credential is not inadvertently deactivated.

Registering the Credential

When you click on the Number field below the Credential category and select the ellipsis button, the Specify the Credential Number dialog box opens. From here, you can enter the credential number manually, scan the user's card with a scanning device connected to your computer, or specify a reader where the user will scan their card. Steps to register each type of card are presented in the next few sections.

Note If you use the reader scan method, the card used must be unassigned.

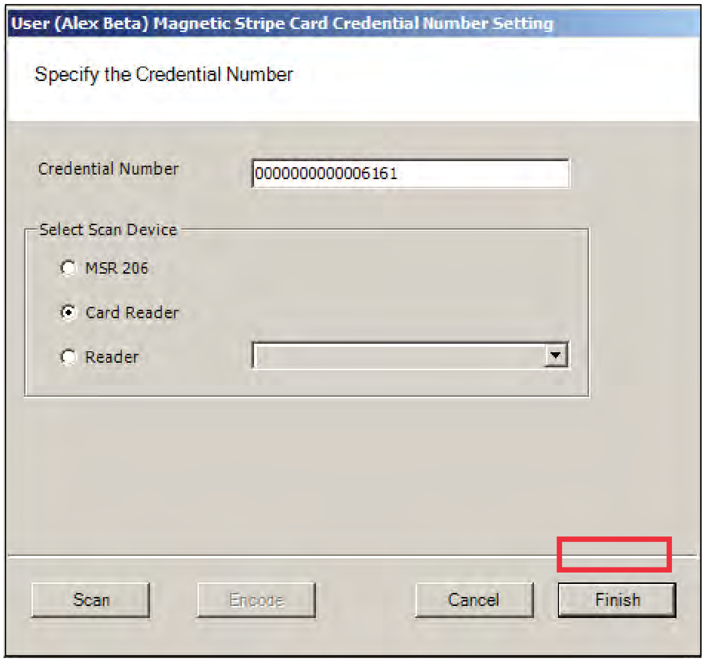
To register a Keypad credential

1. Keypad credentials are automatically registered by the system, and no further steps are required.

To register a Magnetic Stripe Card credential

1. From the User Credential Setup dialog box, select Mag Card from the list.
2. Click in the Number field and select the ellipsis button. The Users Magnetic Stripe Card Credential Number Setting dialog box opens.

Figure 106 Entering a Magnetic Card credential number



User (Alex Beta) Magnetic Stripe Card Credential Number Setting

Specify the Credential Number

Credential Number: 0000000000006161

Select Scan Device

○ MSR 206

● Card Reader

○ Reader

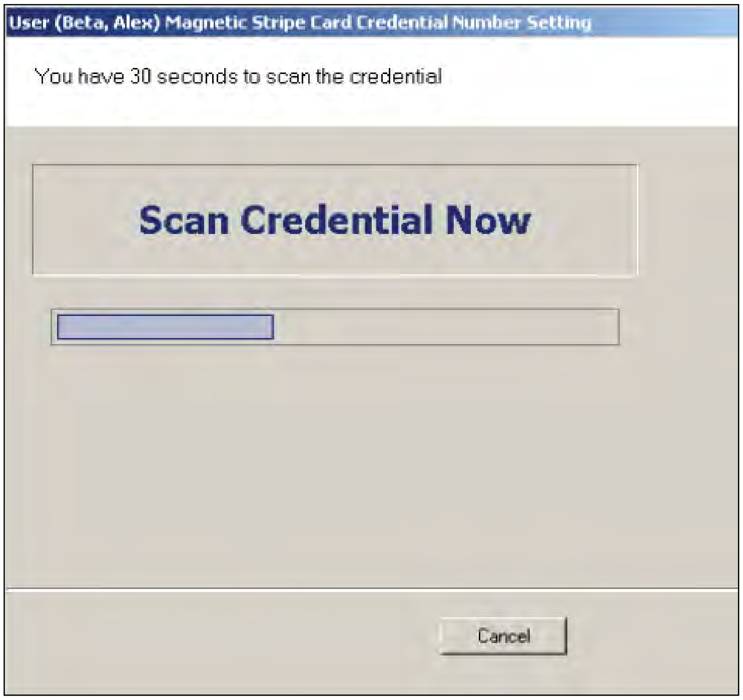
3 Enter a Credential Number manually (must be less than 16 characters, zeros will be appended) or select a scan device.

Using a scanning device to register a credential

You can use a scanning device connected to your computer to register a credential.

1 Select Card Reader. When you are ready to scan the card, select the Scan button. You will have 30 seconds to scan the card.

Figure 107 Scan Credentials



User (Beta, Alex) Magnetic Stripe Card Credential Number Setting

You have 30 seconds to scan the credential

Scan Credential Now

2 When recognized, the number will display in the Credential Number text box.

3 Select Finish and return to the Credential Setup dialog box.

Using a local reader

You can use a local reader to scan the card credentials.

1 Select Reader, and then use the drop-down list to navigate to the reader where the card will be scanned. When you are ready to scan the card, select the Scan button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.

2 Select Finish and return to the Credential Setup dialog box.

Note You may need to expand the drop-down list to view all available readers. Use the highlighted area in the lower right corner.

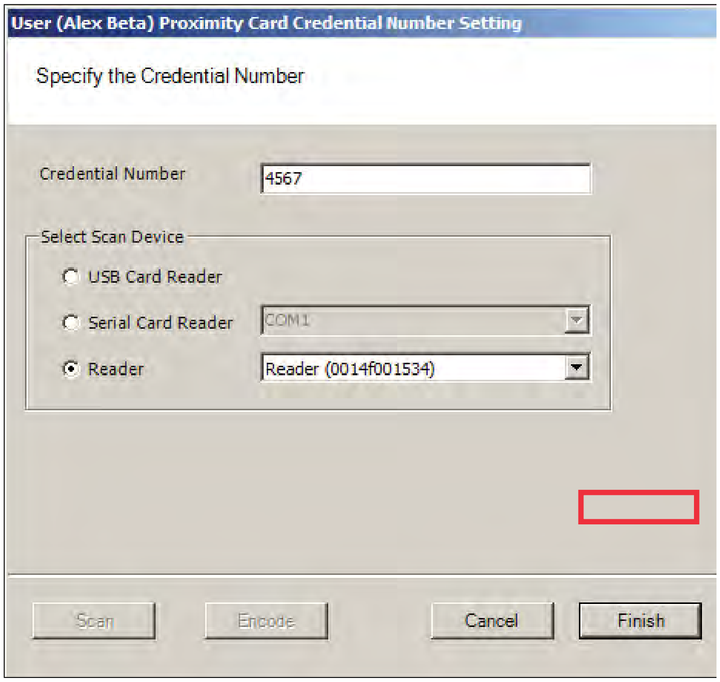
Registering a Prox card credential

In the Proximity Card category, review the Prox Card Type. If the default entry is not the one you will use, select the field and use the down-arrow to select the correct type from the list.

To register a Prox Card Credential

1 Select Prox Card from the list on the left. Click the ellipsis in the Number field, under the Credential category. The User Proximity Card Credential Number Setting dialog box opens.

Figure 108 Entering a Proximity Card credential number



User (Alex Beta) Proximity Card Credential Number Setting

Specify the Credential Number

Credential Number: 4567

Select Scan Device

○ USB Card Reader

○ Serial Card Reader: COM1

● Reader: Reader (0014f001534)

2 Enter a Credential Number manually (must be less than 16 characters, zeros will be appended) or select a scan device:

USB Card Reader

If you have a MSR 206 USB Card reader connected to your computer, select MSR 206.

1 When you are ready to scan the card, select the Scan button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.

2 Select Finish and return to the Credential Setup dialog box.

Serial Card Reader

If you have a Serial Card Reader connected to your computer, select Serial Card Reader and then select the appropriate com port from the drop-down list.

1 When you are ready to scan the card, select the Scan button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.

2 Select Finish and return to the Credential Setup dialog box.

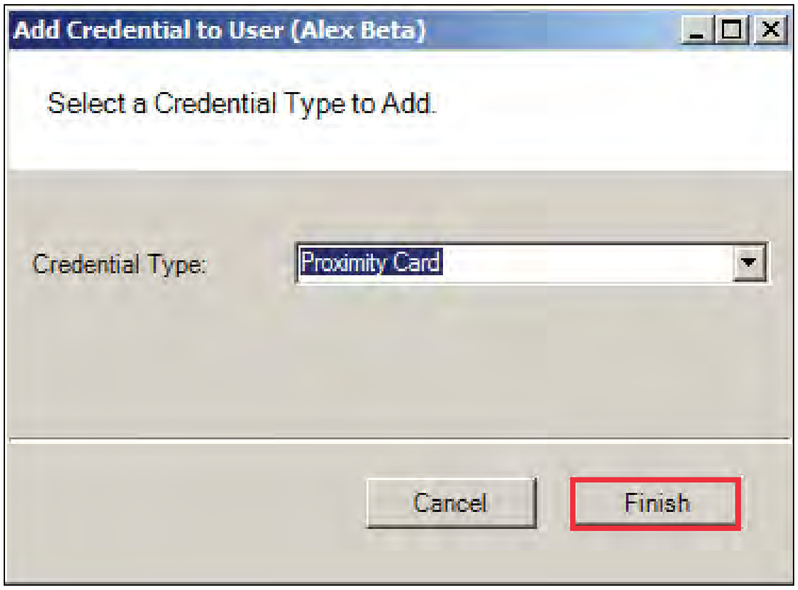
Adding a Credential Type

At least one credential type must be defined for the system. The default credential type in Wi-Q AMS is Keypad. If you use other than keypad credential types, you can add them to the User Credentials Setup dialog box.

To add a card type to the list

1 In the Users Credentials Setup dialog box, select the Add button. The Add Credential to User dialog box opens

Figure 109 Add Credential to User



Add Credential to User (Alex Beta)

Select a Credential Type to Add.

Credential Type: Proximity Card

2 Select the Credential Type from the drop-down list, in this case, Proximity Card.

3 Select Finish. The User <Proximity Card> Credential Number Setting dialog box opens.

4 Now, you may manually enter a credential number or scan the credential with a scanning device.

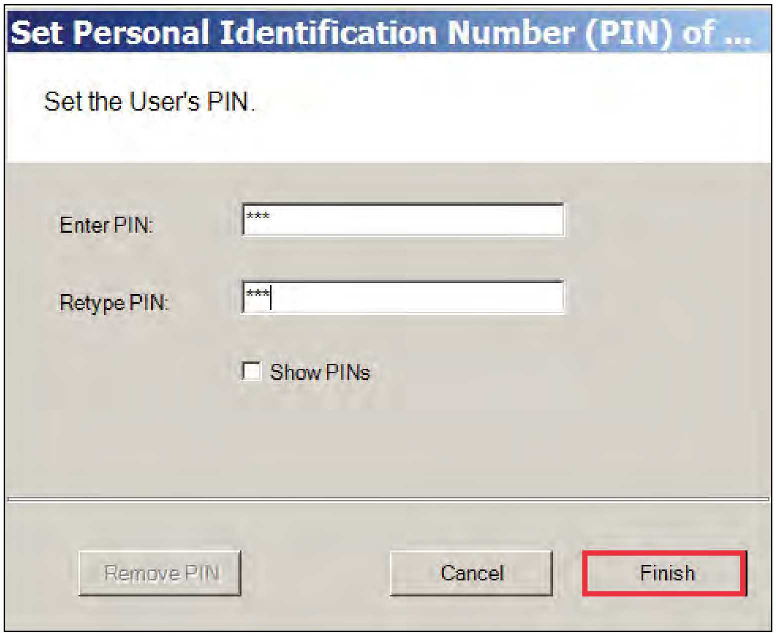
PIN

You can add a level of security by requiring PIN numbers in addition to credentials for all users, or for specific Timezone Intervals. The default displays the PIN number as asterisks in the fields; however, you can choose to show the actual PIN numbers.

To add a PIN Number for a User

1 Under Credential Settings, click the ellipsis button in the field next to PIN. The Set Personal Identification Number dialog box opens.

Figure 110 Set PIN of User



Set Personal Identification Number (PIN) of ...

Set the User's PIN.

Enter PIN: ***

Retype PIN: ***

□ Show PINs

2 Select the Show PINs check box if you wish to view the numbers instead of asterisks as you type them in.

3 Enter a PIN number for the user. Retype the PIN below.

4 Click Finish to save the PIN and exit the dialog box.

Reader Control

The system defaults the amount of time from the moment a reader unlocks until it relocks, and the amount of time a door can stay open before an alarm will be triggered. You can modify reader operate and shunt times for individual users. For example, to be ADA compliant, a user who is in a wheelchair or uses a walker may need more time to pass through a door. You can increase the shunt time for this user.

To modify User Operate Time

In the Reader Control category, click the ellipsis button next to the User Operate Time and select the amount of time you wish to leave the reader in the unlocked position.

To modify User Shunt Time

In the Reader Control category, click the ellipsis button next to User Shunt Time and select the amount of time you wish to allow for passage before an alarm will be triggered.

Settings

Each segment user will be assigned a User and Access type, depending on the tasks they perform and the access mode needed to perform those tasks. The system supports three different types of users: General Users, Managers, and Programmers. You can have up to 65,000 individual users in the system and they can be of any User Type. User types are briefly described in the following paragraphs.

General Users — The majority of users will be assigned as General Users. They are allowed entry only when the access level is set to ID Required. General Users never have access when the reader is in Lockout.

Manager — Managers are one of the most useful types of IDs. This User Type provides the capability to change the access level of a reader with a few simple key presses. These changes can and will be overridden by the time schedule or another manager or programmer. A user with Manager privileges is always allowed access to a reader. For example, when a segment requires an individual to have access at all hours of the day without giving any extra privileges, that individual will be assigned Manager Privileges.

Programmer — Programmers can scan all channels at the keypad reader as well as reset the reader to respond to keypad commands as in manager mode.

Note Managers and programmers are indistinguishable from a general user when no keypad is present.

For a list of Manager and Programmer system override codes, see “System Overrides” on page 177.

To assign User Type

1. Under the User Tab, in the Settings category, select the field next to User Type.
2. Select a User Type from the drop-down list.

Wi-Q Gateway and Reader Control and Messaging

Wi-Q AMS provides a number of features to reset and restore normal operations, override locks and access levels, and temporarily remove reader association with a Portal. These right-click functions send real-time instant messages to the hardware from within the software.

Wi-Q Gateway Controls

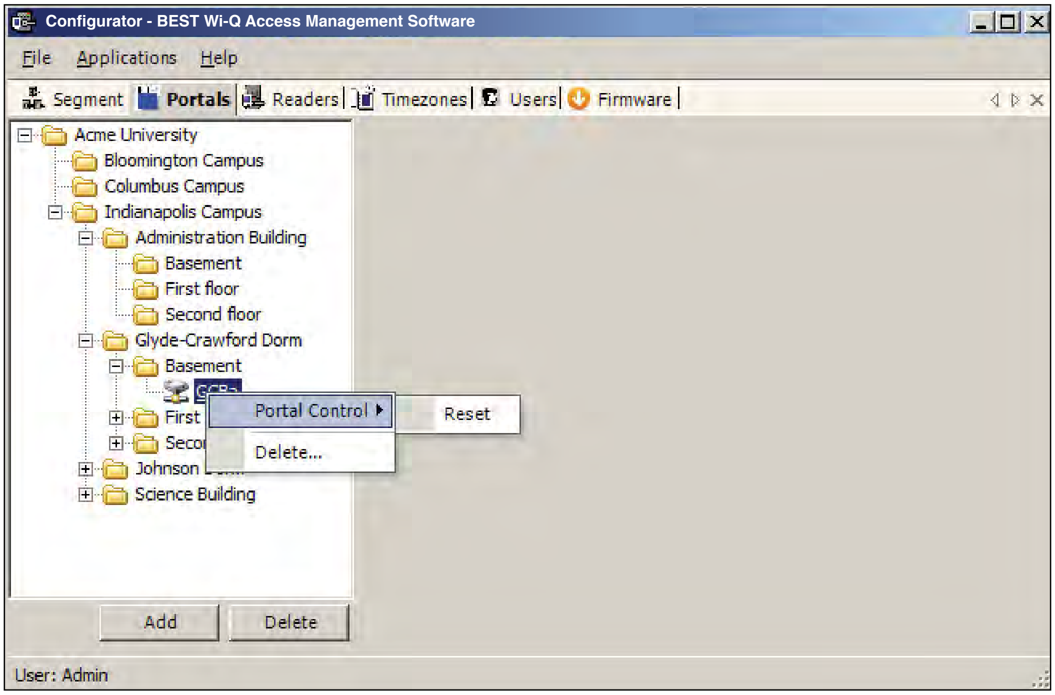
You can delete, reset and restore a Wi-Q Gateway to normal operation without going to the physical location of the Portal. These functions are accessible via a right-click in the Readers tab of the Configurator module. You can also delete a Wi-Q Gateway from the system with the right-click function.

To access right-click Wi-Q Gateway messaging

1 In the Portals Tab, right-click on the Portal and select the option from the drop-down list. The software will ask you if you wish to proceed with the operation.

2 Click Yes. If the Portal is online, the operation is performed. If for any reason the Portal is offline and unable to execute the command, the message will become obsolete after five minutes.

Figure 111 Right-click Portal messaging options



Note Momentary unlocks and overrides must be recognized and executed by the Portal within five minutes of the command or they become obsolete. This feature ensures that commands executed during the period when the hardware cannot respond are not executed when the hardware is back online.

Reader Controls

You can delete, reset and restore a reader to normal operation without going to the physical location of the reader. In addition to these commands, you can momentarily unlock, override the access level, perform a deep reset and remove the reader's association to a Portal all from within the software. These functions are accessible via a right-click in the Readers tab of the Configurator module. You can also delete a reader from the system with the right-click function.

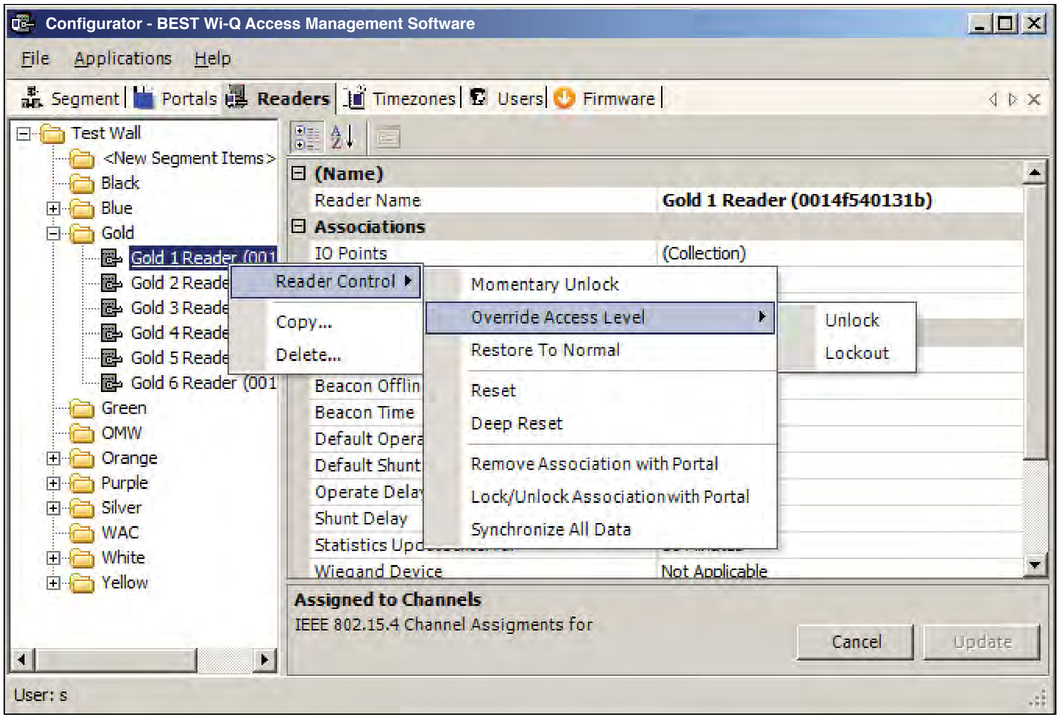
Note To delete more than one reader at a time, hold down the control key (CTRL) and select using the left mouse key.

To Access Right-Click Reader Messaging

1 In the Readers tab Segment Tree, right-click on the reader and select the option from the drop-down list. The software will ask you if you wish to proceed with the operation.

2 Click Yes. If the reader is online, the operation is performed. If for any reason the reader is offline and unable to execute the command, the message will become obsolete after five minutes.

Figure 112 Right-click reader messaging options



(Name)

Reader Name: Gold 1 Reader (0014f540131b)

Associations

IO Points: (Collection)

Beacon Offlin

Beacon Time

Default Opera

Default Shunt

Operate Dela

Shunt Delay

Statistics Upd

Wiegand Device: Not Applicable

Assigned to Channels

IEEE 802.15.4 Channel Assigments for

Momentary Unlock — A user with appropriate permissions can override the standard Timezone conditions to temporarily unlock the door controlled by a reader. The reader goes through a normal unlock-lock cycle where the default shunt and operate times apply. As soon as the command is executed, the standard Timezone conditions are restored.

Override Access Level — A user with appropriate permissions override the reader's access level. The override can be defined to last until the next timezone interval occurrence or to remain until a restore to normal message is sent. As soon as the command is executed, the standard Access Level conditions are restored.

Restore to Normal — Immediately restores all standard normal operation.

Reset and Deep Reset — These options allow you to perform a reset and a deep reset on a reader from within the software. The function is the same as performing a manual reset or deep reset at the reader hardware.

Remove Association with Portal — This command is useful when the reader has associated with a different Portal or is being removed from the segment. When you remove the reader's association with the assigned Portal, it will search for another Portal and resume communication.

Lock/Unlock Association with Portal — Locking a reader's association with a Portal will disallow its communication with other Portals. Unlocking an association will re-allow communication with other Portals in range.

Synchronize All Data — This command will resend all reader information to the Portal and update the reader hardware.

Note All overrides must be recognized and executed by the Portal within five minutes of the command or they become obsolete. This feature ensures that commands executed during the period when the hardware cannot respond are not executed when the hardware is back online.

Configuring Timezones

For the greatest majority of facilities, the default access level provided in the Master Timezone gives you all the options you need to manage your segment. The system works by defining different access levels at a controller rather than different times of day the segment is locked or unlocked. However, it may become necessary to define a new Timezone under certain circumstances. For example, you may want to define a separate Timezone for a specific set of readers that would operate on a totally different schedule from the main system. For this application, you would create a different Timezone and then assign the readers to that Timezone.

Timezones are created and configured in the Timezones tab within the Configurator module. Three sub-tabs exist inside the Timezone tab:

- Interval Collections — this is a collection of recurring ranges of time and days of the week, such as 6:00 am to 6:00 pm weekdays AND 8:00 am to 8:00 pm weekends.
- Reader Control — this is where you assign access levels to readers and determine how the reader will operate during assigned timezone intervals.
- User Group Collections: this is where you can add user groups to a collection and define timezone intervals to the collection.

Note Readers can be assigned to only one Timezone.

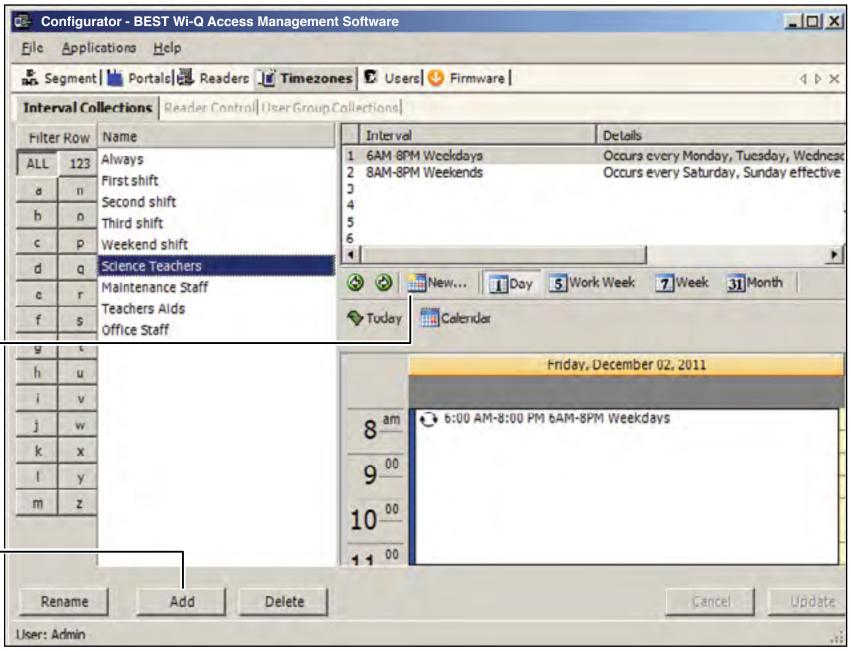
To create a Timezone Interval Collection

1 Select the Interval Collections Tab under the Timezones Tab. The Interval Collection window opens.

2 Click the Add button to create a new Timezone Interval Collection.

3 Click the New button to create a new interval.

Figure 113 Interval Collection



	Interval	Details
1	6AM-8PM Weekdays	Occurs every Monday, Tuesday, Wednesc
2	8AM-8PM Weekends	Occurs every Saturday, Sunday effective
3		
4		
5		
6		

Click New to create a new interval.

Click Add to create an Interval Collection.

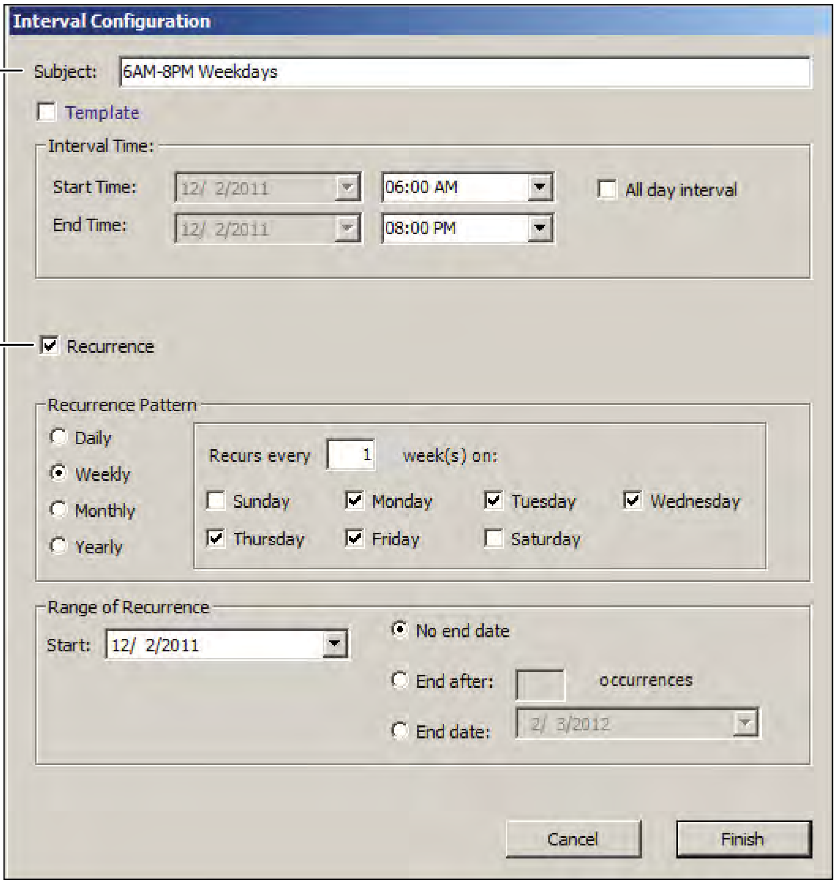
4 The Interval Configuration window opens.

5 Enter a brief name for the Interval.

6 Select the Start and End Time of the Interval.

7 Click the Recurrence checkbox.

Figure 114 Interval Configuration



Name the Interval. Tip: usually good practice to name Intervals by time ranges.

Click Recurrence if the interval repeats.

Interval Configuration

Subject: 6AM-8PM Weekdays

□ Template

Interval Time:

Start Time: 12/ 2/2011 06:00 AM □ All day interval

End Time: 12/ 2/2011 08:00 PM

☑ Recurrence

Recurrence Pattern

○ Daily
● Weekly
○ Monthly
○ Yearly

Recurs every 1 week(s) on:

□ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday
☑ Thursday ☑ Friday □ Saturday

Range of Recurrence

Start: 12/ 2/2011

● No end date
○ End after: occurrences
○ End date: 2/ 3/2012

8 Select the Recurrence Pattern of the Interval.

9 Select the Range of Recurrence for the Interval.

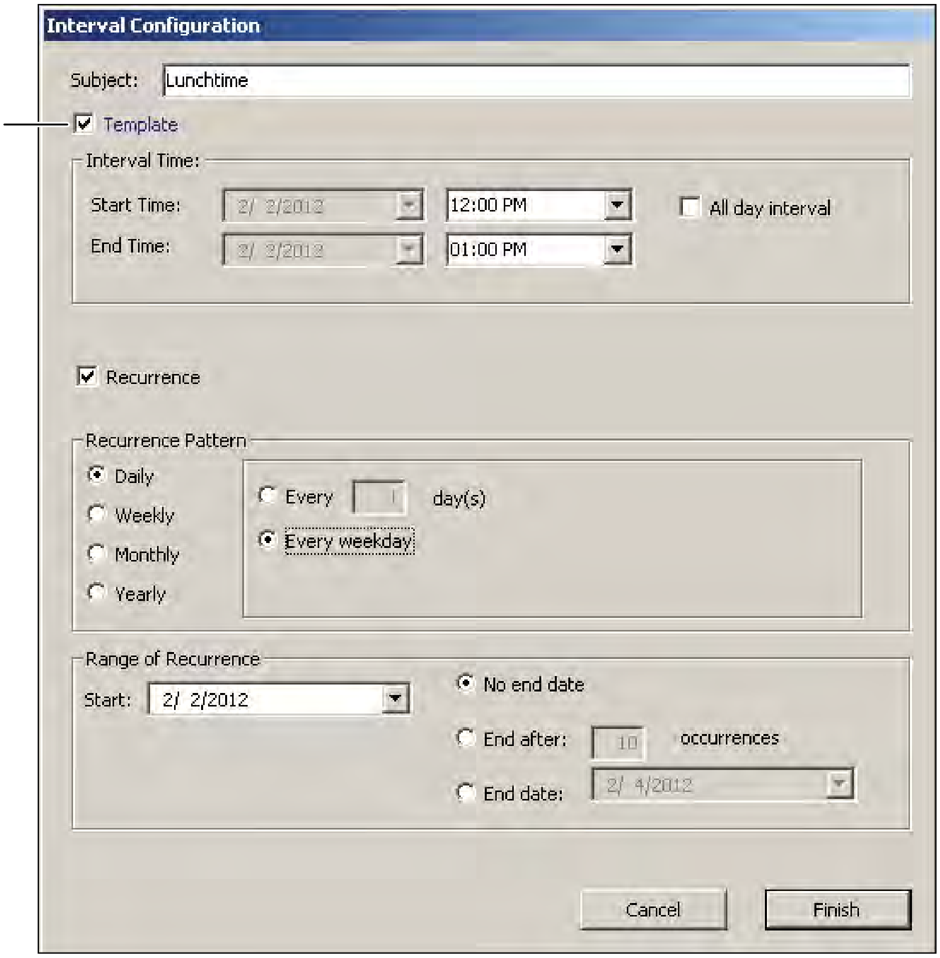
10 Click Finish to save your new Interval. This Interval is now listed as one of the intervals for the Interval Collection.

11 Repeat steps 3 to 9 to create other Intervals until the Interval Collection is complete.

Timezone Interval Template Feature

At the top of the Interval Configuration window, there is a “Template” checkbox. Selecting this box will allow the timezone interval you configure to be used as a template for other intervals. For example, if you create a “Lunchtime” interval collection between 12 pm and 1 pm, and you select the “Template” checkbox (Figure 115), you can add that interval to an existing collection.

Figure 115 Interval Configuration Template



Template

Interval Configuration

Subject: Lunchtime

☑ Template

Interval Time:

Start Time: 2/ 2/2012 12:00 PM □ All day interval

End Time: 2/ 2/2012 01:00 PM

☑ Recurrence

Recurrence Pattern

● Daily
○ Weekly
○ Monthly
○ Yearly

○ Every 1 day(s)
● Every weekday

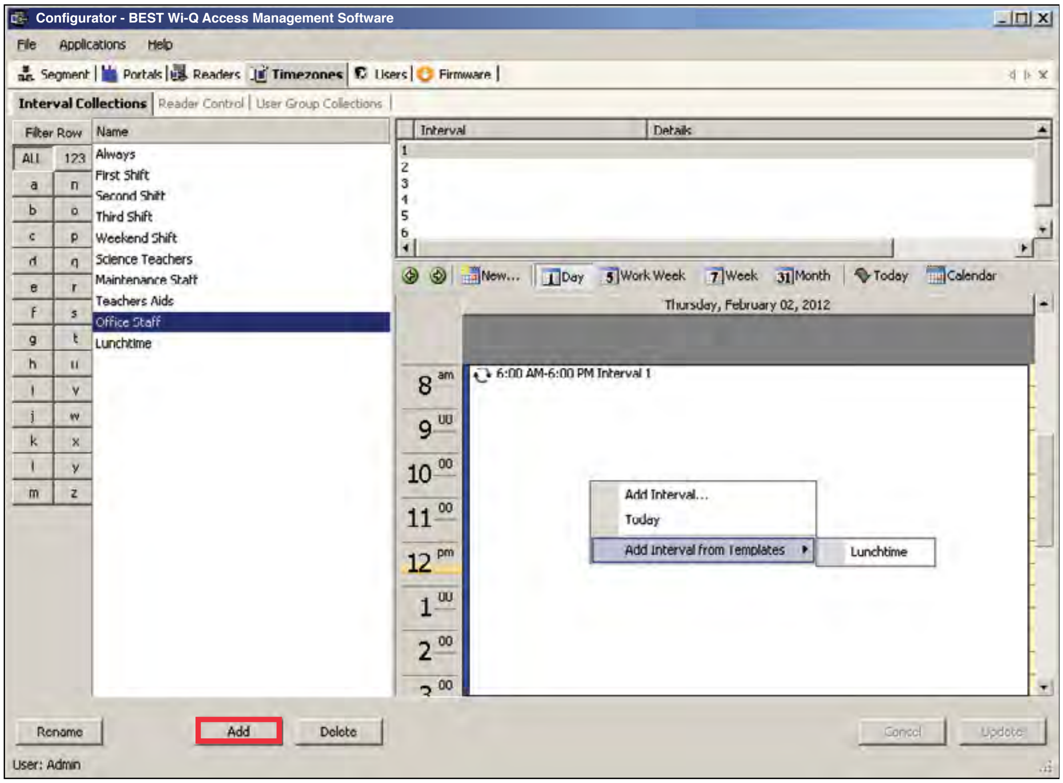
Range of Recurrence

Start: 2/ 2/2012

● No end date
○ End after: 10 occurrences
○ End date: 2/ 4/2012

To add the “Lunchtime” interval to another collection , select the existing interval collection from the list at the left, right-click in the calendar area, and select “Lunchtime” from the Add Interval from Templates options. In our example, we add the Lunchtime interval to the Office Staff Interval Collection. See Figure 116.

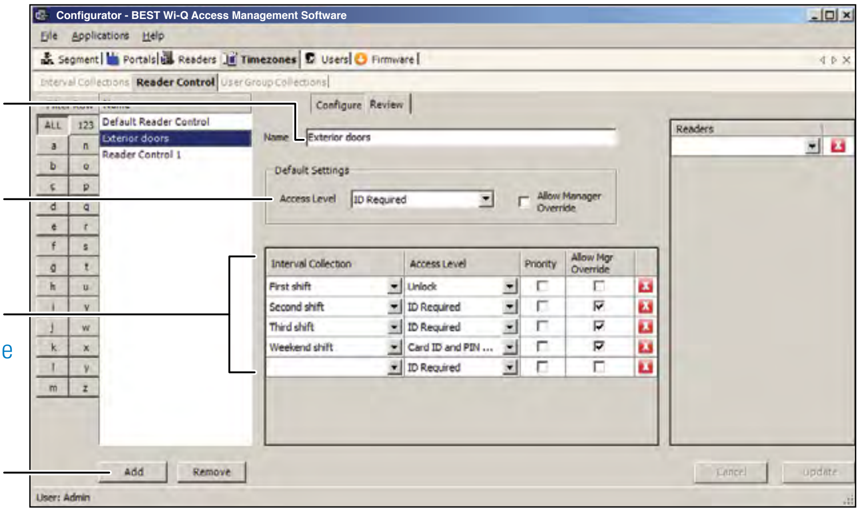
Figure 116 Add Interval from Templates



To create a Timezone Reader Control

1. Select the Reader Control Tab under the Timezones Tab. The Reader Control Window opens.
2. Click Add to create a new Reader Control.
3. Enter a brief name for the Reader Control.
4. Select the default Access Level that will be operate for the Reader Control. This access level can be overridden for specific Interval Collections.
5. Select the Interval Collections when the Reader Control will operate.
6. Use the red X to delete the interval collection if needed.
7. Click Update to complete the Reader Control.
8. Select the Readers that will operate under this Reader Control.

Figure 117 Reader Control


Configurator - BEST Wi-Q Access Management Software
File Applications Help
Segment Portals Readers Timezones Users Firmware
Interval Collections Reader Control User Group Collections
Configure Review
ALL 123 a b c d e f g h i j k l m n o p q r s t u v w x y z
Add Remove Cancel Update
User: Admin

Default Reader Control
Exterior doors
Reader Control 1

Name: Exterior doors

Default Settings

Access Level: ID Required ☐ Allow Manager Override

Interval Collection	Access Level	Priority	Allow Mgr Override
First shift	Unlock	☐	☐
Second shift	ID Required	☐	☑
Third shift	ID Required	☐	☑
Weekend shift	Card ID and PIN ...	☐	☑
	ID Required	☐	☐

Readers

Name the Reader Control.

Select what access level is required for this Reader Control.

Select the Interval Collections when the Reader Control will operate.

Click Add to create a new Reader Control.

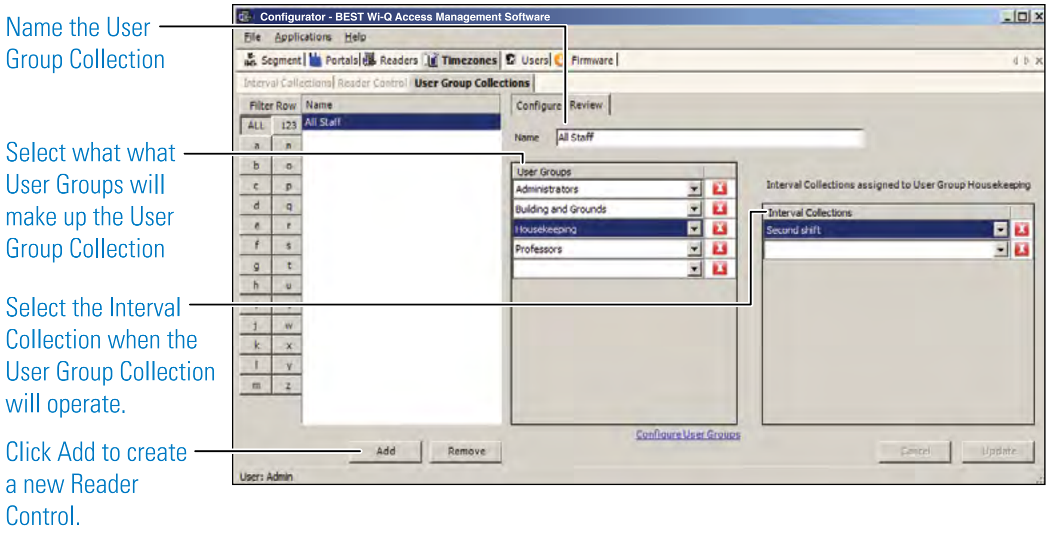
Timezone User Group Collections

You can create up to 32 Timezone User Groups to further define access levels for the Master Timezone. You can restrict access of a certain group of employees to a specific time period. For example, you may want to create a housekeeping group, designate it as a Timezone Group, and then restrict access to dormitories only from 8:00 a.m. to 4:00 p.m., weekdays. This is a two-step process. First, you will create a Users Group and designate it as a Timezone Group; then you will define the Timezone Interval for the new Timezone Group (you may want to review User Groups before starting this task).

To create the Timezone User Group Collection

1. Select the User Group Collection Tab under the Timezones Tab. The User Group Collection window opens.
2. Click Add to create a new User Group Collection.
3. Enter a brief name for the User Group Collection.
4. Select the User Groups that will be a part of the User Group Collection. You must have set up User Group for the selections to be available.
5. Select the Interval Collections when the User Group Collection will operate. You must have set up Interval Collections for the selections to be available.
6. Use the red X to delete the association of User Groups or Interval Collections as needed. This will not delete the User Group or Interval Collections, it will only delete the association.
7. Click Update to complete the User Group Collection.

Figure 118 Creating the timezone user group collection


Configurator - BEST Wi-Q Access Management Software
File Applications Help
Segment | Portals | Readers | Timezones | Users | Firmware |
Interval Collections | Reader Control | User Group Collections
Filter Row
ALL 123
a n
b o
c p
d q
e r
f s
g t
h u
i v
j w
k x
l y
m z
Name
Configure Review
User Groups
Interval Collections
Configure User Groups
Add
Remove
Cancel
Update

Name: All Staff

User Groups: Administrators; Building and Grounds; Housekeeping; Professors

Interval Collections assigned to User Group Housekeeping

Interval Collections: Second shift

User: Admin

Name the User Group Collection

Select what what User Groups will make up the User Group Collection

Select the Interval Collection when the User Group Collection will operate.

Click Add to create a new Reader Control.

6 Using and Managing the System

Wi-Q AMS and Omnilock provides powerful tools to manage your system: Configurator, Transactions, Statistics Monitor and Reports.

If you are the Program Administrator responsible for setting up communications between the software and system Portals and Controllers; you will spend most of your time using Configurator. 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 Configurator. If you are responsible to oversee security for your organization, you will monitor all access and alarm activity using Transactions. If you are the person responsible to ensure the system is operating at maximum performance, you will use the Statistics Monitor. If your organization is small, you may use all three! You can access all applications from the Configurator main menu. You can also access these applications from the Windows Start Menu under BEST Access.

Wi-Q AMS and Omnilock Configurator

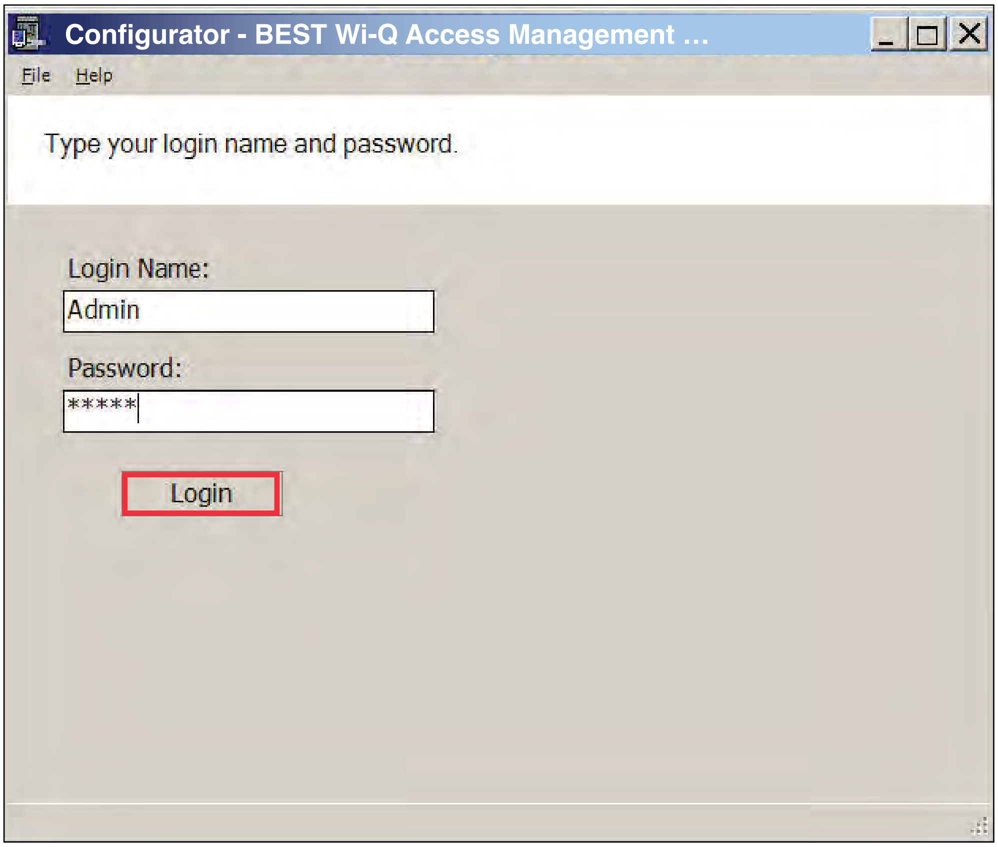
The following sections describe the essential functions you can perform using Configurator.

Launching Wi-Q AMS Configurator

When the software is loaded onto your computer, it places a shortcut to AMS on your desktop.

1 Double-click the Configurator icon to start the application. The splash screen appears briefly, then the Login dialog box opens.

Figure 119 Logging in to Configurator



Configurator - BEST Wi-Q Access Management ...

Type your login name and password.

Login Name: Admin

Password: *****

If you are a AMS User, your System Administrator or IT representative must provide you a Login Name and Password. You will need this to login to the Configurator. If you are a System Administrator, see “Logging in to Configurator” on page 65 for more information about launching the software for the first time.

To Login to the Wi-Q AMS Configurator:

1 Enter your case-sensitive Login Name and Password.

2 Select Login. Configurator opens at the Segment tab.

3 If the System Administrator has created only one segment, you are ready to begin. If more than one segment has been created, select the segment from the drop-down list. Any elements you access in Configurator will be directed to that segment.

WARNING: Once the System login and password have been personalized for your segment, it is important to record the information in hard copy form and safeguard it in a location known to management.

Managing Application Users

Wi-Q AMS and Omnilock ‘Application Users,’(AMS Users) as opposed to ‘cardholders,’ are those individuals who will operate one or all of software applications. For example, an application user might be a person in the Security department who will use only the Transactions software to monitor system access activity. Another AMS User might be a person in Human Resources or Administration who is assigned to add users to the system or change their settings.

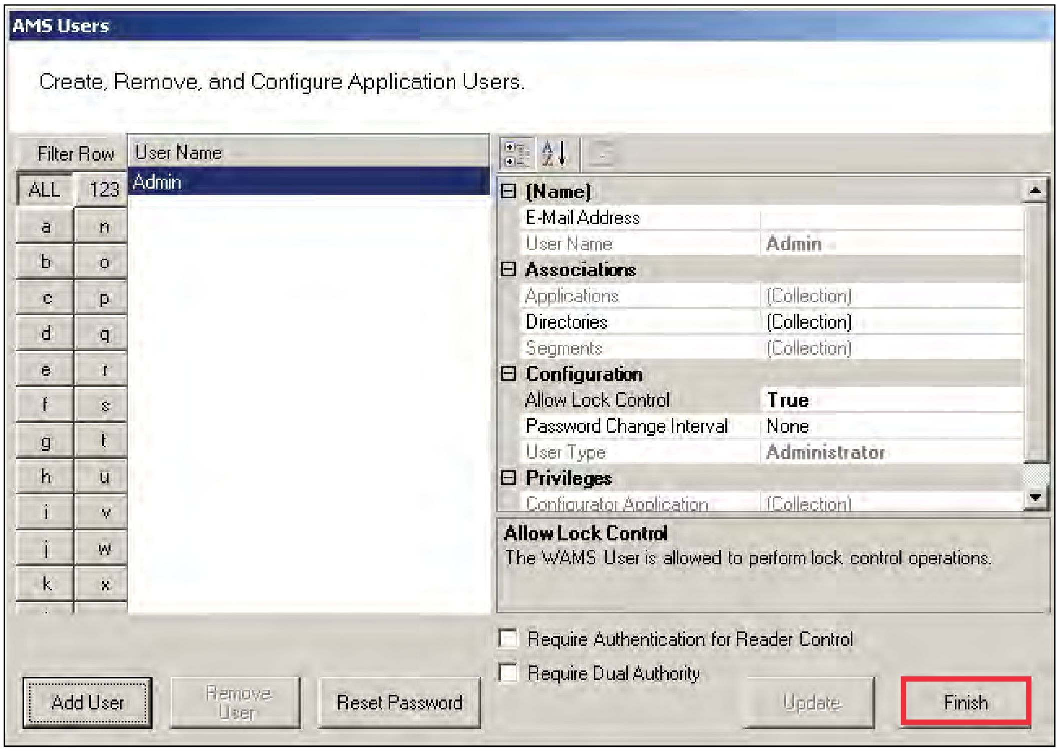
AMS Users must be added to the system as cardholders because they will require some type of physical access to the segment. However, they must also be assigned as AMSUsers and be given User names and Passwords if they are to access and operate application software.

Access the Manage Application Users features via the Configurator File Menu.

To Manage Applications Users:

1 From the Configurator main screen, select File>Manage Application Users. The AMS Users dialog box opens.

Figure 120 AMS Users



AMS Users

Create, Remove, and Configure Application Users.

User Name

Admin

⊟ [Name]

E-Mail Address

User Name Admin

⊟ Associations

Applications (Collection)

Directories (Collection)

Segments (Collection)

⊟ Configuration

Allow Lock Control True

Password Change Interval None

User Type Administrator

⊟ Privileges

Configurator Application (Collection)

Allow Lock Control

The WAMS User is allowed to perform lock control operations.

□ Require Authentication for Reader Control

□ Require Dual Authority

From here you can add or remove an AMS User, associate them with applications and specific facilities, and configure their lock control privileges, password change interval and assign a User Type. You can select whether require authentication for reader control or require dual authority for this user.

To add an AMS User:

1 In the AMS Users dialog box, click Add User. The system creates “User1” in the left column.

2 In the Name category on the right, enter an e-mail address (optional), and the user name.

3 Under Associations, click the Applications field, then click the ellipsis button at the far right.

4 Select which application(s) the User will have access to. Then click Finish.

5 In the Directories field, click the ellipsis button. Select the directories linked to the User. Then, click Finish.

6 In the Segments field, click the ellipsis button. Select which segments the User will have access to and supply contact information as needed.

7 Under the Configuration category, in the Allow Lock Control field, select either True or False from the drop-down list.

8 In the Password Change Interval field, select a change interval from the drop-down list.

9 In the User Type field, select a User Type from the drop-down list. (User Types are defined in the following paragraphs.)

10 If the user will require Authentication for Reader Control or Dual Authority, select these options at the bottom of the sheet.

11 Click Finish to save your settings.

User Types

AMS Users can be one of four User Types: Administrator, Manager, Service, and General. You will be assigned a User Type depending on which applications you will log in to and operate.

Administrator — has access to all applications and all segments. This User Type would be assigned to a System Administrator, that is, someone who is responsible for set up and configuration.

Manager — has access to all applications. This type would, for example, be assigned to someone responsible for adding users to the system. As an additional security measure, this type could be restricted to access specific segments only.

Service — has access to Transactions and Statistics Monitor. This User Type can also be restricted to specific segments only, if needed.

General User — has access only to the Transactions and Reports applications for specific facilities. This user type would be assigned to someone in Security for example, who will monitor daily entry and exit activity and system alarms. They can not access the Configurator application.

Once an Administrator has logged in to the system, they can add AMS Users to the system. If you are designated as an AMS User, you will be assigned a login User Name and Password to access the software application(s) you need.

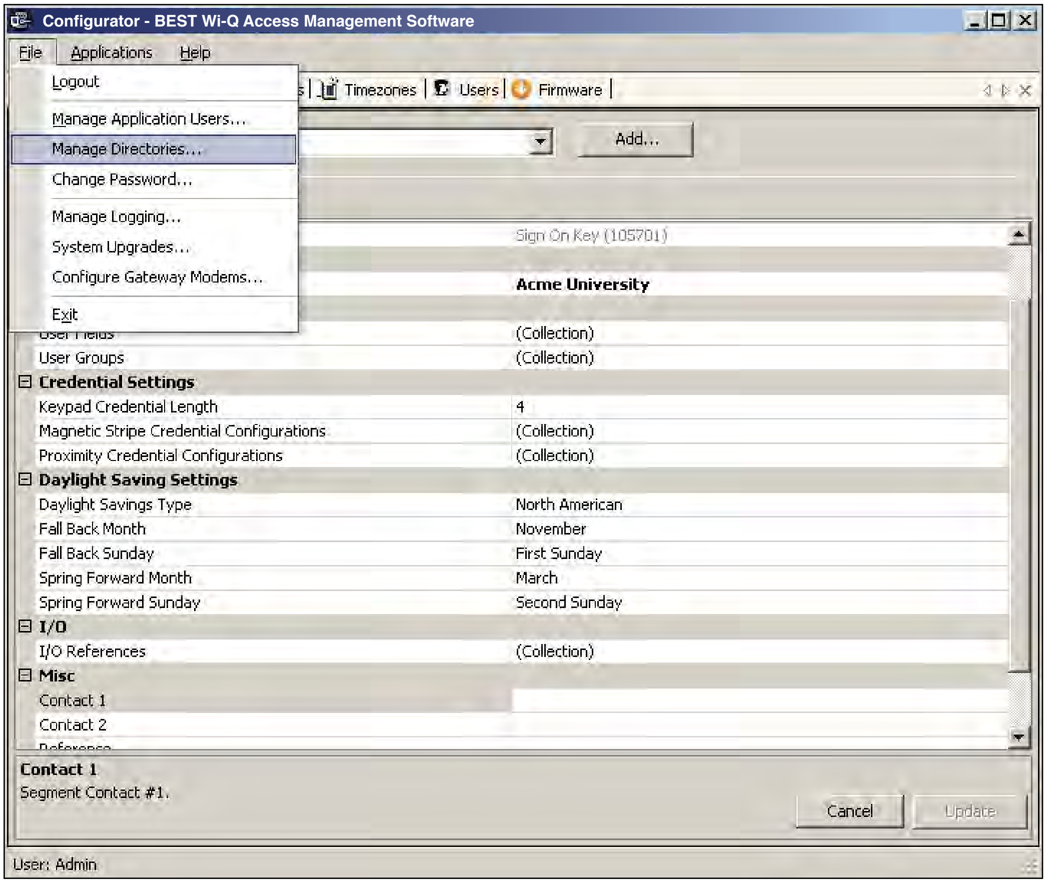
Linking AMS Users' Windows Accounts to Configurator

You can change the Configurator login settings so that your Windows account is linked to Configurator. This way, when you are logged into your Windows account, you won't need a login ID or password when signing in to Configurator.

To link your Windows account to Configurator, perform the following steps.

1 From the Configurator File menu, select Manage Directories.

Figure 121 Manage Directories

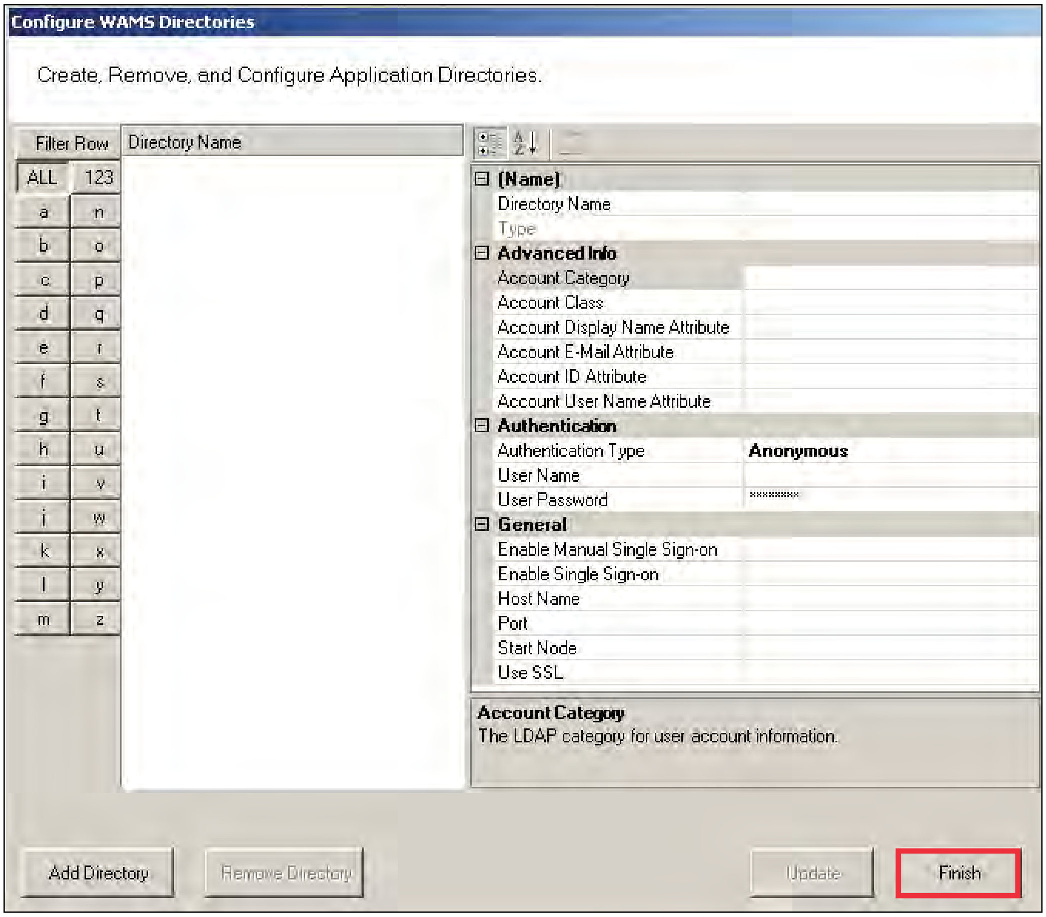


	Sign On Key (105701)
	Acme University
User Fields	(Collection)
User Groups	(Collection)
Credential Settings	
Keypad Credential Length	4
Magnetic Stripe Credential Configurations	(Collection)
Proximity Credential Configurations	(Collection)
Daylight Saving Settings	
Daylight Savings Type	North American
Fall Back Month	November
Fall Back Sunday	First Sunday
Spring Forward Month	March
Spring Forward Sunday	Second Sunday
I/O	
I/O References	(Collection)
Misc	
Contact 1	
Contact 2	
Reference	

Contact 1
Segment Contact #1.

2 The Configure Directories dialog box opens. Click on Add Directory.

Figure 122 Configure Directories


Configure WAMS Directories

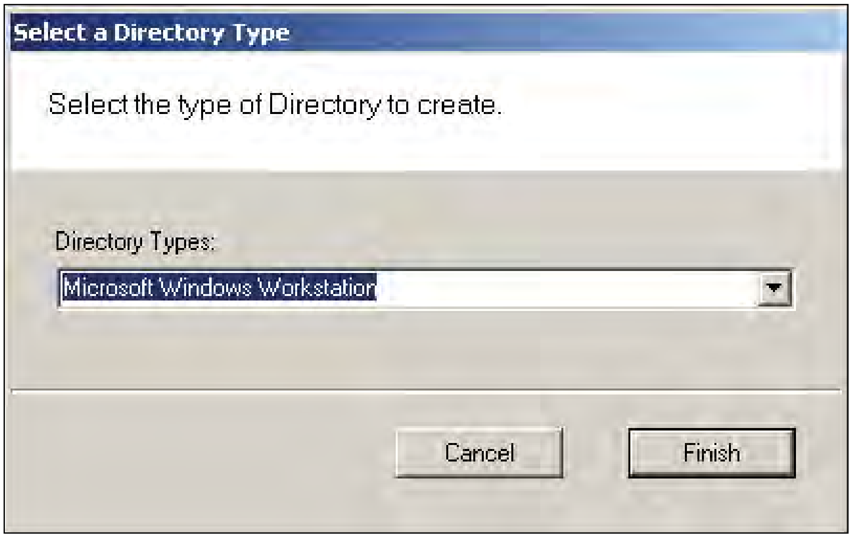
Create, Remove, and Configure Application Directories.

(Name)	
Directory Name	
Type	
Advanced Info	
Account Category	
Account Class	
Account Display Name Attribute	
Account E-Mail Attribute	
Account ID Attribute	
Account User Name Attribute	
Authentication	
Authentication Type	**Anonymous**
User Name	
User Password	********
General	
Enable Manual Single Sign-on	
Enable Single Sign-on	
Host Name	
Port	
Start Node	
Use SSL	

Account Category
The LDAP category for user account information.

3 The Select a Directory Type window opens. From the Directory Types dropdown list, choose Microsoft Windows Workstation. Then, click Finish.

Figure 123 Select a Directory Type


Select a Directory Type

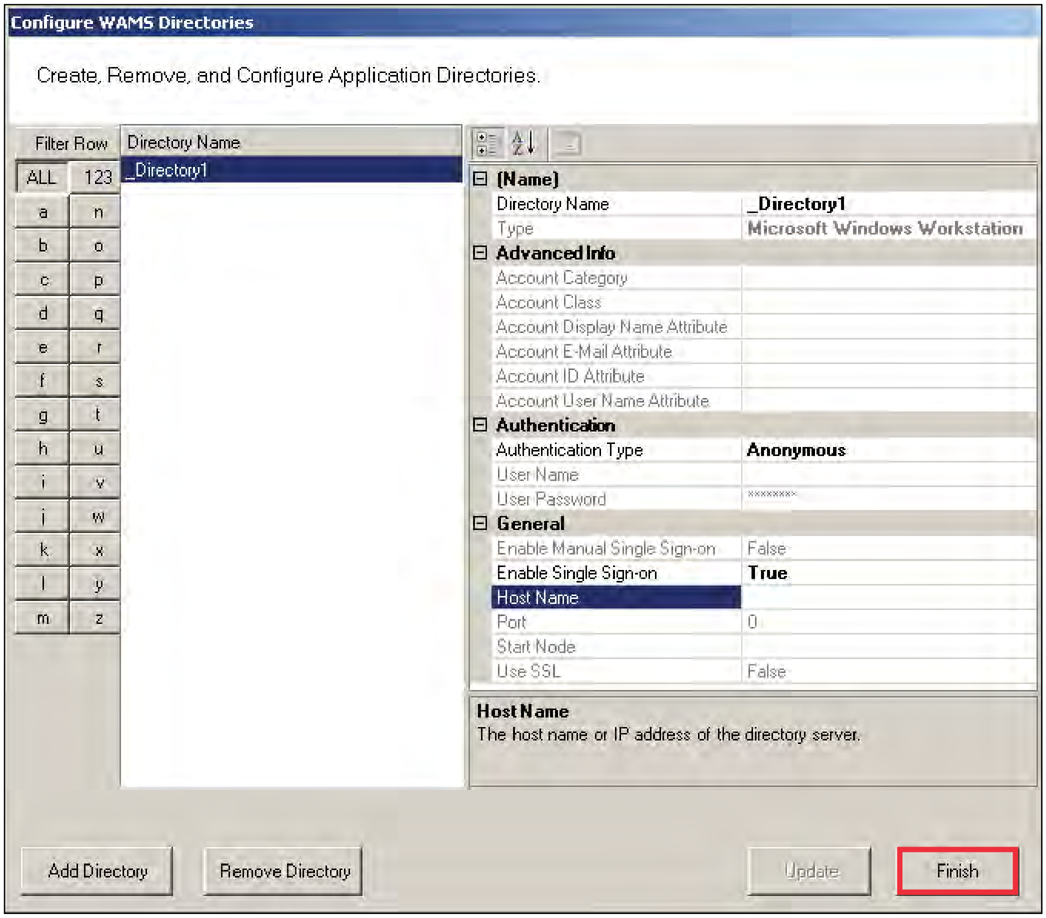
Select the type of Directory to create.

Directory Types: Microsoft Windows Workstation

4 In the Directory Name field, specify a name for the new directory or leave in the default

name. In the Host Name field, under the General category, type in the computer name of the host. Then, click Finish.

Figure 124 Directory and Host Names



Configure WAMS Directories

Create, Remove, and Configure Application Directories.

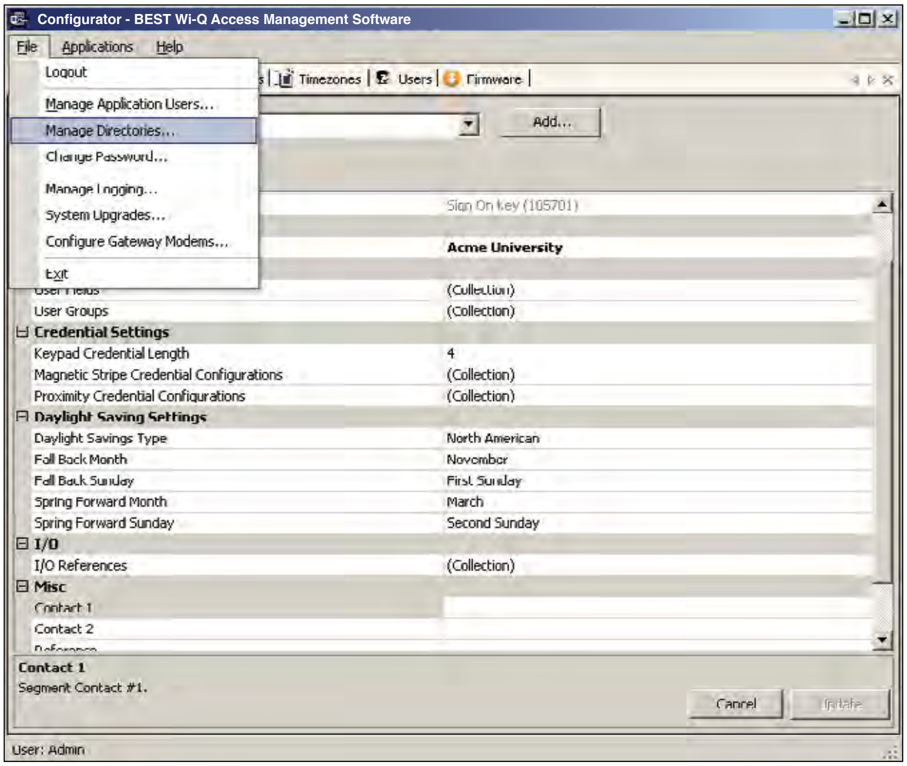
Directory Name
_Directory1

(Name)	
Directory Name	**_Directory1**
Type	Microsoft Windows Workstation
Advanced Info	
Account Category	
Account Class	
Account Display Name Attribute	
Account E-Mail Attribute	
Account ID Attribute	
Account User Name Attribute	
Authentication	
Authentication Type	**Anonymous**
User Name	
User Password	********
General	
Enable Manual Single Sign-on	False
Enable Single Sign-on	**True**
Host Name	
Port	0
Start Node	
Use SSL	False

Host Name
The host name or IP address of the directory server.

5 From the Configurator File menu, select Manage Application Users.

Figure 125 Manage Application Users



Sign On Key (105701)

Acme University

User Fields (Collection)

User Groups (Collection)

⊟ Credential Settings

Keypad Credential Length 4

Magnetic Stripe Credential Configurations (Collection)

Proximity Credential Configurations (Collection)

⊟ Daylight Saving Settings

Daylight Savings Type North American

Fall Back Month November

Fall Back Sunday First Sunday

Spring Forward Month March

Spring Forward Sunday Second Sunday

⊟ I/O

I/O References (Collection)

⊟ Misc

Contact 1

Contact 2

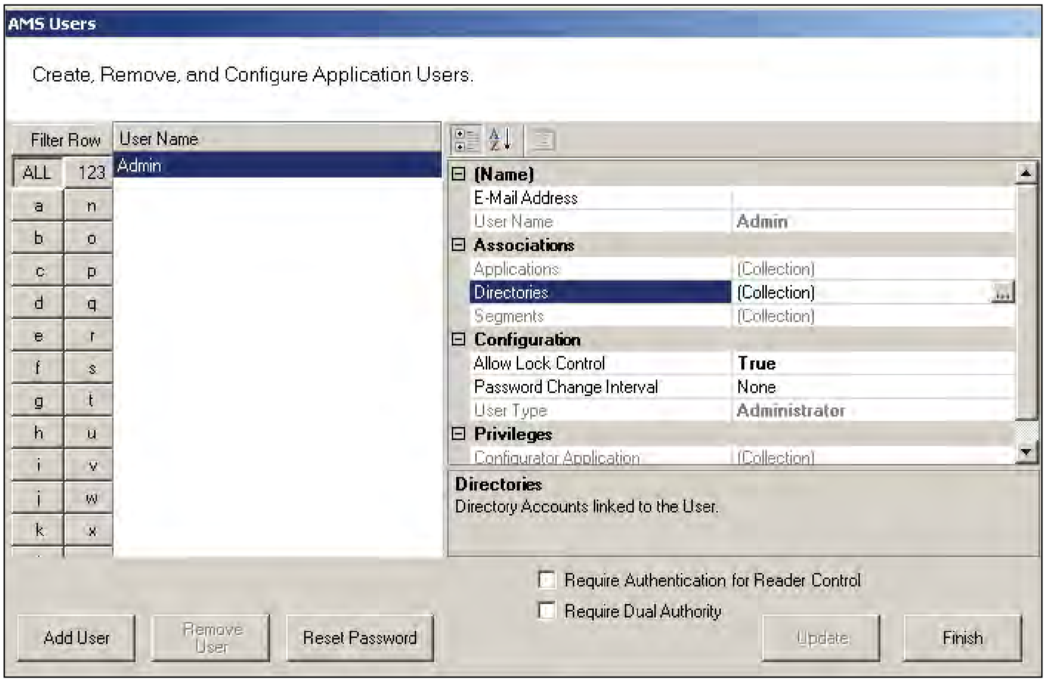
Reference

Contact 1

Segment Contact #1.

6 The AMS Users dialog box opens. Click in the Directories field, under the Associations column, and select the ellipsis button.

Figure 126 AMS Users



Create, Remove, and Configure Application Users.

User Name

Admin

⊟ (Name)

E-Mail Address

User Name Admin

⊟ Associations

Applications (Collection)

Directories (Collection)

Segments (Collection)

⊟ Configuration

Allow Lock Control True

Password Change Interval None

User Type Administrator

⊟ Privileges

Configurator Application (Collection)

Directories

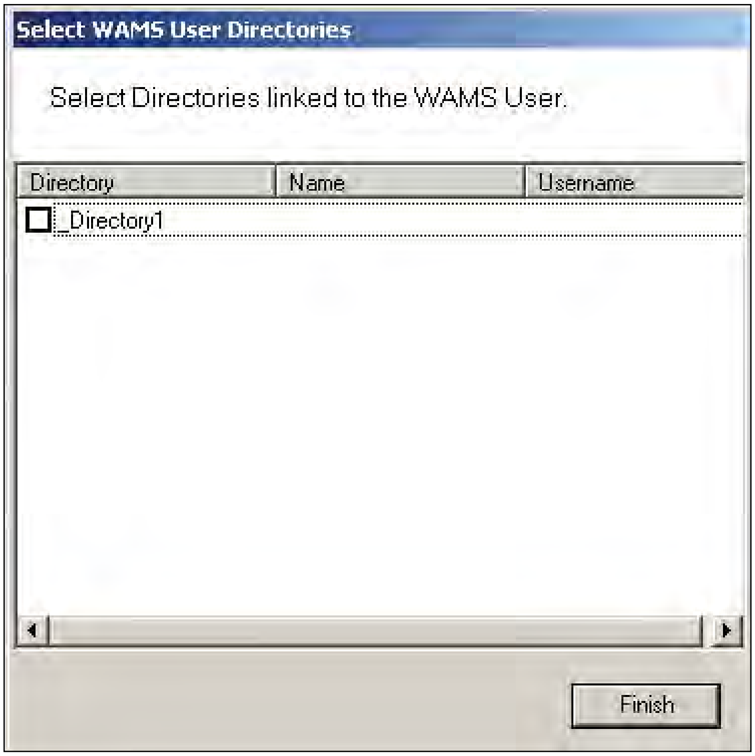
Directory Accounts linked to the User.

□ Require Authentication for Reader Control

□ Require Dual Authority

7 The Select User Directories window opens. Select the directory you created previously.

Figure 127 Select User Directories

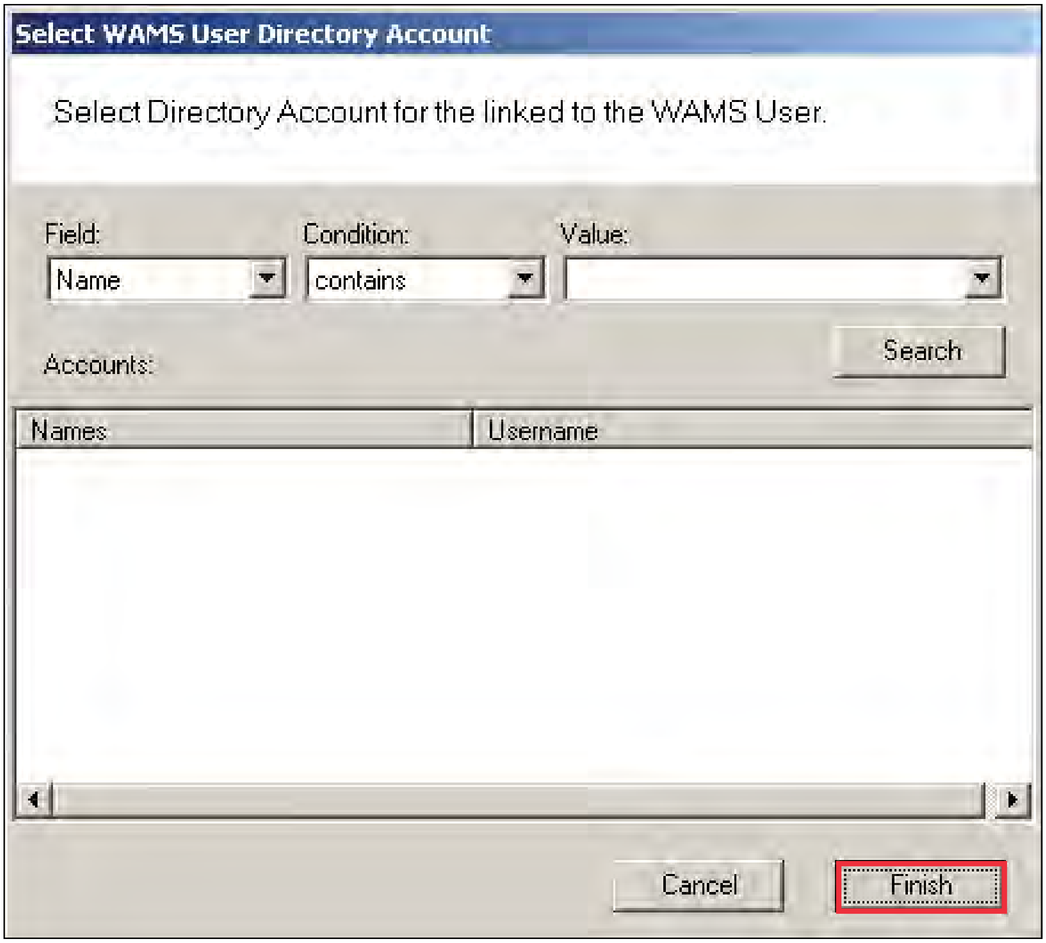


Select Directories linked to the WAMS User.

Directory	Name	Username
□ _Directory1		

8 This will open the Select User Directory Account dialog box. Select Search, and a list of users will be generated below. Select the desired Windows user and then click Finish.

Figure 128 Select User Directory Account



Select WAMS User Directory Account

Select Directory Account for the linked to the WAMS User.

9 Back in the Select User Directories window, the directory will now have a checkmark. Click Finish.

As long as you are logged into Windows using the account you linked to in the previous procedure, you will not be prompted to input a login ID and password the next time you log into Configurator.

Configurator Overview

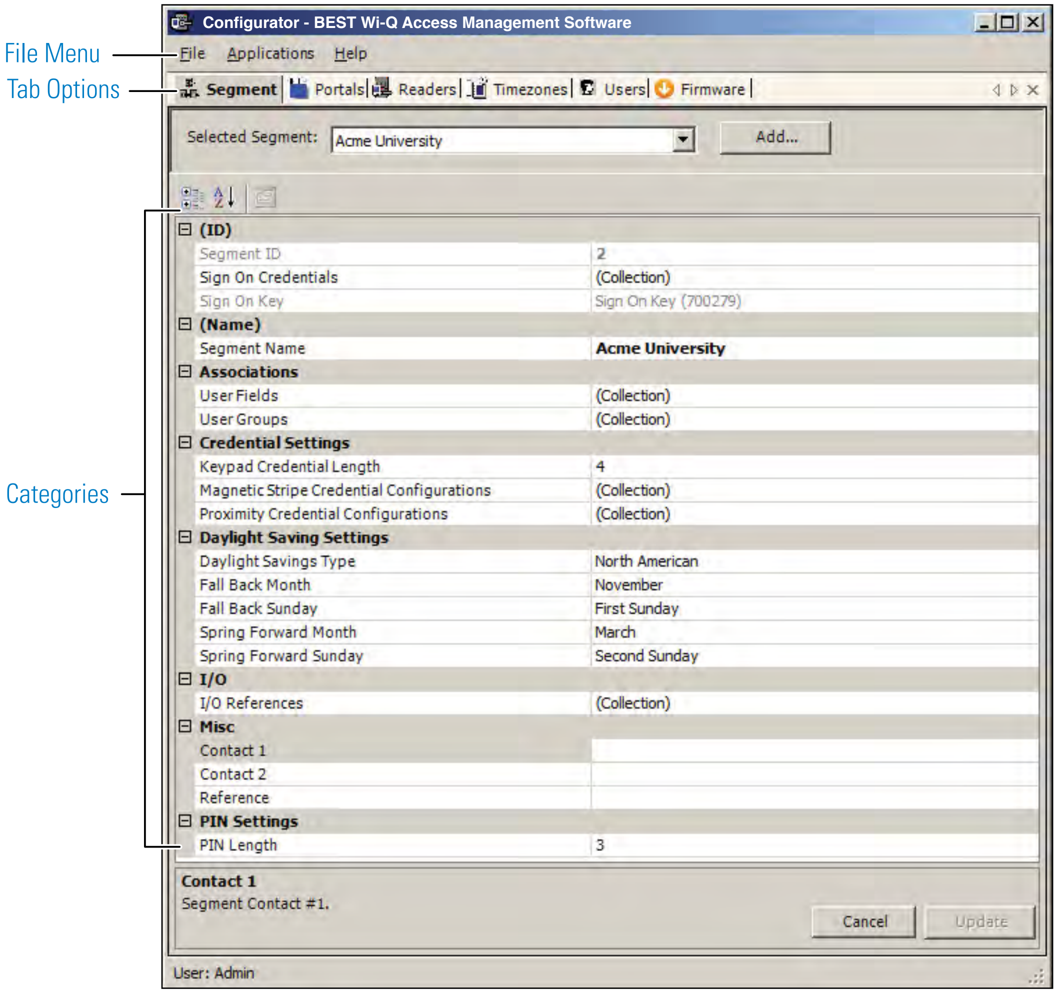
The following sections provide a brief overview of the Configurator module's Display and Tab options.

Display Options

All tasks in Wi-Q AMS and Omnilock start from the Configurator, which has six tabs: Segment, Portals, Readers, Timezones, Users, and Firmware. AMS operates in the Windows environment using its standard Windows conventions. You can use Configurator full screen or resize the window using the min/max buttons in the top right corner of the window.

Following is the Segment Tab in minimized view with the scroll bar visible. This is a useful option if you must run a number of other applications on your desktop and need more space on your desktop.

Figure 129 Segment Tab



File Menu

Tab Options

Categories

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
Magnetic Stripe Credential Configurations	(Collection)
Proximity Credential Configurations	(Collection)
Daylight Saving Settings	
Daylight Savings Type	North American
Fall Back Month	November
Fall Back Sunday	First Sunday
Spring Forward Month	March
Spring Forward Sunday	Second Sunday
I/O	
I/O References	(Collection)
Misc	
Contact 1	
Contact 2	
Reference	
PIN Settings	
PIN Length	3

Contact 1
Segment Contact #1.

User: Admin

In the Segment and Users Tabs, you can display items by category or sort alphabetically. This is useful when displaying the Configurator in full-screen view. A number of global operations are also available from the program File menu.

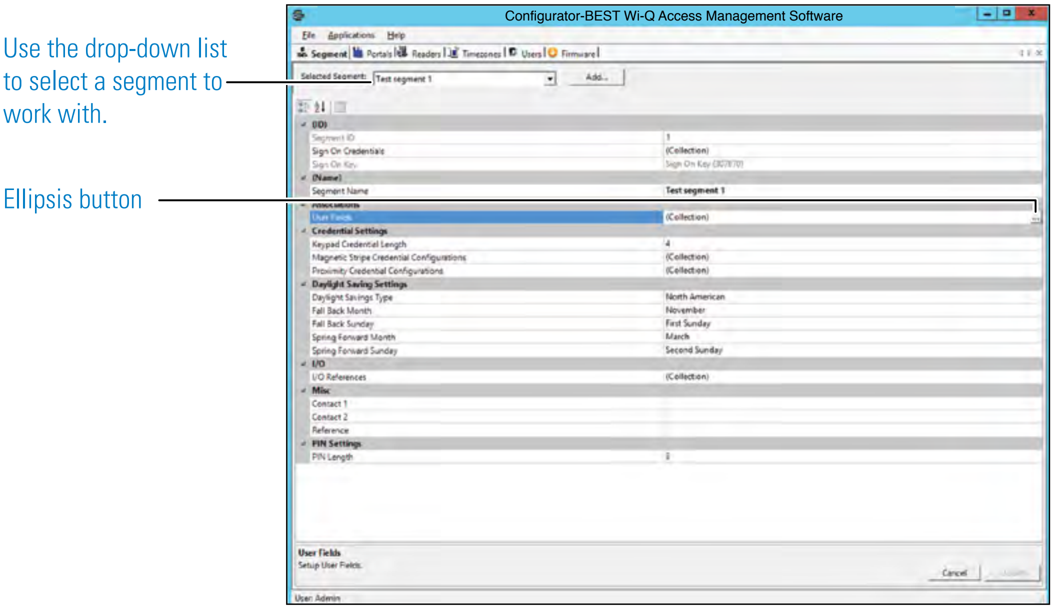
Segment Tab

Most Segment set up tasks are performed in the Segment Tab, Figure 130. Here, the Program Administrator will create User Groups and configure the software to work with the type of segment access cards or keypad credentials you will use.

If your Program Administrator has created more than one segment, you will first select a segment to work with in the Segment Tab before moving on to work in the other tabs.

Once you select a category within Configurator, you can use the ellipsis button to configure additional settings.

Figure 130 Segment Tab Categories



Use the drop-down list to select a segment to work with.

Ellipsis button

Selected Segment: Test segment 1

(ID)	
Segment ID	1
Sign On Credentials	(Collection)
Sign On Key	Sign On Key (307870)
(Name)	
Segment Name	**Test segment 1**
Associations	
User Fields	(Collection)
Credential Settings	
Keypad Credential Length	4
Magnetic Stripe Credential Configurations	(Collection)
Proximity Credential Configurations	(Collection)
Daylight Saving Settings	
Daylight Savings Type	North American
Fall Back Month	November
Fall Back Sunday	First Sunday
Spring Forward Month	March
Spring Forward Sunday	Second Sunday
I/O	
I/O References	(Collection)
Misc	
Contact 1	
Contact 2	
Reference	
PIN Settings	
PIN Length	[illegible]

User Fields
Setup User Fields.

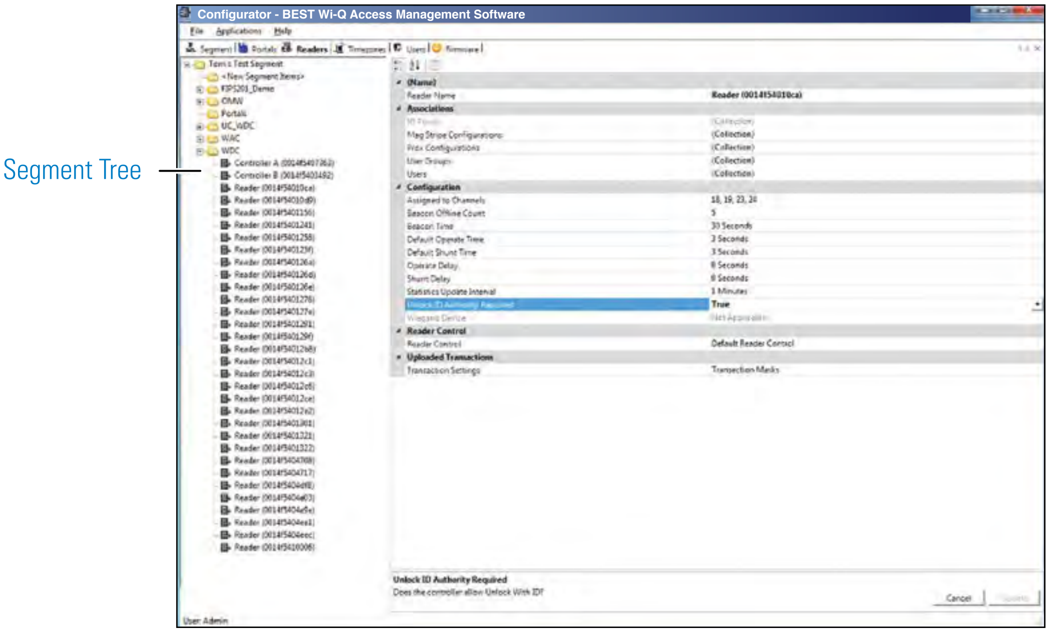
User: Admin

Portals and Readers Tabs

The Portals and Readers tabs displays the Segment Tree, which is a visual representation of all Wi-Q Gateways, Controllers, and I/O devices connected to the software. Once the devices are organized in the Segment Tree, the various paths to associate Controllers and Portals are available when you add new users to the system.

Information about creating the Segment Tree and assigning devices to the various folders in the tree is presented in Chapter 4, “Configuring Segments, Wi-Q Gateways and Controllers” . Typically, only the Program Administrator will perform tasks using the Readers Tab, Figure 131.

Figure 131 Readers Tab



(Name)	
Reader Name	**Reader (0014f54010ca)**
Associations	
I/O Points	(Collection)
Mag Stripe Configurations	(Collection)
Prox Configurations	(Collection)
User Groups	(Collection)
Users	(Collection)
Configuration	
Assigned to Channels	18, 19, 23, 24
Beacon Offline Count	5
Beacon Time	30 Seconds
Default Operate Time	3 Seconds
Default Shunt Time	3 Seconds
Operate Delay	0 Seconds
Shunt Delay	0 Seconds
Statistics Update Interval	1 Minutes
Unlock ID Authority Required	**True**
Wiegand Device	Not Applicable
Reader Control	
Reader Control	Default Reader Control
Uploaded Transactions	
Transaction Settings	Transaction Masks

Unlock ID Authority Required

Does the controller allow Unlock With ID?

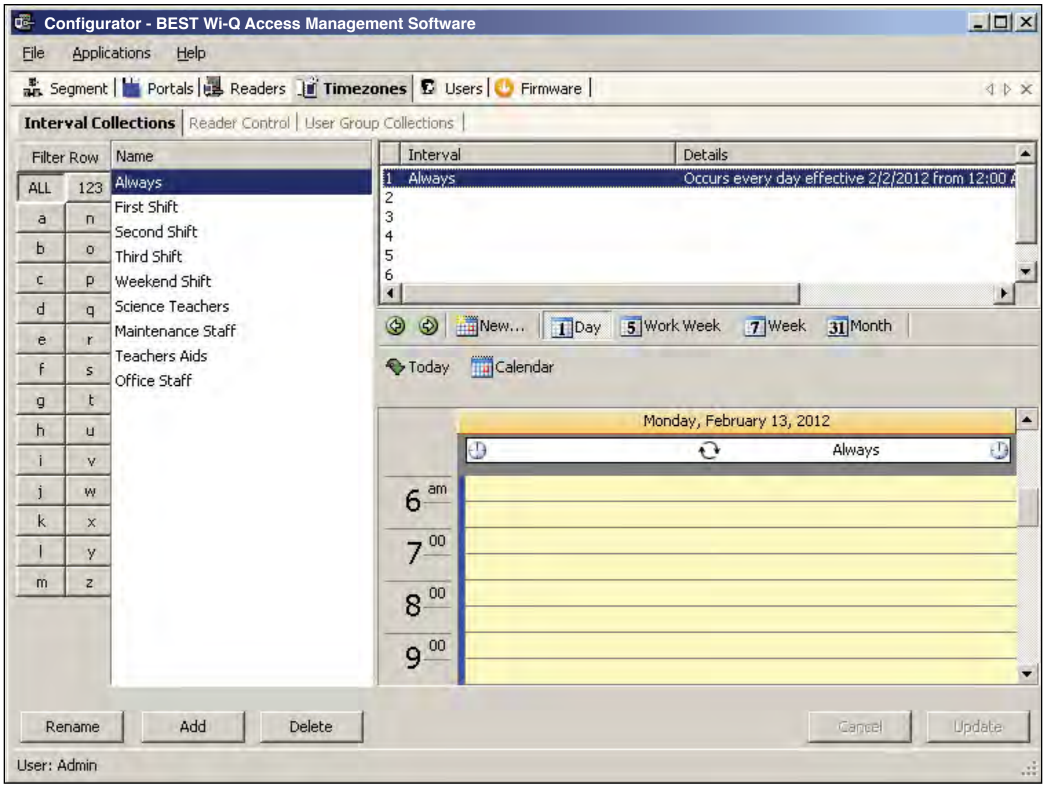
Timezones Tab

The software automatically assigns all Controllers to a Master Timezone. Your Program Administrator can create any number of Timezone Intervals Collections and Timezone User Group Collections to modify user access within the Master Timezone. The Timezones tab displays the default Master Timezone, a calendar that operates similar to Microsoft Outlook, and any Timezone User Groups that have been created.

You can choose to display the calendar detail as one day, a work week, a full week or by the month, or click on the calendar to display a specific date.

More information about creating Timezone Intervals and Timezone Groups is presented in later in Chapter 5, "Configure AMS Software (Task 11)" on page 112.

Figure 132 Setting up the Timezones

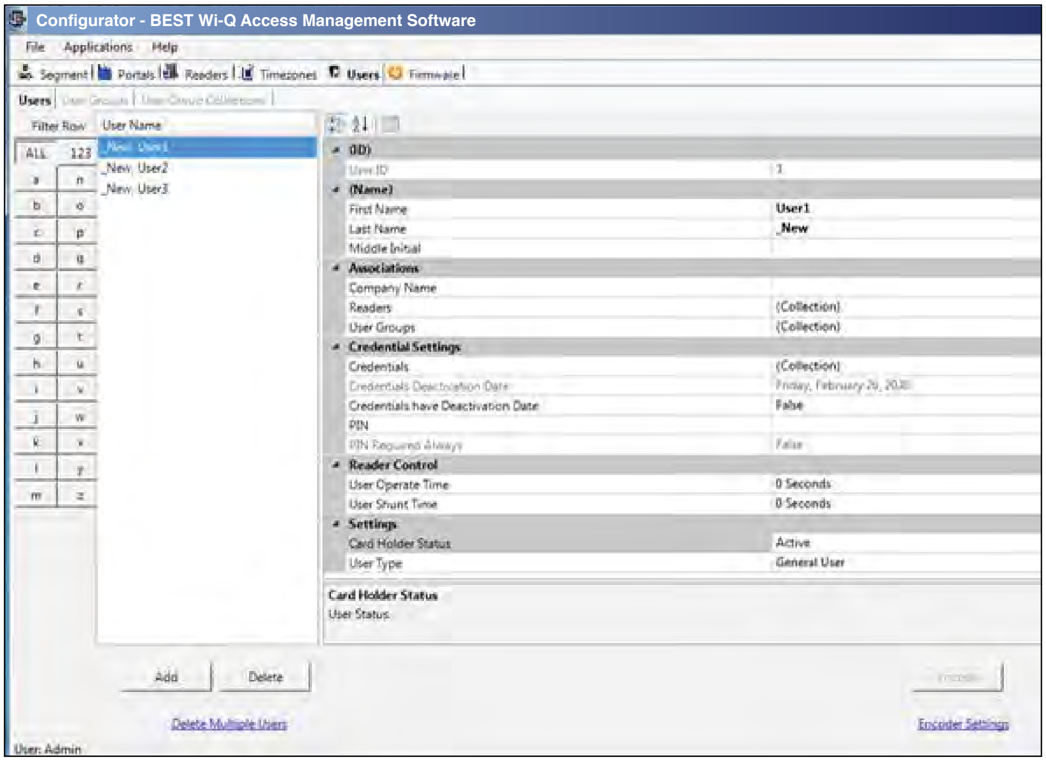


Interval	Details
1 Always	Occurs every day effective 2/2/2012 from 12:00 A
2	
3	
4	
5	
6	

Users Tab

If you have been assigned responsibility to add or maintain general cardholder users of the system, your tasks will be performed in the Users Tab. All users currently in the system are displayed in the column at the left. To display a User profile, simply select their name from the list.

Figure 133 Users Tab



User Name
_New, User1
_New, User2
_New, User3

(ID)	
User ID	1
(Name)	
First Name	User1
Last Name	_New
Middle Initial	
Associations	
Company Name	
Readers	(Collection)
User Groups	(Collection)
Credential Settings	
Credentials	(Collection)
Credentials Deactivation Date	Friday, February 29, 2020
Credentials have Deactivation Date	False
PIN	
PIN Required Always	False
Reader Control	
User Operate Time	0 Seconds
User Shunt Time	0 Seconds
Settings	
Card Holder Status	Active
User Type	General User

Card Holder Status
User Status

More information about adding users to the system is presented in Chapter 5, “Configure AMS Software (Task 11)” on page 112.

Firmware Tab

Firmware updates will be sent to you periodically by dormakaba Technical Support. You can upload these firmware files to your database by using the System Administrator Application, and then you can send the updates to your hardware from the Configurator’s Firmware Tab.

System Overrides

Manager Override at Keypad Controller

When an AMS User is assigned the Manager Type, that user can change the current access level at a Controller with a keypad. Once their credential has been presented to a Controller and it has cycled, the following keys can be used to change the Controller's access level:

Note MC refers to Manager Credential.

Item	WDC	WAC	Omnilock	Function
Manager Code	MC#	MC	MC	Momentary Unlock.
Restore to Normal	MC# + 0#	MC + 0000	MC + 0 + CL	Return to normal operation from an override.
Toggle with ID	MC# + 1#	MC + 1111	MC + 1 + CL	Places the device in a mode to toggle between locked and unlocked with a credential.
Unlock	MC# + 2#	MC + 2222	MC + 2 + CL	Places the device in an unlocked state.
Unlock with ID	MC# + 3#	MC + 3333	MC + 3 + CL	Places the device in a mode to unlock with credential.
Unlock with ID and PIN	MC# + 4#	MC + 4444	MC + 4 + CL	Places the device in a mode to unlock with credential and PIN.
ID Required	MC# + 5#	MC + 5555	MC + 5 + CL	Places the device in a mode where a credential is required to enter.
PIN Required	MC# + 6#	MC + 6666	MC + 6 + CL	Places the device in a mode where a PIN is required to enter.
Facility Card	MC# + 7#	MC + 7777	MC + 7 + CL	Places the device in a mode where all credentials with the correct facility ID have access.
Lockout	MC# + 8#	MC + 8888	MC + 8 + CL	Places the device in a mode where only manager credentials have access.
Toggle with ID and PIN	MC# + 9#	MC + 9999	MC + 9 + CL	Place the device in a mode to toggle between locked and unlocked with a credential and PIN.

Programmer Override at Keypad Reader

When an AMS User is assigned a Programmer Type, that user can present their credential and perform the following.

Note PC refers to Programmer Credential.

Item	WDC	WAC	Omnilock	Function
Programmer Code	PC#	PC	PC	Momentary Unlock.
Soft Reset	PC# + 1#	PC + 1111	PC + 1	Soft resets device.
Motor Reset	PC# + 2#	PC + 2222	PC + 2	Resets the motor drive.
Comm. Processor Reset	PC# + 7#	PC + 7777	PC + 7	Resets the communication processor.
Motor Test	PC# + 8#	PC + 8888	PC + 8	Runs motor test.
Deep Reset	MC# + 9#	MC + 9999	MC + 9	Deep resets device.

Deep Reset

At times it may be necessary to perform a Deep Reset on a Controller. For example, when you install a dial up gateway modem, you must temporarily clear reader data. If the reset button inside the Controller housing is not accessible, you can use the Programmer Override to perform a Deep Reset. You can also perform a deep reset from within Configurator.

To Perform a Deep Reset from within Configurator

1 In the Configurator's Readers Tab, navigate to the desired reader using the Segment Tree.

2 In the list on the right, right-click on the reader and select Deep Reset from the drop-down list. Reader data will be cleared.

3 To bring the reader back into the software, you must perform a standard sign on procedure.

Note If the reader does not respond and perform the Deep Reset within five minutes, the action will be aborted.

Segment Item Upgrades

As you continue to add users and readers to your system it may become necessary to expand your Portal and reader capacities. This is performed via the File menu in Configurator.

When you near maximum capacity in one or all of the system segment items, it's time to use one of the upgrade licenses you purchased with your system, or call dormakaba for additional Upgrades. You can purchase system upgrades to expand the user and Controller capacity of each segment in your organization.

Each Wireless Controller begins with support for 2000 user credentials and can be upgraded to support up to 18000 Users. Upgrade licenses are available in maximum capacities of 2000, 10000, and 18000 users.

Each Wi-Q Gateway begins with support for 16 readers and can be upgraded to support 32 and 64 wireless readers. Upgrade licenses are available in maximum capacities of up to 64 readers.

Determine Segment Reader and Portal Capacity

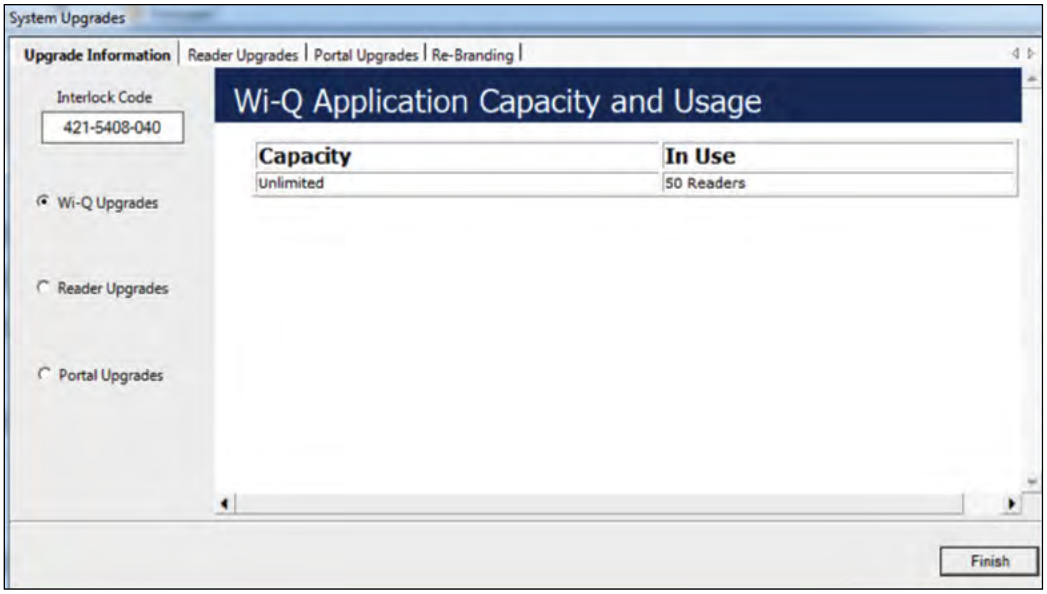
An AMS user with Administrator privileges can monitor system capacity by segment from within Configurator. From here it is easy to see how many licensed upgrades are in use and how many are available.

To view Wi-Q AMS and Omnilock Upgrade use

1 In Wi-Q AMS Configurator, Segment Tab, select the Segment you wish to review for upgrade use.

2 From the Wi-Q AMS Configurator File menu, select System Upgrades from the dropdown list. The System Upgrades window opens at the Upgrade Information Tab.

Figure 134 Upgrading your system capacity



Interlock Code
421-5408-040

● Wi-Q Upgrades

Wi-Q Application Capacity and Usage

Capacity	In Use
Unlimited	50 Readers

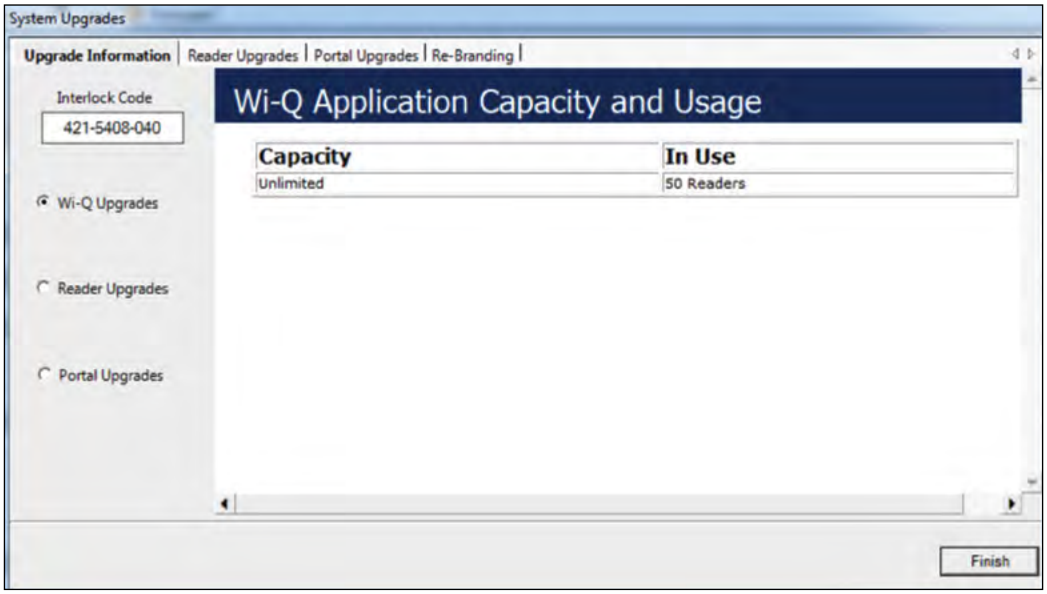
AMS Upgrades

With the Wi-Q AMS Upgrades radio button selected on the left, the property sheet displays the current reader capacity for the segment and how many of those readers are currently in use.

Wi-Q AMS now offers free upgrades. All capacities can be set to unlimited without a new interlock code.

Reader Licenses in Use — With the Reader Upgrades radio button selected on the left, the property sheet displays the number of Licensed Upgrades in each user capacity value, and how many of those Licensed Upgrades are currently in use.

Figure 135 Upgrading your system capacity



Interlock Code: 421-5408-040

● Wi-Q Upgrades

○ Reader Upgrades

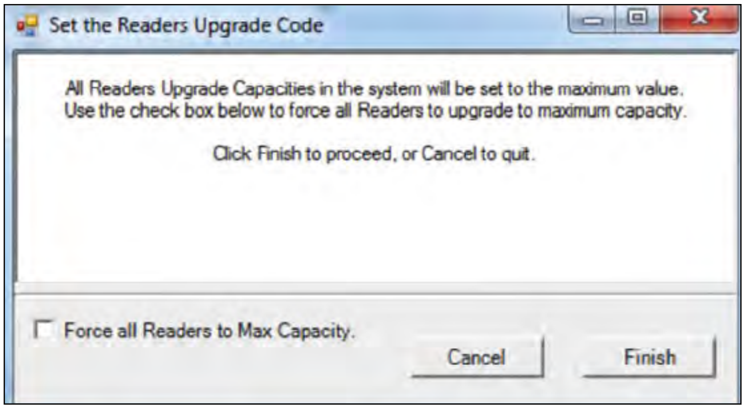
○ Portal Upgrades

Wi-Q Application Capacity and Usage

Capacity	In Use
Unlimited	50 Readers

Select the upgrade all link if additional user capacity is needed.

Figure 136 Set the Readers Upgrad Code



All Readers Upgrade Capacities in the system will be set to the maximum value.
Use the check box below to force all Readers to upgrade to maximum capacity.

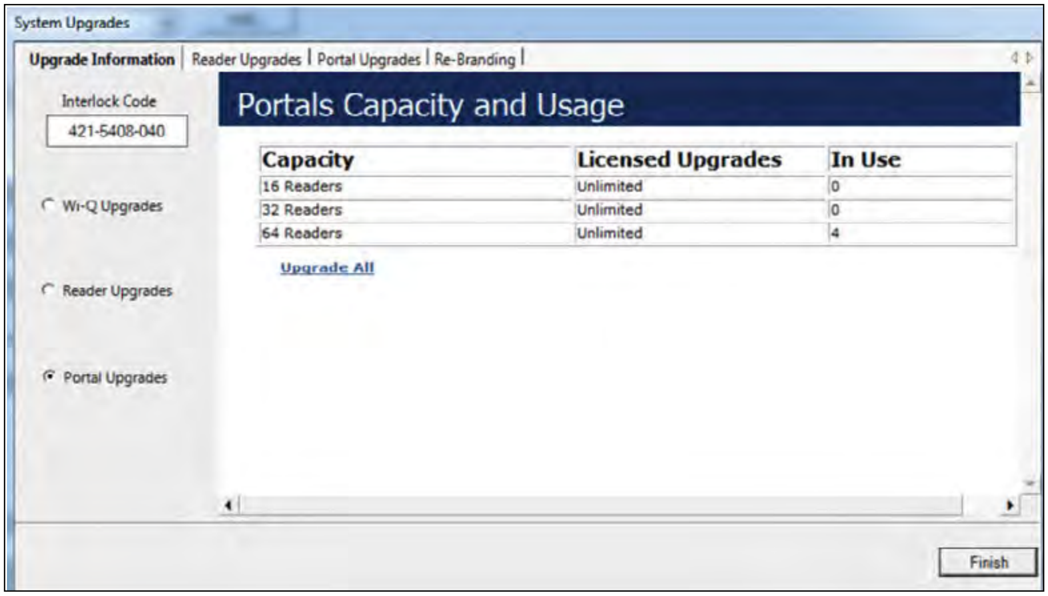
Click Finish to proceed, or Cancel to quit.

□ Force all Readers to Max Capacity.

Select force all readers to max capacity and click finish.

Portal Licenses in Use — With the Portal Upgrades radio button selected on the left, the property sheet displays the number of Licensed Upgrades in each reader capacity value, and how many of those Licensed Upgrades are currently in use.

Figure 137 Upgrading your system capacity



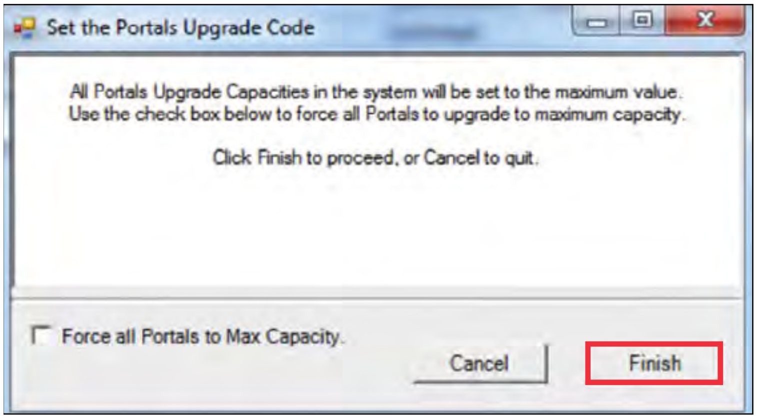
Interlock Code: 421-5408-040

Portals Capacity and Usage

Capacity	Licensed Upgrades	In Use
16 Readers	Unlimited	0
32 Readers	Unlimited	0
64 Readers	Unlimited	4

Select the upgrade all link if additional reader capacity is needed.

Figure 138 Upgrading your system capacity



All Portals Upgrade Capacities in the system will be set to the maximum value. Use the check box below to force all Portals to upgrade to maximum capacity.

Click Finish to proceed, or Cancel to quit.

□ Force all Portals to Max Capacity.

Select force all portals to max capacity and click finish.

System Administrator

System Administrator is an application accessed inside Configurator or from the Windows Start menu. With System Administrator, you can archive and restore Portal statistics, reader statistics, and reader transactions. From here you can also import data from an existing database or comma-delimited file. You must be an AMS User with Administrator privileges to use this feature. It is a good idea to archive records on a regular basis. It will be helpful to establish a protocol and ensure that it is carried out according to plan.

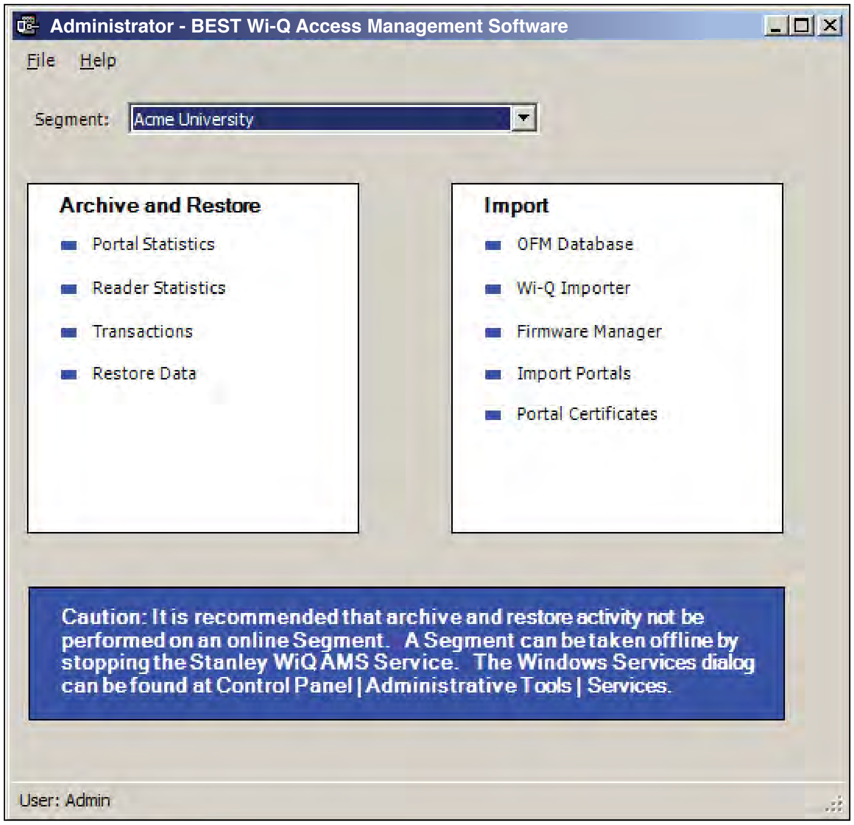
Note Archiving and restoring transactions and statistics is not the same as performing a full AMS database back up. Full back up and restore is performed using Microsoft SQL Server Management Studio Express (installed with AMS). Complete steps are described later in this chapter.

Establish an Archive Protocol

An industry best practice for use of any archiving systems is to establish a protocol for who, when and how much data to archive, depending on the volume and nature of the data being archived. For security purposes, it will be important to ensure the protocol is being implemented by also establishing an audit practice.

Using System Administrator

Figure 139 System Administrator



Caution: It is recommended that archive and restore activity not be performed on an online Segment. A Segment can be taken offline by stopping the Stanley WiQ AMS Service. The Windows Services dialog can be found at Control Panel | Administrative Tools | Services.

From here you can archive and restore statistics in the AMS database, import data to AMS from the OFM Database, or import data from standard comma-delimited files such as .txt and .csv.

Archiving Statistics in the AMS Database

It is important to maintain your database in optimum condition. On the basis of the statistics volume in your segment, you should establish a protocol to regularly archive data that are not likely to be used again. For example, each month, you may want to archive data that are three months old. When you archive records from the software using the System Administrator application, the data is removed from the database. The statistics can be fully restored to AMS in the future, if necessary.

The archive feature operates the same for Portal statistics, Reader statistics, and Transactions. The following steps illustrate how to archive Portal statistics; however, the steps are the same for each type. You can archive statistics in all devices or select a specific Portal or reader for archive.

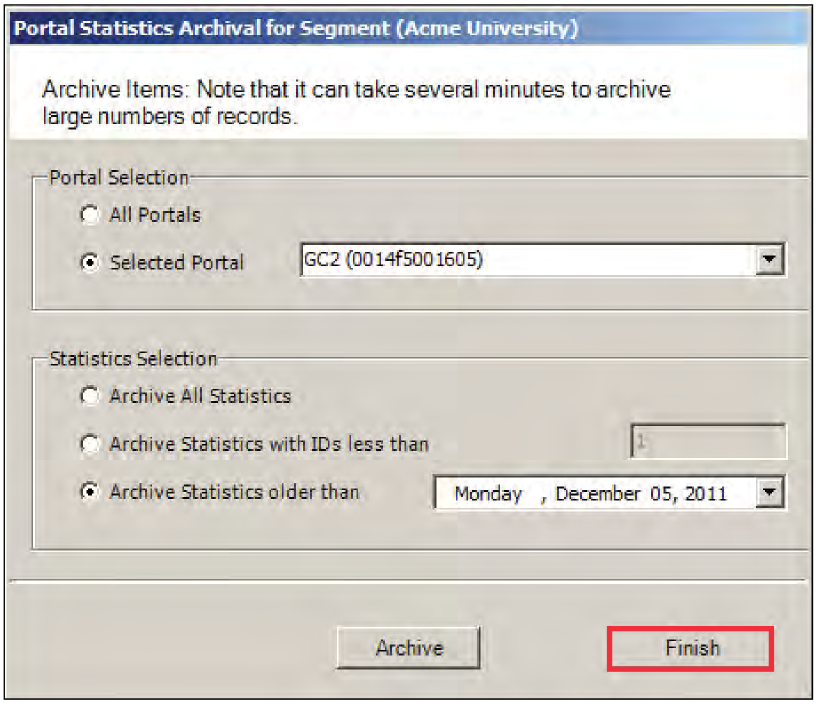
Once you've selected the Portal or reader to archive, you can also select what statistics to archive; for example, all statistics, only those statistics greater than a specific ID, or specify a range of statistics older than a specific date.

To Archive Statistics

1 In the System Administrator application, select the segment for which you wish to archive statistics.

2 In the main window, under Archive and Restore, select a Statistics type, such as Portal Statistics.

Figure 140 Portal Statistics Archival for Segment



Portal Statistics Archival for Segment (Acme University)

Archive Items: Note that it can take several minutes to archive large numbers of records.

Portal Selection

○ All Portals

● Selected Portal GC2 (0014f5001605)

Statistics Selection

○ Archive All Statistics

○ Archive Statistics with IDs less than 1

● Archive Statistics older than Monday , December 05, 2011

3 In the Portal Selection box, select one of the following:

- All Portals — All Portals' data will be archived.
- Selected Portal — Choose a Portal ID from the drop-down list. Data from only that Portal will be archived.

4 In the Statistics Selection box, select one of the following:

- Archive All Statistics — All statistics in the database will be archived.
- Archive Statistics with IDs less than — Define an ID number. Only statistics with IDs less than the defined number will be affected.
- Archive Statistics older than — Select a date. Only data older than the date selected will be archived.

5 When you have selected the appropriate options, click the Archive button and click Yes if you wish to continue with the archive.

6 In the Windows browser, navigate to a folder or create a new one in which to archive the file. You should create a filename that will be meaningful to your segment (for example, all_Portals, or siteA_Portals). These files will be accessible under this location should you wish to restore them at a later date.

7 Click OK. The system will display the status of the archive activity as it proceeds.

8 Click Finish to exit Portal Statistics Archive.

Restoring Data to the Database

You can restore data that have been archived by System Administrator back into the database. Once this is done, you will be able to view them in Configurator and its related applications.

To Restore Data to AMS

1 From the Configurator Segment Tab, select the segment for which you wish to archive statistics.

2 From the Applications menu on the Configurator menu bar, select System Administrator. The Systems Administrator window opens.

3 Select the Segment you wish to work with. From the left window pane, select Restore Data. The Windows browser window opens.

4 Select the file you wish to restore to AMS, then click Open.

5 The system reports that the records will be restored to the Segment. Click Yes to continue. The system will display the status of the archive activity as it proceeds.

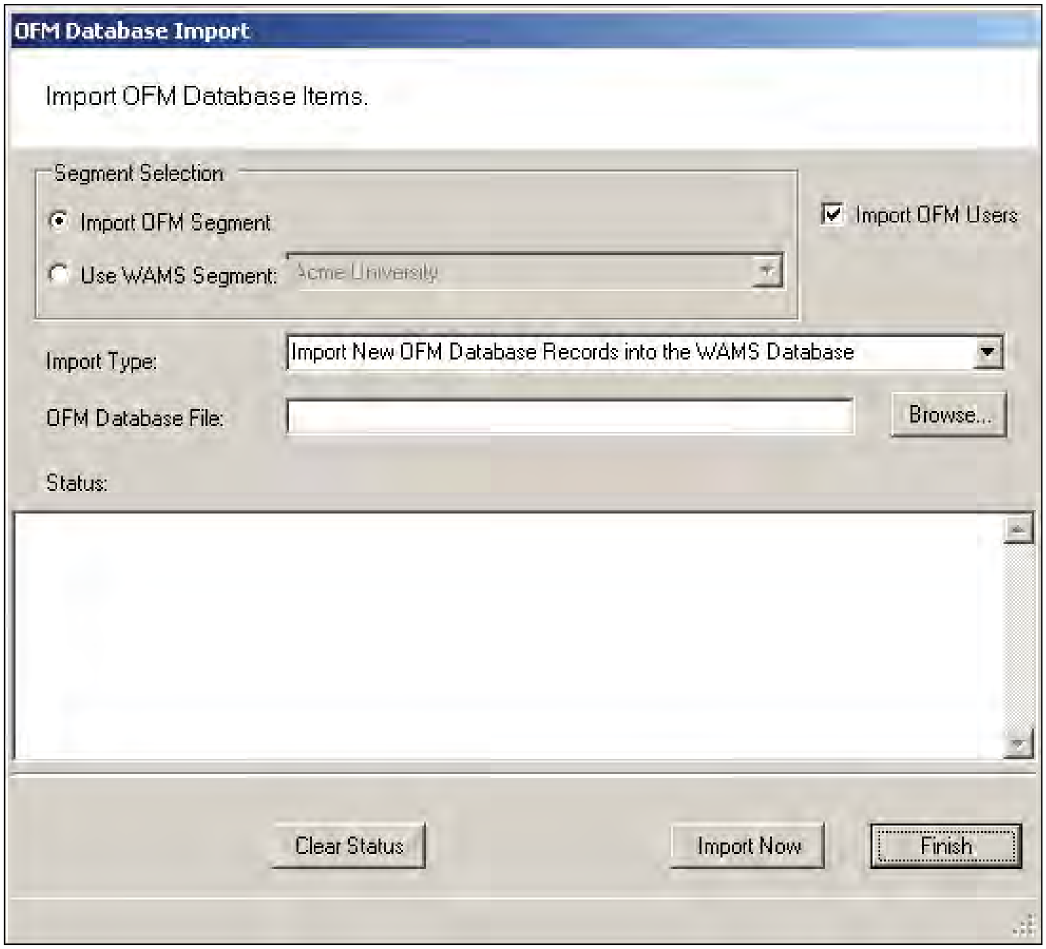
Importing Data from a Legacy OFM Database

You can import an entirely new segment into the software from a legacy OFM database, or you can import all or some elements of data into an existing segment and overwrite any data with the latest data in the OFM. When you import an entire segment from an OFM database, AMS creates a segment with the segment name of the old database.

To Import Data to AMS

1. From the Applications menu on the Configurator menu bar, select System Administrator. The System Administrator window opens.
2. From the right window pane, select OFM Database. The Windows browser window opens.

Figure 141 OFM Database Import



OFM Database Import

Import OFM Database Items.

Segment Selection

● Import OFM Segment

○ Use WAMS Segment: Acme University

☑ Import OFM Users

Import Type: Import New OFM Database Records into the WAMS Database

OFM Database File:

Status:

3 In the Segment Selection box, select one of the two options:

- Import OFM Segment — This option imports a new segment in its entirety and automatically gives it the name of the existing Segment in the OFM Database.
- Use Segment — This option activates the drop-down list. Select the Segment into which you wish to import data. It will import any new data and update any existing records with the same ID based on the import type.

4 Select the Import OFM Users option if you want to include OFM Database existing Users and User Groups.

5 From the Import Type dropdown menu, select the type of import you wish to perform:

- Import New OFM Records into the Database — This will import only new records.
- Merge New and Changed OFM Data into the Database — This will import all data and add or update any records that are new since the last import.

6 Select Browse to find the OFM Database File.

7 Select Import Now. The data will begin to transfer and you will see the records scroll through the Status window. This should take only a few minutes, depending on the size of the data being imported.

Import Data from a Standard Comma-Delimited File

You can also create a comma-delimited .txt or .csv file containing Names, Credentials and other AMS information and import the data directly to the database, including any of the following data:

- Last Name
- First Name
- Middle Initial
- Proximity Card Credential
- Proximity Card Type
- Magnetic Stripe Card Credential
- Keypad Credential

In addition, you can include data for any user fields created for the segment selected for import.

AMS Importer imports files in a few easy steps:

- Create the data file in the appropriate program, such as Microsoft Word, Excel, or other text-based program and save it as a .txt or .csv format.
- Prepare the Wi-Q AMS Import Utility to accept the file.
- Import the data.
- Send the Data to the database.

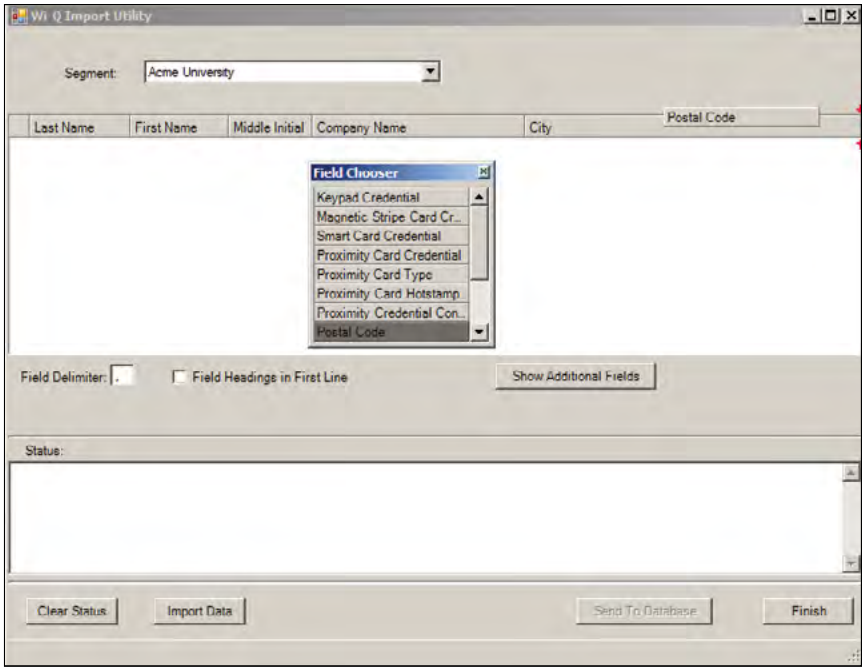
In the Import Utility, you can view the data as it imports into the window and make any corrections to the file or column headers until you are satisfied with the import before you actually send it to the database.

Detailed instructions are presented in the next few sections.

To prepare Wi-Q AMS Import Utility

1. From the Applications menu on the Configurator menu bar, select System Administrator. The System Administrator window opens.
2. From the right window pane, select Wi-Q (or Omnilock) Importer. The Import Utility opens.

Figure 142 Import Utility



Segment: Acme University

Field Delimiter: ,

□ Field Headings in First Line

3. Use the cursor to drag the column headers into any order you wish.

4 If you wish to import additional data into user fields associated with the segment, click Show Additional Fields to display the Field Chooser and double-click or drag to add them to the header.

5 Enter the appropriate Field Delimiter for the import file, the default is a comma.

6 If you have field headings in the first line of your data file, click the Field Heading in First Line check box.

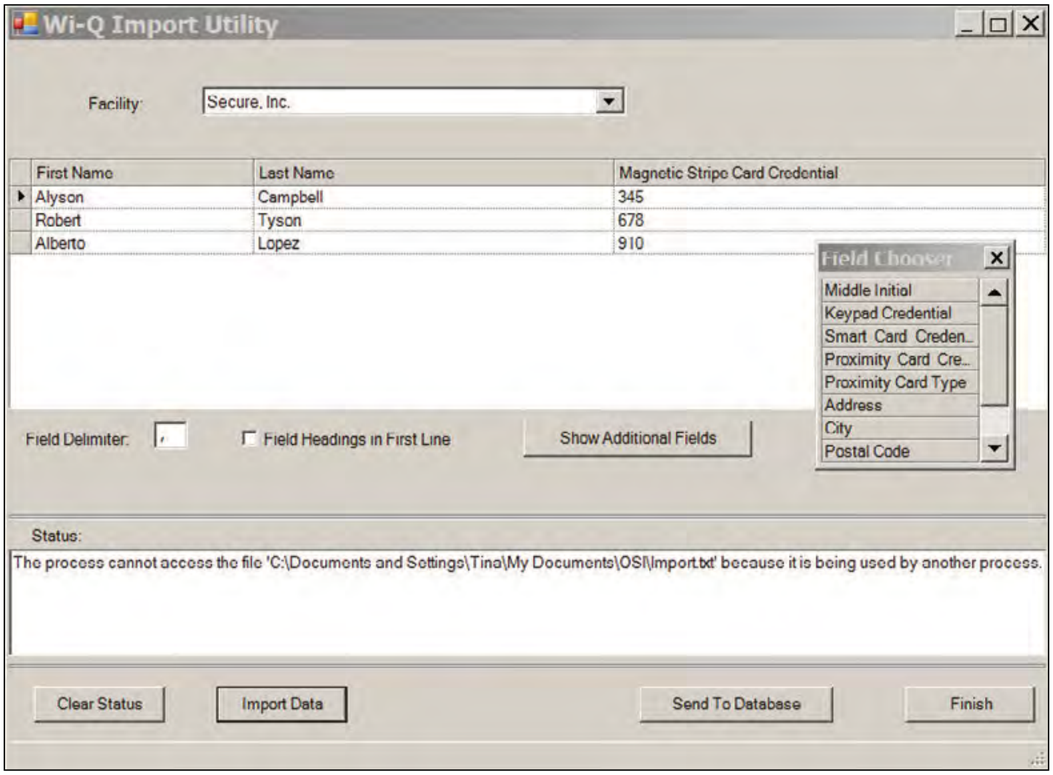
To import the data

1 Once all column headers are in the order you wish, click Import Data.

2 Navigate to the location of the data file you created and click Open.

3 The Data appears under the appropriate column headers in the upper window. If the file is large, you can watch the progress in the Status box on the bottom of the window.

Figure 143 Using the Import Utility



Facility: Secure, Inc.

First Name	Last Name	Magnetic Stripe Card Credential
Alyson	Campbell	345
Robert	Tyson	678
Alberto	Lopez	910

Field Delimiter: ,

□ Field Headings in First Line

Status:

The process cannot access the file 'C:\Documents and Settings\Tina\My Documents\OSI\Import.txt' because it is being used by another process.

4 Review the data import. Scroll the window to ensure the data has imported in the appropriate column headers. If not, you can rearrange the column headers and import the file again. You can do this as many times as you need to ensure you will get a good import.

5 Once you are satisfied that the data has imported as intended, click Send to Database. The data will now appear in the appropriate fields throughout AMS.

Backing Up and Restoring Your AMS Database

Full backup and restore functions are performed outside of AMS using Microsoft SQL Server Management Studio Express (installed with the software). You should plan to perform this function on a regular basis. You can also use this program to move the database to a different computer.

WARNING: This operation should be performed only by an IT professional who is designated as an AMS User with Admin or Programmer privileges.

Backing Up the Database

Perform the following steps to back up the database.

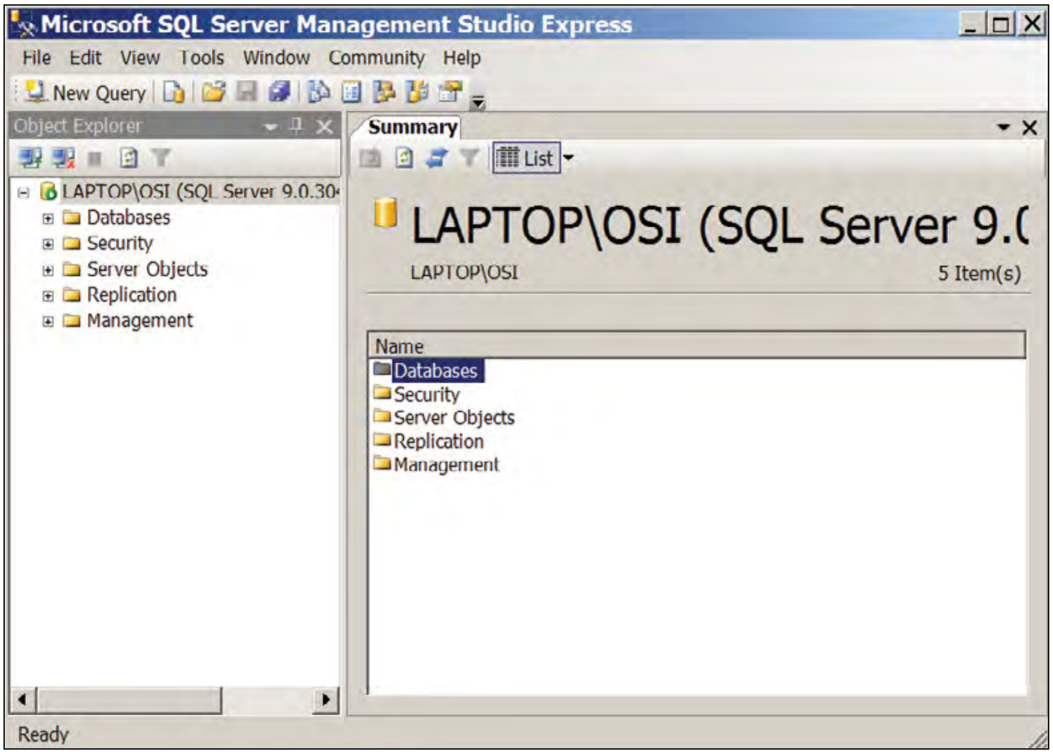
1 Exit AMS.

2 From the Windows Start menu, select Programs>Microsoft SQL Server Management Studio Express. The connect to Server dialog box opens.

3 Enter the Server type, Server name, and choose your Authentication type.
Then, click Connect.

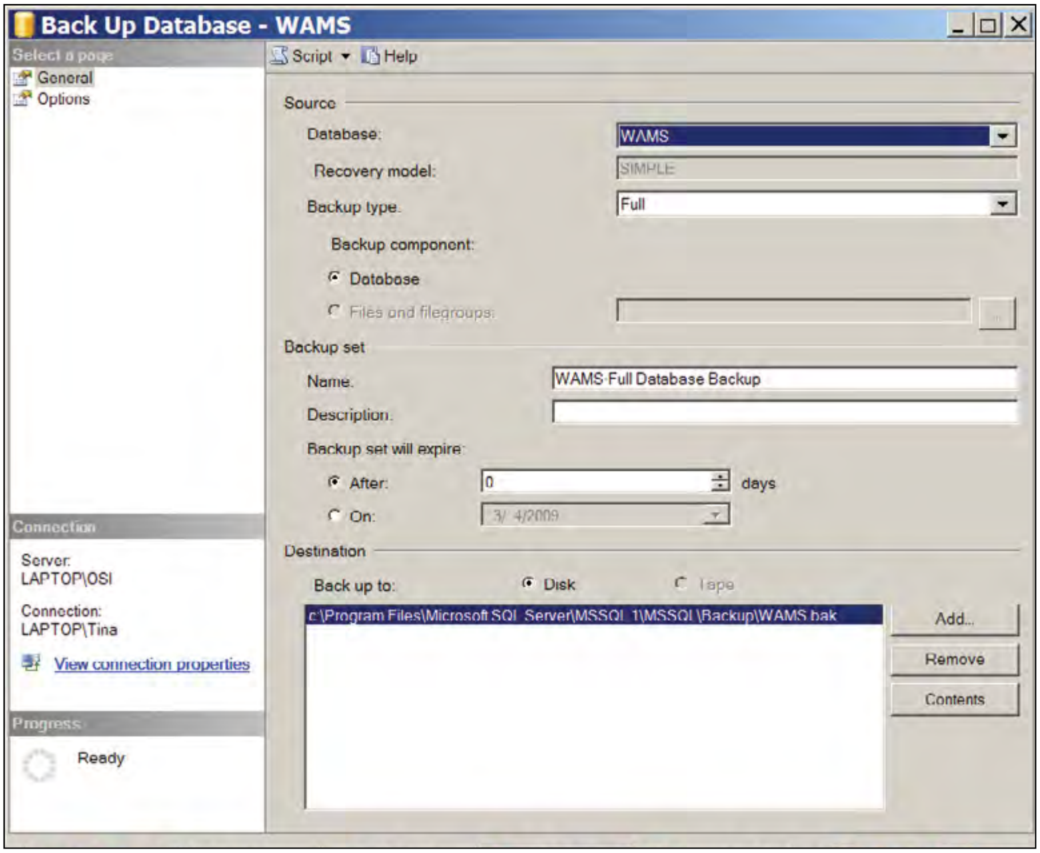
4 The program opens at the default database location.

Figure 144 Default database display in SQL Server



5 Double-click on databases, then right-click on the folder and select tasks>Backup. The backup database dialog box opens.

Figure 145   Backup Database



Source

Database: WAMS

Recovery model: SIMPLE

Backup type: Full

Backup component:

● Database

○ Files and filegroups:

Backup set

Name: WAMS-Full Database Backup

Description:

Backup set will expire:

● After: 0 days

○ On: 3/ 4/2009

Destination

Back up to: ● Disk ○ Tape

c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Backup\WAMS.bak

Connection

Server: LAPTOP\OSI

Connection: LAPTOP\Tina

Progress

Ready

6 Define a Backup Type (full or differential) and add a description of the backup (optional).

7 The default destination displays. You can change the destination, if needed, for example if you wish to move the database to a new location on a different computer.

8 Click OK. The backup progresses and the system reports when the backup is complete.

To Restore the database

1 Exit AMS.

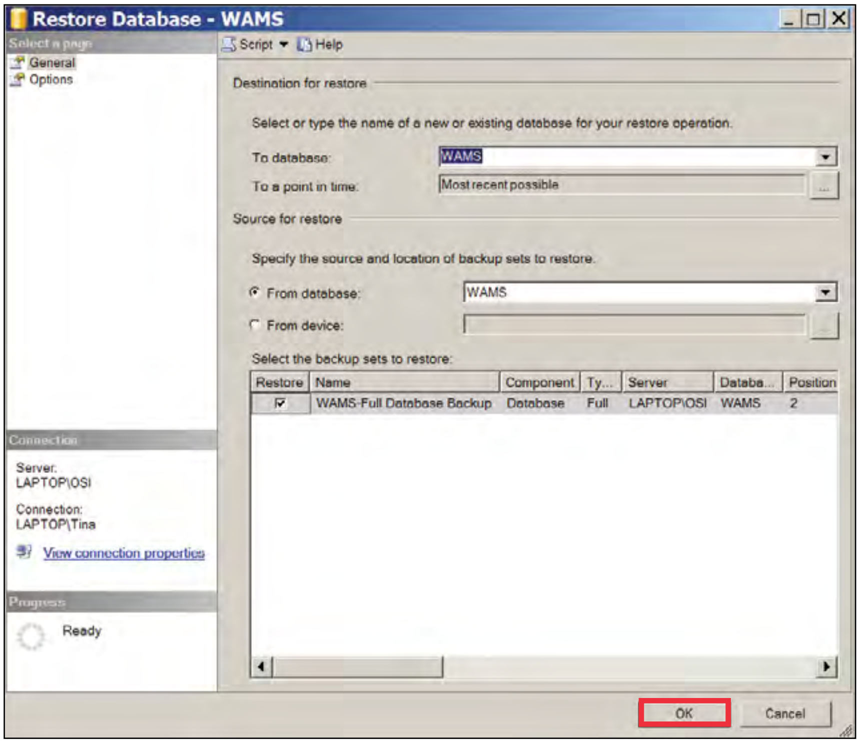
2 From the Windows Start menu, select Programs>Microsoft SQL Server Management Studio Express. The connect to Server dialog box opens.

3 Enter the Server type, Server name, and choose your Authentication type. Then, click Connect.

4 The program opens at the database location.

5 Double-click on databases, then right-click on the folder and select tasks>Restore>database. The restore database dialog box opens.

Figure 146 Restore Database



Restore Database - WAMS

Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database: WAMS

To a point in time: Most recent possible

Source for restore

Specify the source and location of backup sets to restore.

● From database: WAMS

○ From device:

Select the backup sets to restore:

Restore	Name	Component	Ty...	Server	Databa...	Position
☑	WAMS-Full Database Backup	Database	Full	LAPTOP\OSI	WAMS	2

Connection

Server:
LAPTOP\OSI

Connection:
LAPTOP\Tina

Progress

Ready

6 The location defaults to the original location. You can specify a different location, for example, if you wish to more the database to a different computer.

7 Specify the source from which to restore and select a backup set to restore.

8 Select the backup set you wish to restore from the available list.

9 Click OK. The restore progresses and the system reports when the restore is complete.

Firmware Updates

Firmware updates will be sent to you periodically by dormakaba Technical Support. You can upload these firmware files to your database by using the System Administrator Application, and then you can send the updates to your hardware from the Configurator’s Firmware Tab. This section will guide you through the firmware update process.

Firmware File Types

Every Controller has two firmware files:

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

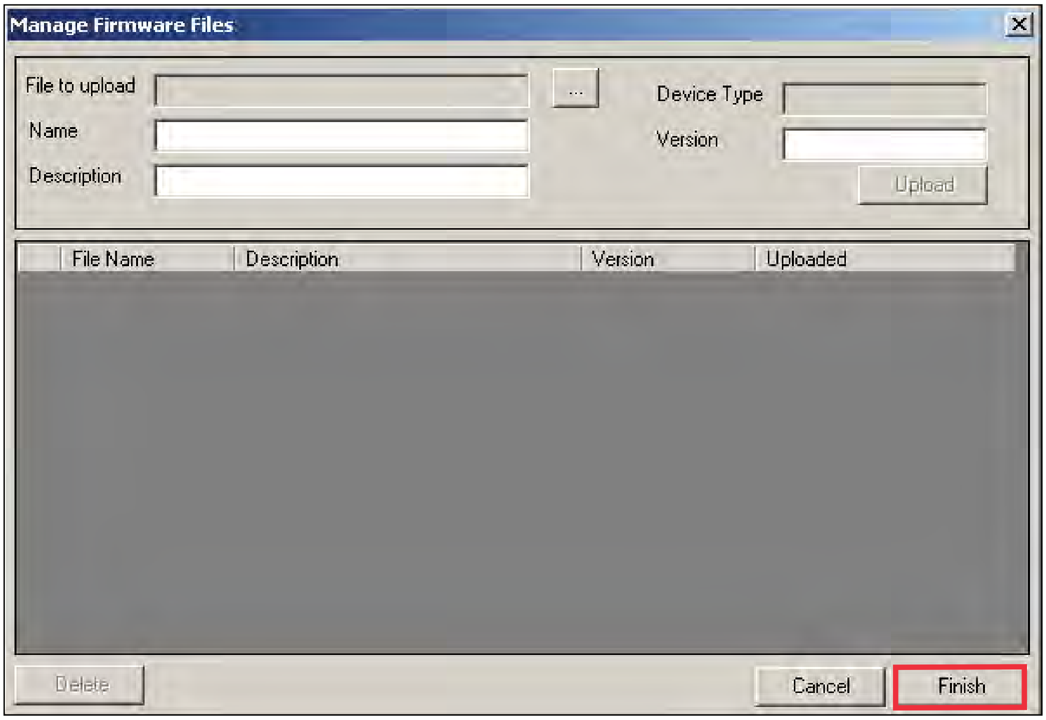
The application file is what is typically reprogrammed by the BEST Team, but it is possible that the bootloader file will require reprogramming as well. Controller firmware files will always have a “binhe” file extension.

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

Uploading Firmware Files

1 In the System Administrator application, choose Firmware Manager from the Import list on the right. The Manage Firmware Files dialog box opens.

Figure 147 Manage Firmware Files



2 Click on the ellipsis button next to the File to upload field. Browse to your Wi-Q Gateway or Controller file(s). Once you've located your file, click Open.

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

4 Click Upload. The firmware file will be added to the list at the bottom of the screen and added to your database.

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

5 Click Finish once all of your files are uploaded.

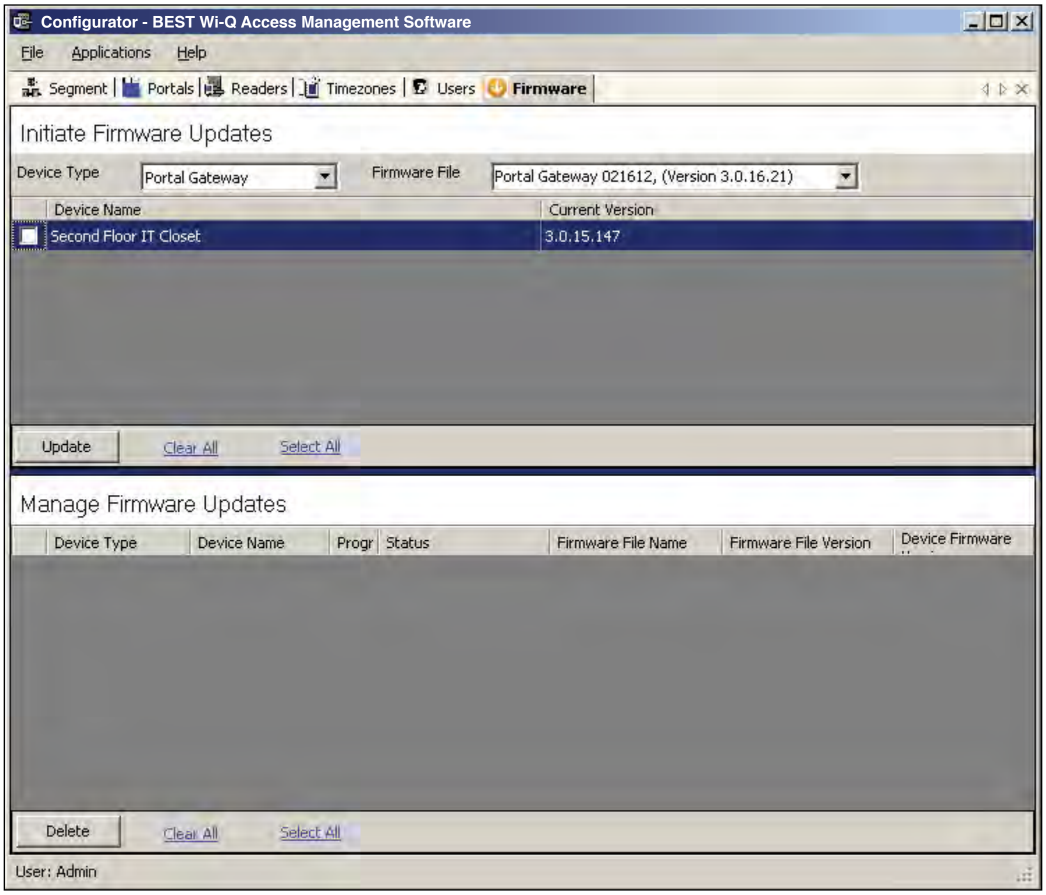
You are now ready to send the updates to your hardware.

Firmware Reprogram

Perform the following steps to send firmware updates to your hardware.

1 If not already open, launch the Configurator application and click on the Firmware tab.

Figure 148 Configurator Firmware Tab



Device Type: Portal Gateway

Firmware File: Portal Gateway 021612, (Version 3.0.16.21)

	Device Name	Current Version
□	Second Floor IT Closet	3.0.15.147

User: Admin

2 Choose your device type from the dropdown menu, and choose the appropriate firmware file.

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

3 Check the boxes next to the devices that need updating. You can click Select All or Clear All as needed.

4 Once you’ve made your selections, press Update.

5 The devices will be added to the Manage Firmware Updates queue below, where you can view the download progress and status.

Transactions Monitor

Each time a user accesses the system, the software collects a transaction from the Controller/Wi-Q Gateway network. Once the system is signed on and users begin accessing the system, transactions begin including any alarm activity. You can monitor all this activity in Transactions. Access Transactions via the Windows Start menu.

To Launch Transactions

1 Select Start>All Programs>BEST Access>BEST Wi-Q AMS>Transactions.

2 Enter your Login and Password. Transactions opens at the Transactions Tab.

3 From here you can view all transaction and alarm activity for the segment you select.

Note: If you have been assigned the Manager or Administrator User Type, you can launch Transactions from the Applications menu in Configurator.

Transactions Overview

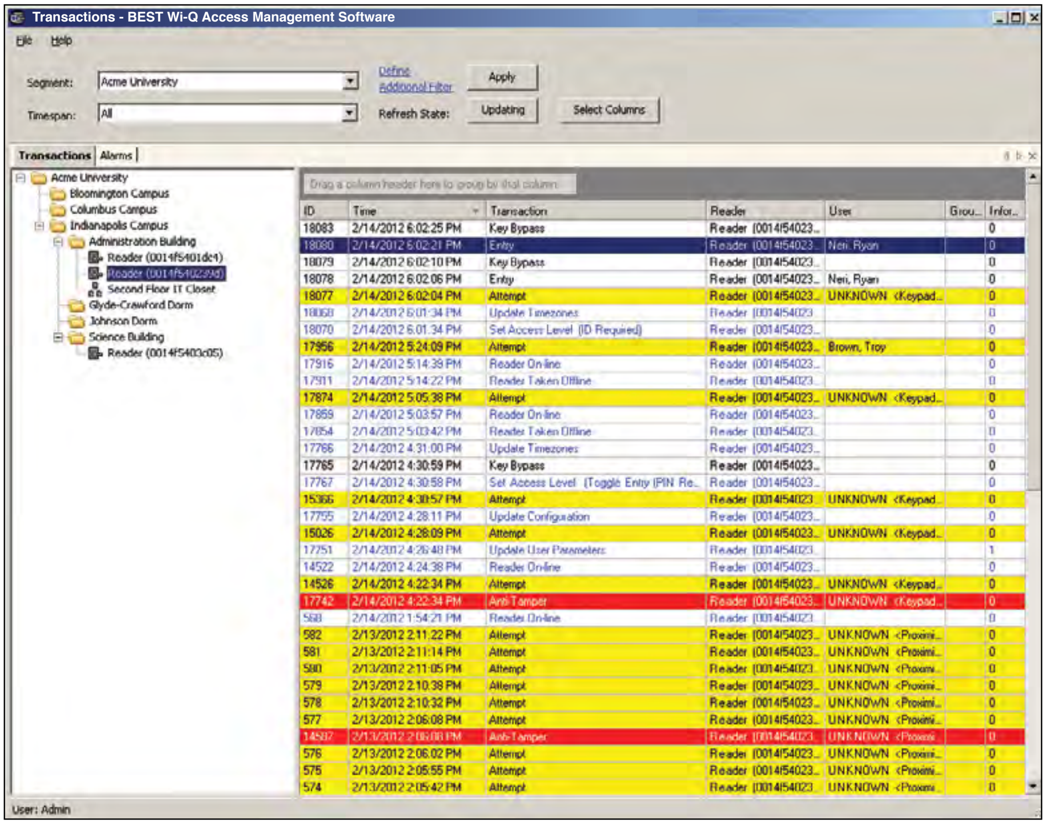
As activity takes place throughout the segment, AMS tracks each event as a transaction. The most obvious use of Transactions is to recognize and investigate when security has been compromised. You can immediately locate the source of an alarm and take the action necessary to respond according to your segment policy and procedure.

AMS gives each transaction in the database a unique ID, records the time and type of transaction, the Controller where the transaction occurred and the User ID and Group name associated with the transaction. You can monitor all this activity, real time, from the Transactions application. The transactions can be organized and sorted according to how you want to use the data. In addition, you can temporarily pause data updating if you need to review a transaction in more detail.

Transactions Tab

You can view all transactions as they occur in the Transactions Tab. Alarm transactions such as Forced Entry or Anti Tamper display in red. Access requests “attempted but not allowed” displays in yellow. Successful access requests display in black on a white background.

Figure 149 Transactions



Segment: Acme University

Timespan: All

Refresh State: Updating

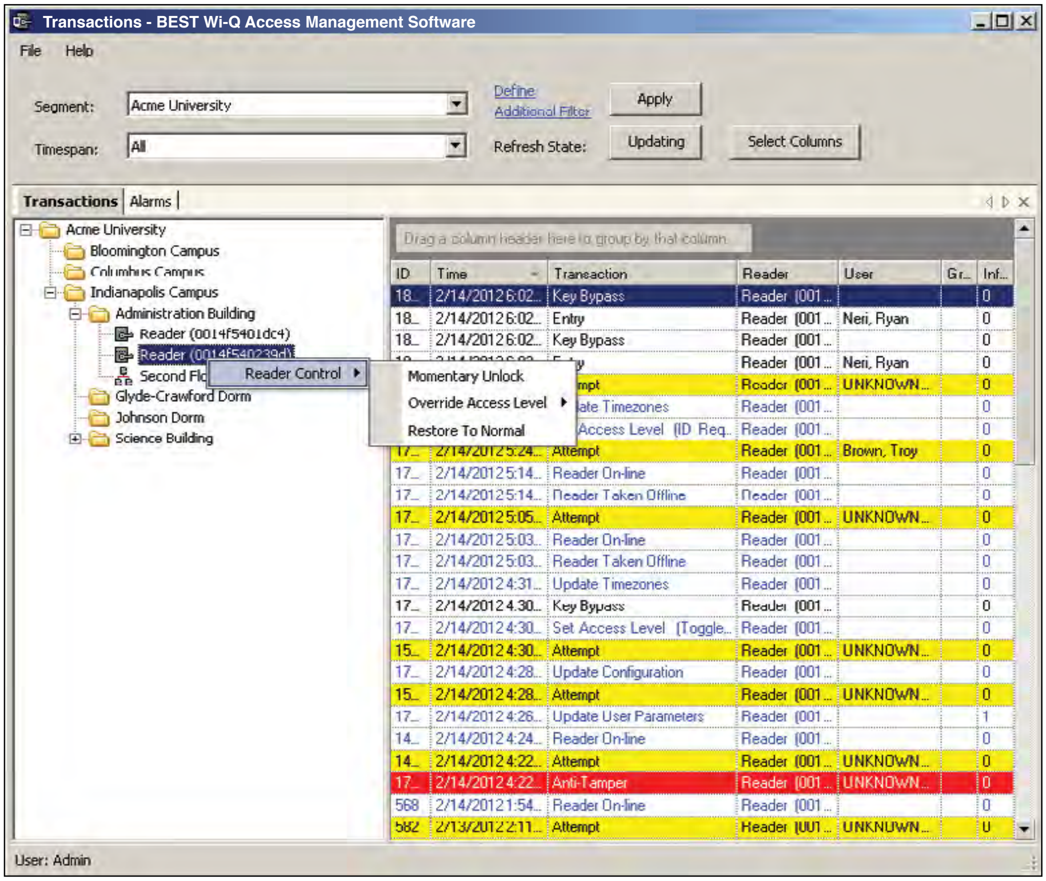
ID	Time	Transaction	Reader	User	Grou…	Infor…
18083	2/14/2012 6:02:25 PM	Key Bypass	Reader (0014f54023…			0
18080	2/14/2012 6:02:21 PM	Entry	Reader (0014f54023…	Neri, Ryan		0
18079	2/14/2012 6:02:10 PM	Key Bypass	Reader (0014f54023…			0
18078	2/14/2012 6:02:06 PM	Entry	Reader (0014f54023…	Neri, Ryan		0
18077	2/14/2012 6:02:04 PM	Attempt	Reader (0014f54023…	UNKNOWN <Keypad…		0
18068	2/14/2012 6:01:34 PM	Update Timezones	Reader (0014f54023			0
18070	2/14/2012 6:01:34 PM	Set Access Level (ID Required)	Reader (0014f54023…			0
17956	2/14/2012 5:24:09 PM	Attempt	Reader (0014f54023…	Brown, Troy		0
17916	2/14/2012 5:14:39 PM	Reader On-line	Reader (0014f54023…			0
17911	2/14/2012 5:14:22 PM	Reader Taken Offline	Reader (0014f54023…			0
17874	2/14/2012 5:05:38 PM	Attempt	Reader (0014f54023…	UNKNOWN <Keypad…		0
17859	2/14/2012 5:03:57 PM	Reader On-line	Reader (0014f54023…			0
17854	2/14/2012 5:03:42 PM	Reader Taken Offline	Reader (0014f54023…			0
17766	2/14/2012 4:31:00 PM	Update Timezones	Reader (0014f54023…			0
17765	2/14/2012 4:30:59 PM	Key Bypass	Reader (0014f54023…			0
17767	2/14/2012 4:30:58 PM	Set Access Level (Toggle Entry (PIN Re…	Reader (0014f54023…			0
15366	2/14/2012 4:30:57 PM	Attempt	Reader (0014f54023…	UNKNOWN <Keypad…		0
17755	2/14/2012 4:28:11 PM	Update Configuration	Reader (0014f54023…			0
15026	2/14/2012 4:28:09 PM	Attempt	Reader (0014f54023…	UNKNOWN <Keypad…		0
17751	2/14/2012 4:26:48 PM	Update User Parameters	Reader (0014f54023…			1
14522	2/14/2012 4:24:38 PM	Reader On-line	Reader (0014f54023…			0
14526	2/14/2012 4:22:34 PM	Attempt	Reader (0014f54023…	UNKNOWN <Keypad…		0
17742	2/14/2012 4:22:34 PM	Anti-Tamper	Reader (0014f54023…	UNKNOWN <Keypad…		0
568	2/14/2012 1:54:21 PM	Reader On-line	Reader (0014f54023…			0
582	2/13/2012 2:11:22 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
581	2/13/2012 2:11:14 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
580	2/13/2012 2:11:05 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
579	2/13/2012 2:10:38 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
578	2/13/2012 2:10:32 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
577	2/13/2012 2:06:08 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
14587	2/13/2012 2:06:08 PM	Anti-Tamper	Reader (0014f54023…	UNKNOWN <Proximi…		0
576	2/13/2012 2:06:02 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
575	2/13/2012 2:05:55 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0
574	2/13/2012 2:05:42 PM	Attempt	Reader (0014f54023…	UNKNOWN <Proximi…		0

System transactions such as changing an access level or clearing an alarm display in blue on a white background. To review and respond to alarms, select the Alarms Tab.

Reader and Portal Controls

You can access reader and Portal controls from inside the Transactions tab. From here you can override access levels of readers to unlock or lockout one or a whole related group of readers. To use this feature, simply right click on the Portal or reader and select an option.

Figure 150 Accessing Portals and Readers in the Transactions tab



Segment: Acme University

Timespan: All

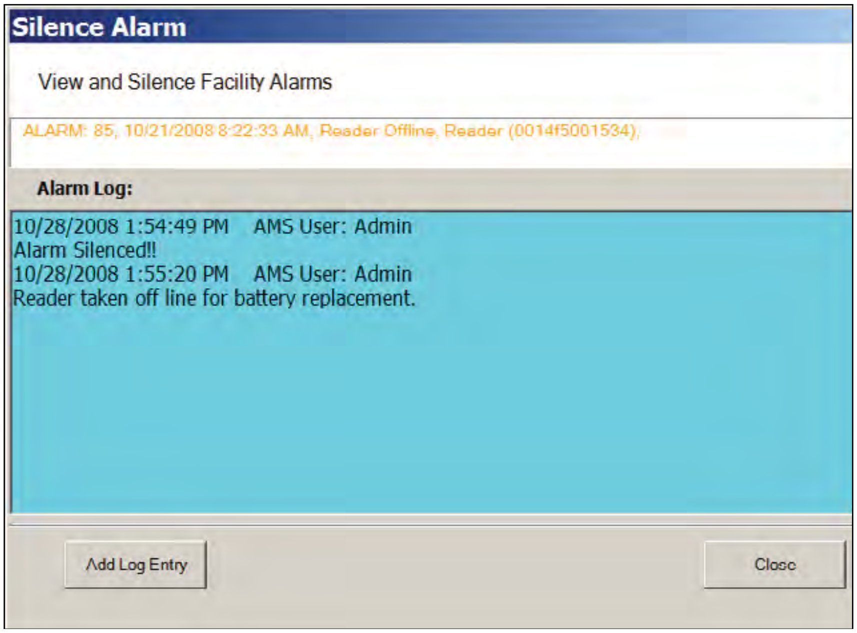
ID	Time	Transaction	Reader	User	Gr...	Inf...
18...	2/14/2012 6:02...	Key Bypass	Reader (001 ...			0
18...	2/14/2012 6:02...	Entry	Reader (001 ...	Neri, Ryan		0
18...	2/14/2012 6:02...	Key Bypass	Reader (001 ...			0
		y	Reader (001 ...	Neri, Ryan		0
		mpt	Reader (001 ...	UNKNOWN ...		0
		ate Timezones	Reader (001 ...			0
		Access Level (ID Req...	Reader (001 ...			0
17...	2/14/2012 5:24...	Attempt	Reader (001 ...	Brown, Troy		0
17...	2/14/2012 5:14...	Reader On-line	Reader (001 ...			0
17...	2/14/2012 5:14...	Reader Taken Offline	Reader (001 ...			0
17...	2/14/2012 5:05...	Attempt	Reader (001 ...	UNKNOWN ...		0
17...	2/14/2012 5:03...	Reader On-line	Reader (001 ...			0
17...	2/14/2012 5:03...	Reader Taken Offline	Reader (001 ...			0
17...	2/14/2012 4:31...	Update Timezones	Reader (001 ...			0
17...	2/14/2012 4:30...	Key Bypass	Reader (001 ...			0
17...	2/14/2012 4:30...	Set Access Level (Toggle...	Reader (001 ...			0
15...	2/14/2012 4:30...	Attempt	Reader (001 ...	UNKNOWN ...		0
17...	2/14/2012 4:28...	Update Configuration	Reader (001 ...			0
15...	2/14/2012 4:28...	Attempt	Reader (001 ...	UNKNOWN ...		0
17...	2/14/2012 4:26...	Update User Parameters	Reader (001 ...			1
14...	2/14/2012 4:24...	Reader On-line	Reader (001 ...			0
14...	2/14/2012 4:22...	Attempt	Reader (001 ...	UNKNOWN ...		0
17...	2/14/2012 4:22...	Anti-Tamper	Reader (001 ...	UNKNOWN ...		0
568	2/14/2012 1:54...	Reader On-line	Reader (001 ...			0
582	2/13/2012 2:11...	Attempt	Reader (001 ...	UNKNOWN ...		0

Alarms Tab

When an alarm is triggered, such as a door is blocked open or forced entry, the system creates an alarm record. When you select the Alarms tab, unanswered alarms display in red and activate an alarm sound .wav file on your computers sound system.

When you “silence” an alarm in Transactions, you are simply telling the system that you have recognized the alarm condition. The alarm sound .wav file will stop on your computer system for that alarm and the display color changes from red to yellow. A log will be generated recording the time and date the alarm was silenced. You can add a comment to this log to further define the incident

Figure 151 Silencing an alarm in the Alarms tab



Silence Alarm

View and Silence Facility Alarms

ALARM: 85, 10/21/2008 8:22:33 AM, Reader Offline, Reader (0014f5001534),

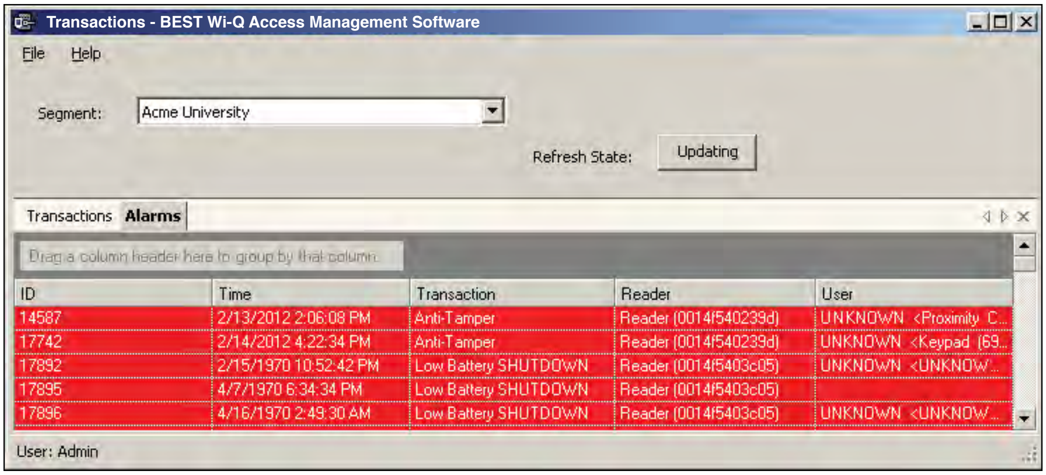
Alarm Log:

```
10/28/2008 1:54:49 PM    AMS User: Admin
Alarm Silenced!!
10/28/2008 1:55:20 PM    AMS User: Admin
Reader taken off line for battery replacement.
```

Create an Alarm Response Protocol

Remember, when you "Silence" an alarm in Wi-Q AMS Transactions, you are only silencing a .wav file; you are not resolving the problem. It is important to establish Alarm Response protocols within your segment and follow up with action. See "Responding to Alarms" on page 206.

Figure 152 Alarms Tab



Transactions - BEST Wi-Q Access Management Software
File
Help
Segment:
Acme University
Refresh State:
Updating
Transactions
Alarms
Drag a column header here to group by that column.

ID	Time	Transaction	Reader	User
14587	2/13/2012 2:06:08 PM	Anti-Tamper	Reader (0014f540239d)	UNKNOWN <Proximity C...
17742	2/14/2012 4:22:34 PM	Anti-Tamper	Reader (0014f540239d)	UNKNOWN <Keypad (69...
17892	2/15/1970 10:52:42 PM	Low Battery SHUTDOWN	Reader (0014f5403c05)	UNKNOWN <UNKNOW...
17895	4/7/1970 6:34:34 PM	Low Battery SHUTDOWN	Reader (0014f5403c05)	
17896	4/16/1970 2:49:30 AM	Low Battery SHUTDOWN	Reader (0014f5403c05)	UNKNOWN <UNKNOW...

User: Admin

Transaction Types

The database records transactions by category. Under normal operating conditions, the most common transaction types will be Entry and Request to Exit. The system recognizes various alarm and status categories, such as:

- Alarm Cleared (All)
- Alarm Cleared (Forced Entry)
- Anti-Tamper

Organizing and Sorting Transactions

AMS makes it easy to manage high transaction traffic. You could view every transaction in the system, real time. However, in large systems where hundreds of transactions can occur in a very short time, you may want to limit the number of transactions displayed, or group them in a way that makes sense for system activity. For example, you can limit the transactions list to only those that occurred in the last ten minute timespan; you can sort ascending or descending by column header; and you can arrange the columns in any order you wish. In addition, you can create a hierarchy, rather than a columnar view.

Display by Timespan

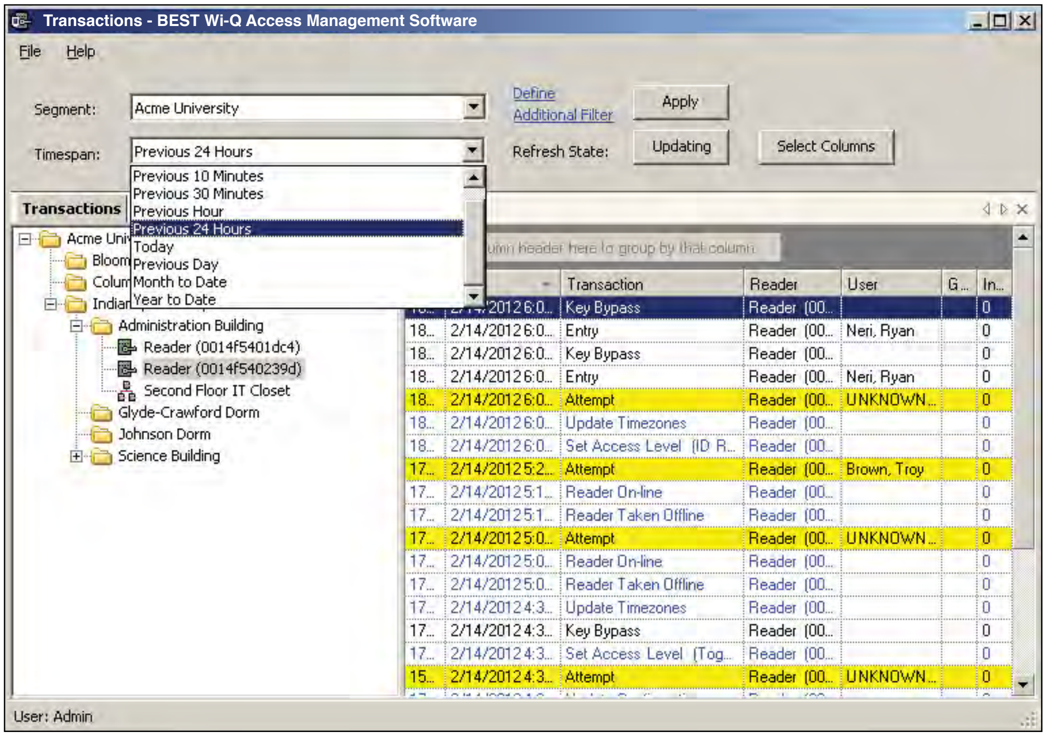
By default, Transactions displays all transactions in the order they occur. If you are monitoring all transactions, you may want to simply watch them as they occur. However, in large systems, your effort may best be served by limiting transactions to only those that have occurred in the previous ten minutes, or previous hour. The software gives you a number of options from All to year to date.

To set the display timespan

In the Transactions Tab, select the Segment you wish to monitor.

Under Timespan, select the timespan you wish to display from the drop-down list. The display list on the right changes to reflect your selection.

Figure 153 Transactions Timespan



Transactions - BEST Wi-Q Access Management Software

Segment: Acme University

Timespan: Previous 24 Hours

Refresh State: Updating

- Acme Univ
  - Bloom
  - Colum
  - Indian
    - Administration Building
      - Reader (0014f5401dc4)
      - Reader (0014f540239d)
      - Second Floor IT Closet
    - Glyde-Crawford Dorm
    - Johnson Dorm
    - Science Building

		Transaction	Reader	User	G...	In...
18...	2/14/2012 6:0...	Key Bypass	Reader (00...			0
18...	2/14/2012 6:0...	Entry	Reader (00...	Neri, Ryan		0
18...	2/14/2012 6:0...	Key Bypass	Reader (00...			0
18...	2/14/2012 6:0...	Entry	Reader (00...	Neri, Ryan		0
18...	2/14/2012 6:0...	Attempt	Reader (00...	UNKNOWN...		0
18...	2/14/2012 6:0...	Update Timezones	Reader (00...			0
18...	2/14/2012 6:0...	Set Access Level (ID R...	Reader (00...			0
17...	2/14/2012 5:2...	Attempt	Reader (00...	Brown, Troy		0
17...	2/14/2012 5:1...	Reader On-line	Reader (00...			0
17...	2/14/2012 5:1...	Reader Taken Offline	Reader (00...			0
17...	2/14/2012 5:0...	Attempt	Reader (00...	UNKNOWN...		0
17...	2/14/2012 5:0...	Reader On-line	Reader (00...			0
17...	2/14/2012 5:0...	Reader Taken Offline	Reader (00...			0
17...	2/14/2012 4:3...	Update Timezones	Reader (00...			0
17...	2/14/2012 4:3...	Key Bypass	Reader (00...			0
17...	2/14/2012 4:3...	Set Access Level (Tog...	Reader (00...			0
15...	2/14/2012 4:3...	Attempt	Reader (00...	UNKNOWN...		0

User: Admin

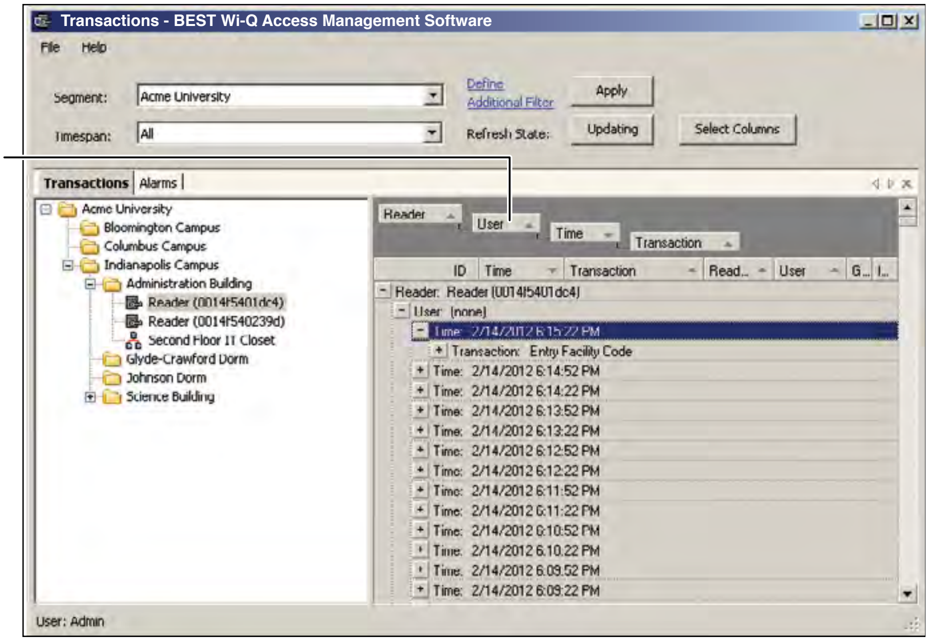
Sort by Column Header

You can sort Transactions by column header in ascending or descending order. This is helpful, depending on what you are looking for. If you simply want to watch transactions in the order they occur, the default setting—sorted by ID, descending—will display the most recent transaction on the top line of the list. However, if you have an interest in viewing all the activity of a particular user, you can sort alphabetically by User credential. As with common database programs, you can move the columns in the column header to any order you wish. Transactions will remember your changes and display in the new order when you next open the program.

View Transactions in Tree Levels

You can display transactions similar to the way you view the Segment Tree in Configurator. This is useful to minimize and organize the amount of data you view at one time.

Figure 154 Transactions in Tree Levels



Drag column headers to gray area.

Transactions - BEST Wi-Q Access Management Software

Segment: Acme University

Timespan: All

Refresh State: Updating

- Acme University
  - Bloomington Campus
  - Columbus Campus
  - Indianapolis Campus
    - Administration Building
      - Reader (0014f5401dc4)
      - Reader (0014f540239d)
      - Second Floor IT Closet
    - Glyde-Crawford Dorm
    - Johnson Dorm
    - Science Building

```
Reader: Reader (0014f5401dc4)
  User: (none)
    Time: 2/14/2012 6:15:22 PM
      Transaction: Entry Facility Code
    Time: 2/14/2012 6:14:52 PM
    Time: 2/14/2012 6:14:22 PM
    Time: 2/14/2012 6:13:52 PM
    Time: 2/14/2012 6:13:22 PM
    Time: 2/14/2012 6:12:52 PM
    Time: 2/14/2012 6:12:22 PM
    Time: 2/14/2012 6:11:52 PM
    Time: 2/14/2012 6:11:22 PM
    Time: 2/14/2012 6:10:52 PM
    Time: 2/14/2012 6:10:22 PM
    Time: 2/14/2012 6:09:52 PM
    Time: 2/14/2012 6:09:22 PM
```

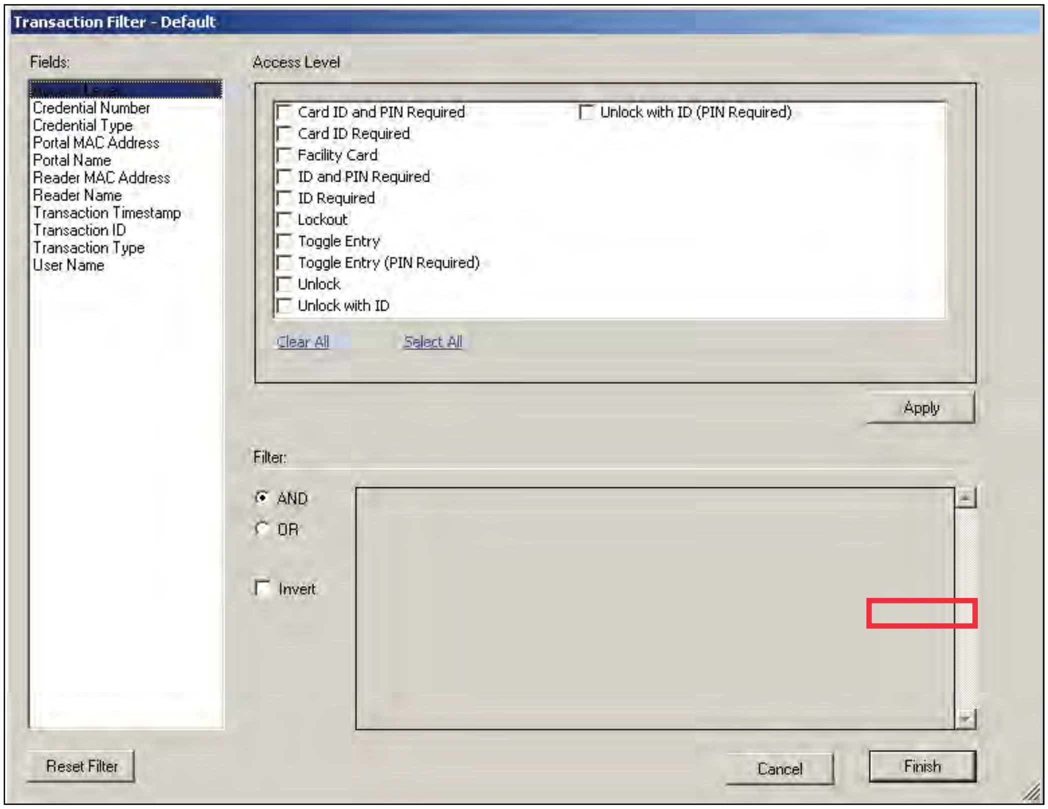
User: Admin

In this example, we placed Readers at the top of the tree; however, you can place them in any hierarchy you wish. When you select the plus sign next to the top level, the second and third level items expand to display. It’s easy to create a Transactions Tree: simply drag and drop the column headers into position.

Transaction Filters

If you want to search for a specific transaction by certain criteria (user name, reader name, etc.), click on Define Additional Filter at the top of the Transactions module. The Transaction Filter dialog box will open.

Figure 155 Transaction Filters



Transaction Filter - Default

Fields:

- Access Level
- Credential Number
- Credential Type
- Portal MAC Address
- Portal Name
- Reader MAC Address
- Reader Name
- Transaction Timestamp
- Transaction ID
- Transaction Type
- User Name

Access Level

□ Card ID and PIN Required
□ Card ID Required
□ Facility Card
□ ID and PIN Required
□ ID Required
□ Lockout
□ Toggle Entry
□ Toggle Entry (PIN Required)
□ Unlock
□ Unlock with ID
□ Unlock with ID (PIN Required)

Filter:

● AND
○ OR
□ Invert

A list of fields is located on the left side of the dialog box. Clicking on a field will bring up checkbox or dropdown options specific to the selected field. In Figure 155, the Access Level field is selected. Here, you can check multiple options. Once you've selected your options, click Apply. The Filter section at the bottom of the dialog box will reflect what filter you've applied.

You can turn on multiple filters with the use of the AND/OR selection options in the Filter section. If you'd like to search your transactions by a specific access level and reader name, apply both filters and select AND.

If you want to omit certain transactions from your list, you can click the Invert checkbox once you've applied your filters. Inverting will adjust your list so that the applied filters are not shown.

When finished creating filters, click Finish. If you would like to clear your filters, click on Reset Filter.

Responding to Alarms

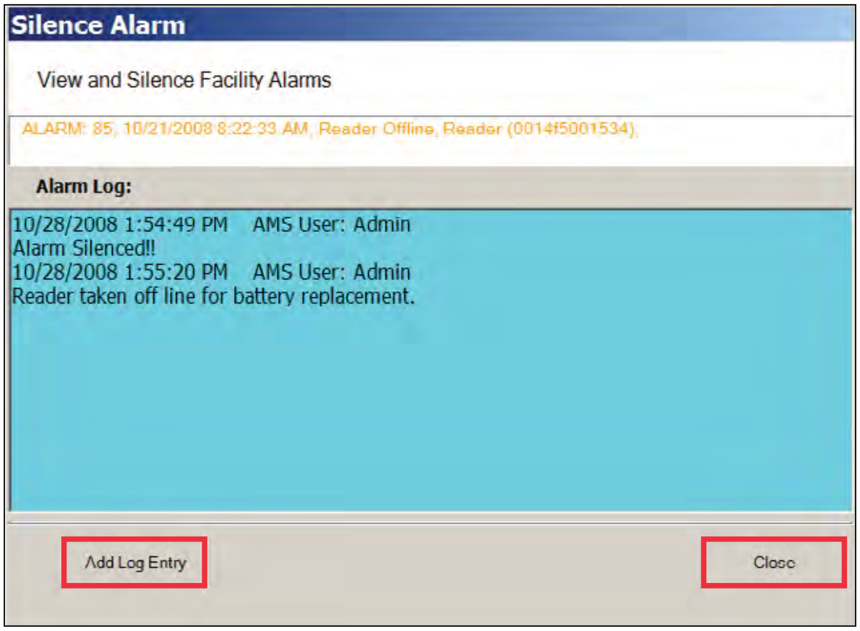
When an alarm occurs, the system immediately displays it in red in the Transactions Tab. The alarm will be categorized as either an Anti-Tamper or a Forced Entry type. At this point, you will take action according to your segment's security plan. In a small segment, you may simply dispatch a person to physically investigate the source of the alarm. In larger facilities with I/O devices in the system, the alarm may trigger a video recorder, a lighting plan, or other I/O device. In either case, you will respond to the alarm in Transactions using the Alarms Tab.

As with the Transactions Tab, you can sort the alarms in ascending and descending order with a column, and change the order in which the columns display, and create an Alarms Tree.

To respond to and silence an alarm

1. Select the Alarms Tab.
2. Double-click on an active alarm (displaying in red). The Silence Alarm text box opens. Alarm details display in red text in the message area.
3. Click on Silence Alarm.
4. To add a log entry, click Add Log Entry.
5. Enter a comment in the text box.
6. When finished, click Add to Log.
7. The message entered will become the record for the alarm event.

Figure 156 Log Entry Recorded



Silence Alarm

View and Silence Facility Alarms

ALARM: 85, 10/21/2008 8:22:33 AM, Reader Offline, Reader (0014f5001534),

Alarm Log:

```
10/28/2008 1:54:49 PM    AMS User: Admin
Alarm Silenced!!
10/28/2008 1:55:20 PM    AMS User: Admin
Reader taken off line for battery replacement.
```

8 Select Close. In the Alarms Tab, the alarm line changes from red to yellow and the alarm sound stops.

9 You can continue to add comments in the alarm's log until the condition is resolved.

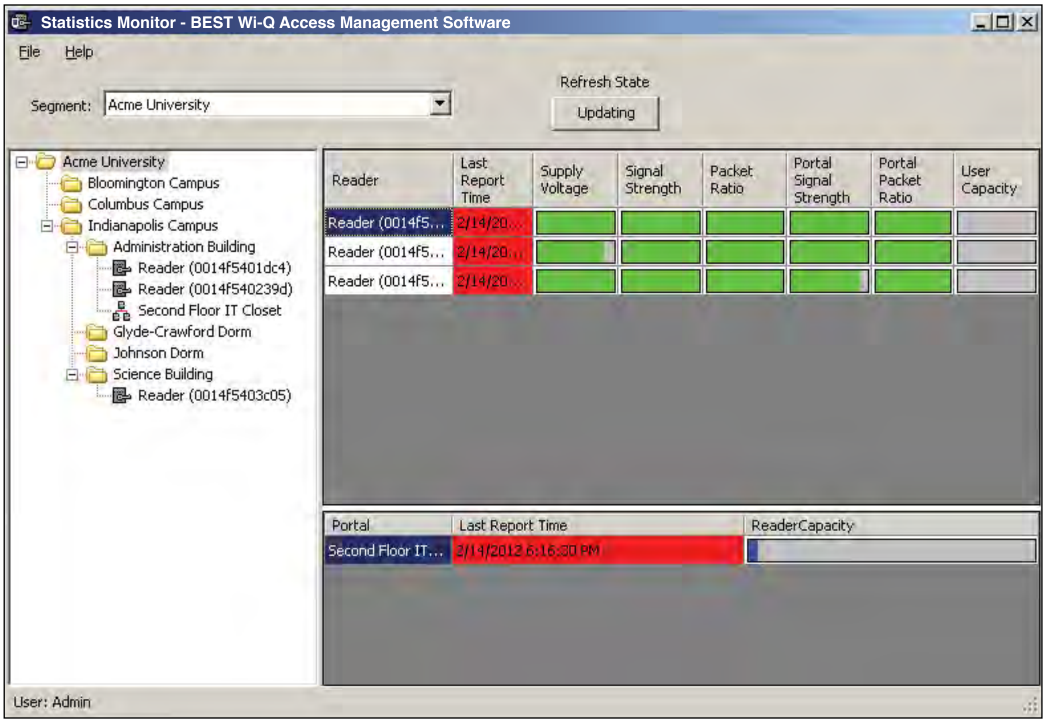
Statistics Monitor

The Statistics Monitor is a powerful tool that displays a real-time, color coded overview of system performance. When you set up your new system, and want to monitor ongoing system performance, you will use the Statistics Monitor. This tool appears similar to the Configurator, displaying the Segment Tree for the segment you select on the left of the screen, and the hardware categories on the right. To check the performance of the entire system, select the segment at the top of the tree. Reader statistics display at the top of the screen and Portal statistics display at the bottom.

You can access the Statistics Monitor from the Applications menu at the top of the Configurator Main Screen or launch it from the Windows Start menu as a separate application

Reader Statistics

Figure 157 Viewing Reader Statistics



Segment: Acme University

- Acme University
  - Bloomington Campus
  - Columbus Campus
  - Indianapolis Campus
    - Administration Building
      - Reader (0014f5401dc4)
      - Reader (0014f540239d)
      - Second Floor IT Closet
    - Glyde-Crawford Dorm
    - Johnson Dorm
    - Science Building
      - Reader (0014f5403c05)

Reader	Last Report Time	Supply Voltage	Signal Strength	Packet Ratio	Portal Signal Strength	Portal Packet Ratio	User Capacity
Reader (0014f5...	2/14/20...	🟩	🟩	🟩	🟩	🟩	
Reader (0014f5...	2/14/20...	🟩	🟩	🟩	🟩	🟩	
Reader (0014f5...	2/14/20...	🟩	🟩	🟩	🟩	🟩	

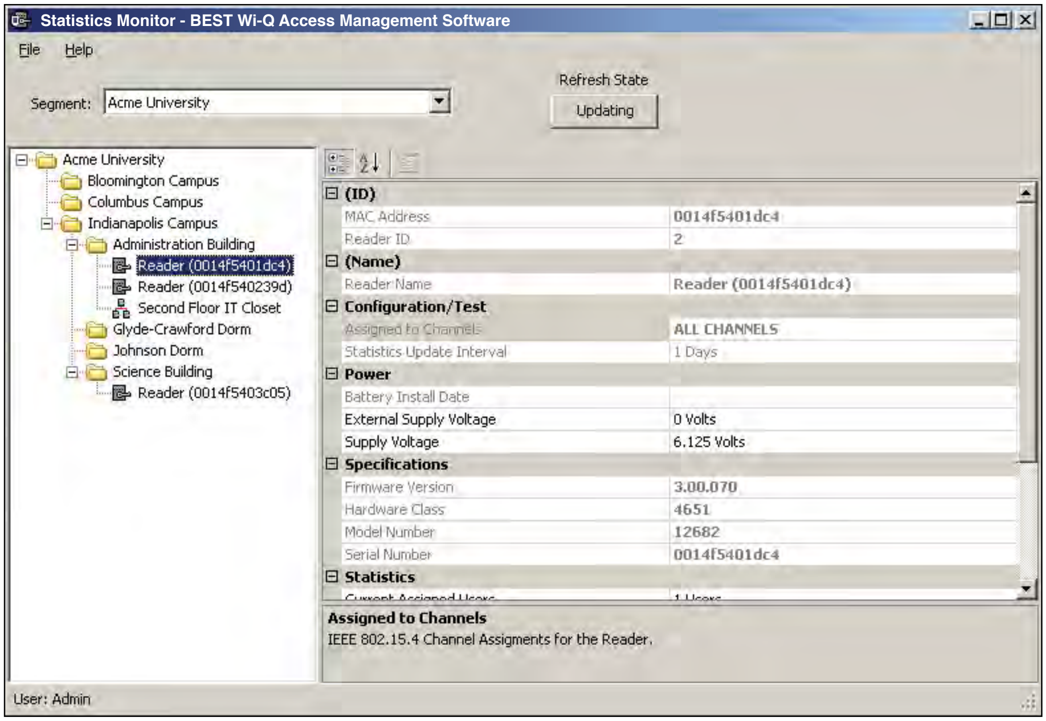
Portal	Last Report Time	ReaderCapacity
Second Floor IT...	2/14/2012 6:16:30 PM	

User: Admin

In this example, the system is performing well, delivering transactions at an acceptable level. To display the actual measurement, hover the cursor over a bar.

To get more detail; for example, to diagnose the problem of low signal for a particular reader, you can navigate to that reader in the Segment Tree and see data for only that reader. You can also double-click the reader on the right panel. Specific information for the selected reader displays in the list on the right.

Figure 158 Display reader detail



Segment: Acme University

(ID)	
MAC Address	0014f5401dc4
Reader ID	2
(Name)	
Reader Name	Reader (0014f5401dc4)
Configuration/Test	
Assigned to Channels	ALL CHANNELS
Statistics Update Interval	1 Days
Power	
Battery Install Date	
External Supply Voltage	0 Volts
Supply Voltage	6.125 Volts
Specifications	
Firmware Version	3.00.070
Hardware Class	4651
Model Number	12682
Serial Number	0014f5401dc4
Statistics	
Current Assigned Users	1 Users

Assigned to Channels
IEEE 802.15.4 Channel Assignments for the Reader.

User: Admin

Here, you can see the reader's MAC Address, ID, Reader Name, and the Portal associated with it. You can also view the reader's power performance.

Automatic Updates

The Updating button can be used to pause automatic updating to view a snap shot of data. This is especially useful when viewing the top level, where the values may be changing rapidly.

Configuration/Test

Under the Configuration/Test category inside a reader's property list, you can see the Statistics Update Interval. This value can be changed in the Readers tab of the Configurator application. For more information on configuring readers, see Chapter 4, "Configuring Segments, Wi-Q Gateways and Controllers".

Power

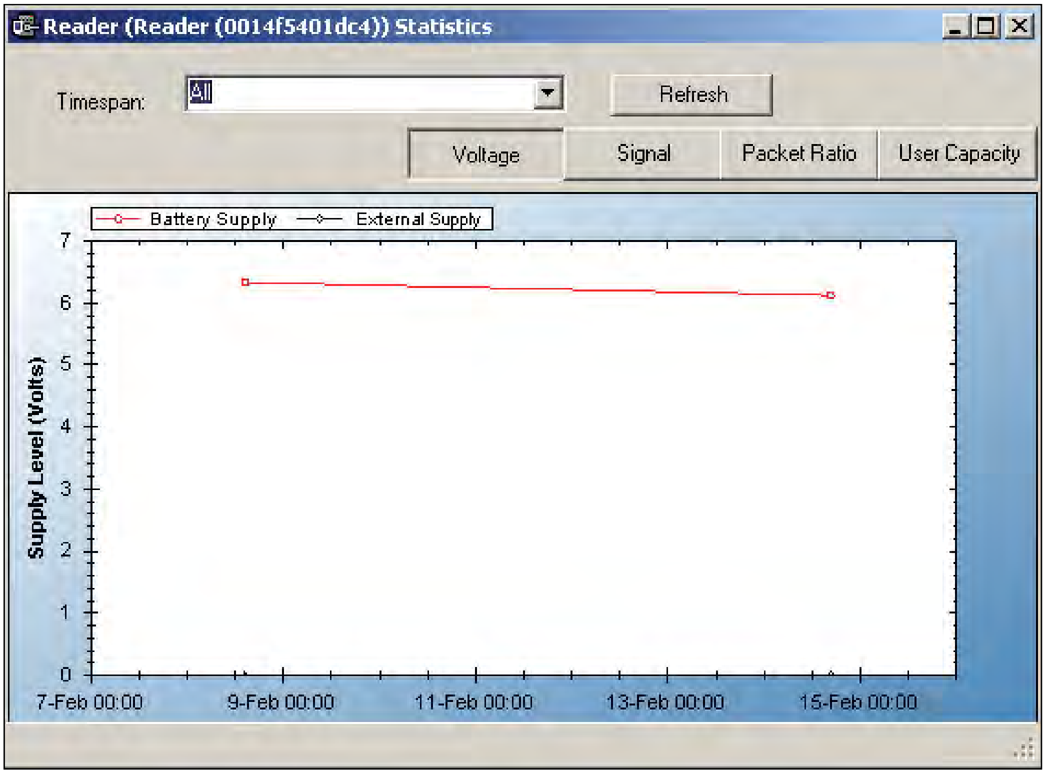
To view individual reader performance:

1. Under the Power Category, place the cursor in the field next to Supply Voltage, and select the ellipsis button.
2. The Reader Statistics chart opens at the Voltage Tab. From here you can also check the Signal, Packet Ratio, and User Capacity.

Voltage Tab

The Voltage Tab displays battery and external power supply to ensure battery integrity and longevity. If you see a downward trend, you should consider replacing the battery for preventive maintenance.

Figure 159 Reader Statistics Voltage Tab



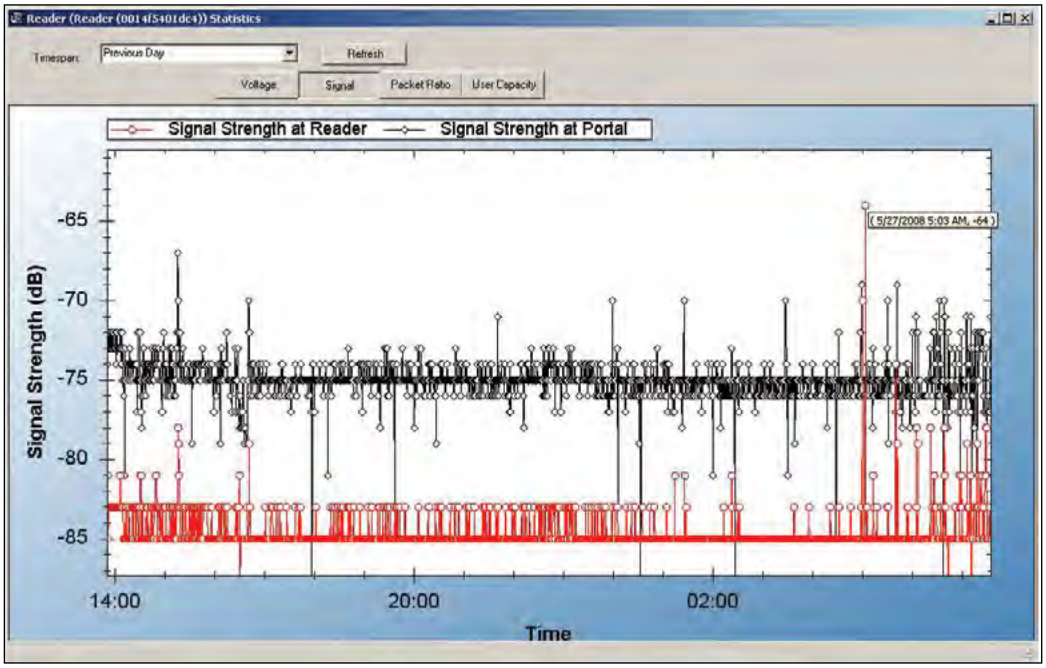
Every minute, the reader sends a beacon to the Wi-Q Gateway with signal strength, battery voltage, external supply voltage and packet transfer ratio information. These statistics are stored at the rate defined by the Statistics Update Interval.

Select Refresh to get the latest readings, or you can reset the timespan to various intervals relevant to your diagnostic evaluation. You can move through the tabs as you check the system performance.

Signal Tab

The Signal Tab displays the signal strength at the reader and at the reader’s Portal.

Figure 160 Reader Statistics Signal Tab



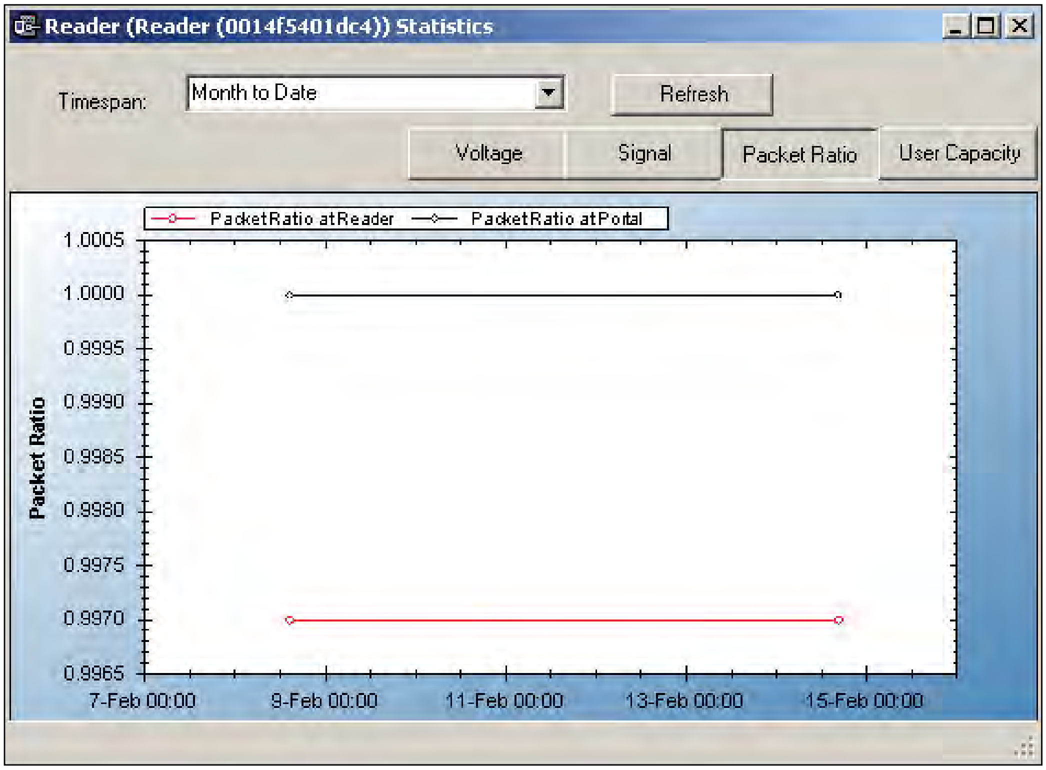
Reader (Reader (0014f5401dc4)) Statistics

Timespan: Previous Day

Packet Transfer Ratio Tab

The Packet Transfer Ratio at Reader is the number of valid packets received versus the total number of packets sent to the reader. The Packet Transfer Ratio at Portal is the number of valid packets sent from the reader versus the total number of packets received at the Portal. If the Packet Ratio is high (near 1, or 100%) your readers are performing well, even though signal strength might be low. If signal strength is high and Packet Ratio is low, you may have a problem at the reader, or there may be interference on the channel that the Portal is using.

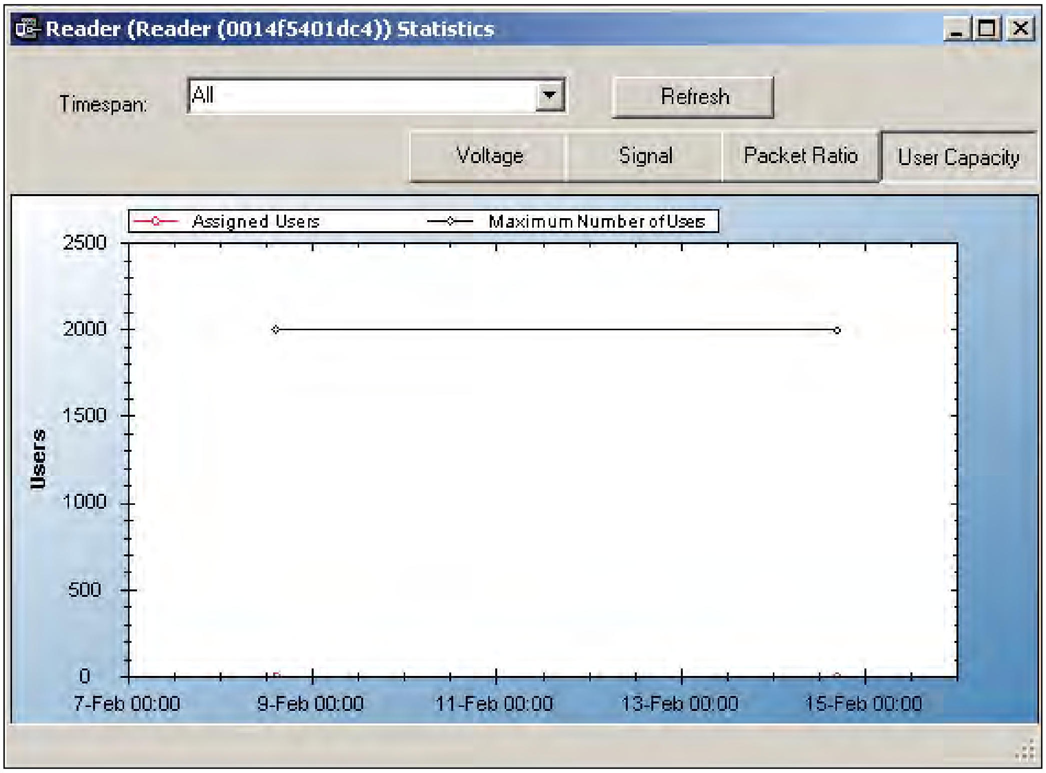
Figure 161 Reader Statistics Packet Radio Tab



User Capacity

This chart shows the Max allowable users for this reader and the current use. If you find that the use is nearing capacity, you may want to consider upgrading the reader capacity. See "Segment Item Upgrades" on page 179.

Figure 162 Reader Statistics User Capacity Tab

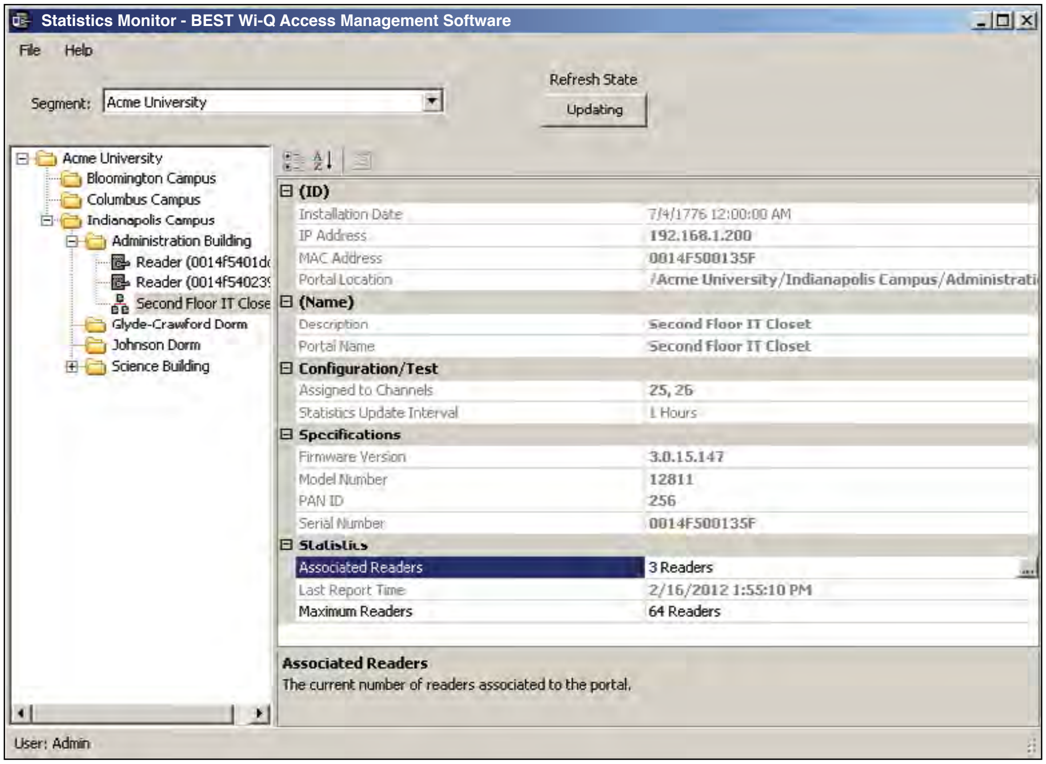


Portal Statistics

Portal Statistics display at the bottom of the Statistics Monitor. Select the top level in the Segment Tree to display all Portals in the system. See Figure 163.

Clicking on a Portal within the Segment Tree in the Statistics Monitor will display the Portal’s properties on the right.

Figure 163 Statistics Monitor Portal Properties



Segment: Acme University

(ID)	
Installation Date	7/4/1776 12:00:00 AM
IP Address	192.168.1.200
MAC Address	0014F500135F
Portal Location	/Acme University/Indianapolis Campus/Administrati
(Name)	
Description	Second Floor IT Closet
Portal Name	Second Floor IT Closet
Configuration/Test	
Assigned to Channels	25, 26
Statistics Update Interval	1 Hours
Specifications	
Firmware Version	3.0.15.147
Model Number	12811
PAN ID	256
Serial Number	0014F500135F
Statistics	
Associated Readers	3 Readers
Last Report Time	2/16/2012 1:55:10 PM
Maximum Readers	64 Readers

Associated Readers
The current number of readers associated to the portal.

The Portal ID, Name, Specifications such as Firmware Version, Model Number, PAN ID, and Serial Number display on the right. In the Statistics category, you can see how many readers are associated with the Portal and its current maximum reader capacity.

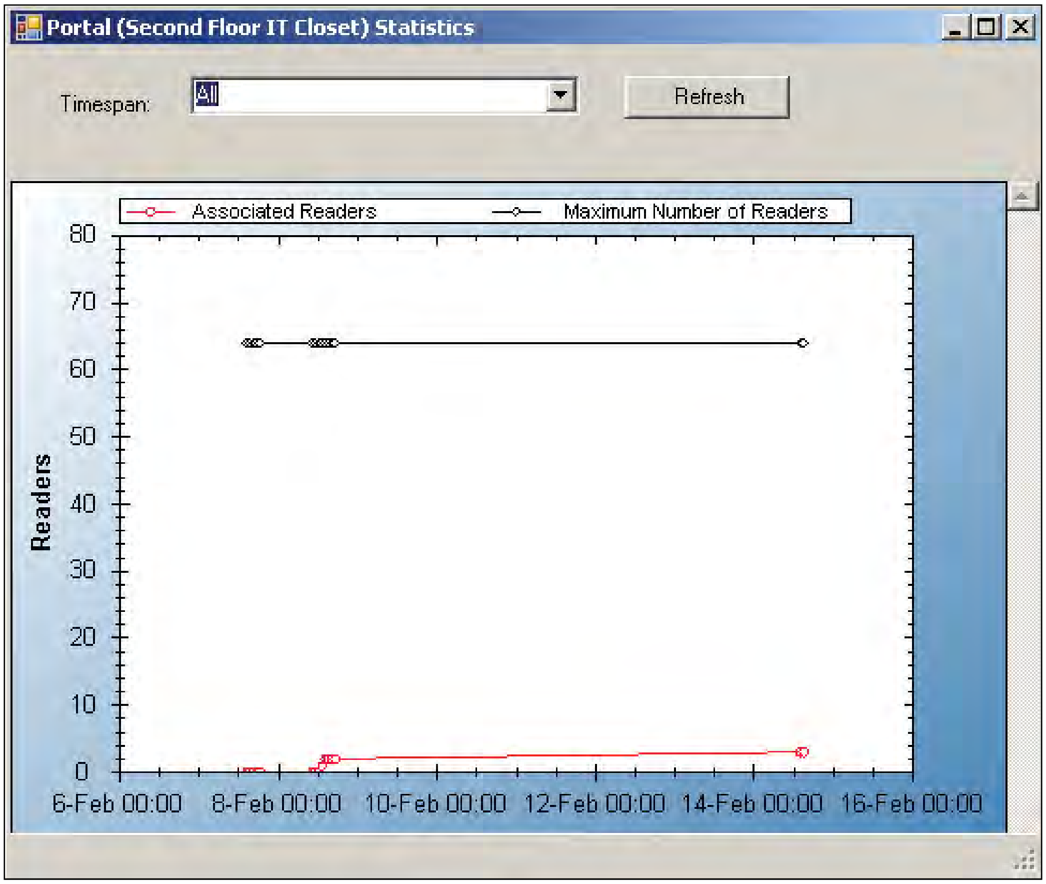
Portal Diagnostics

You can check the reader counts associated with a Portal over time for a detailed look at Portal capacity. This is useful to determine if some readers are operating intermittently or dropping out of range at intervals.

To review associated readers at Portals

1 In the Portal detail display, Statistics Category, place the cursor in the Maximum number of Readers field and select the ellipsis button. The Portal statistics chart opens for the Portal selected.

Figure 164 Portal Statistics



If the Associated Readers line appears steady and reflects the number of readers you know are associated with the Portal, your readers are consistently being recognized by the Portal. If this line is erratic; for example, showing a drop or fluctuation on associated readers over time, you may want to review the readers to see if there is a problem with power supply or signal that is making one or more of them drop out of range.

Configuration/Test

In the Configuration/Test category, the Statistic Update Interval is visible. You can modify this value in the Configurator application's Portals Tab.

Reports

You can view a wide variety of reports based on data collected in Configurator and Transactions. You can access Reports from the Applications menu at the top of the Configurator Main Screen or launch it as a separate application.

To Launch Wi-Q AMS Reports

1. Select Start>All Programs>BEST Access>BEST Wi-Q AMS>Reports.
2. Enter your Login and Password. Reports opens.

Reports Overview

The software provides seven reports that you can modify:

Users of Readers — Generate a report that lists all readers and the users currently assigned to them, or you can specify a particular reader and view only the users for that reader.

Users of Groups — Generate a report that lists all user groups and the users currently assigned to them, or you can specify a particular user group and view only the users for that group.

Users Entry Log — Generate a report that lists user entry data for all users and all readers, or you can specify which readers and users to list. You can also specify a timespan or Begin and End dates on which to report.

Users Entry/Exit Log — Generate a report that lists user entry/exit data for all users and all readers, or you can specify which readers and users to list. You can also specify a timespan or Begin and End dates on which to report.

Alarms Log — Generate a report by alarm for all readers in all timespans, or specify which alarms, timespans, or Begin and End dates.

Reader Alarms — Generates a report by reader for all alarms in all timespans, or specify which readers, timespans, or Begin and End dates.

Transactions — Generate a report for all transactions at all readers for all users during all timespans, or specify which transactions you wish to list.

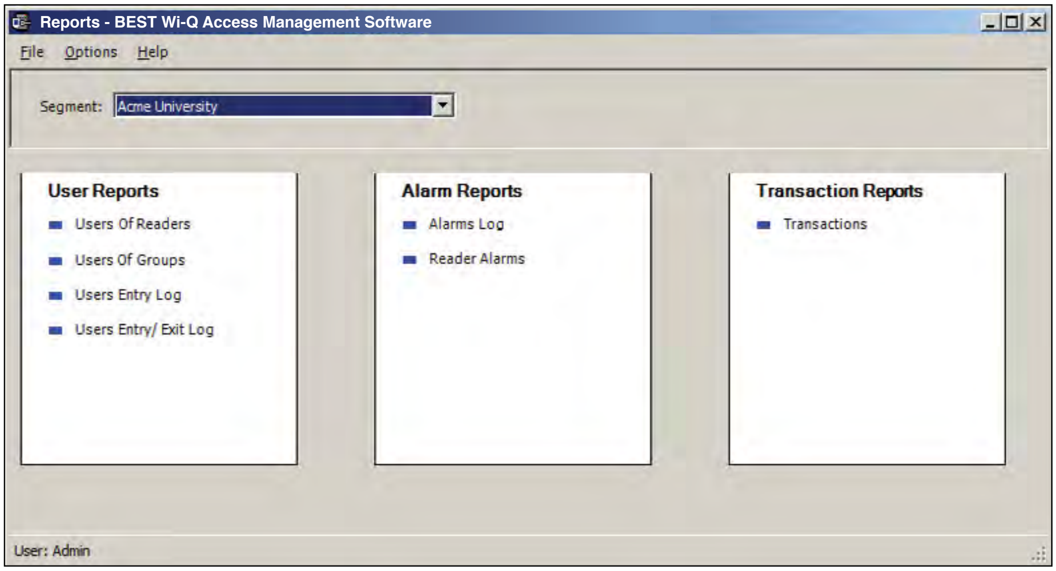
Creating Reports

The first step in creating reports in the software is to configure report settings. Here you can enter your company name and include a picture or logo that will be included in any files exported or printed from the application. Once you have configured your report settings you are ready to choose a report type and generate the report. From there you can print the report, or export the report to any number of file formats such as .doc, .rtf, .rpt, etc.

To get started, launch Reports from the Configurator main menu.

Once you enter your login and password, the Reports main screen opens.

Figure 165 Reports



Reports - BEST Wi-Q Access Management Software

Segment: Acme University

User: Admin

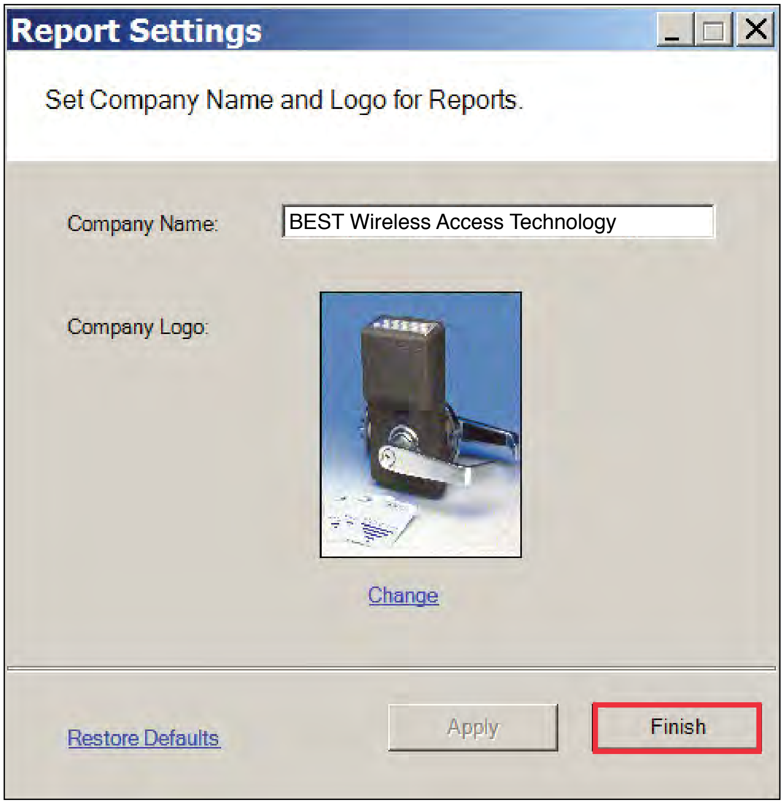
Configure Report Settings

You can include your company or organization name and logo with any report. Wi-Q AMS supports both .bmp and .jpg image formats. Perform the following steps:

1 In the Segment box, select the Segment for which you wish to create the setting.

2 Select Options>Report Settings. The Set Company Name and Logo for Reports dialog box opens.

Figure 166 Setting up a company name for a report



Set Company Name and Logo for Reports.

Company Name: BEST Wireless Access Technology

3 In the Company Name field, type in the company name you wish to appear on your reports.

4 Under Company logo, click the Change link. Use the Select Logo browser to navigate to the file you wish to include.

5 Click Open. The file is now uploaded to the Reports settings.

6 Click Finish to save your settings and begin working with Reports.

Generating a Report

This section presents steps to create some example reports. Once you are familiar with the basic operations, you will be able to create your own reports using the selections available in Reports. First we'll look at a Users of Readers report with All Users selected. Then we'll look at a filtered report using the options under the Report Settings categories.

Note The Reports application won't show much data until you have configured your system added Users and User Groups, and begun collecting transactions. Once this occurs, you can experiment with the options to get the reports that will be most significant for your operation.

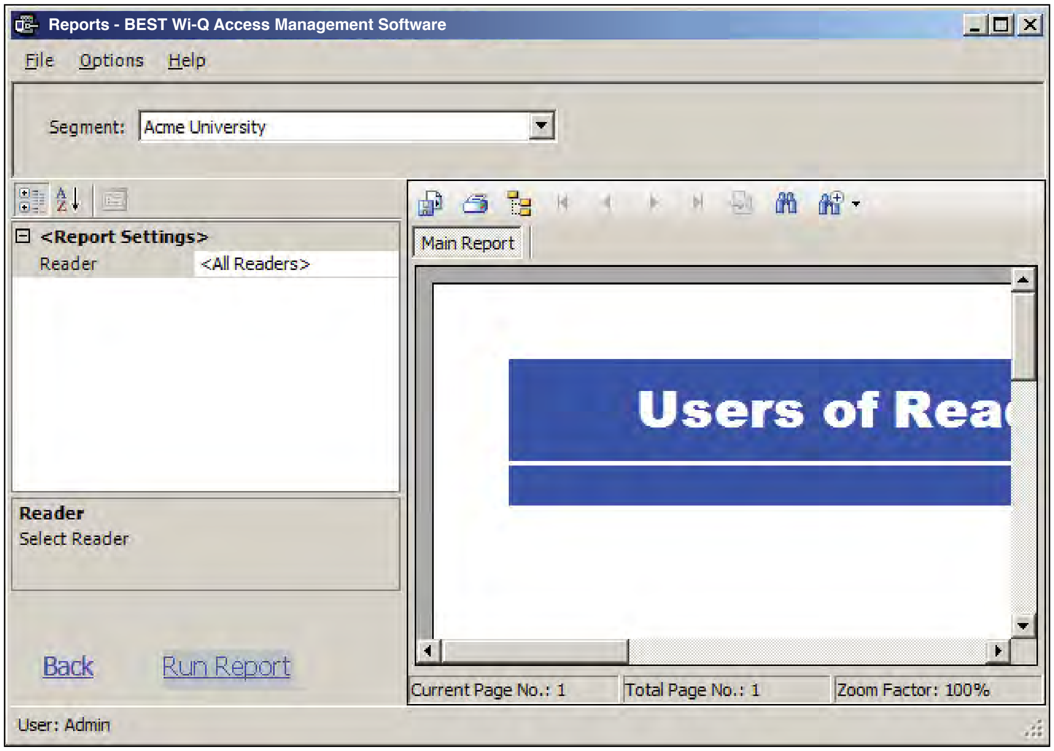
To Generate a Report

1 In the Reports main screen, under the User Reports box, click on Users of Readers. Reports opens at the basic users of Readers Reports generator.

2 In the Segment box, select the Segment you wish to report on.

3 Available report settings are listed on the left, and the results are shown on the right. For this particular report, the default will be <All Readers>.

Figure 167 Viewing System Reports



Reports - BEST Wi-Q Access Management Software

Segment: Acme University

<Report Settings>

Reader <All Readers>

Reader

Select Reader

Current Page No.: 1

Total Page No.: 1

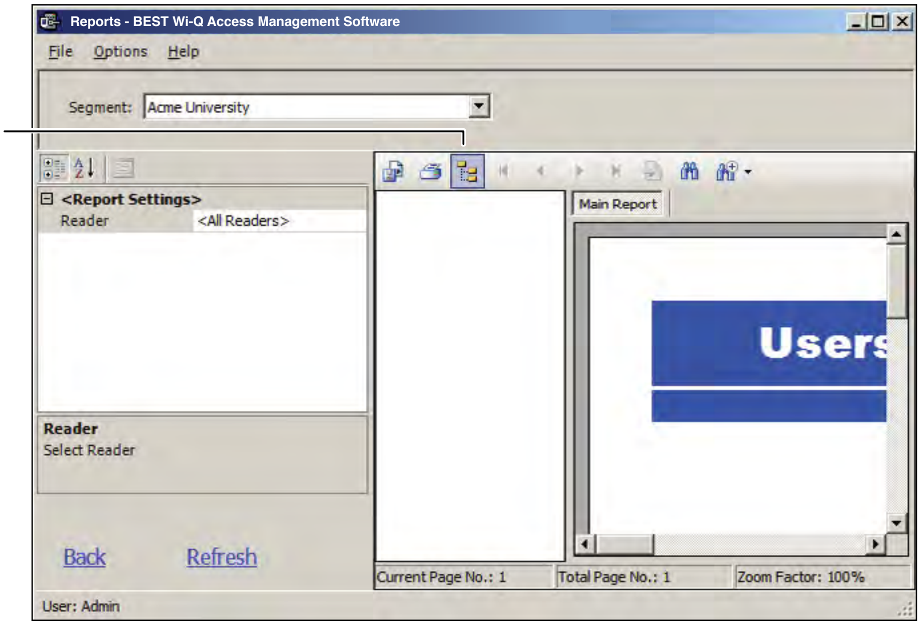
Zoom Factor: 100%

User: Admin

4 Use the scroll bars to view the data, use menu icons to export, print, scroll through multi-paged reports, or use the Zoom tools to get a closer look.

5 If you have a large number of readers, Click the Toggle Group Tree icon and highlight a specific reader to jump to its section in the report.

Figure 168 Toggle Group



Segment: Acme University

<Report Settings>

Reader <All Readers>

Reader
Select Reader

Current Page No.: 1 Total Page No.: 1 Zoom Factor: 100%

User: Admin

6 Click Run Report (bottom left of screen) to return to the Report Generator screen.

Generating Filtered Reports

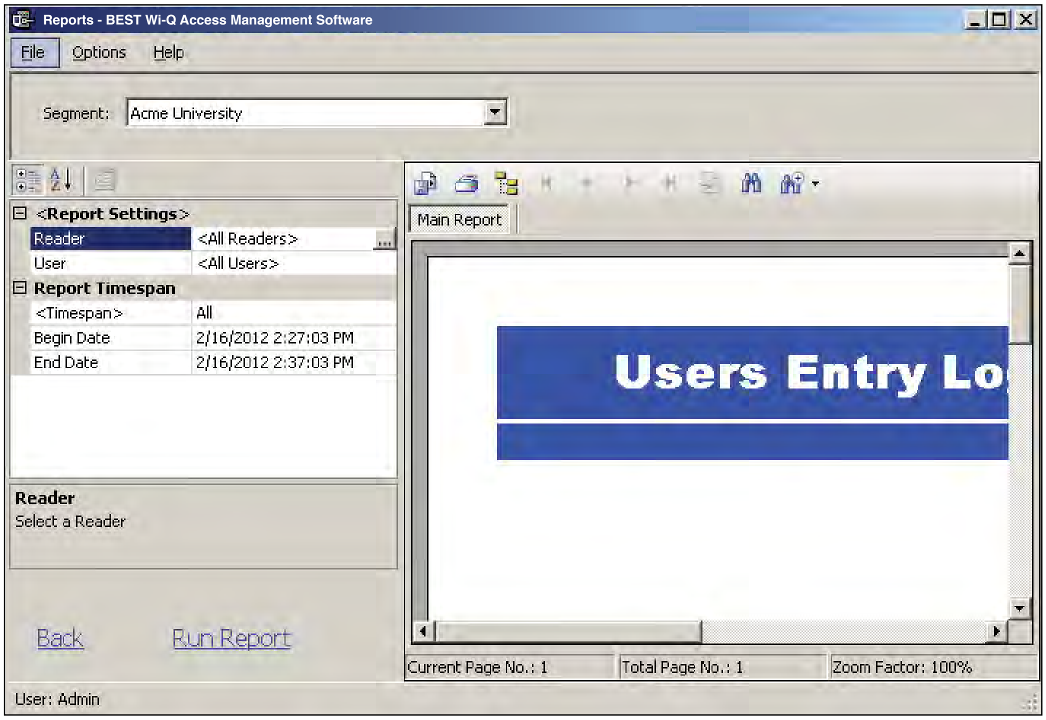
The report generator defaults to print all records. For example, when you select the Users of Readers report, report content displays users of all readers in the system. You can filter the report to display the users of only one specific reader, as in the following example.

To create filtered report

1 In the Reports main screen, select the Segment you wish to report on.

2 Under the User Reports box, click on Users Entry Log. The report opens. In this report set up, more selections are available for this report than for the Users of Readers report, including Reader, User, and Report Timespans. You can use any or all of these selections to filter your report. Each report type will have different selections available depending on the data available for the report. The defaults are always All.

Figure 169 Users of Readers Report



Segment: Acme University

<Report Settings>	
Reader	<All Readers>
User	<All Users>
Report Timespan	
<Timespan>	All
Begin Date	2/16/2012 2:27:03 PM
End Date	2/16/2012 2:37:03 PM

Reader
Select a Reader

Current Page No.: 1 Total Page No.: 1 Zoom Factor: 100%

User: Admin

3 To select a specific reader for this report, click on the Reader field's ellipsis button. The Select Reader dialog box opens.

4 Clear the All Readers box just below the drop-down list box.

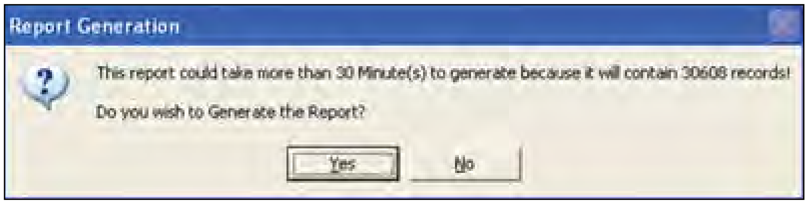
5 Select the reader to filter from the drop-down list.

6 Click Finish. The report results will display data for only the reader you selected.

Generating Larger Reports

The more records you include in your report, the longer the report will take to generate. During report generation, you can use other AMS applications; however, you can generate only one report at a time in the Reports application. If you define a report that will take more than 30 minutes to generate based on the records included, the software will present the following message:

Figure 170 Report Generation



This report could take more than 30 Minute(s) to generate because it will contain 30608 records!

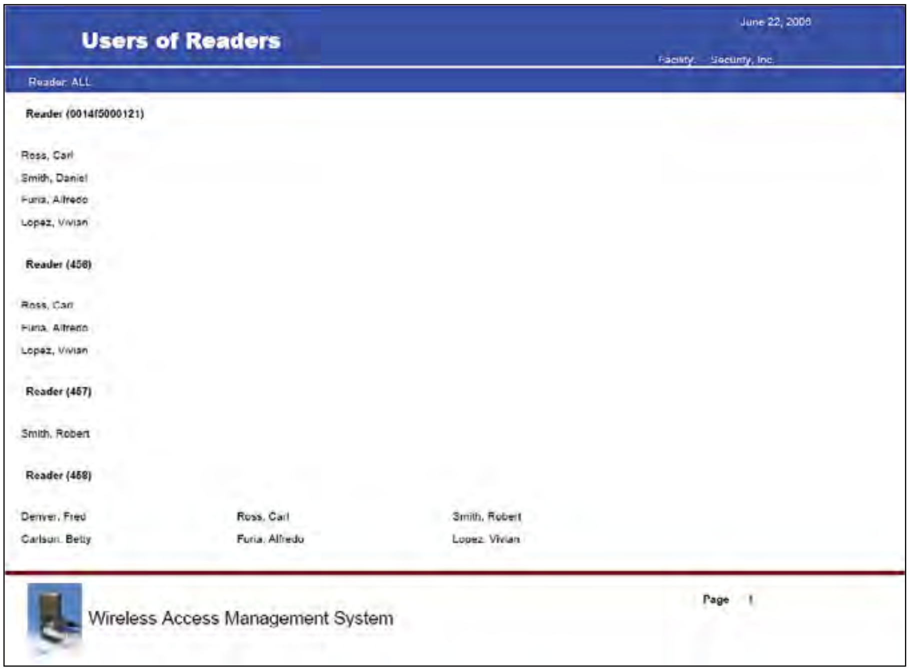
Do you wish to Generate the Report?

In the example, AMS detected that the defined report contains over 30,000 records and will take more than 30 minutes to generate. If this is acceptable, simply select Yes and the report will be generated. Select No if this is an inconvenient time to generate the report, or review your report definitions to see if you can further filter the report and still get the information you need. When you select Yes, the report begins to generate and AMS displays the Elapsed Time as the report runs.

Printing and Exporting Reports

Once you are satisfied with your report, you can print to a local or networked printer, or export the report in several formats. Your results will be determined by the options you select and how you wish to use the data. For example if you export to a Microsoft Excel file, you may get a different formatting result than if you export to an Adobe Acrobat file or print directly from AMS. However, you may wish to export to an Excel file and use the data in another format. The following example was printed from an Adobe Acrobat .pdf file exported from Reports. It retains all the formatting as displayed in Reports.

Figure 171 Sample report file



June 22, 2006

Users of Readers

Facility: Security, Inc.

Reader: ALL

Reader (0014f5000121)

Ross, Carl
Smith, Daniel
Furia, Alfredo
Lopez, Vivian

Reader (456)

Ross, Carl
Furia, Alfredo
Lopez, Vivian

Reader (457)

Smith, Robert

Reader (458)

Denver, Fred
Carlson, Betty
Ross, Carl
Furia, Alfredo
Smith, Robert
Lopez, Vivian

Wireless Access Management System

Page 1

To print a report

1 Create the report using the features described in the previous sections.

2 Click the Printer icon in the menu bar.

3 Navigate to the printer you wish to use.

4 Print using the appropriate actions for the chosen printer.

To export a report

1 Create the report using the features described in the previous sections.

2 In the menu bar, click the Export Report option.

3 In the Export Report dialog box, select a format type from the drop-down list. The available types are:

- Crystal Reports (*.rpt)
- Adobe Acrobat (*.pdf)
- Microsoft Excel (*.xls)
- Microsoft Excel Data Only (*.xls)
- Microsoft Word (*.doc)
- Rich Test Format (*.rtf)

4 Navigate to the location you wish to export to.

5 Enter a filename for the file.

6 Click Save.

Now you can use the report in any manner you wish, depending on the format exported.

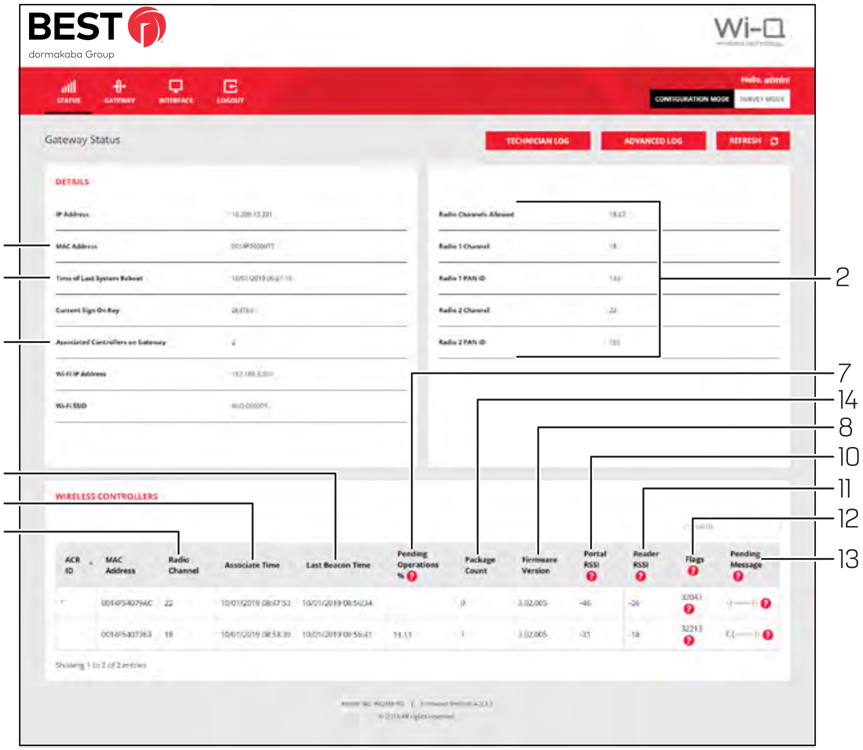
7 Wi-Q Gateway Web User Interface

This section provides an overview on the Wi-Q Gateway status webpage. You can access the status webpage for a specific Wi-Q Gateway by typing your desired Wi-Q gateway's IP address directly into your web browser. You will have to log into the Wi-Q gateway web page to get to the STATUS page.

- Inside the Portal Configuration Module, locate the desired Portal in the list and click on its hyperlink. See Figure 45.
- Type your desired Wi-Q Gateway's IP address directly into your internet browser.

Your browser will display the status of your Wi-Q Gateway and associated devices. See Figure 172.

Figure 172 Wi-Q Gateway Status Webpage



Gateway Status

DETAILS

IP Address	10.200.12.221
MAC Address	0014F5000075
Time of Last System Reboot	10/01/2019 06:47:16
Current Sign On Key	263761
Associated Controllers on Gateway	2
Wi-Fi IP Address	192.168.2.200
Wi-Fi SSID	WiQ-000075

Radio Channels Allowed	18,22
Radio 1 Channel	18
Radio 1 PAN ID	142
Radio 2 Channel	22
Radio 2 PAN ID	155

WIRELESS CONTROLLERS

ACR ID	MAC Address	Radio Channel	Associate Time	Last Beacon Time	Pending Operations %	Package Count	Firmware Version	Portal RSSI	Reader RSSI	Flags	Pending Message
[illegible]	0014F54079AC	22	10/01/2019 08:47:53	10/01/2019 08:54:34		0	3.02.005	-46	-26	32043	-|-----|-
	0014F5407363	18	10/01/2019 08:53:39	10/01/2019 08:56:41	11.11	1	3.02.005	-31	-18	32213	C|-----|-

Showing 1 to 2 of 2 entries

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

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

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

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

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

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

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

6. **Last Beacon Time**

   Column shows the time of the last Controller beacon.

7. **Pending Operations %**

   Column shows progress percentage of pending operations.

8. **Firmware Version**

   Column shows the firmware version number of associated Controller.

9. **Radio Channel**

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

10. **Portal RSSI**

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

11. **Reader RSSI**

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

12. **FLAGS**

    Column shows the current operational status of the associated device.

13. **Pending Message**

    Column shows the abbreviation of the message currently in operation.

14. **Package Count**

    Displays the number of packets being sent to the controller.

Status Flags in the FLAGS Column

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

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

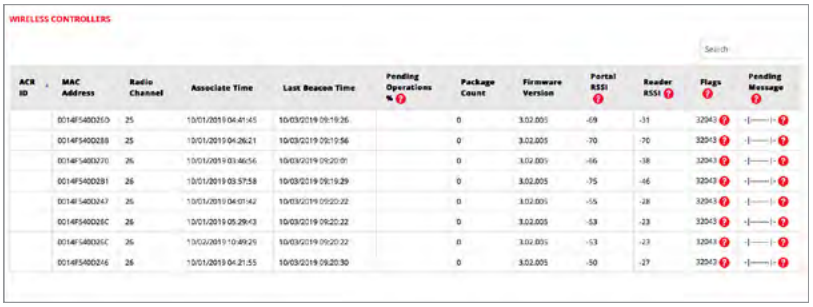
Table 1. Example Chart

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

Update Flags in the PEND Column

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

Figure 173 Wi-Q Controllers



WIRELESS CONTROLLERS

Search

ACR ID	MAC Address	Radio Channel	Associate Time	Last Beacon Time	Pending Operations % ?	Package Count	Firmware Version	Portal RSSI ?	Reader RSSI ?	Flags ?	Pending Message ?
	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 ?	-|——|- ?
	0014F540D28C	26	10/01/2019 05:29:43	10/03/2019 09:20:22		0	3.02.005	-53	-23	32043 ?	-|——|- ?
	0014F540D26C	26	10/02/2019 10:49:29	10/03/2019 09:20:22		0	3.02.005	-53	-23	32043 ?	-|——|- ?
	0014F540D246	26	10/01/2019 04:21:55	10/03/2019 09:20:30		0	3.02.005	-50	-27	32043 ?	-|——|- ?

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

- **Flags** – The Flags indicate the device status. Common device statuses for Wi-Q Controllers when they are connected to a Gateway are below:

- **010001** – Controller initial connection to the Gateway.
- **30207** – Controller connected to the Gateway and is waiting for segment updates.
- **30063** – Controller has a deep reset command pending.
- **30017** – Controller waiting to be pulled into the segment and has not received segment updates.
- **30007** – Controller has received segment updates and is waiting in the "New Segment Items" folder in Wi-Q AMS Configuration software.
- **30043** – Controller is signed in to the ACS, connected, configured, and not locked to the Gateway.
- **30053** – Controller is taking configuration updates.
- **32043** – Controller is signed in to the ACS, connected, configured, and locked to the Gateway.
- **32243** – Controller is locked to Wi-Q Gateway but has not been added to an access level or a direct assignment to a User. No user credentials are assigned to the controller in the software.
- **38053** – Controller has a firmware update pending.
- **38043** – Controller is receiving a firmware update.
- **32207** – Controller completed the firmware update and is waiting for updates from the Wi-Q Gateway.

Pending Messages– The letters in the pending messages column are update messages that are being sent to the controller.

- **S** – Segment information (pin length, DST Times)
- **C** – Card formats
- **L** – Controller configuration (beacon time settings, channels, transaction masks, etc.)
- **U** – User credentials and properties
- **T** – Timezone intervals
- **I** – WAC I/O
- **F** – Firmware
- **P** – Ping (missing LIF data after association or updates)

A Glossary

100Base-T The most common Ethernet wiring standard.

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

access panel A circuit board with on-board memory that is responsible for making most of the decisions in an access control system.

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

antipassback A configuration limiting the ability of consecutive uses for a credential at a reader. Usually, configured with readers installed on both the secure and non-secure side of an opening. Once a credential has been used in a reader to gain access on one side of the opening, the credential cannot be used in the same reader until the credential is used to gain access to a reader from the opposite side of the opening.

APB exempt Antipassback exempt. The cardholder with this privilege is exempt from antipassback rules.

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

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

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

cardholder An individual who is issued a particular credential.

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

common door A configuration setting that allows for the allocation of duplicate badge ID ranges in separate offline locks.

communication port The connector on the bottom of a Lock that allows the lock to be connected to a reader.

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

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

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

deadbolt override The ability for an authorized credential to retract both the spring latch and the deadbolt when the deadbolt is engaged

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

dual access The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening.

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

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

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

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

Host The computer on which Wi-Q AMS software is installed and set up to manage Wi-Q Gateways and readers on the network.

IP address The numeric address (like 192.168.1.1) that identifies each device in a TCP/IP network.

input A hardware connection point used for status reporting of a particular sensor.

intelligent system controller (ISC) ***See access panel.***

I/O device A device, such as an alarm or parking gate that can be configured to operate on the network using a Wireless Access Controller.

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

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

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

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

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

passage mode The ability to double present an authorized credential within the strike time to unlock an opening. The lock is returned to its original status by a second, double presentation of an authorized credential.

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

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

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

sign-on key Number generated within AMS to establish the connection between the readers and the Portals, and ultimately to a segment in the software.

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

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

time zone A defined range of time for assignment to various access control activities. A time zone may be applied to a reader or readers when creating an access level, to a reader to change the mode of operation, to a relay to activate and deactivate, to an input to mask and unmask, and a host of other operations.

unlock duration The time that the lock momentarily unlocks.

use limit A configuration limiting a credential to a defined number of uses.

Web Interface The software program that allows setup and communication between the Wi-Q Gateway and the Host Computer.

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

Wireless Access Controller Wireless Access Controller provides additional capability to connect stand-alone controllers and locks.

wireless reader lock The wireless reader lock controls user access at the door and grants user requests according to how they are configured in the software.