BEST

dormakaba Group

Wi-Q

wireless technology

WI-Q™ C-CURE

USER GUIDE

Wireless Intelligence That Stands Alone

Credits/Copyright

Written and designed at dormakaba USA Inc.
6161 East 75th Street
Indianapolis, IN 46250

A85299_C June 2020

FCC Certification

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

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.
Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

THIS DEVICE COMPLIES WITH INDUSTRY CANADA LICENCE-EXEMPT RSS STANDARD(S).
Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) this device must accept any interference, including any interference that may cause undesired operation of the device. This Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

CET APPAREIL EST CONFORME À LA NORME RSS INDUSTRIE CANADA EXEMPT DE LICENCE.
Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas provoquer d'interférences et (2) cet appareil doit accepter toute interférence, y compris les interferences pouvant causer un mauvais fonctionnement du dispositif. This Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations. Cet appareil numérique de la classe [B] respecte toutes les exigences du Réglement sur le matériel brouilleur du Canada.

Approved Antennas

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

WARNING: Changes or modifications not expressly approved by dormakaba could void the user's authority to operate the equipment. Approved antennas are listed below and antennas not included in this list are strictly prohibited for use with these devices.

UL Evaluation

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

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

- Wiring methods used shall be in accordance with the National Electrical Code, ANSF/NFPA70.
- UL evaluated with standard antennas.

For UL installations using PoE, the following must be observed:

- Compliance with IEEE 802.3 (at or af) specifications was not verified as part of UL 294.
- Locations and wiring methods which shall be in accordance with the National Electrical Code, ANSI/NFPA 70.
- This product is not intended for outside wiring as covered by Article 800 in the National Electrical Code, NFPA 70.
- Category 5e cabling is the minimum performance category recommended.
- The minimum conductor gauge permitted to connect between the PSE or power injector and the PD shall be 26 AWG (0.13 mm2) for patch cords, 24 AWG (0.21 mm2) for horizontal or riser cable.
- Connected through standard eight-pin RJ-45 connectors.
- Evaluated for Mode B only.
- PoE power is to be supplied by an Access Control System Unit (ALVY), Class 2 power limited, PoE injector (PSE) providing 44-52VDC and 15W for maximum output.

Table of Contents

1
Overview

This manual is your guide to the integration of dormakaba (BEST Access Systems) Wi-Q wireless hardware into your Software House C·CURE 9000 Access System.

The information in this guide is presented in a linear manner; however, tasks to install hardware and software and configure the system for the first time do not necessarily progress in a linear manner. You will find a Setup Checklist at the end of this section to take you through the initial setup and configuration tasks in a logical sequence.

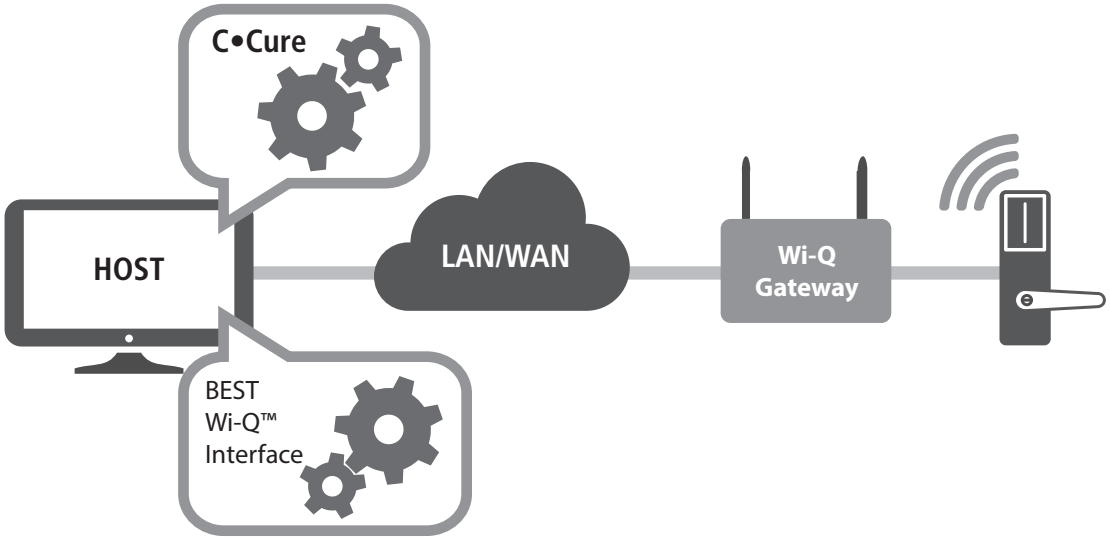
System Overview

A Software House C·CURE 9000 Access System with integrated Wi-Q Technology combines access control software with Wi-Q Gateways, Wireless Access Controllers, and multiple controller formats that work together to enable all decision making at the door. The Wi-Q system runs remotely with no need for hard wiring, providing innovative access control in any environment. The C·CURE Wi-Q Interface system is versatile, so you can create a whole new system, retrofit existing hardware, and include various video camera, alarms, and inputs/outputs.

Basic Wi-Q Components

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

Figure 1 Four Basic Components



1 C·CURE Server with C·CURE System Software

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

Note The C·CURE System Software must be installed and operational prior to the installation and operation of the Wi-Q Interface Software.

2 Wi-Q Router Service

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

3 **Wi-Q Gateway**

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

4 **Wireless Controller**

The Wireless Controller is equipped with Wi-Q Technology that controls user access at the door. The basic configuration is battery operated, with either keypad or card reading capability and an internal antenna that communicates with the Wi-Q Gateway. The Wireless Controller grants user requests according to how they are configured in the C·CURE 9000 Software.

Note The terms "Controller" and "Lock" are used synonymously throughout this guide. The C·CURE 9000 Software uses the term "Reader" and "Door" to refer to wireless locks, while the Wi-Q Interface Software uses the term "Controller."

Basic Operation

A user enters Sign-On Key/Credential at a Wireless Controller, either using an access card or by entering a code on a keypad. If the controller recognizes the credential from the configured settings downloaded from the Host via the Wi-Q Gateway to the controller, the door opens. The controller also sends regular signals 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

C·CURE 9000 Wi-Q Interface Software supports various system configurations. For example, some segments at your location may already be hard wired with legacy equipment or additional input or output devices. You can include a Wireless Access Controller that links a hard wired strike and controller with a Wi-Q Gateway. For more information about various applications you can adapt for use with Wi-Q, see "Hardware Overview" on page 11.

Software Overview

C·CURE 9000 provides powerful features to manage your system. The Wi-Q Interface Software allows you to add Wi-Q Gateways, Controllers and Segment Sign on Credentials to C·CURE 9000 system. The Wi-Q Interface Software also allows you to send firmware updates to your Wi-Q Gateways and wireless locks as they become available. Once your Wi-Q components are added into C·CURE 9000, you may manage your online and wireless systems together as one.

Setup Checklist

Wi-Q is set up in ten basic tasks. Completing these tasks will ensure you get your system up and running as quickly and efficiently as possible. Some tasks are performed at the Host computer or server and some at the site. It is appropriate to perform some tasks concurrently. For example, you may have someone prepare your computer and install the software concurrently with site plan development and hardware installation. However, you must have the software installed and Wi-Q Gateways 'online' before you can sign on controllers.

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

- Task 1: Develop a Site Plan
  See page 14.
- Task 2: Position Wi-Q Gateways
  See page 17.
- Task 3: Organize Segment Data
  See page 30.
- Task 4: Prepare your Computer
  See page 31.
- Task 5: Install C·Cure Wi-Q Interface Software
  See page 41.
- Task 6: Configuring the Hardware in C·CURE Wi-Q Interface Software
  See page 59.
- Task 7: Install Wi-Q Gateways
  See page 20.
- Task 8: Install Door Hardware
  See page 23.
- Task 9: Signing on Controllers
  See page 24.
- Task 10: Configuring the Software
  See page 79.

2
Hardware Installation

This chapter will guide you through performing the following tasks:

Task 1 — Develop a Site Plan

Task 2 — Position Wi-Q Gateways

Task 7 — Install Wi-Q Gateways

Task 8 — Install Door Hardware

Task 9 — Signing on Controllers

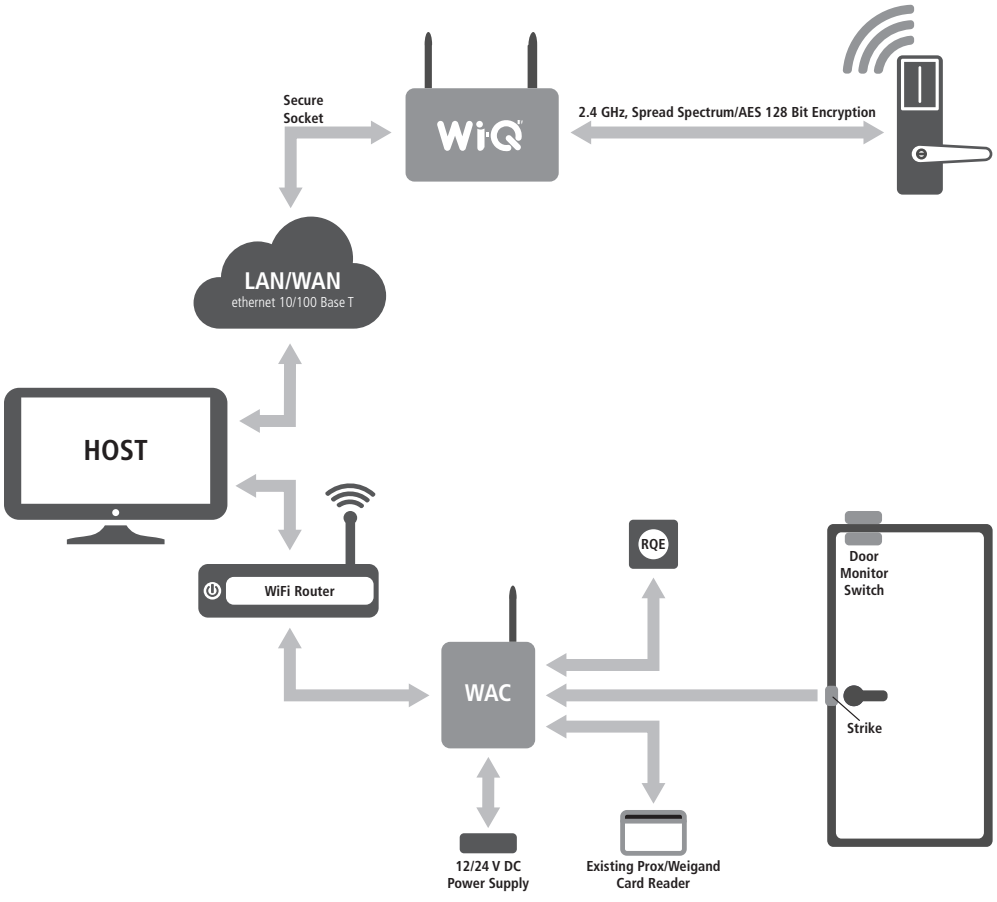
Hardware Overview

The Wi-Q Interface Software integrates wireless hardware into your existing hard-wired C·CURE 9000 system. Wi-Q is designed for versatility so you can retrofit existing Wi-Q Gateways and include various I/O devices.

Note Once Wi-Q Technology locks are installed, you will need to sign them on in the C·CURE 9000 Wi-Q Interface Software. Therefore, it is appropriate to install the Wi-Q Interface Software before or concurrent with hardware installation. For more information, see "Signing on Controllers (Task 9)" on page 24.

Below, figure 2 shows a block diagram with various configurations. Wi-Q Interface Software supports all Wi-Q Technology Wireless Controllers via Wi-Q Gateways (A); and existing Prox/Wiegand, RQE, door strike, and door monitor switch configurations via Wireless Access Controllers (WAC) (B). Configuration types are briefly described in the following paragraphs. Full installation instructions are provided in the following sections.

Figure 2 Example System Configurations



Wi-Q Gateways

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

Wi-Q Gateways provide bi-directional radio frequency communication between Wireless Controllers and the associated host computer(s). All communications are via secure AES 128-Bit encrypted 2.4 HGz using spread spectrum RF Radio technology. The Wi-Q Gateway communicates to the Host computer through web services via either Ethernet 10/100 BaseT or an approved commercial RF carrier-enabling a wireless solution end-to-end. Transmit range from Wi-Q Gateways will vary based on building construction. Directional antennas are also available to further extend range.

Wireless Controllers

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

- Card or Keypad ID with PINs
- Magnetic Stripe, Prox, MIFARE (card number only)
- 512 Timezones (per Segment)
- 14000 User Credentials per door (based on licensing)
- Cardholder access level definition
- Dynamic memory for IDs vs Transactions
- Locally stored and transmitted transactions
- ADA Compliant
- No AC required at door

Wireless Access Controllers

You can retrofit any existing controller configuration to communicate with Wi-Q Technology Wi-Q Gateways using Wi-Q Technology 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 12 VDC or an optional 12/24 VDC power supply, sealed, lead acid battery pack. They seamlessly integrate existing door hardware into the C·CURE 9000 system, supporting Wiegand- compatible keypad controller inputs.

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

Antenna Types and Applications

To optimize system performance, it is important to position Wi-Q Gateways to receive maximum signal strength from the Wireless Controllers. Once all door hardware has been installed, you will be ready to position Wi-Q Gateways using the Wi-Q Technology Site Survey Tool. Wi-Q Technology supports two antenna types: Omni-directional, designed to provide coverage in all directions; and Directional antennas that focus the signal from point-to-point over longer distances and through obstacles. For more information, see "Position Wi-Q Gateways (Task 2)" on page 17.

Installing System Hardware

A C·CURE 9000 system with integrated Wi-Q Technology can operate with Best 45HQ Mortise locks, Best 9KQ Cylindrical locks, Best EXQ Trim, Wireless Access Controllers and Wi-Q Technology Wi-Q Gateways. Detailed installation instructions are provided in the following sections and in the lock instructions provided with the hardware.

What you will need

- Engineering drawings or segment map
- Wi-Q Technology Site Survey Kit
- For keypad controllers, you will need the sign-on credential from the Wi-Q Interface Software.
- For magnetic stripe or proximity card readers, you will need the Temporary Operator Card (supplied with the controller) and Sign on Card (supplied in the Wi-Q Interface Software package). You will also need the appropriate magnetic stripe or proximity USB enrollment reader to create a proximity sign-on credential.
- Locks to be installed on doors, including cores and keys supplied with specific model
- Installation instructions for specific lock brand and model
- Wi-Q Gateways
- Access to standby power for 120 VAC non-switch circuit for 12 VDC plug-in transformer
- 10/100/1 GigE Base-T network connection
- Crossover Ethernet cable if direct connection between Wi-Q Gateway and Host will be used
- Wireless Access Controllers, if used, and knowledge of existing hardware and switches for any retrofit installations
- Installation tools
- Drill motor/hole saw with bits appropriate for the specific lock (see the template included with your lock)
- Phillips-head and flat-head screw drivers
- Access to the Host, a networked workstation, or wireless laptop computer

Develop a Site Plan (Task 1)

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

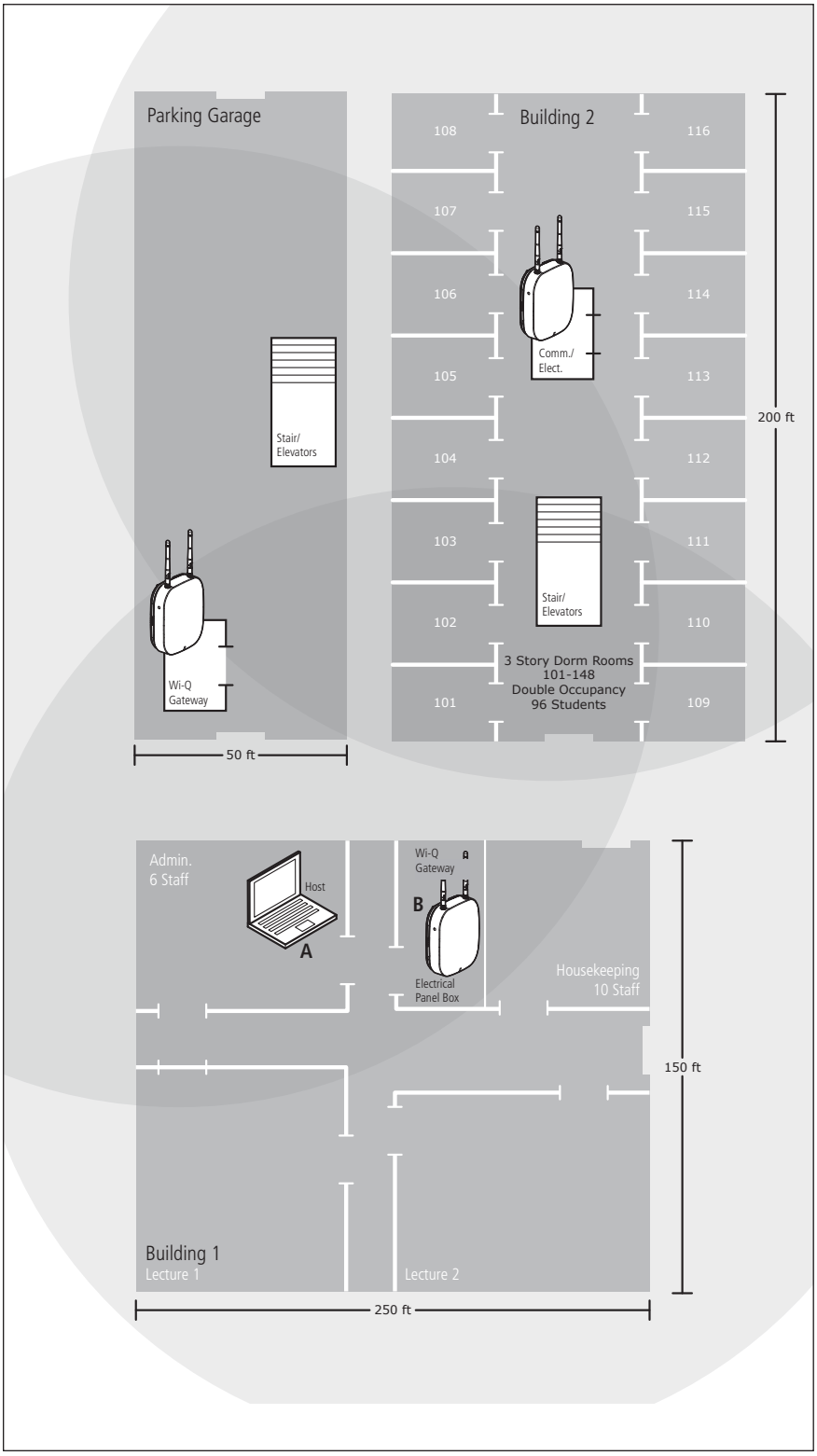
Transmit range from Wi-Q Gateway to controller varies based on building construction. Site characteristics such as reinforced concrete walls could interfere or weaken the signal; open spaces and low interference can increase signal strength.

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

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

The Parking Garage Wi-Q Gateway (D) is positioned to cover the pedestrian door near the dorm and the stairway and elevator doors. Its range also extends to the entrance of Buildings 1 and 2.

Figure 3 Sample Site Installation Plan



Plotting the Plan

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

Device Identification

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

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

When you move on to configure the Host computer, it is essential to have a list identifying each Controller and Wi-Q Gateway recognized by the system. We recommend creating a temporary label for each device that includes the MAC address, device name, location, capacity, and type of antenna so that installers on the site will have a reference for installing the correct device in a location.

Interference

Wi-Q Technology transfers information between devices in the form of data packets over the 2.4 GHz ISM band. This band frequency is very heavily used in many devices such as wireless computer networks and cordless phones, which increases the risk of lost packets, that is, packets that do not make it from a controller to a Wi-Q Gateway because of interference. Interference can also reduce controller battery life due to the constant re-broadcasting of packets and lost connections to the Wi-Q Gateways. To achieve maximum efficiency, this frequency range must be managed effectively. Therefore, the installer must know the positions and channels of all the 2.4 GHz wireless devices in the segment and ensure channels are assigned to each device so that there is minimum frequency overlap with adjacent or nearby devices.

Extended Range

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

Note Actual distances will vary based on building construction.

Position Wi-Q Gateways (Task 2)

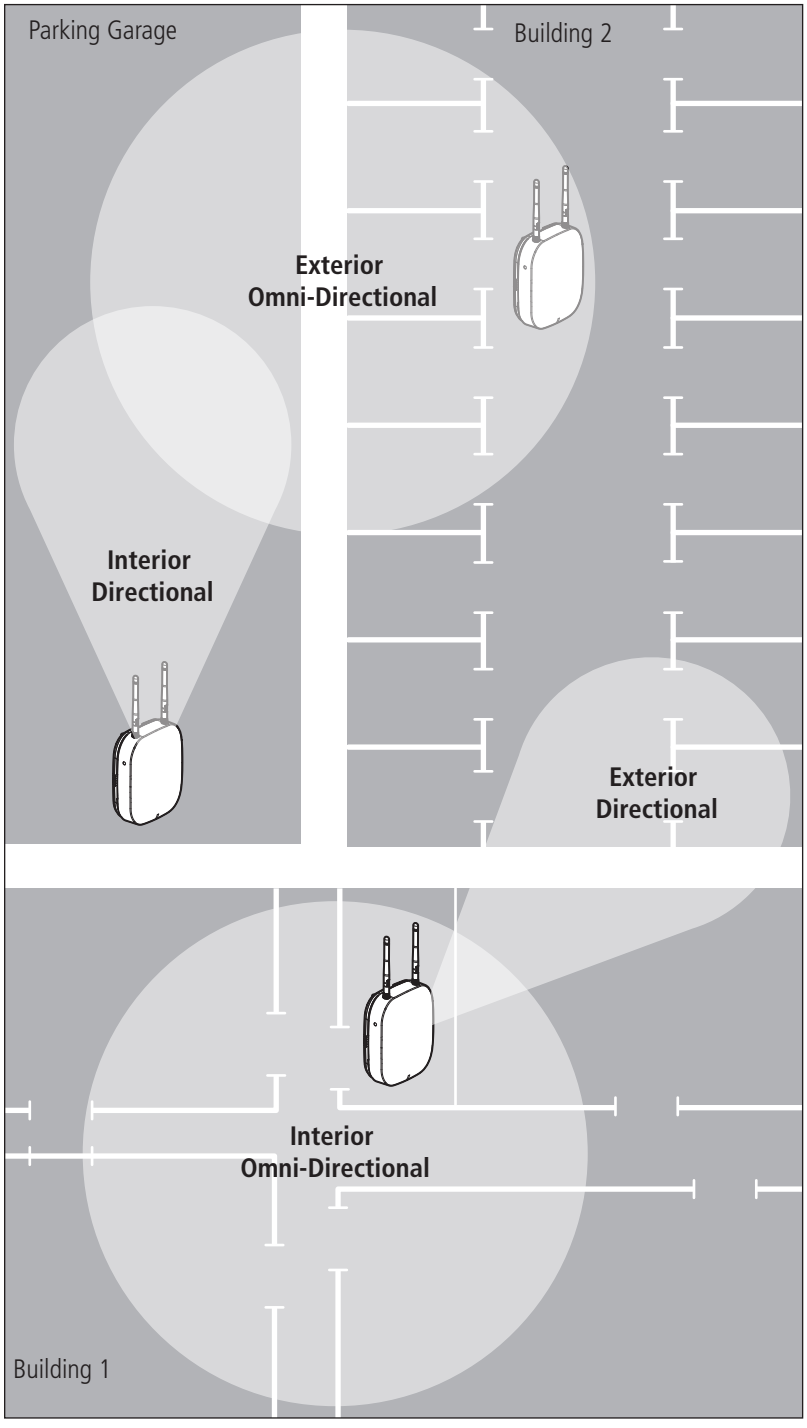
Once all door hardware and controllers have been installed, you are ready to determine the final placement of Wi-Q Gateways using the results from the Wi-Q Technology Site Survey Kit. The Site Survey Kit helps you determine the number and optimum location of Wi-Q Gateways and verify signal strength before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

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.

Antenna types

Wi-Q Technology supports two antenna types: Omni-directional, designed to provide coverage in all directions; and Directional antennas that focus the signal from point-to-point over longer distances and through obstacles. If you have trouble verifying signals, you may need to consider some antenna type options. Figure 4 shows the available antenna types.

Figure 4 Antenna Types



Power Supply

Wi-Q Gateways must be PoE powered or 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 10/100 Base T network connection
- Proximity to other I/O device(s) if used
- Placement within range of controllers

Note Transmit range will vary based on building construction.

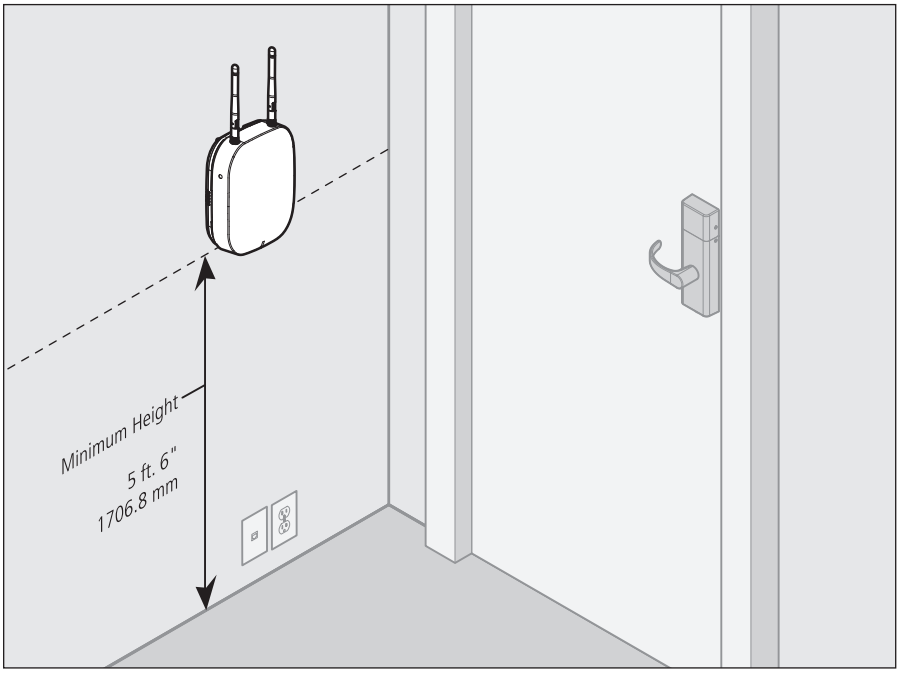
Next steps

When you are satisfied with signal performance, you can proceed to configure Wi-Q Gateways with the C·CURE 9000 Software. See "Configuring the Hardware in C·CURE Wi-Q Interface Software (Task 6)" on page 59.

Install Wi-Q Gateways (Task 7)

The most common installation site is inside an existing protected area such as a locked room or other secure enclosure, or above ceiling level. If you are installing inside a dealer-supplied locked enclosure, refer to the instructions provided with that equipment. Figure 5 shows a Wi-Q Gateway positioned in a protected area.

Figure 5 Installing a Wi-Q Gateway in a protected area

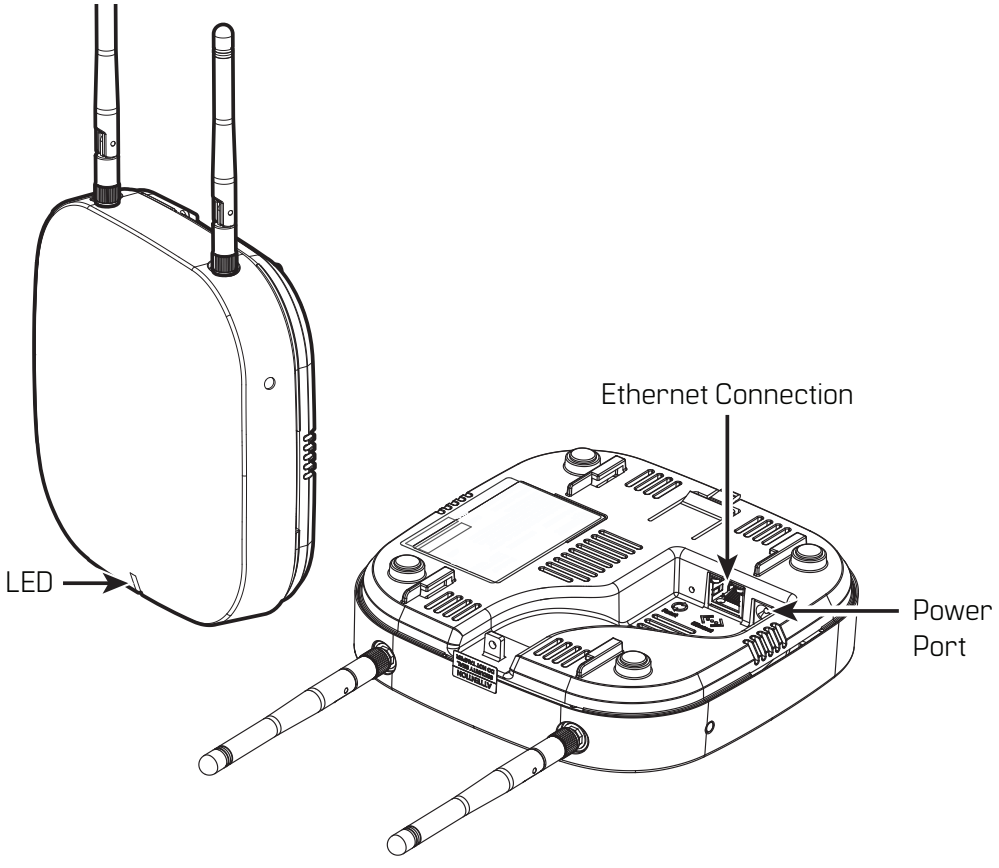


Connecting the Wi-Q Gateway and Verifying Operation

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

1. Connect the power supply to the Wi-Q Gateway and plug the transformer into a dedicated AC power supply (wall outlet). The Power Indicator light should come on. See Figure 6.
2. Insert the Ethernet cable into the Ethernet connection on the bottom of the Wi-Q Gateway. The Link Indicator light should come on. After about 30 seconds, the yellow activity indicator light will flash under normal operation.

Figure 6 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

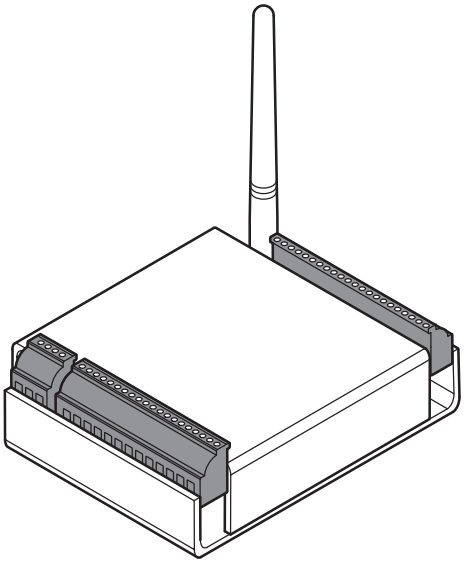
The Wi-Q Technology Wireless Access Controller (WAC) provides an optional way to retrofit an existing hard-wired application, or where the installed controller may be obsolete or unable to handle additional

controller inputs. It supports Wiegand-compatible keypad controllers and is configured and monitored in the C·CURE 9000 Software, just like a standard controller.

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

Using the Wireless Access Controller (Figure 7), 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 7 Wireless Access Controller



Installation

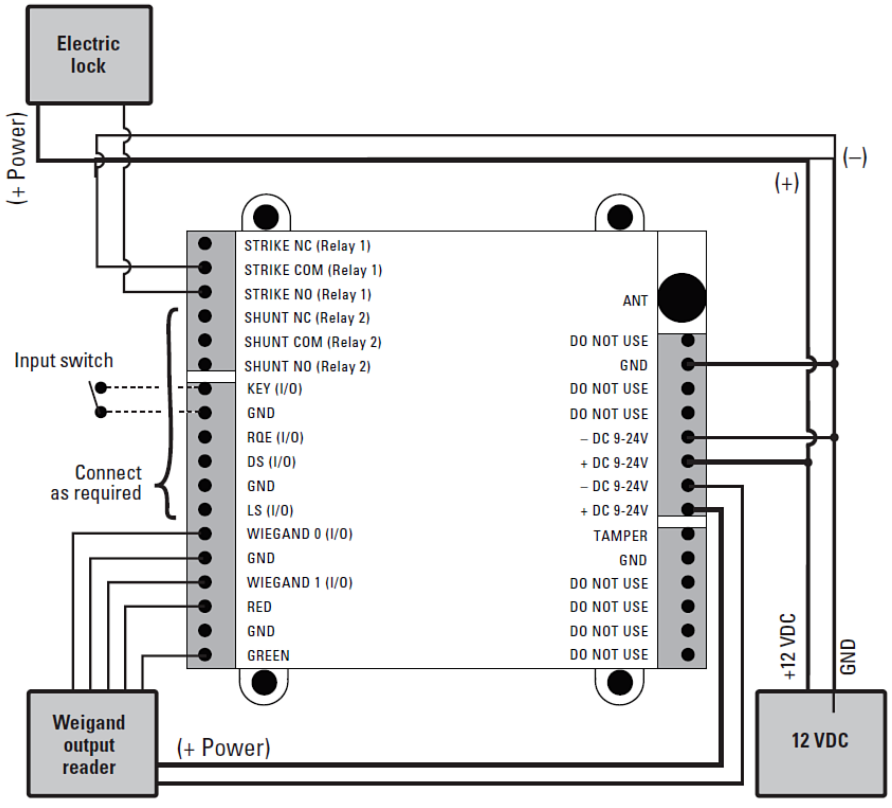
Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

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

Wireless Access Control Wiring

The Wireless Access Controller can be installed with its own 12 VDC power supply or slaved to the existing installation. Figure 8 is a wiring diagram illustrating both configurations. Dotted lines represent optional connections for the slaved configuration.

Figure 8 Connecting devices to a WAC



Once the WAC is installed and all points connected, it will be recognized by C·CURE 9000 Interface as a 'Controller' in the system. The WAC is configured in an almost identical manner as a Controller. For more information about configuring the WAC in the C·CURE 9000 Software, see www.swhouse.com.

Install Door Hardware (Task 8)

Complete instructions for installing locks are packaged with the hardware. You will also find instructions for dormakaba (BEST Access Systems) Wi-Q Technology Best 45HQ Mortise Locks, Best 9KQ Cylindrical Locks and Best EXQ Trim on
https://dhwsupport.dormakaba.com/hc/en-us.

Before You Begin

Before you begin, consider the following:

- Record device MAC address before installing device. You will need this when configuring the controller in the C·CURE 9000 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. Alkaline batteries cease to operate if they reach a temperature of -20°F.

- Wi-Q Technology controllers are designed for use on 1-3/4 inch doors. If you need to install on non-standard doors, contact dormakaba Customer Service for more information.
- Lock 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 lock for hand change instructions.
- If you are installing locks on unprepared (un-drilled) doors, use the template provided with your specific lock.

Check Controller Operation

Verify controller operation using the steps appropriate for your controller type (Magnetic Card or Keypad) in your hardware's installation instructions. If the system does not operate properly, please contact dormakaba Technical Support at 800-392-5209.

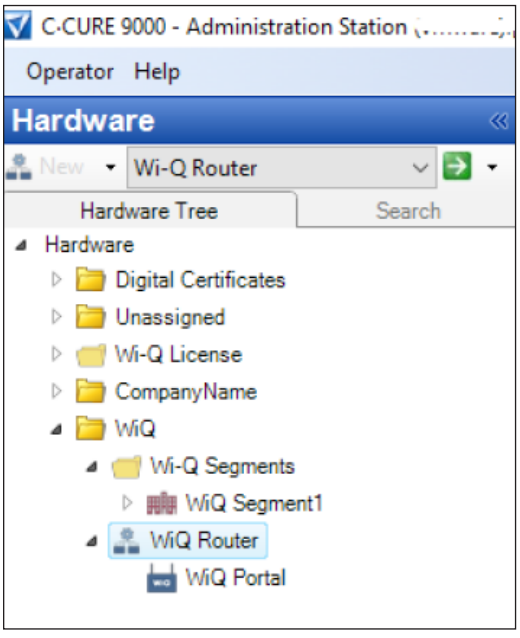
Signing on Controllers (Task 9)

When all hardware is installed and tested, you are ready to sign on your system controllers. To do this, the Wi-Q Interface Software must be installed on your Host computer. At a minimum, you will need to create a segment, router and a Wi-Q Gateway to the Hardware tree in your C·CURE 9000 Wi-Q environment before you can sign on the controllers. Once that is done you can return to the site and sign on the controllers. To complete controller sign on, you must perform steps at the Host and the controllers.

At the Host

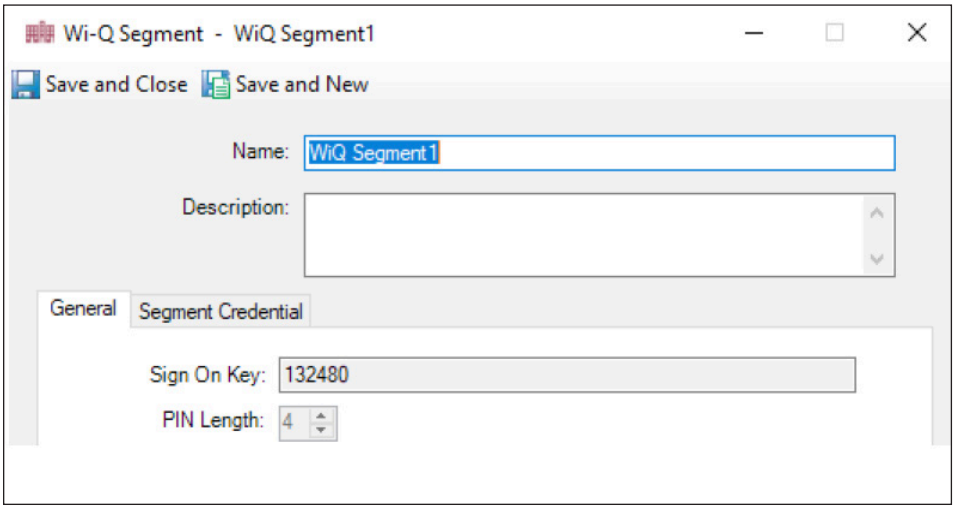
Once you have installed the C·CURE Wi-Q Interface Software and created a segment, a sign on key number is generated for that segment. You will need this number when you return to the site and sign on the controllers. To locate the sign on key number, select the segment to which the controller is to be assigned.

Figure 9 Select the Wi-Q Segment



1 Click on the Hardware bar in the left column to display the Hardware tree in the display panel if it is not already displayed. Expand the hardware folder (In this example it is named CompanyName), and the Segments folder, if needed, to see the available segments created. Double click the desired segment.

Figure 10 Locating the Segment Sign On Key



2 In the Wi-Q Segment dialog box that appears, select the general tab and note the Sign On Key number.

At the Controllers

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

Signing on Keypad Controllers

If your segment uses keypad controllers, use the following steps, in sequence, to register each controller in the segment. Once this is done, the controllers will appear in the C·CURE Hardware tree listed under their respective Wi-Q Gateways.

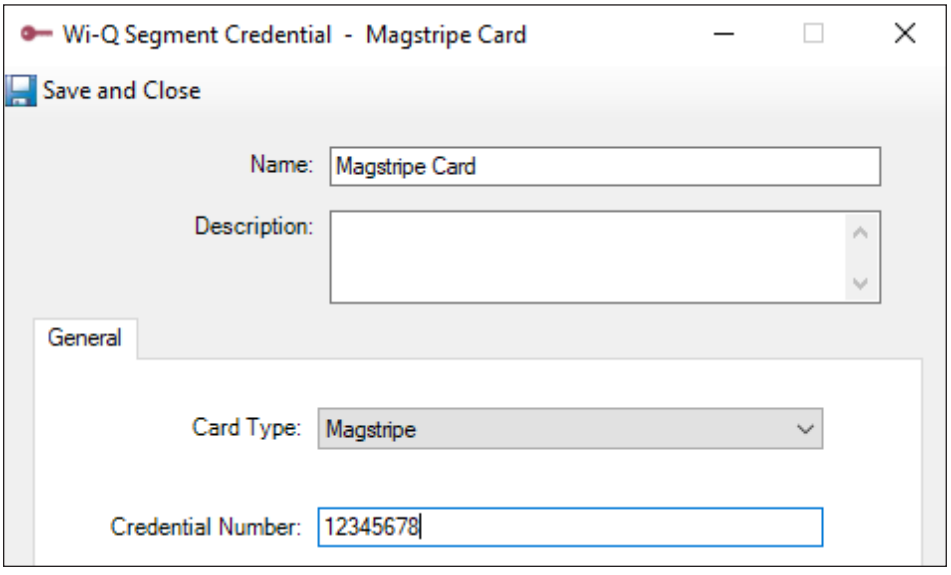
Note The following sequence is timed. Be sure to have your segment sign on key ready to enter at the appropriate time.

1. Have your six-digit segment sign on key number ready.
2. At a keypad controller, press the following number sequence on the keypad: 5678# (for a Wireless Door Controller) or just 5678 (without a "#" for a WAC). The green light will flash three times.
3. Within five or six seconds, begin to enter the six-digit segment sign on key number, followed by #. You will have about five seconds to enter each number. The sequence will time out if more than five seconds elapses between numbers.
4. Once the key number is completed, the controller begins to alternately flash green and red to signify that it is searching for Wi-Q Gateways in range. The blue light indicates that the controller is communicating with the Wi-Q Gateway. If the sequence was completed successfully, three green flashes, and/or an up beat tone, indicate the controller has accepted the sign on key.
5. If you see three red flashes, and/or a down beat tone, 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.

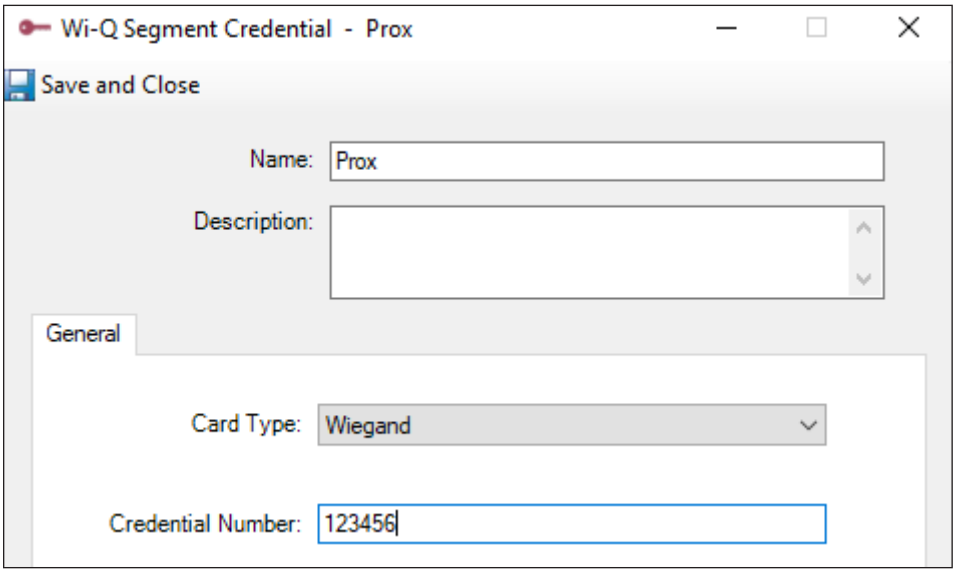
Steps to Add Segment/Sign on Credential

Figure 11 Magnetic Sign-on Credential



1 Click on the Hardware bar in the left column to display the Hardware tree in the display panel if it is not already displayed. Expand the hardware folder, and the Segments folder, if needed, to see the available segments created. Double click the desired segment.

Figure 12 Proximity Sign-on Credential



2 In the Wi-Q Segment dialog box that appears, select the Segment Credential tab and click on Add button.

3 a) Enter desired Name and Description.
b) Select "Wiegand/Magstripe" Card Type and Click Save and Close button.

Signing on Card Readers

If your segment uses card readers, either Magstripe or Prox, you may want to register one of your cards as a segment credential number, See "Selecting and Configuring a Card Format" on page 87. This card will be used to sign on card readers to the system. You can register a separate card and hold it specifically for this purpose, or register one that belongs to a user such as the Administrator's card. Once this is done, you will use the card to sign on each card reader in the system.

To do this, you would first use the temporary operator card that comes with the reader to enable programming of the reader and then use the sign-on credential card to sign on the reader to the segment.

Verify Signal Strength, Voltage and Packet Ratio

If you used the Wi-Q Gateway Site Survey Kit, you have already verified basic controller signal strength. Once the controllers are signed on and Journaling Statistics Messages are enabled in the controller configuration client, you can use the C·Cure Monitoring Station 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 C·CURE Monitoring Station application, see www.swhouse.com.

Replacing a Controller

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

1 Inside the C·CURE Software Tool, right-click on the Controller that must be replaced and delete it.

Note If the controller was online at the time of deletion, the controller will be sent a deep reset command and removed from the Wi-Q Gateway.

2 Remove and replace the Controller hardware.

3 Sign on the Controller. The configuration information should be set up.

3
Software Installation

This chapter will guide you through performing the following tasks:

Task 3 — Organize Segment Data

Task 4 — Prepare Your Computer

Task 5 — Install C·Cure Wi-Q Interface Software

Organize Segment Data (Task 3)

As the technical team works on planning and installing hardware using the Site Plan, a program administrator or other person responsible for the software side of program setup should be making plans to populate and configure the Wi-Q Interface Software into the C·CURE 9000 Software.

Device Information

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

User Information

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

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:

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

Start listing other considerations that may apply to your situation, such as:

- What User Groups will help you manage security?
- Do you have shift workers who are allowed on site only during certain days or hours?
- Will there be areas off limits to certain groups?
- Do some users need extra time to pass through a door, such as to accommodate a food cart or wheel chair?

Start thinking about these elements and begin organizing the data as soon as possible so you'll be ready when your equipment and software are ready. It is a good idea to use a spreadsheet software such as Microsoft® Excel® for this purpose. That way you can sort the data to help you plan your segment.

Importing Data

If you have an existing database that already contains some of the information you need, you may want to modify a version and import it into your C·CURE System using the program's System Administration feature. See www.swhouse.com for C·CURE 9000 instructions.

Prepare Your Computer (Task 4)

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

- Ensure that your system is equipped with an appropriate operating system, database and server. The Wi-Q Interface Software requirements are the sames as the C·CURE Software.
- Configure your Windows Firewall Ports.
- Obtain your Wi-Q Interface Software from dormakaba (BEST Access Systems).
- Stop your Communication Server (if required).
- Install your Wi-Q Interface Software.

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

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

Configure Windows Firewall Ports

Several ports must be enabled in your Windows Firewall settings to allow proper communication. You must add any configured Wi-Q Router Port to the Windows Firewall if it is different from the default 8000 port. See "Figure 48 The Router Dialog Box" on page 67. Also, add any configured Wi-Q Gateway: "Portal Service Port" and "Portal Config Service Port" to the Windows Firewall if they are different from the default 8000 and 11000 ports. See "Figure 50 Portal Dialog Box" on page 69. The following ports must also be enabled:

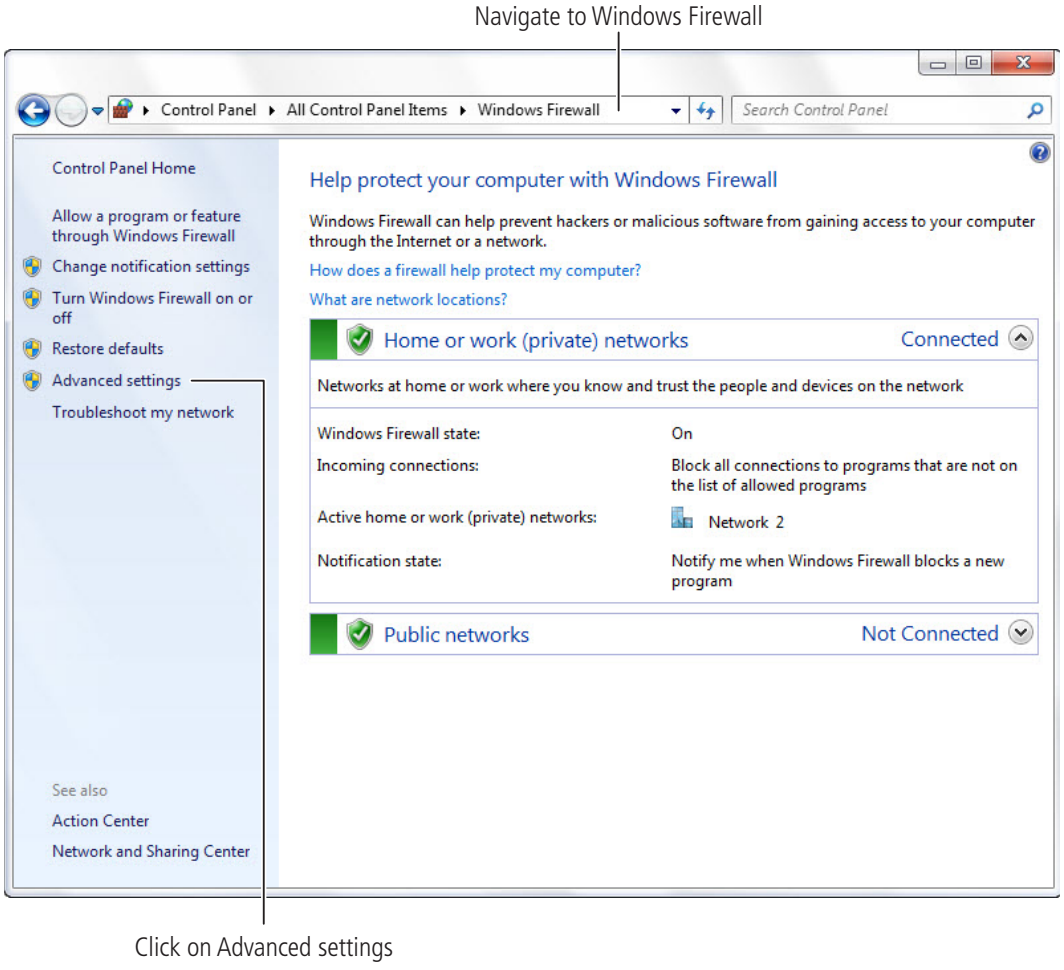
- Port 80
- Port 443
- Port 1433
- Port 1434
- Port 5353
- Port 8000 (default)
- Port 9000
- Port 9001

Note Additional ports will be needed as Routers are added.

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.

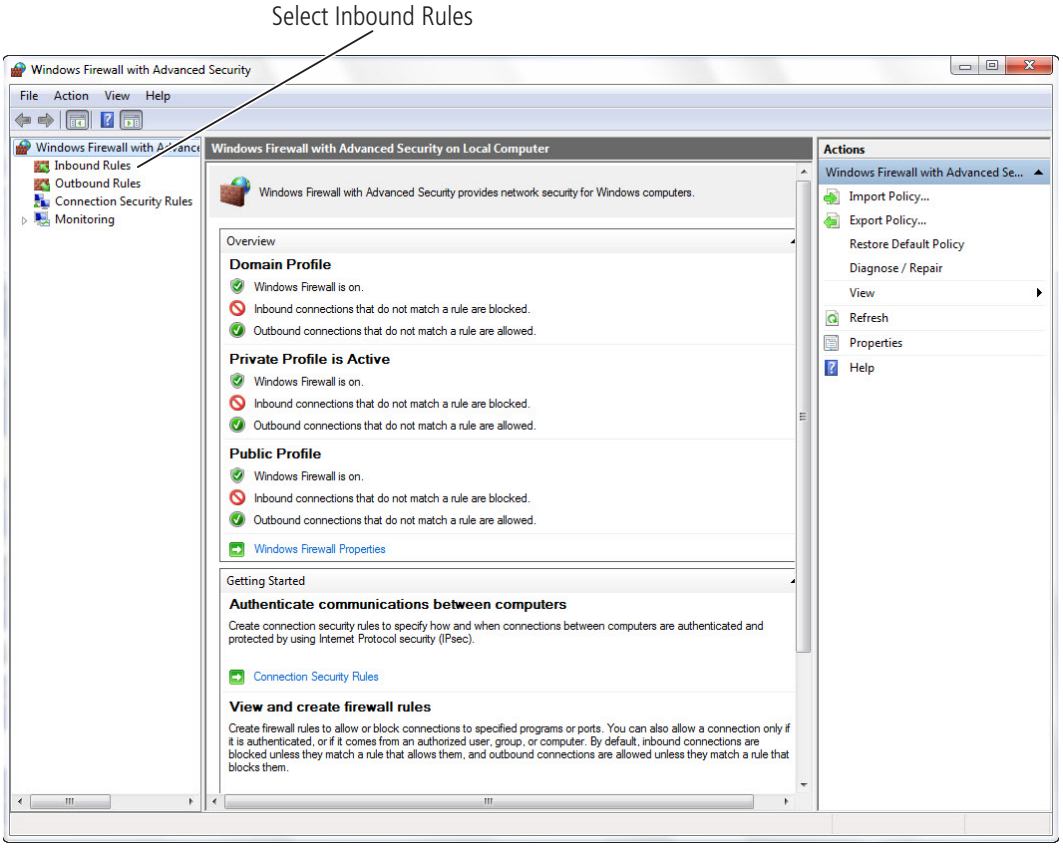
Note The screen shots below reflect a Windows 7 operating system. Navigating through the firewall settings in other editions of Windows will be slightly different.

Figure 13 Windows Firewall



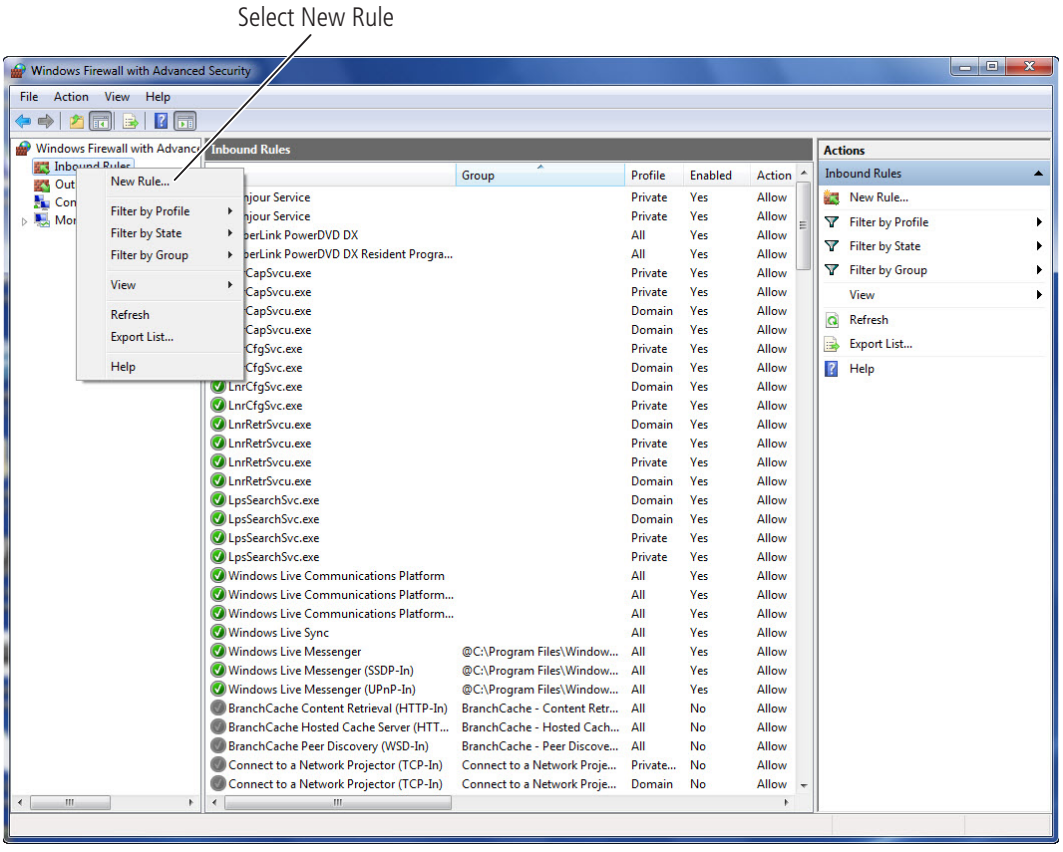
1 Navigate to your Windows Firewall settings from your PC's control panel. Then, click on Advanced settings.

Figure 14 Inbound Rules



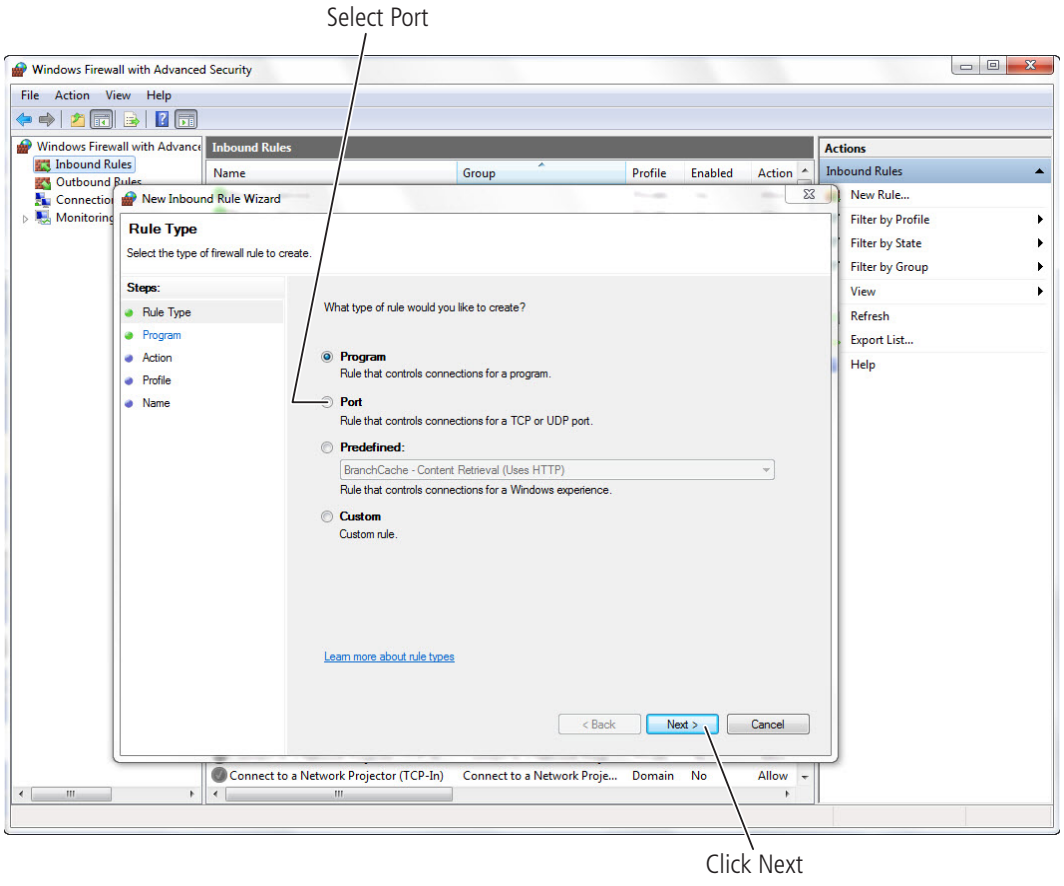
2 Select Inbound Rules.

Figure 15 New Rule



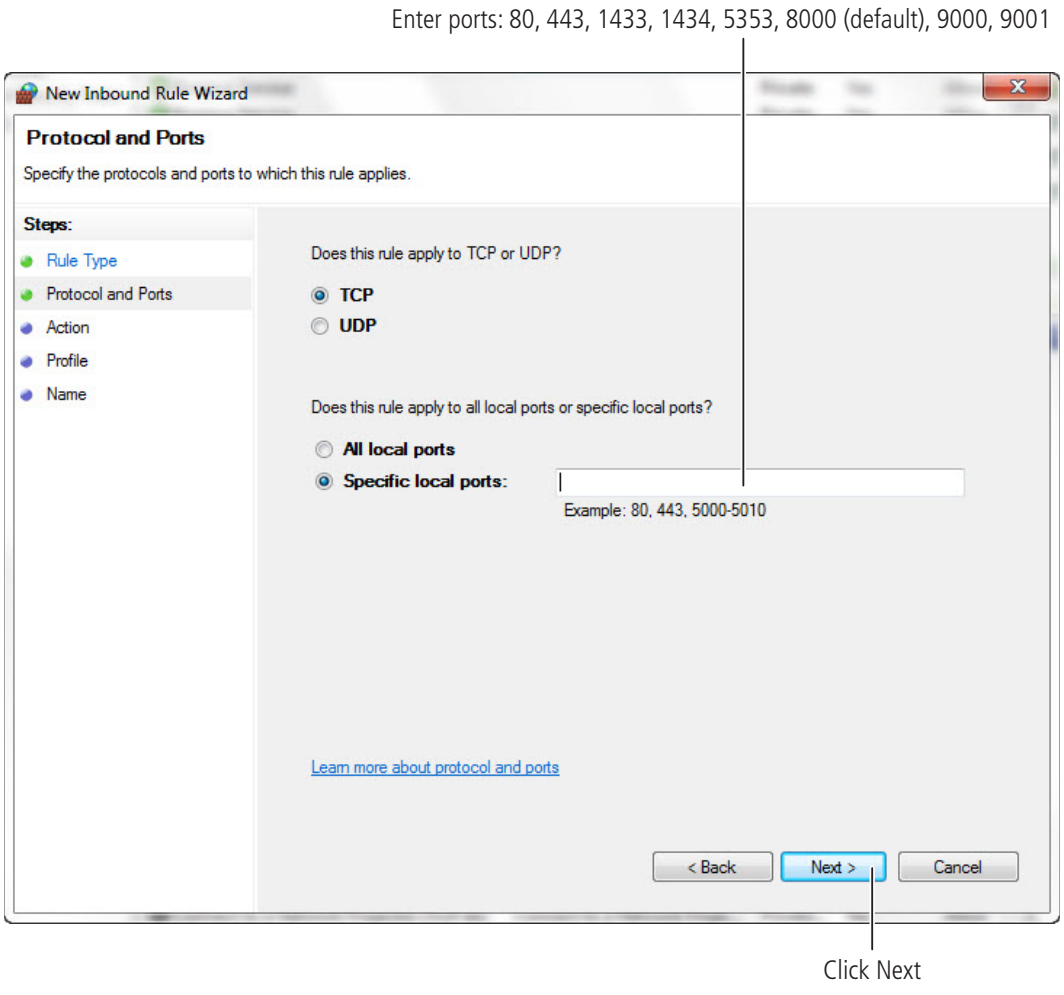
3 Right click on Inbound Rules to open an option menu. Select New Rule from the menu.

Figure 16 Create Port Rule



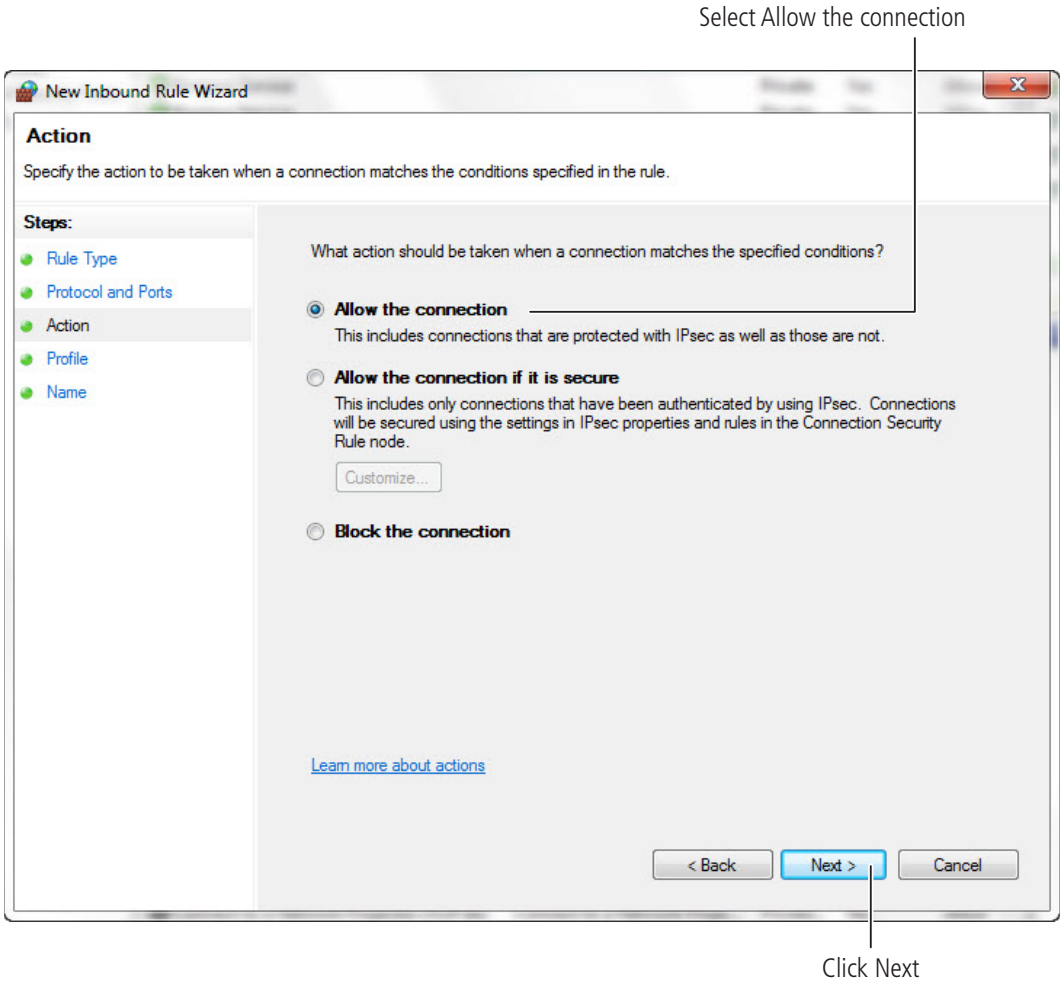
4 In the New Inbound Rule Wizard window, select Port. Click Next to continue.

Figure 17 Enter Ports



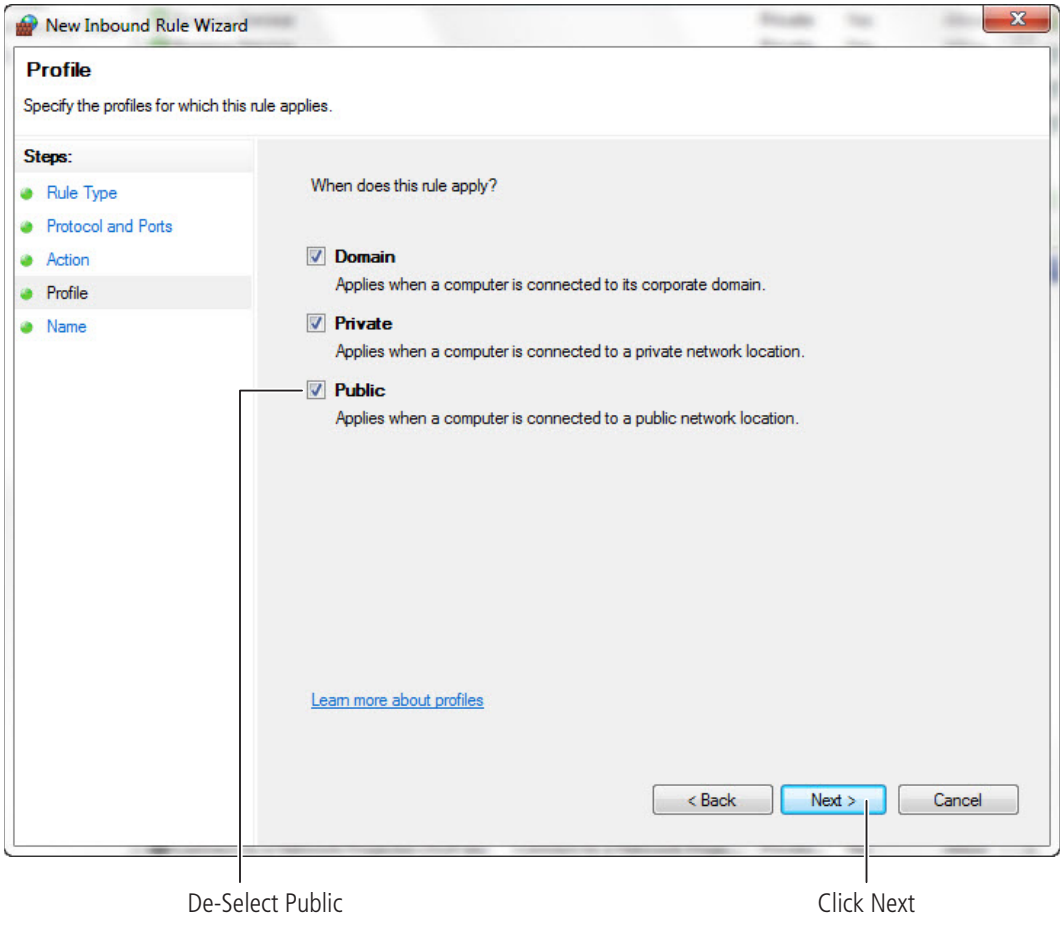
5 Enter the following ports into the "Specific local ports" field: 80, 443, 1433, 1434, 5353, 8000 (default), 9000, 9001. Then, click Next to continue.

Figure 18 Allow the Connection



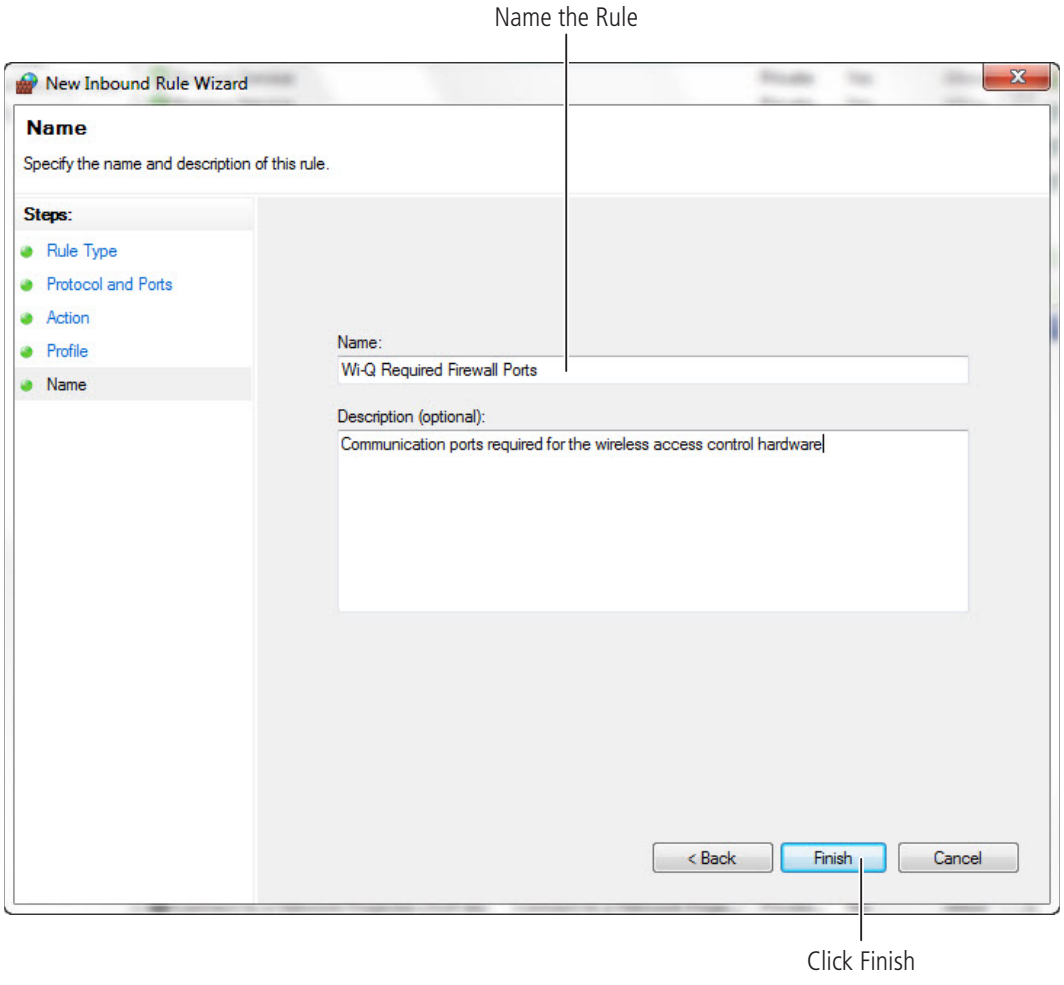
6 Select Allow the connection. Click Next to continue.

Figure 19 De-select Public



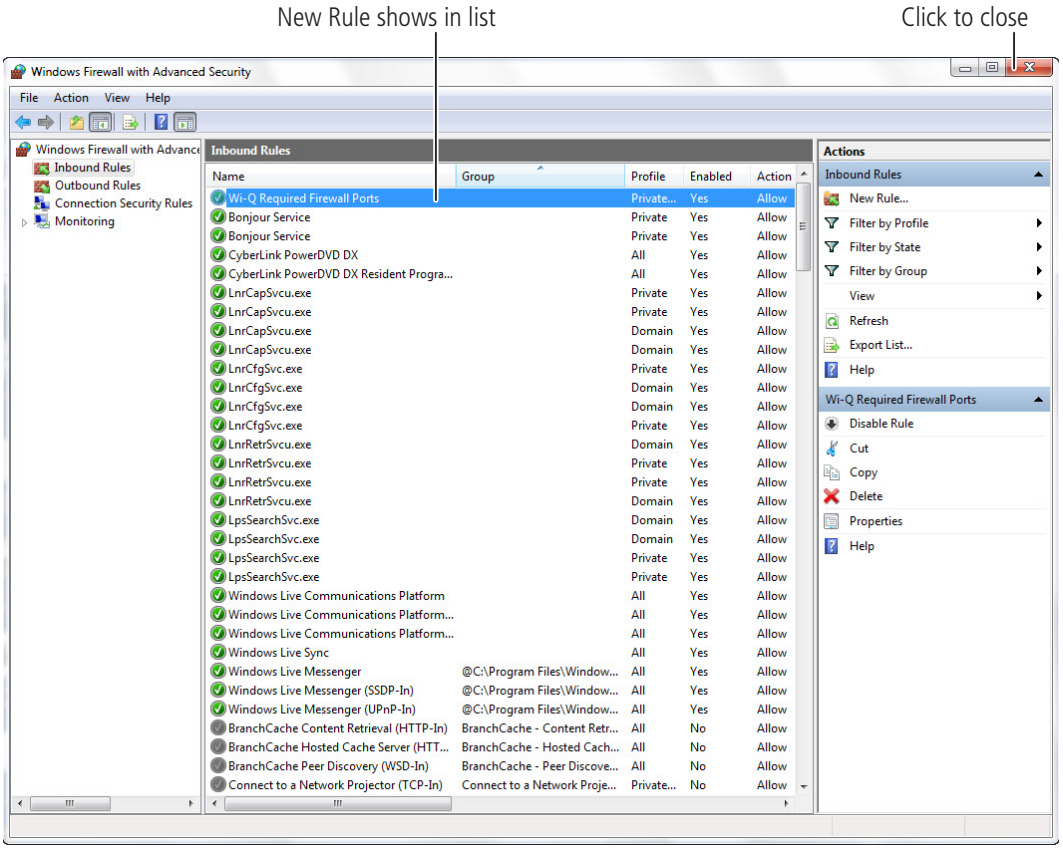
7 De-select the Public option. Click Next.

Figure 20 Name the Rule



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

Figure 21 Inbound Rules List



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

10 Repeat steps 1-9 for Outbound Rules.

Note Previous steps 1-10 also needs to take place on a computer with a remote router host.

Obtain the dormakaba (BEST Access Systems) C·CURE Wi-Q Interface Software

Before you can install the C·CURE Wi-Q Interface Software, you must contact Software House Customer Service Team. You can find their contact information at www.swhouse.com. They will provide you with a license and installation package.

Install C·CURE Wi-Q Interface Software (Task 5)

The Wi-Q Interface Software is a powerful tool that will help you integrate Wi-Q Technology into your system. The Wi-Q Interface Software must be installed on the main C·Cure 9000 machine as well as any C·Cure 9000 client machines, which only the Wi-Q client and Wi-Q Gateway Configuration tool will be installed. The software consists of three parts:

- **Wi-Q Interface Server** — Provides a communication link between the Crossfire Server and Wi-Q Router Host. The Interface server is responsible for transmitting and receiving all access control information.
- **Wi-Q Client Components** — Provides user controls for the Wi-Q objects in the C·Cure 9000 Software.
- **Wi-Q Gateway Configuration Tool** — Provides a list of Wi-Q Gateways on the network to configure.

The following prerequisites are required:

- .NET Framework 4.5
- Message Queuing
- Bonjour Print Services SDK

Note .NET Framework 4.0 or higher is required for C·Cure 9000, so it should already be installed.

Wi-Q Router Host

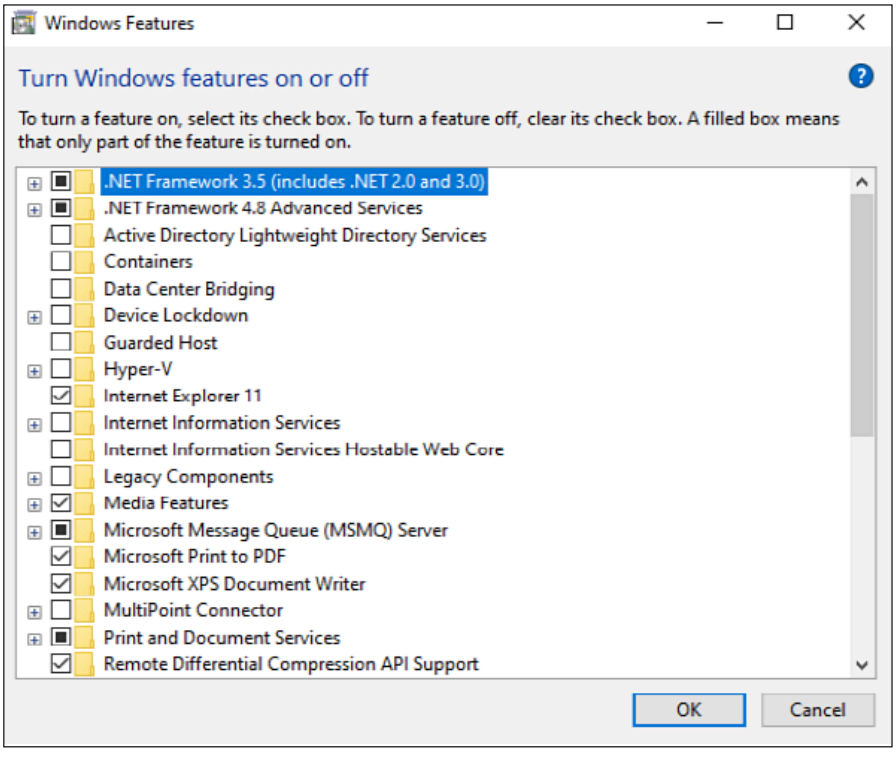
The second installation file packaged along with the Wi-Q Interface Software provides a communication link to the Wi-Q Gateways.

Starting with C·Cure Wi-Q Interface version 1.1.0.4 the Wi-Q Router host installation is included with the Interface installation. However it can be excluded from the installation and installed separate using the custom setup options.

Enabling .NET Framework and Microsoft Message Queuing Windows 10 Pro

1 Enter "windows features" into the Start Menu search bar and select "Turn Windows features on or off" from the results.

Figure 22 Turn windows features on or off



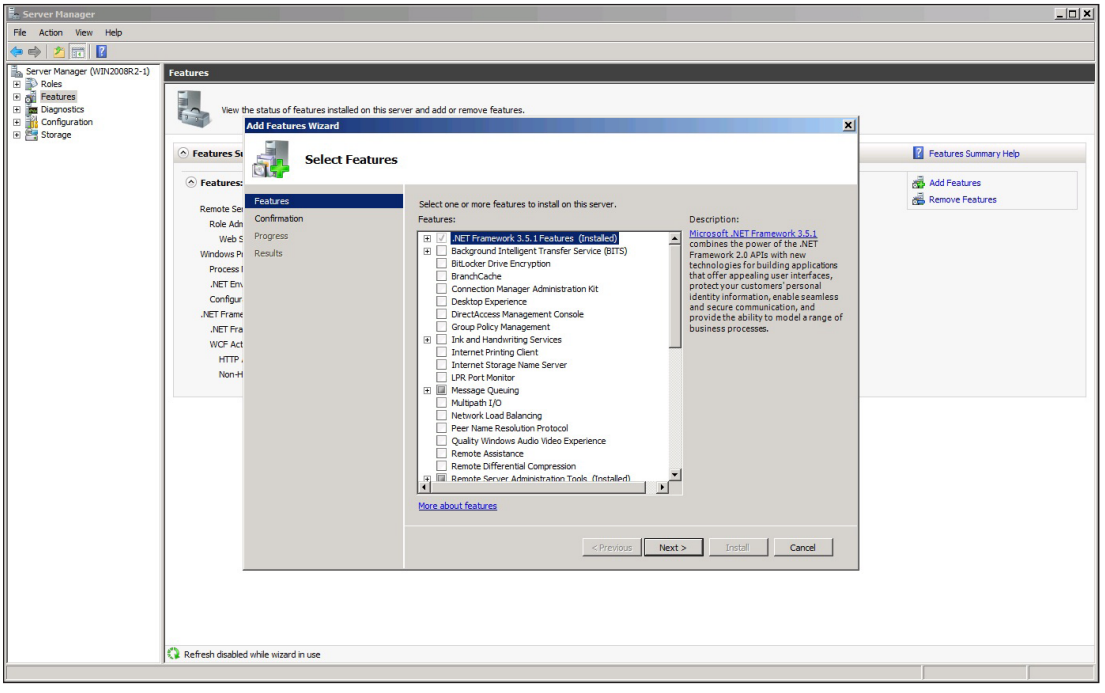
2 Check/fill in the check-boxes for Microsoft .NET Framework 3.5.1 and Microsoft Message Queue (MSMQ) Server if they are not already checked/filled in.

3 Select OK button to install.

Enabling .NET Framework and Microsoft Message Queuing for Windows Server 2016

Enter "windows features" into the Start Menu search bar and select "Turn Windows features on or off" from the results.

Figure 23 Add features wizard



4 Select the Features section and, when selectable, select Add Features link.

5 Check/fill in the check-boxes for Microsoft .NET Framework 3.5.1 and Microsoft Message Queue (MSMQ) Server if they are not already checked/filled in.

6 Select Next button.

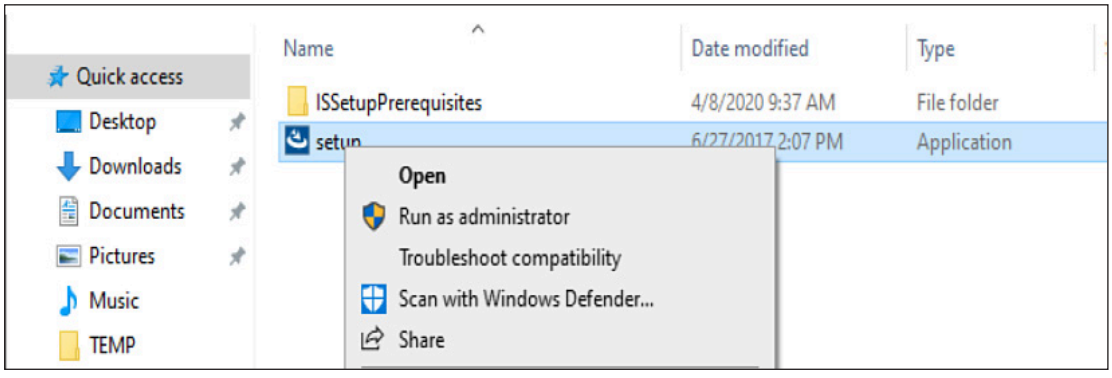
7 Select Install button for installation to begin.

8 Select Close button.

Start the BEST Wi-Q Integration Installation Wizard

If you have not already done so, download the **Integration dormakaba (BEST Access Systems) Wi-Q Interface** file from the dormakaba Technical Support website or Insert the software disc into your machine's disc reader.

Figure 24 Setup (Wi-Q Interface)

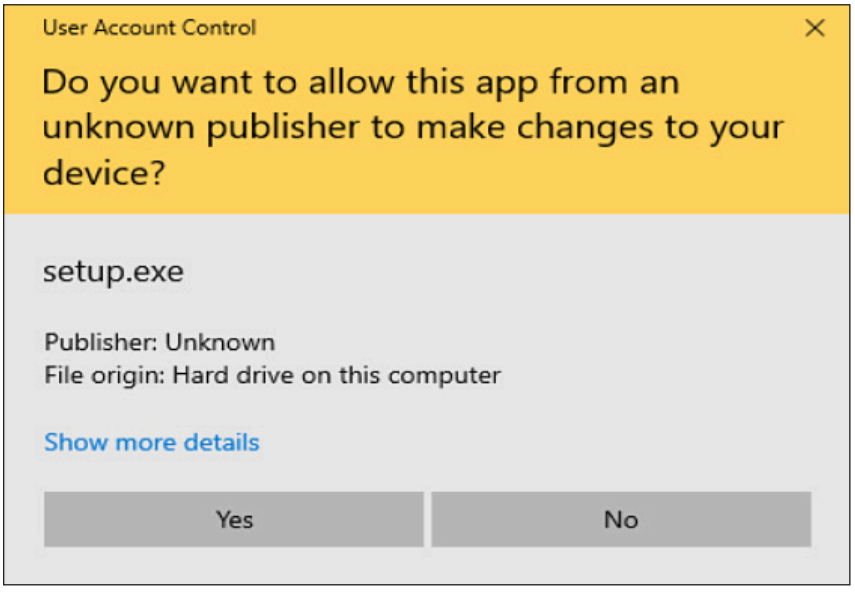


1 Right click the **BEST Wi-Q Interface setup.exe** file and select **Run as Administrator**.

2 Select **Yes** when asked for permission to make changes to the computer.

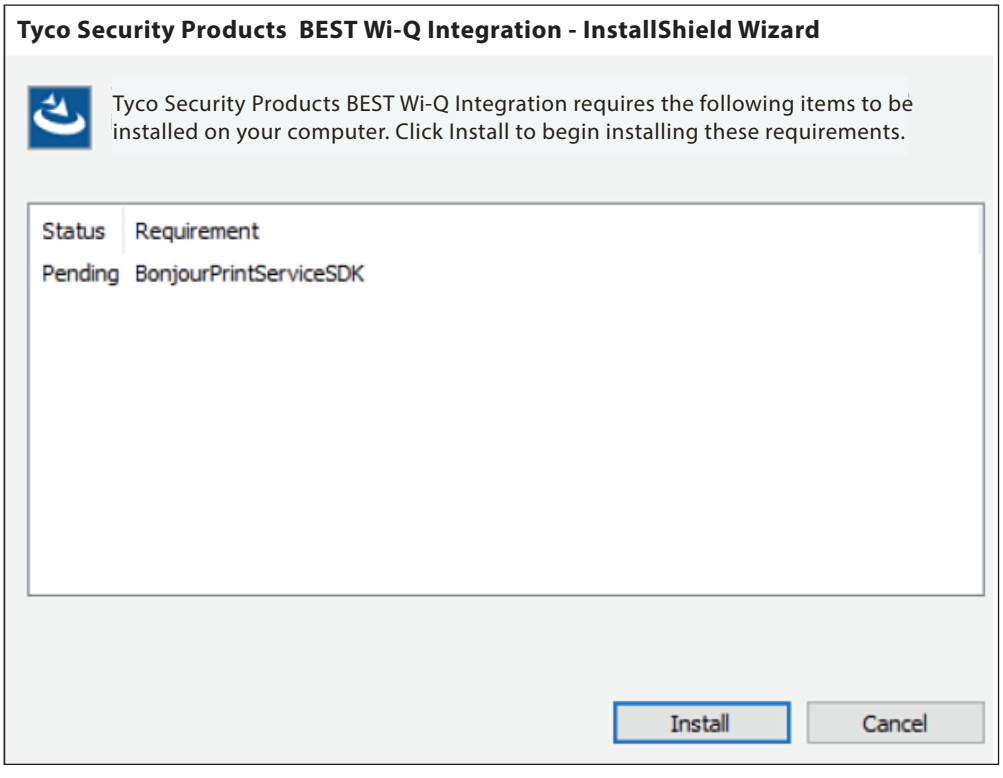
Installing the Bonjour Print Services

Figure 25 The Bonjour Print Services - InstallShield Wizard



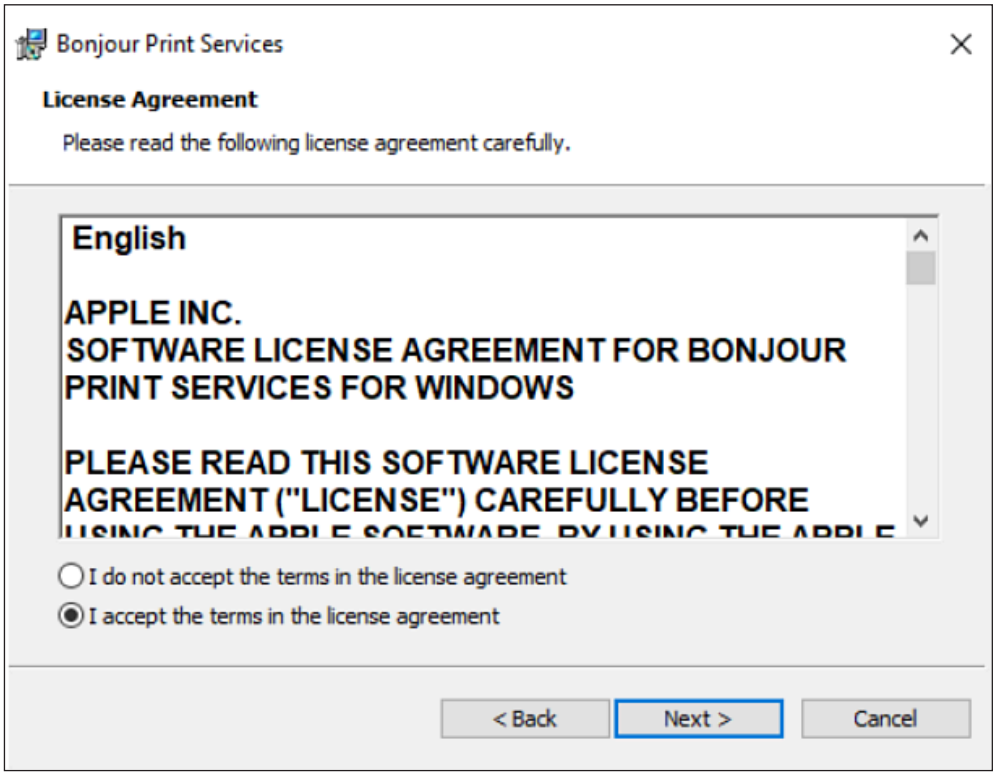
1 If the Bonjour Print Service SDK is not installed on the machine, a prompt to install this prerequisite will appear. To continue, select **Install**.

Figure 26 Bonjour End User License Agreement



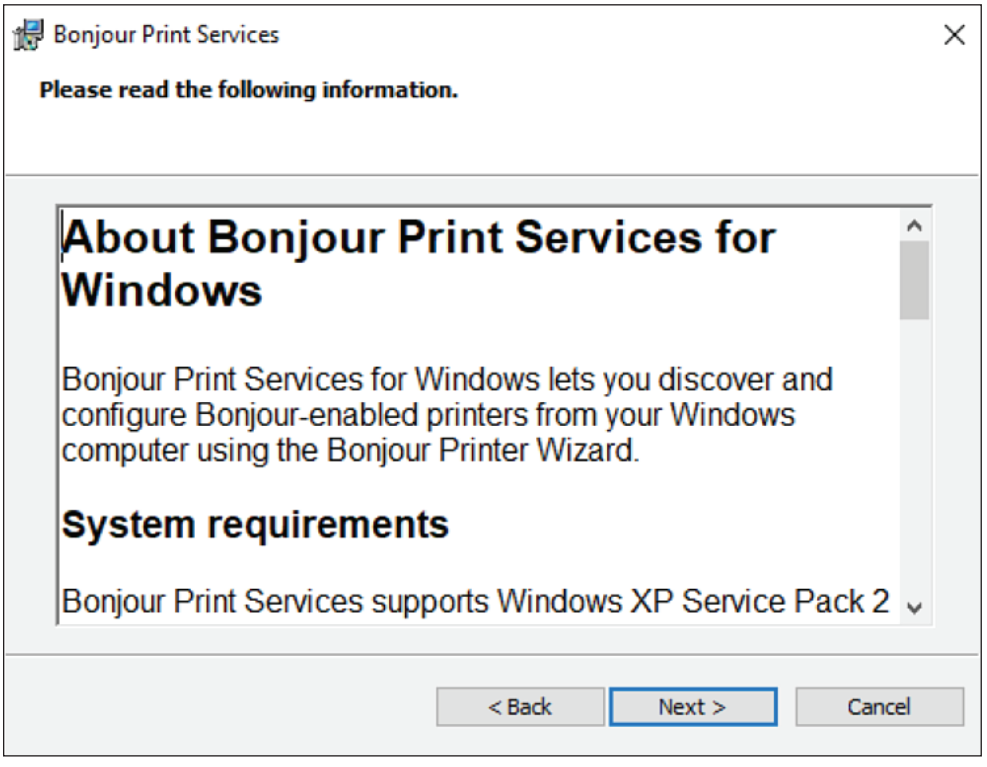
2 Select Next to continue to the End User License Agreement.

Figure 27 Bonjour End User License Agreement



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

Figure 28 Requirements Listing



4 Select **Next** at the requirements listing.

5 Choose whether to create a desktop shortcut and/or to enable automatic updates of the Bonjour Print Services SDK. Select **Install** to continue.

Figure 29 Installation Options

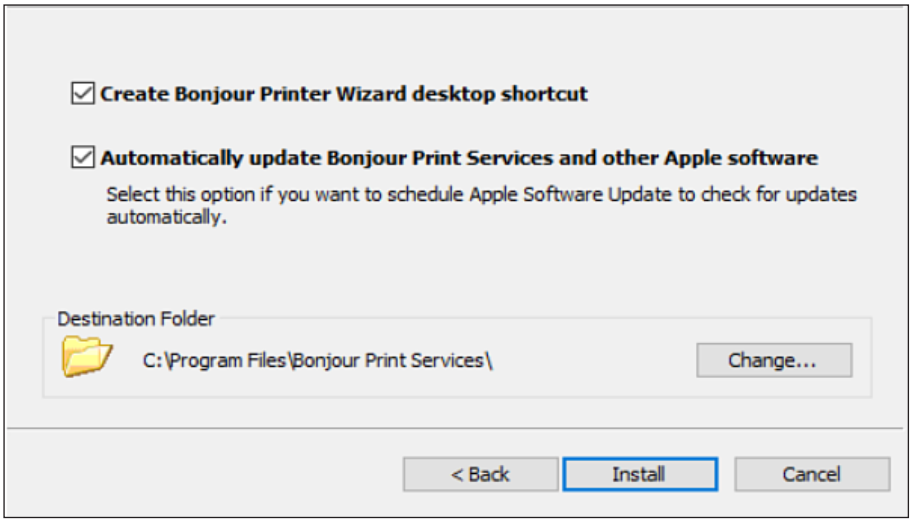
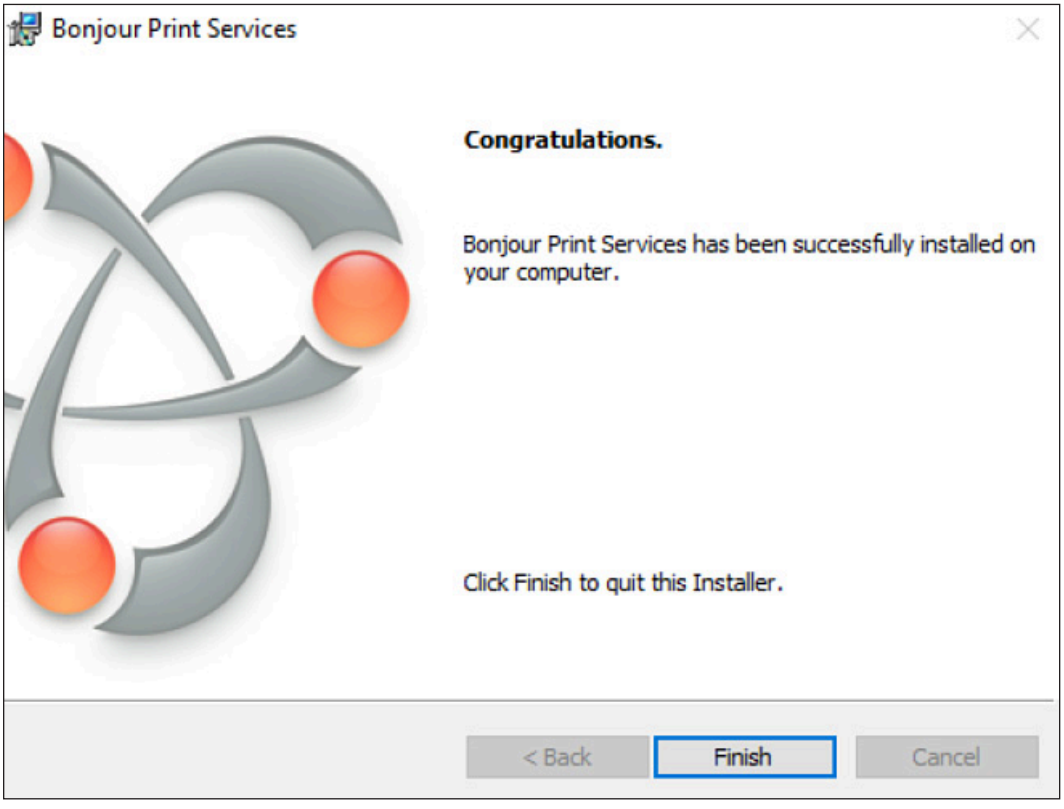
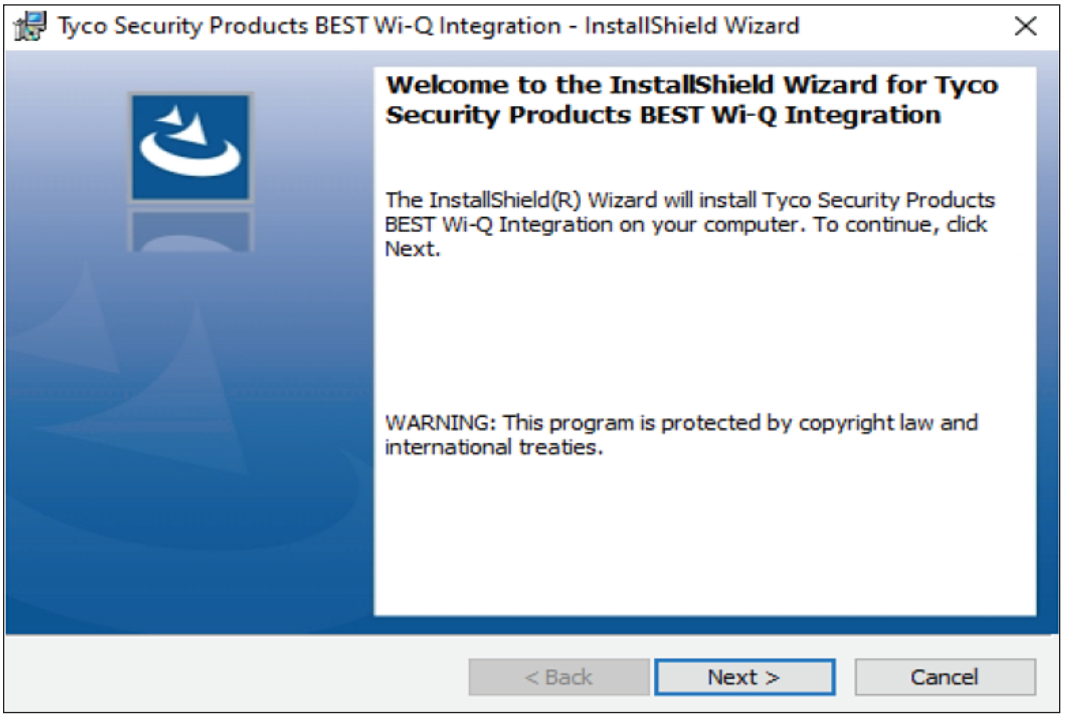


Figure 30 Finish Installation



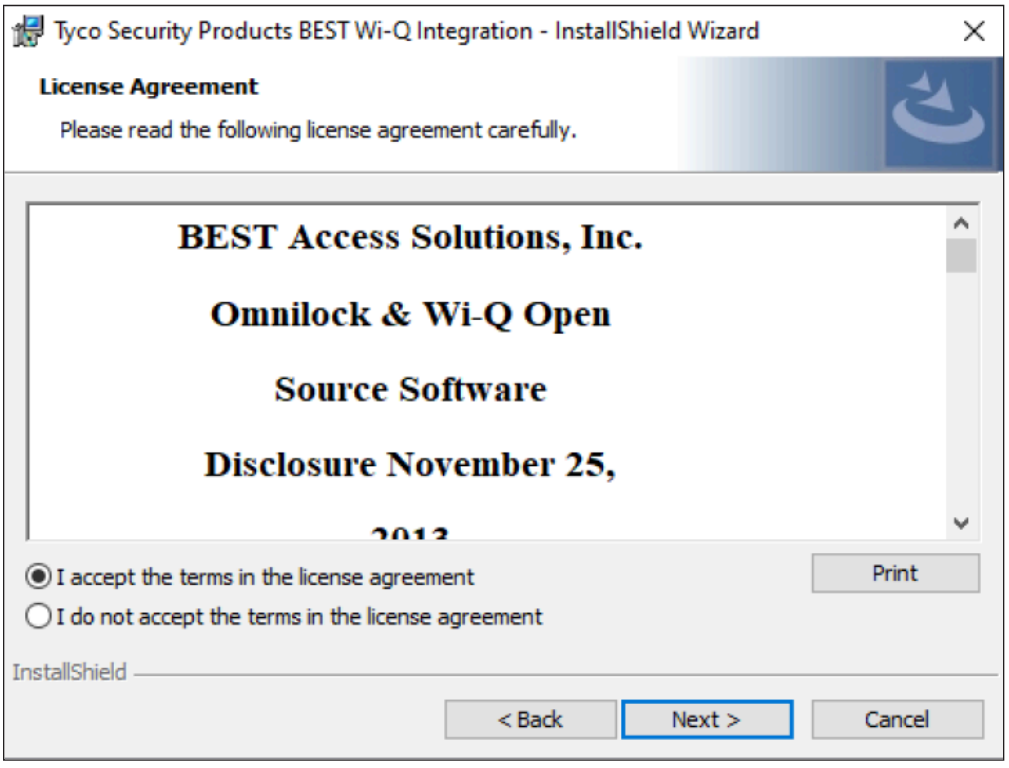
6 Once the installation is complete, select **Finish**.

Figure 31 The Wi-Q Integration - InstallShield Wizard



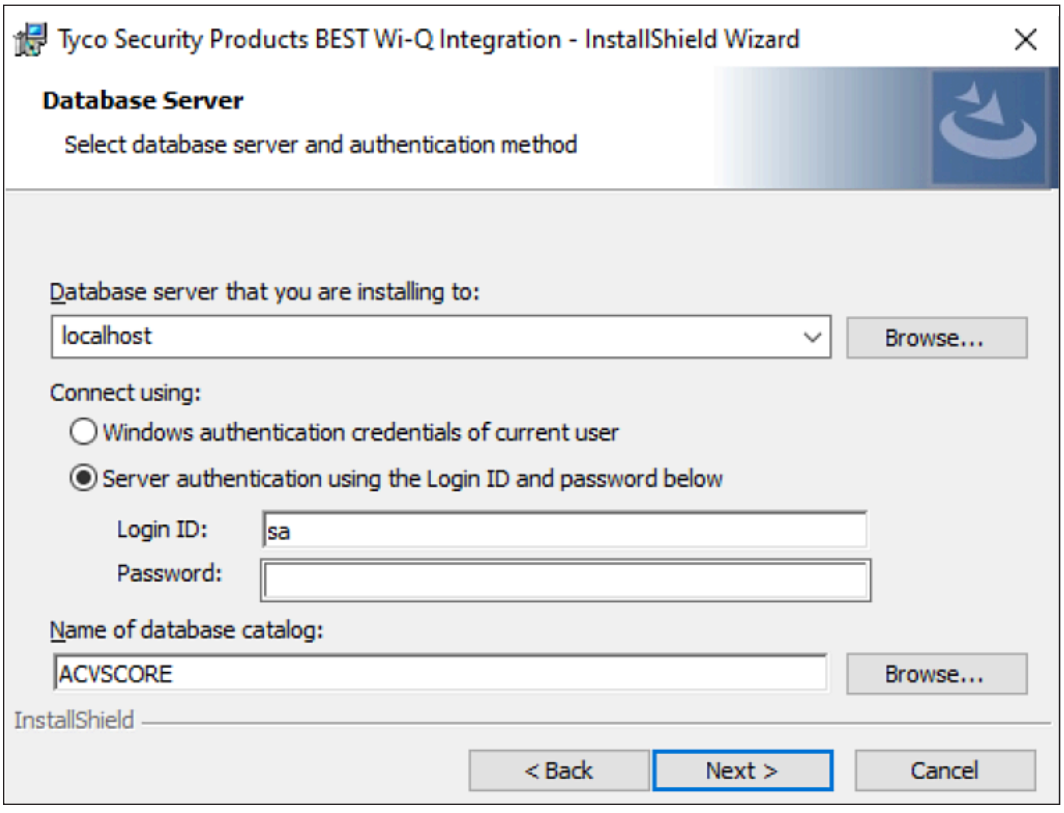
1 Select **Next** to continue to the End User License Agreement.

Figure 32 Wi-Q C·CURE End User License Agreement



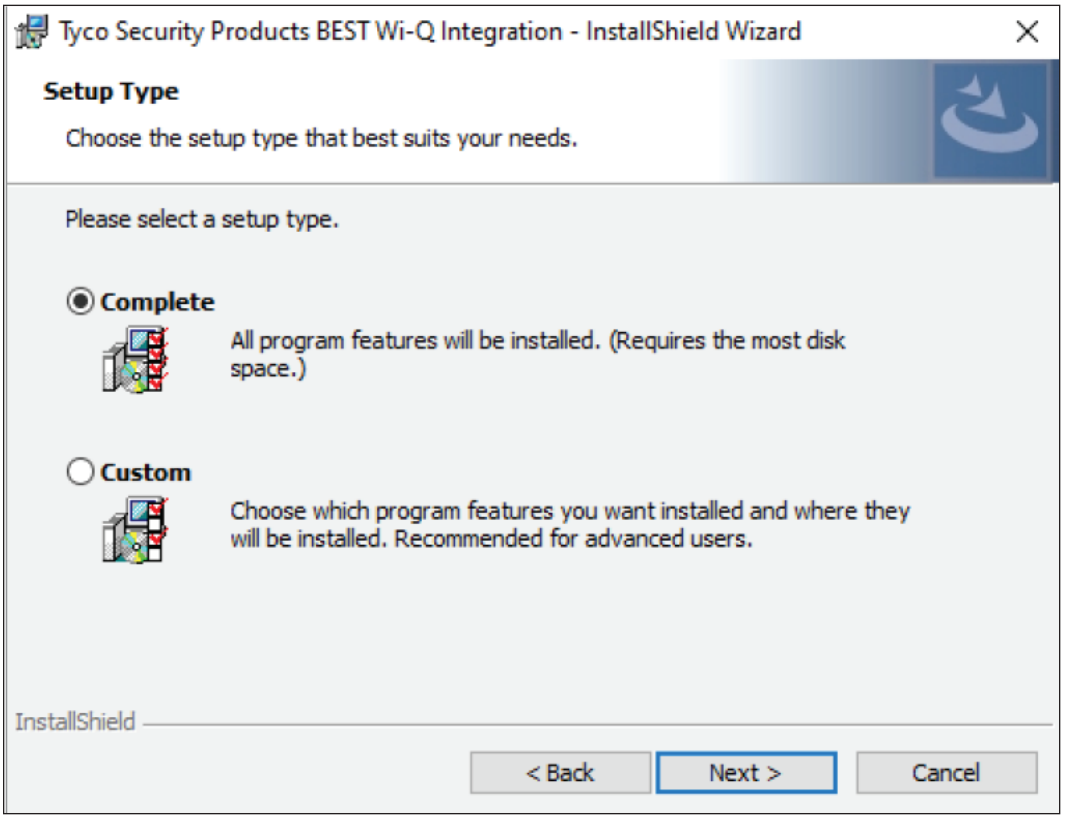
2 Read the License Agreement. To continue with the installation, click "I accept the terms in the license agreement," then press **Next**.

Figure 33 Authentication



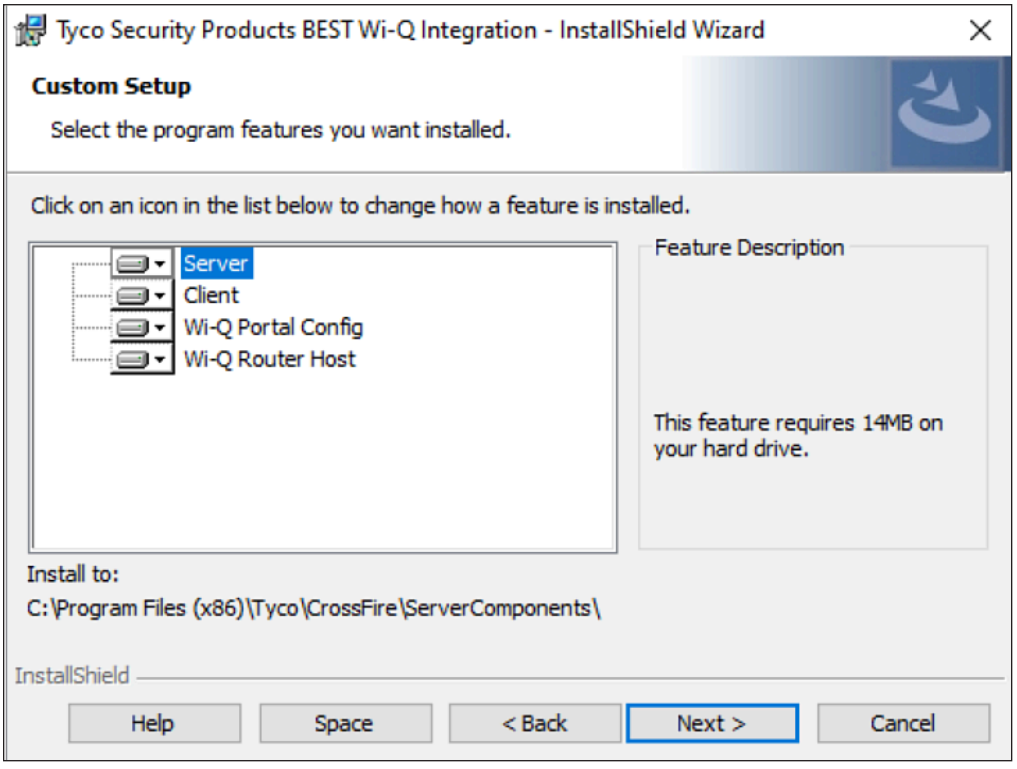
3 Select either Windows authentication or enter a Server authentication for the SQL database being used by the current C·Cure system. Select **Next**.

Figure 34 Complete or Custom Installation



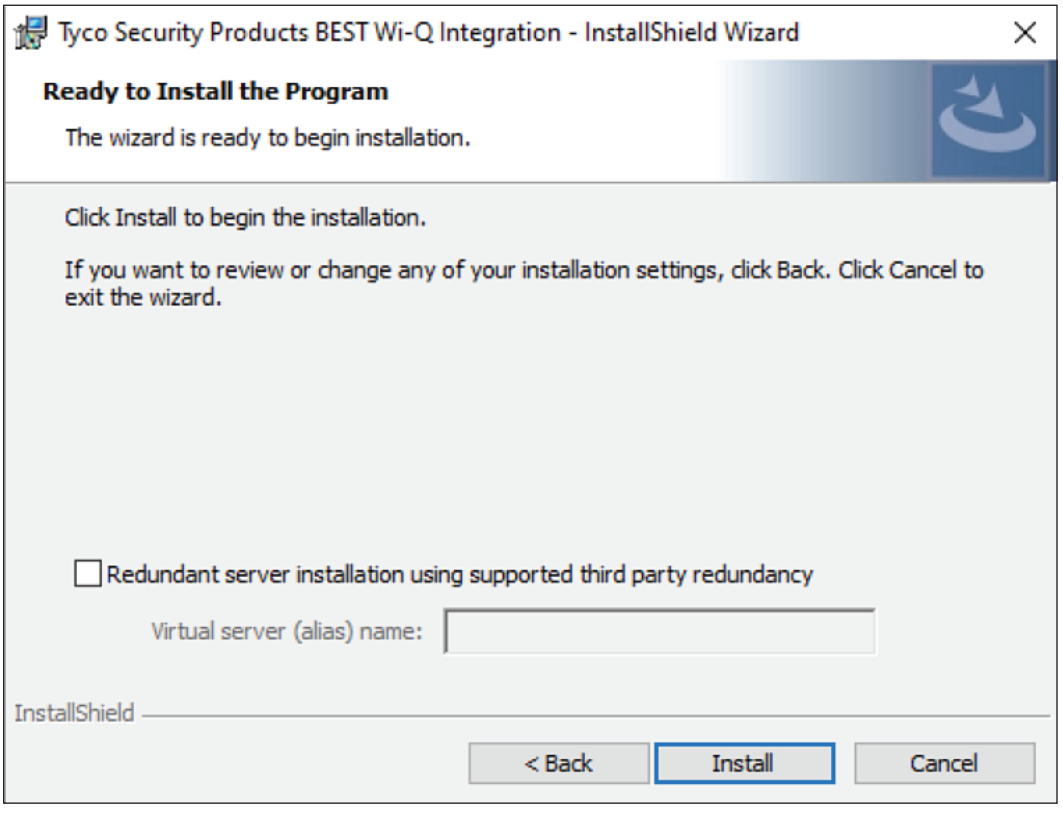
4 Select a Complete or Custom Installation and select **Next**.

Figure 35 Custom Installation



5 If a Custom setup was chosen, an installation option for each component must be selected. Then click **Next** to continue.

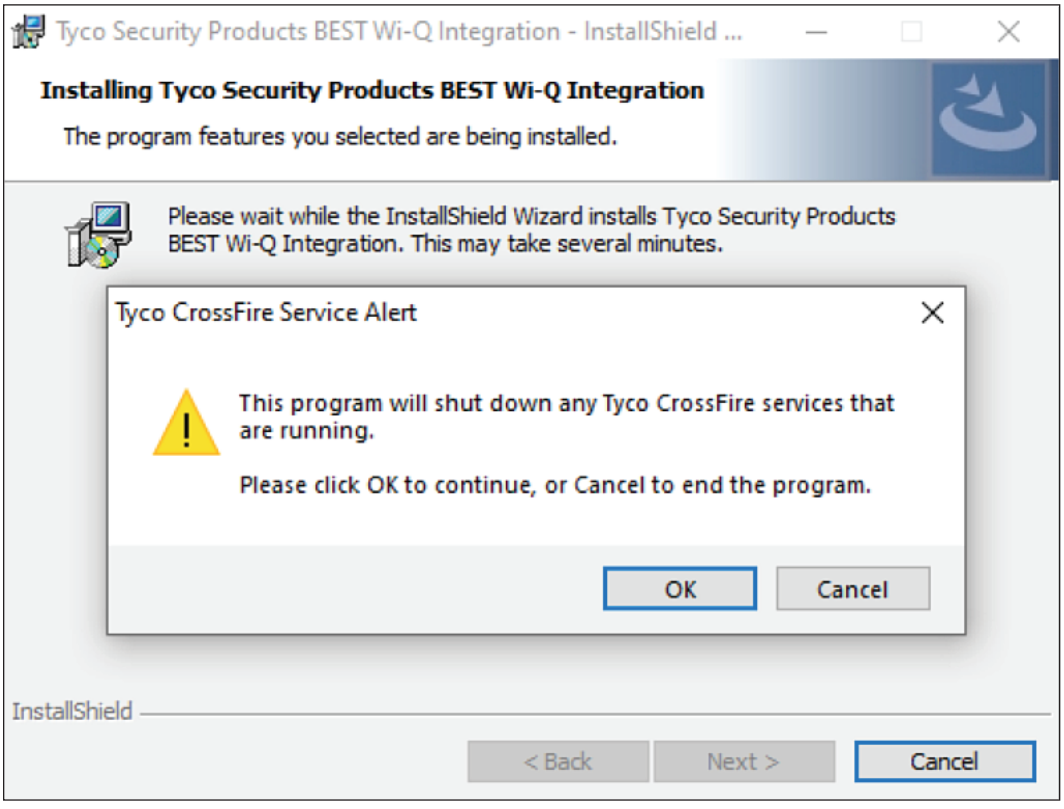
Figure 36 Install the Software



6 Select the **Install** button.

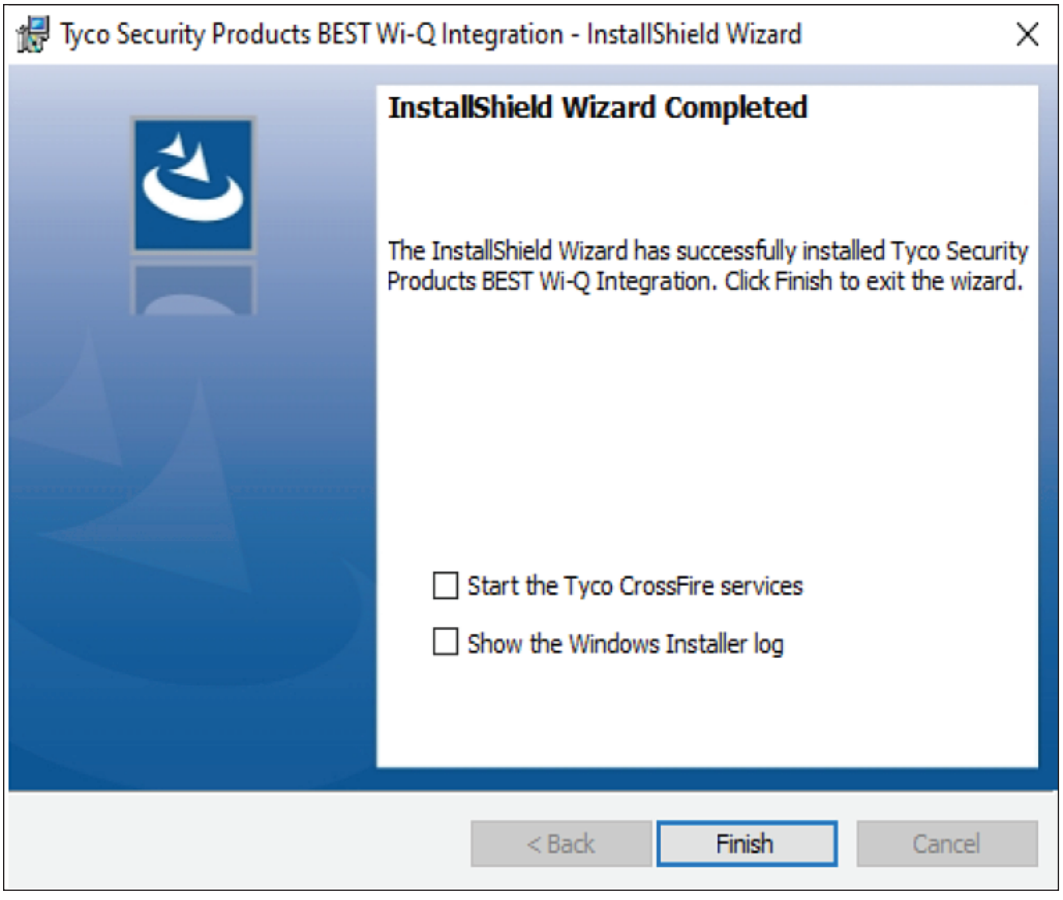
Note A redundant server installation using a third party redundancy option is not supported in BEST Wi-Q Interface integration with C·Cure. 9000.

Figure 37 Stop the CrossFire Services



7 Select **OK** to stop any currently running Tyco CrossFire services to continue with the installation.

Figure 38 Finishing the Installation



8 Choose whether to start the Tyco CrossFire and dormakaba (BEST Access Systems) Wi-Q Services.

9 Choose whether to see the Windows Installer log.

10 Select **Finish** to complete the installation.

4
Software Configuration

This chapter will guide you through performing the following tasks:

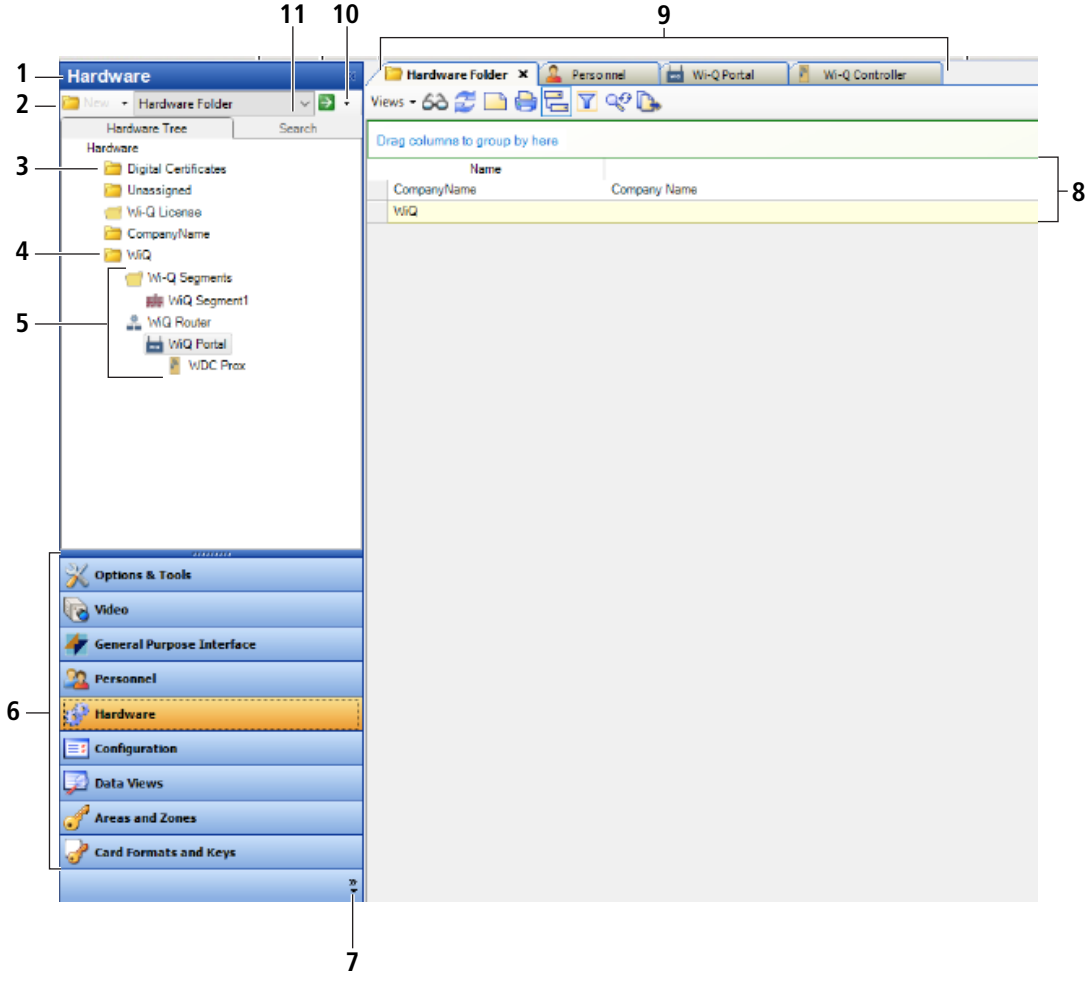
Task 6 — Configure Hardware on Host

Task 10 — Configure Software and Firmware Updates

C·CURE Wi-Q Pane Overview

This section will provide a brief overview of the components in the C·CURE Wi-Q Navigation Pane of the Administrative Workstation with the Hardware Navigation Button selected. See Figure 39.

Figure 39 C·CURE Wi-Q Pane



1 Current Selection

Indicates the Navigation Button currently selected from the Navigation Button Pane (Item 6).

2 Available Actions Pop-up Menu

Lists the actions associated with the task or item selected in the Navigation Button Drop-Down List to the right of it (Item 12). Alternatively, the associated actions are also available by right clicking on an object or data field.

3 Display Panel

Shows the Hardware tree or other options associated with the Navigation Button selected (Item 6).

4 **Hardware folder**
A Hardware folder contains a list of the hardware components. The folder and its contents are commonly given descriptive names to help in the location of components.

5 **Hardware Tree**
When expanded, displays a graphical list of the hardware components showing their relationships.

6 **Navigation Button Pane**
Selects the items appearing in the Display Panel (Item 3).

7 **Navigation Button Pane Options**
Select Navigation Pane Options to change the order of the buttons and to control the button display.

8 **View**
Displays the results of a search for the item displayed in the Navigation Button Drop-Down List (Item 11).

9 **View Tabs**
Searches can be opened in the same Dynamic View window or in their own tabs.

10 **Search Button**
Initiates a search for the item displayed in the Navigation Button Drop-Down List (Item 11) and displays the results in the Dynamic View window.

11 **Navigation Button Drop-Down List**
Lists the items associated with the current button selected in the Navigation Button Pane.

Configuring the Hardware in C·CURE Wi-Q Interface Software (Task 6)

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

For large installations, see www.swhouse.com for information on setting up dialog box templates to speed up the process. Some dialog boxes also offer the option of **Save and New** to save and bring up a new dialog box when entering certain hardware items to save the extra step of right clicking for a new dialog box. Hovering over a text box will often pop up a tool tip with a brief explanation.

Installing a Wi-Q Controller License

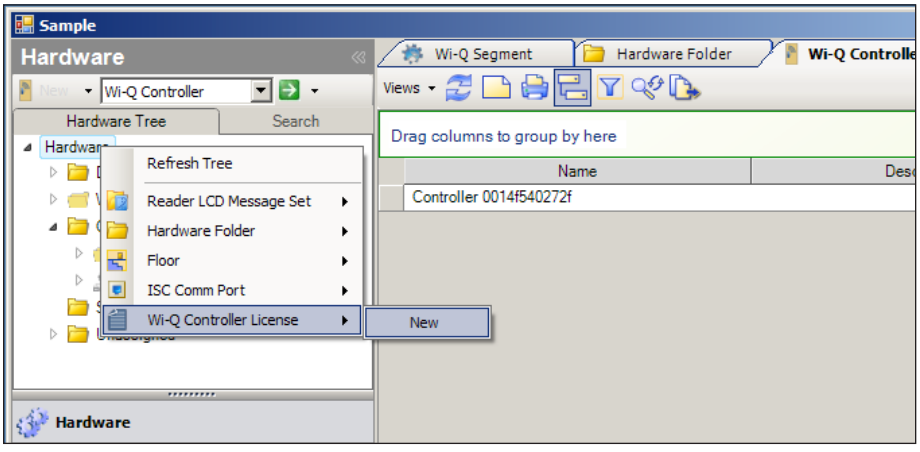
If not already accomplished during the installation of the Wi-Q Interface Software, or to install an upgrade, complete the following steps. Please see www.swhouse.com for contact information regarding controller licenses.

Obtaining a Wi-Q Controller License

To obtain a license, you must contact Software House Customer Service Team. You can find their contact information at www.swhouse.com.

Adding a New Controller License

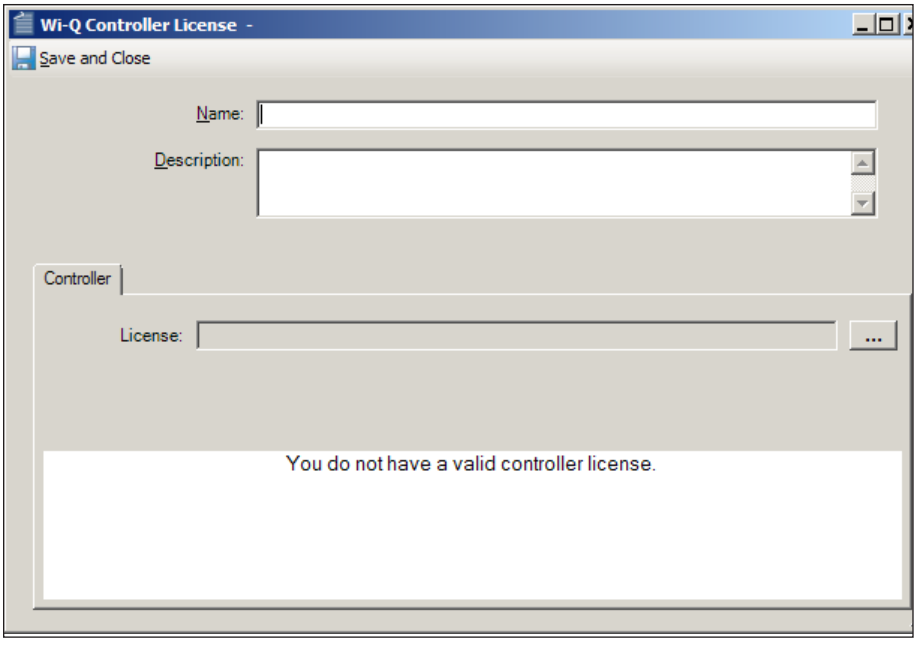
Figure 40 Adding a New Controller License



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel above it.

2 Right click the Hardware heading at the top of the hardware tree and select **Wi-Q Controller License -> New** to display the Wi-Q Controller License dialog box.

Figure 41 Enter Wi-Q License



3 Name your license and enter an optional description if desired.

4 In the License text box enter the path to the license file or click the Ellipsis button to the right to browse for the file. Information about your license and controllers will appear in the display box below it.

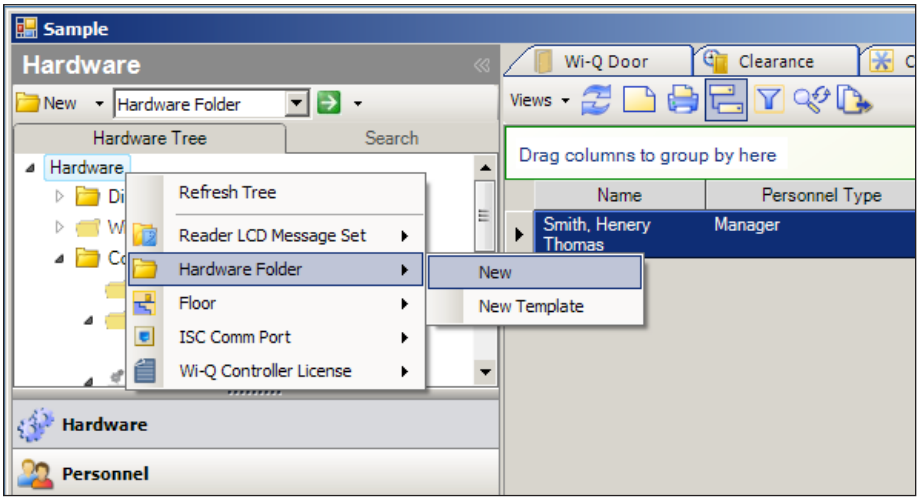
5 Click **Save and Close** in the upper left hand corner of the dialog box to finish.

Note Your licenses will appear in a folder in the hardware tree.

Create a Hardware Folder

Hardware folders are used to contain segments, routers and controllers and display the relationship between them in the hardware tree.

Figure 42 Creating a Hardware Folder



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel if it is not already displayed.

2 Right click the Hardware heading at the top of the hardware tree and select **Hardware Folder -> New.**

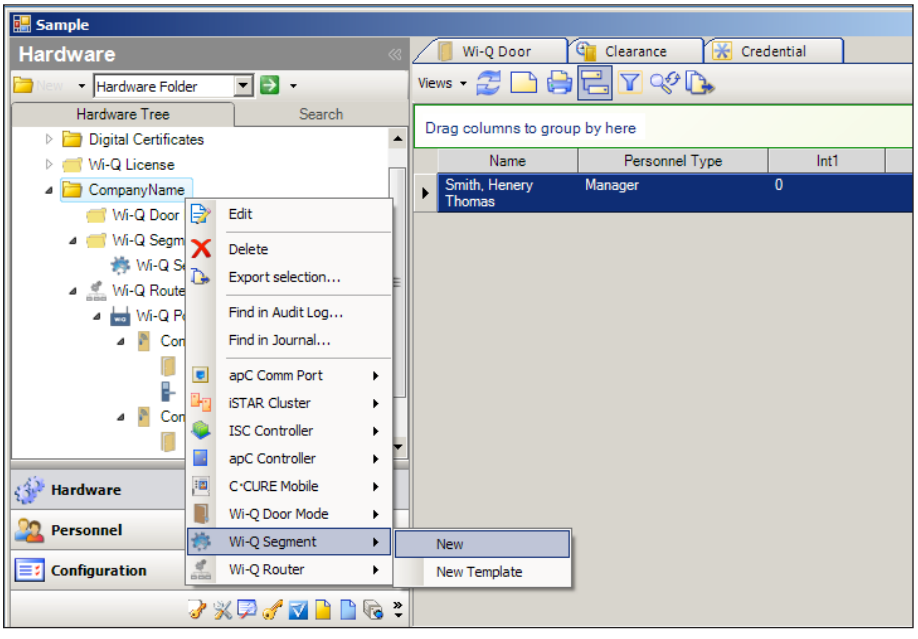
3 In the dialog box that appears, name the folder and add an optional description if desired.

4 Click **Save and Close** in the upper left hand corner to finish. The folder will appear in the hardware tree.

Creating and Configuring Wi-Q Segments

Segments are used for grouping like locations or hardware such as building groups, the same card formats, facility codes, etc. It also provides the sign on codes for the controllers. There are no limitations to the number of Wi-Q Gateways that can be assigned to one segment, and there are no limitations to the number of segments.

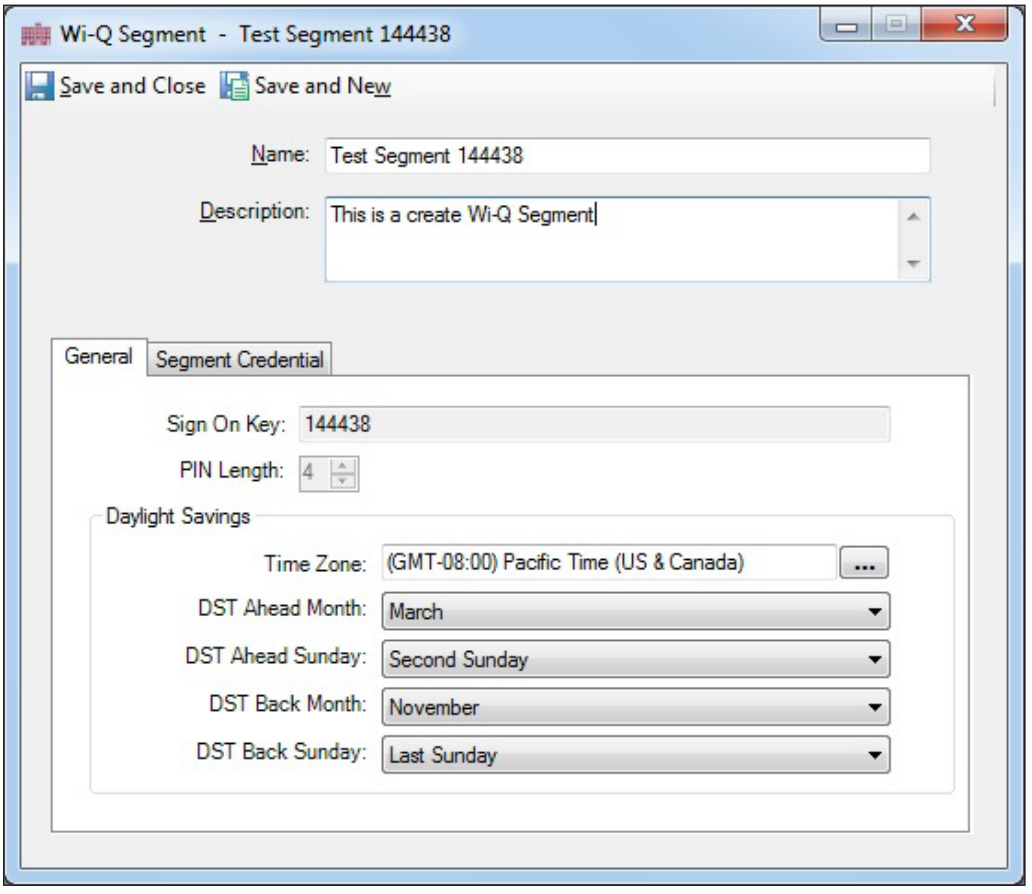
Figure 43 Creating a New Wi-Q Segment



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel if it is not already displayed.

2 Right click the Hardware folder you just created in the hardware tree (In this example it is named CompanyName) and select **Wi-Q Segment -> New.**

Figure 44 Wi-Q Segment Dialog Box



3 In the Wi-Q Segment dialog box that appears, enter the segment name and optional description developed and gathered in Tasks 1 and 3.

4 Click the **General** tab. A unique Segment Sign On Key number is automatically generated for the Sign On Key field. This Sign On Key number is used when signing on all Wireless keypad controllers in this segment (See "Signing on Controllers (Task 9)" on page 24). It is important that this number is recorded or its location remembered for later use in signing on the key pads.

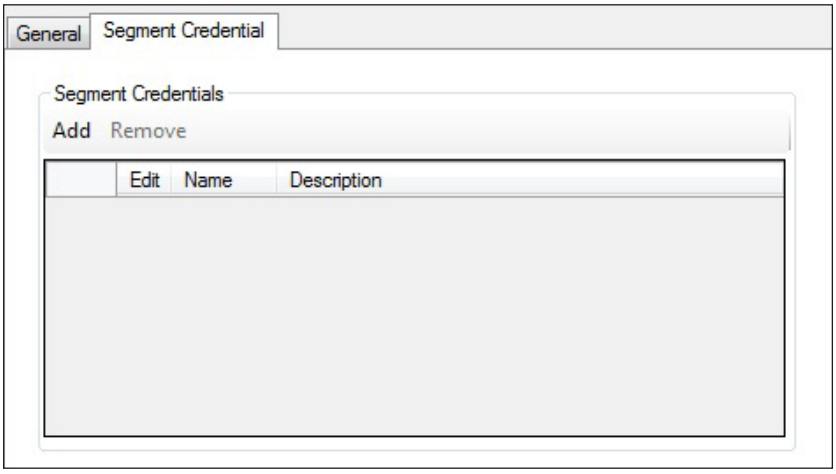
5 Set the Pin Length field to 4. This affects the length of the key pad in addition to the personal pin.

6 In the Daylight Savings box, click the Ellipsis button to the right of the Time Zone field to select your time zone from the list. The remaining 4 fields will auto populate, but can be changed if the Daylight Savings standards change. You can click **Save and Close** to finish or click the **Segment Credential** tab to continue on and Configure a Magstripe or Prox Card as a Sign on Credential.

Configuring a Magstripe or Prox Card as a Sign On Credential

The **Segment Credential** tab allows you to add a Card Sign On Credential so you can use a card to sign on wireless card readers.

Figure 45 The Segment Credential Tab in the Wi-Q Segment Dialog Box



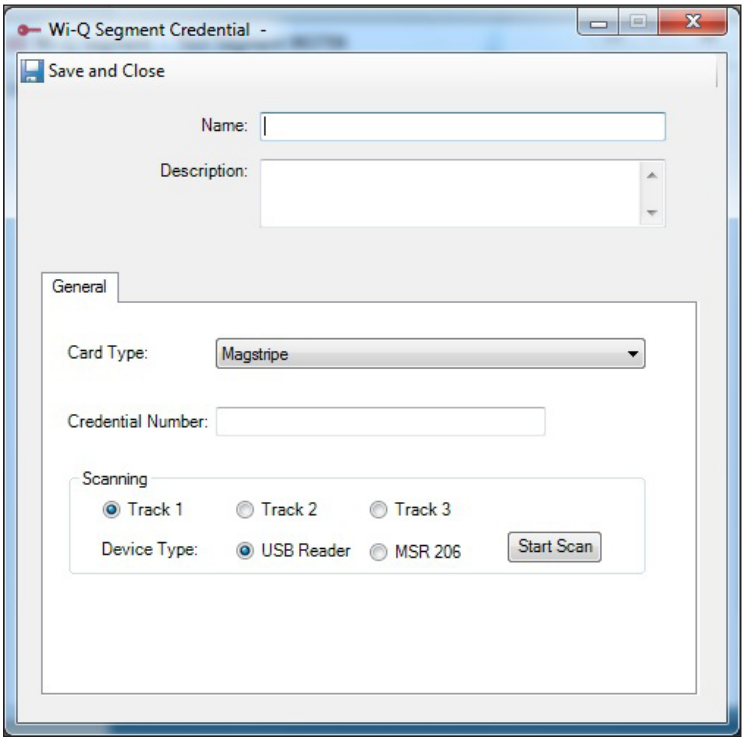
1 Click the **Segment Credential** tab.

2 Click the **Add** button and the Wi-Q Segment Credential Dialog Box will appear.

3 Enter the segment sign on credential name and description developed and gathered in Tasks 1 and 3.

4 If "Display Card In Journal" is set to "True" in System Variables, the card number will be displayed in transaction monitoring or the Journal when it is swiped at the Controller.

Figure 46 Wi-Q Segment Credential Dialog Box



Note The full card number will only be displayed if the format of the card has not been added to the reader.

5 Enter the card's credential number in the Credential Number field. This is the number encoded on the card and will be provided with the card when it is created.

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

7 You can click the **Add** button again to enter another card.

8 The Keypad option from the Card Type drop-down menu can be used to enter a different Sign On Key number from the auto-generated one, but if this is done, the credential number must be 6 digits. If the number is less than 6 digits, it must be padded out with leading zeros to make it 6 digits. Be aware that doing this also increases the chances of duplicate Sign On Key numbers.

9 Click **Save and Close** in the upper left hand corner of the Wi-Q Segment Credential dialog box to return to the Wi-Q Segment dialog box.

10 Click **Save and Close** in the upper left hand corner of the Wi-Q Segment dialog box to finish. The new segment will appear in the hardware tree.

In order to sign on your card readers, there must be at a minimum, a segment, a router, and a Wi-Q Gateway created first. See "Signing on Controllers (Task 9)" on page 24.

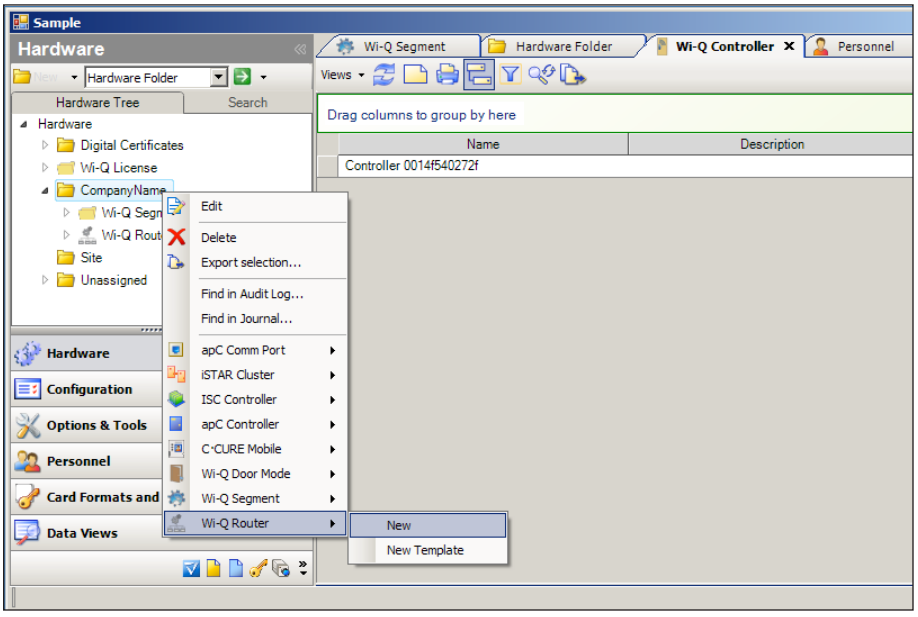
Note The option to delete a segment from the Segment tree becomes available when you right-click the segment from within the tree.

Adding and Configuring Wi-Q Routers

Wi-Q routers are implemented in software and must run on a computer and have a unique IP address. A Wi-Q router can run on a computer providing other services, but each router must run on a separate computer to have a unique IP address. For every one router, 1 host is needed.

When the router software is installed, the IP address, subnet mask and gateway of the computer should be recorded and provided for use during configuration.

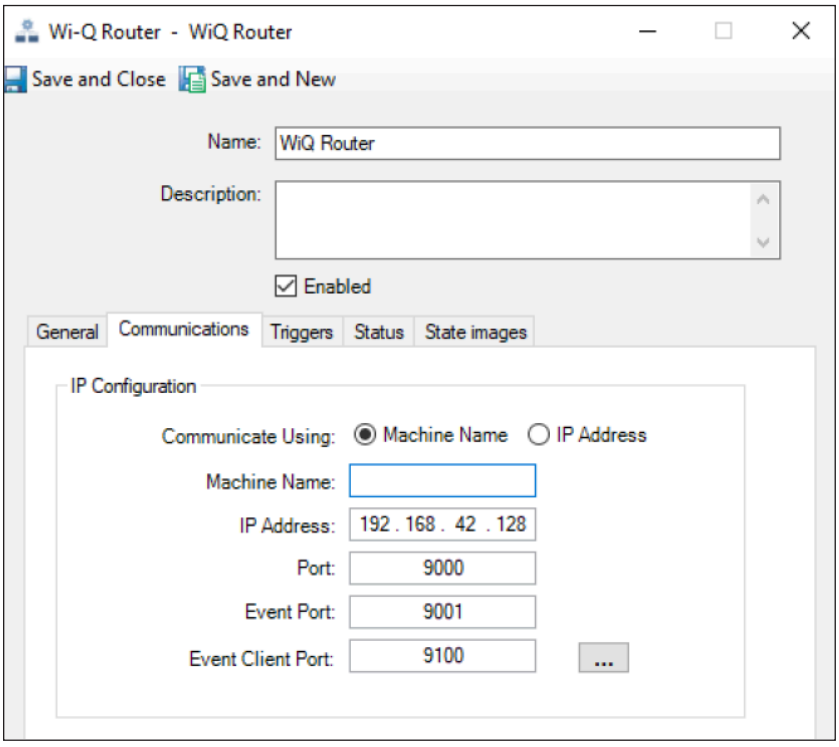
Figure 47 Adding a New Router



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel if it is not already displayed.

2 Right click the Hardware folder you just created in the hardware tree (In this example it is named CompanyName) and select **Wi-Q Router -> New.**

Figure 48 The Router Dialog Box



3 Enter the router name and description developed and gathered in Tasks 1 and 3.

4 Click on the **Communications** tab and enter the IP address or machine name of the computer that the desired Wi-Q router is installed on. This address will need to be gathered and previously supplied by the installer of the Wi-Q router software. The default port of 9000 can be left, but can be changed if needed. Refer to "Configure Windows Firewall Ports" on page 31.

5 Click the **Enable** check box to allow communications. It is important to note that the router and all items below the router on the hardware tree must be enabled to allow communication.

The following additional tabs are available, but no configuration changes are required at this time. See www.swhouse.com for more information.

- General Tab — This tab is auto-filled with general information once communications start and can not be changed.
- Triggers Tab — Assigns an action if certain events are detected.
- Status Tab — Displays the Host Communication status and can not be changed.
- State Images Tab — Displays the icons that will appear in C·CURE monitoring programs.

6 Click **Save and Close** in the upper left hand corner of the Wi-Q Router dialog box to finish. The new router will appear in the hardware tree.

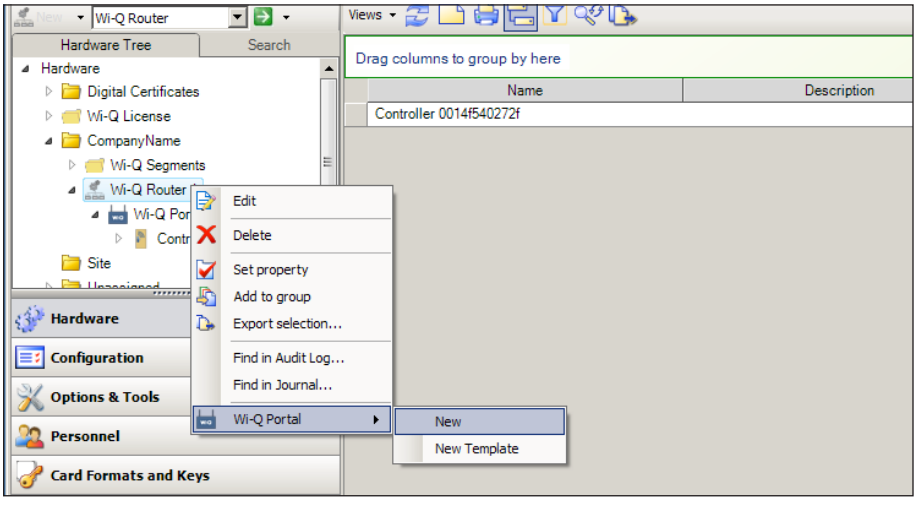
Adding and Configuring Wi-Q Gateways

Wi-Q Gateways can now be added and configured within the C·CURE Wi-Q Panel. This can be performed on a single Wi-Q Gateway or multiple Wi-Q Gateways at a time.

Wi-Q Gateways are configured from the factory with an IP address of 192.168.1.200. When configuring a Wi-Q Gateway, it is best to connect directly to the Wi-Q Gateway before placing it on the network. This removes the possibility of duplicate IP addresses on the network.

Note Your IT personnel will need to create and reserve a range of IP addresses for your Wi-Q Gateways before proceeding with Wi-Q Gateway configuration. A separate Wi-Q Site Survey Kit is available to help with this.

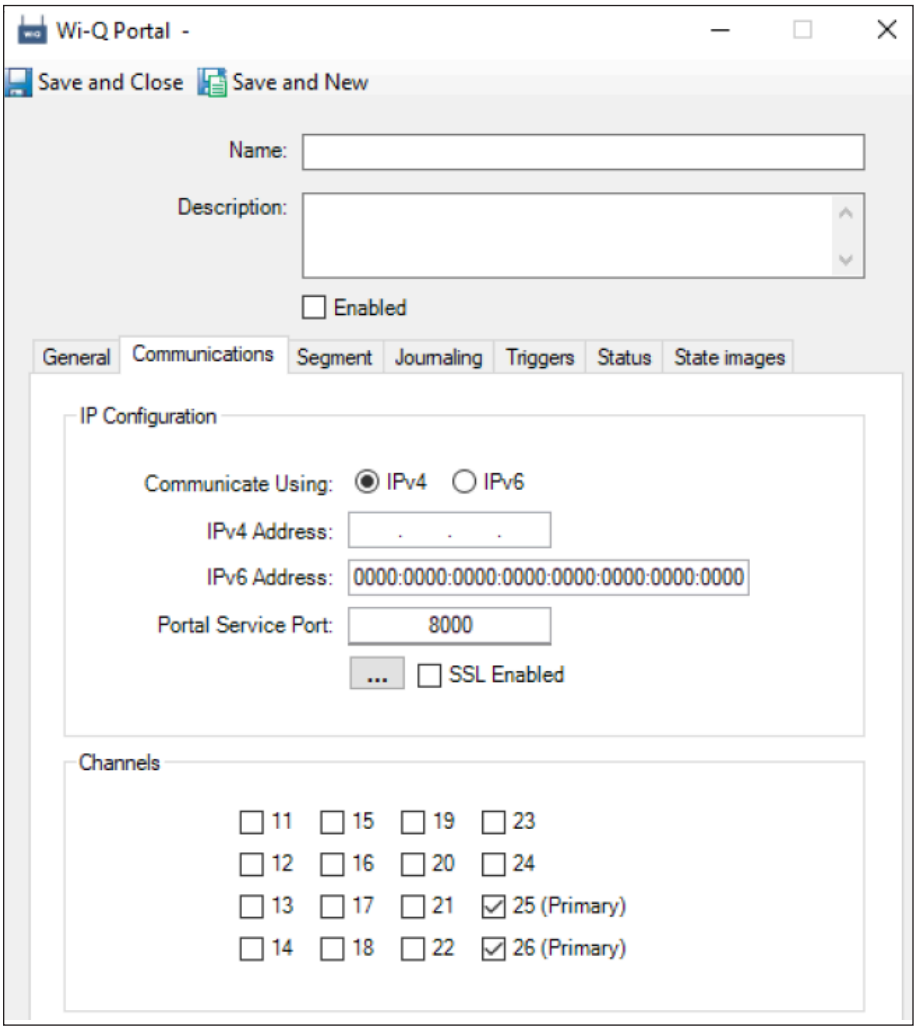
Figure 49 Adding a Wi-Q Gateway to a Router



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel if it is not already displayed. Expand the Hardware folder (In this example it is named CompanyName), if needed, to see the routers.

2 Right click the router you are assigning the Wi-Q Gateway to in the hardware tree and select **Wi-Q Portal -> New.**

Figure 50 Portal Dialog Box



3 Enter the Wi-Q Gateway name and description developed and gathered in Tasks 1 and 3.

4 Click the **Enabled** check box to allow communications.

5 Click the **Communications** tab and enter the IP address, either IPv4 or IPv6, of the Wi-Q Wi-Q Gateway. Contact your IT personnel for this information.

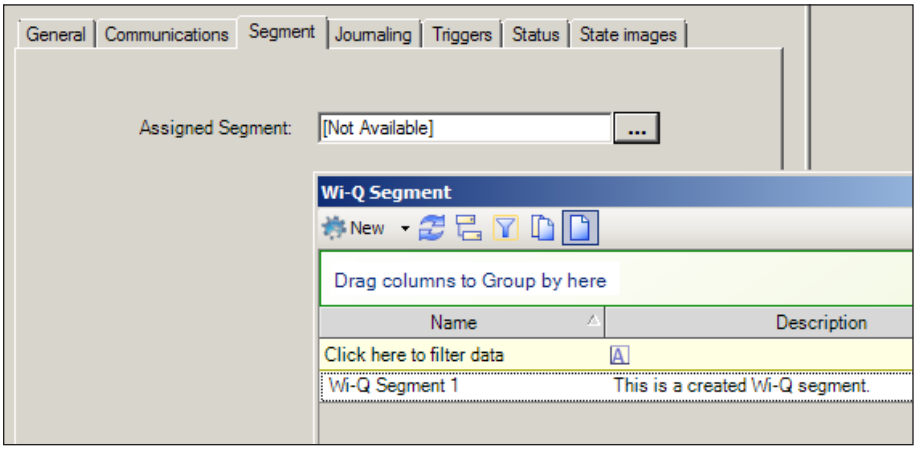
6 The default ports of 8000 can be left, but can be changed if needed.

7 Select the **SSL** (Secure Socket Link) check box for extra security, only if SSL was setup at the Wi-Q Gateway with the Wi-Q Gateway Configuration tool in the Site Survey Kit, which is also in the interface installation. This encrypts the data transmitted. Stanley highly recommends SSL enabled on every Wi-Q Gateway.

8 Select the radio channels you wish this Wi-Q Gateway to use. Each Wi-Q Gateway has two radios that communicate on separate channels; the default channels are 25 and 26. In an environment with several

Wi-Q Gateways or other wireless devices in close proximity, alternate channels should be selected. Otherwise they can be left at the default settings.

Figure 51 Assigning a Wi-Q Gateway to a Segment



9 Click the **Segment** tab and then click the Ellipsis button to the right of the Assigned Segment text box. From the dialog box that appears, select a segment from the list of segments you have created.

The following additional tabs are available, but no configuration changes are required at this time. See www.swhouse.com for more information.

- General Tab — This tab is auto filled with general information once communications start and can not be changed.
- The Journaling Tab — Shows the defaults for how often data logging occurs.
- Triggers Tab — Assigns an action if certain events are detected.
- Status Tab — Shows the Communications and router connection status and the number of controllers signed on.
- State Images Tab — Displays the icons that will appear in C·CURE monitoring programs.

10 Click **Save and Close** in the upper left hand corner of the Wi-Q Gateway dialog box to finish. The new Wi-Q Gateway will appear in the hardware tree.

Note When right-clicking on a Wi-Q Gateway, the following options become available:

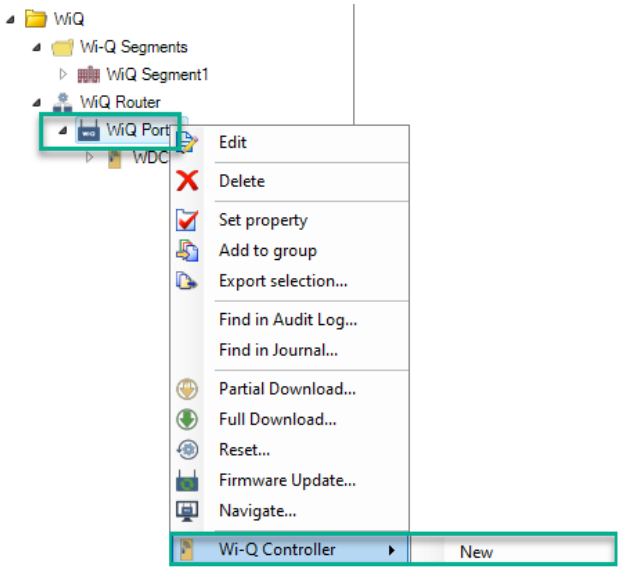
- Edit, Delete, Set property, Add to group, Export selection, Find in audit log, Find in journal, Partial download, Full download, Reset, Firmware update, Navigate, Wi-Q controller

Adding and Configuring Wi-Q Controllers

There are 2 options for adding the controllers, Automatic or Manual:

- You can let the software discover and add the controllers automatically as they are signed on in the field. This is the typical method. See "Signing on Controllers (Task 9)" on page 24.
- You can use the controller's MAC address and manually create a controller in the hardware tree with that MAC address and when that controller is recognized online it will be matched with the controller configuration in the hardware tree with that same MAC address. Follow instructions below:
  - Click on the Hardware bar in the left column to display the hardware tree in the display panel if it is not already displayed. Expand the Hardware folder (In this example it is named CompanyName), if needed, to see the routers.
  - Right click the Wi-Q Gateway you are assigning the Controller to in the hardware tree and select Wi-Q Controller -> New.

Figure 52 Wi-Q Controller

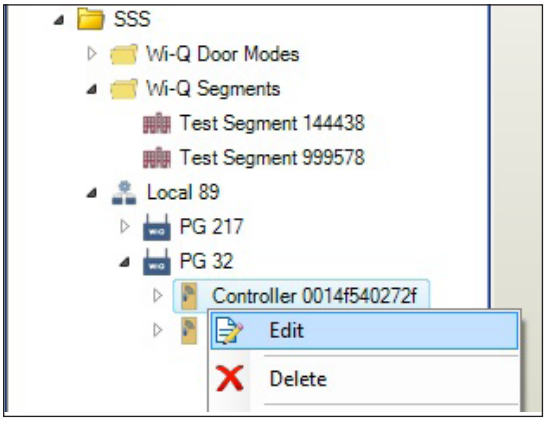


- Enter the controller name and description.
- Enter the MAC address of the controller in the appropriate field.
- Configure the controller as described in the following sections.
- Click Save and Close in the upper left hand corner of the Wi-Q Controller dialog box to finish. The new controller will appear in the hardware tree.

Once the controllers are signed on in the field they should appear in the hardware tree under the Wi-Q Wi-Q Gateways they are assigned to. Now they need to be enabled and configured.

Selecting a Wi-Q Controller

Figure 53 Selecting a Wi-Q Controller to Configure

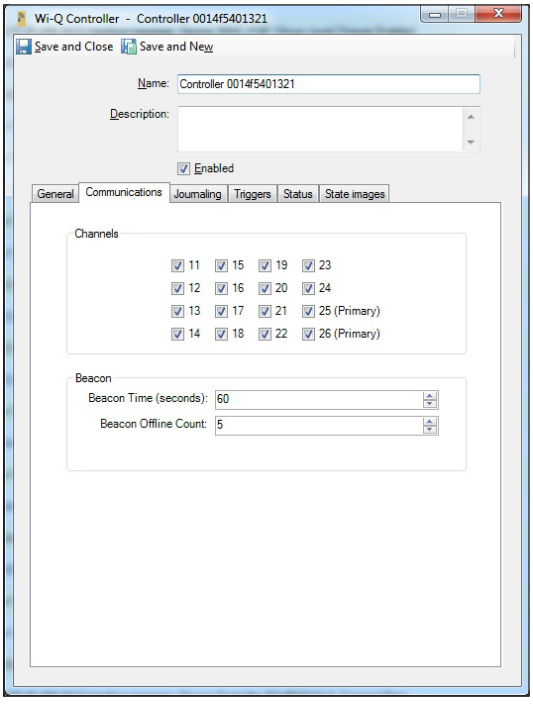


1 Click on the Hardware pane in the left column to display the hardware tree in the display panel and expand the folders, as required, to see the controllers under the Wi-Q Gateways.

2 Right click the controller you are configuring and select **Edit**, or double click the controller icon.

Configuring Wi-Q Controllers - Communications Tab

Figure 54 Configuring Wi-Q Controllers - Communications Tab



1 Click the **Enabled** check box to allow communications.

At this point your Wi-Q controllers have had the minimum configuration to begin operation with the factory defaults. The Wi-Q card readers still need to have card formats assigned. You can click **Save and Close** or continue to change the defaults. For additional configuration, please see "Configuring the Wi-Q Doors and Readers" on page 79.

2 Click the **Communications** tab. By default all of the channels are selected so that a newly installed controller can search through the channels to find a Wi-Q Gateway. Once a controller has found a Wi-Q Gateway, it will continue to use that channel and not search through the channels again unless communications is lost. Generally all of the channels are left selected on the controller and specific channels selected on the Wi-Q Gateway.

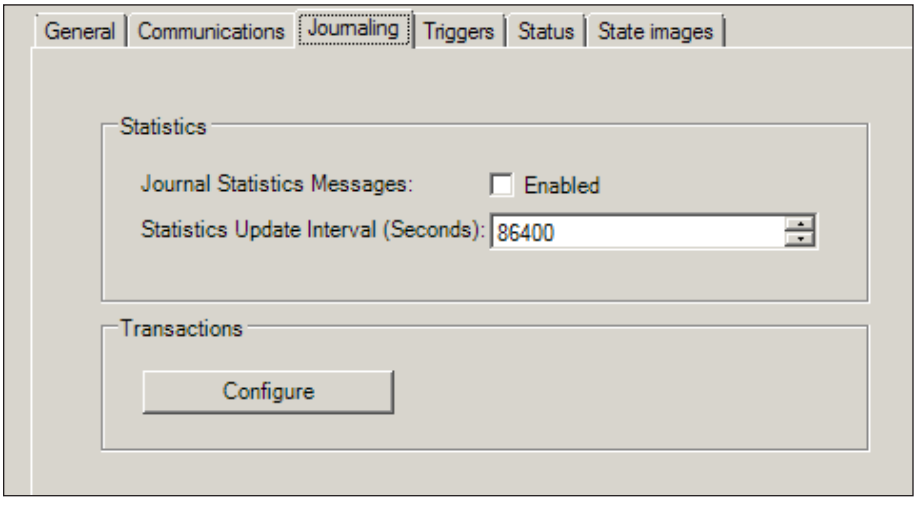
3 The Beacon Time is how often (in seconds) the controller turns on its radio and exchanges messages with its Wi-Q Gateway. Since the controller downloads all of the ID credentials, schedules, etc. to memory, there is no need to be in constant contact. The default is 60 seconds (1 minute), but a value of 10 seconds to 255 seconds (4.25 minutes) may be entered. Keep in mind, the more frequent the beacon time, the more battery power used, so it is not recommended to set it lower than 60 seconds.

4 The Beacon Offline Count is multiplied with the Beacon Time to give a value that is used by the Wi-Q Gateway to time-out its efforts to establish contact with the controller, after which the Wi-Q Gateway

kicks the controller offline and reports the controller as offline to the router. In this example, with a Beacon Time of 60 Sec. times a Beacon Offline Count of 5, it would be 300 Sec. or 5 minutes.

Configuring Wi-Q Controllers - Journaling Tab

Figure 55 Configuring Wi-Q Controllers - Journaling Tab

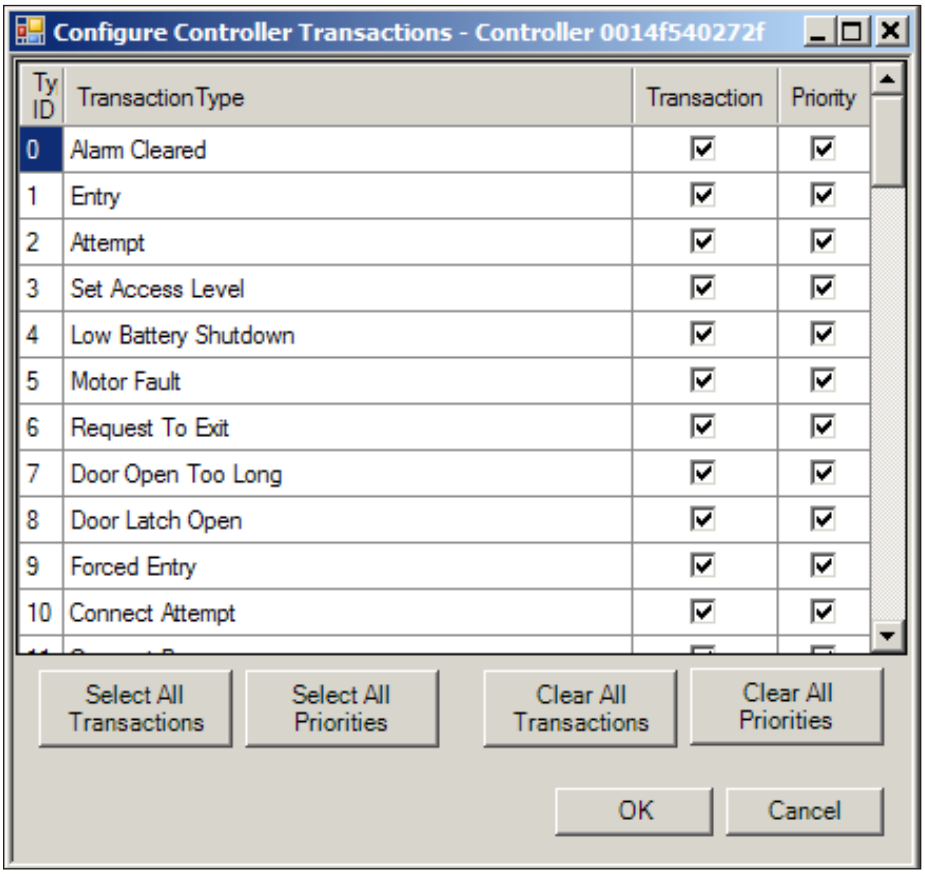


1 Click the **Journaling** Tab.

2 By default, the journaling of statistics is not enabled. If statistics (battery level, signal strength, etc.) are desired, select the **Enabled** check box and enter a value in the Statistics Update Interval box. To reduce traffic and conserve journaling space, it is not necessary to continually upload the statistics, so choose a large value. The default value is 86400 seconds which is 24 hours.

3 Click the **Configure** button in the Transactions box to display the transaction dialog box.

Figure 56 Configuring Wi-Q Controllers - Transactions Dialog Box



4 Select the desired transactions in the transactions column and set their priority in the priority column.

Transactions are events that occur at the door that can be reported to the system. This means that when an event occurs, that is enabled and set to priority, the controller turns on its radio and reports it immediately, regardless of the Beacon setting for uploads. If you uncheck priority for an event, it is going to wait for the regular upload as set by the Beacon setting. Not all events may apply to all installations, so they can be disabled by unchecking their check box in the transactions column.

5 Once the transactions are configured, click **OK** to return to the controller dialog box.

The following additional tabs are available, but no configuration changes are required at this time. See www.swhouse.com for more information.

- General Tab — This tab is auto filled with general information once communications start and can not be changed.
- Triggers Tab — Assigns an action if certain events are detected.
- Status Tab — Shows the Communications status, battery level, etc. for the controller.
- State Images Tab — Displays the icons that will appear in C·CURE monitoring programs.

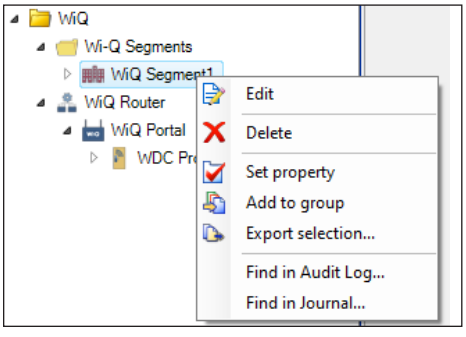
6 Click **Save and Close** in the upper left hand corner of the Wi-Q Controller dialog box to finish.

Options Available when right clicking on the Segment

Right clicking on an item (not a folder) in the hardware tree will provide the following additional options.

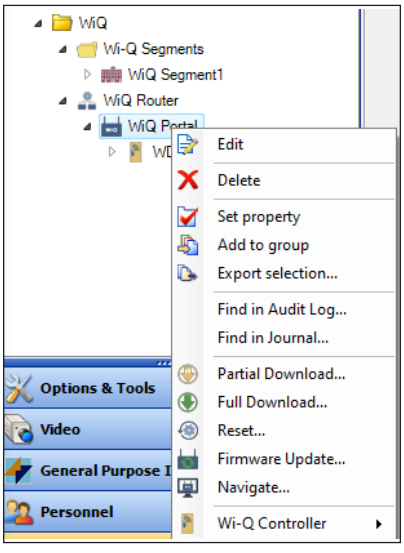
- Segment -> Delete — Allows a segment to be deleted if no Wi-Q Gateways or controllers are associated with it.

Figure 57 Segment Right Click Options



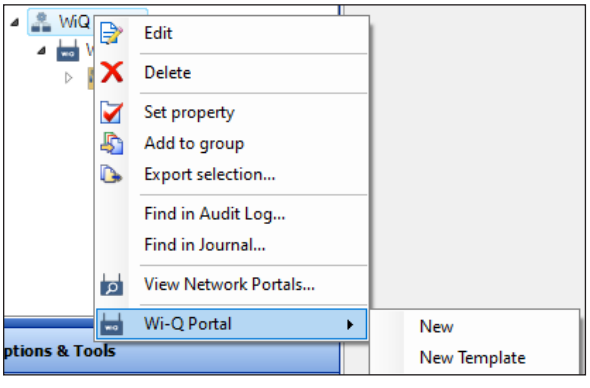
- Portal -> Delete — Allows a Wi-Q Gateway to be deleted if no controllers are associated with it.
- Portal -> Partial Download — Sends a partial download of data to a Wi-Q Gateway.
- Portal -> Full Download — Sends a full download of data to a Wi-Q Gateway.
- Portal -> Reset — Resets a Wi-Q Gateway.
- Portal -> Firmware Update — Updates firmware.
- Portal->Navigate — Opens up the gateway web login page

Figure 58 Portal Right Click Options



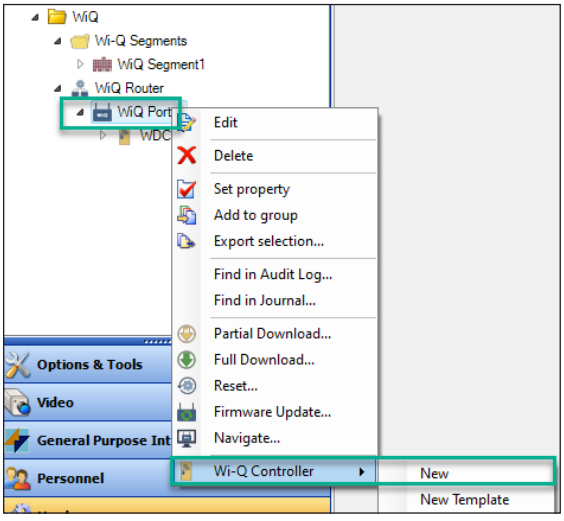
- Router -> Delete — Allows a router to be deleted if no Wi-Q Gateways are associated with it.
- Router -> View Network Portals — Displays the Wi-Q Gateways that are on the network.

Figure 59 Router Right Click Options



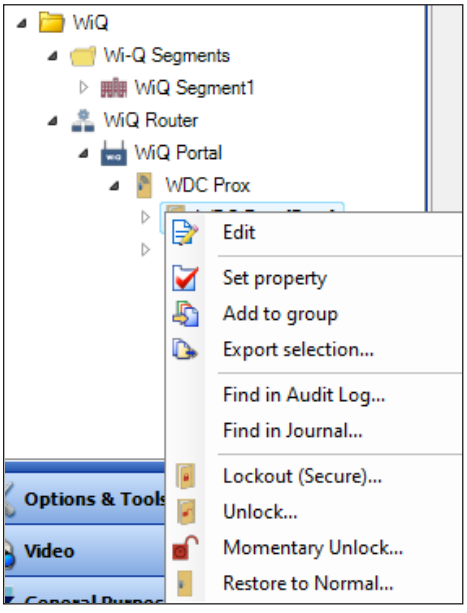
- Controller -> Deep Reset — Sends a deep reset to a controller and returns it to its factory default state.
- Controller -> Full Download — Sends a full download to the associated controller.
- Controller -> Delete — Deletes a controller.
- Controller -> Reset — Resets a controller.
- Controller -> Remove Association — Removes the association between the Wi-Q Controller and Wi-Q Wi-Q Gateway.
- Controller -> Firmware Update — Updates firmware.

Figure 60 Wi-Q Controller



- Door -> Lockout (Secure) — Locked door mode.
- Door -> Unlock — Overrides the door mode to unlock.
- Door -> Momentary Unlock — Unlocks the door for the configured operation time.
- Door -> Restore to Normal — Restores door to the current active door mode

Figure 61 Door Right Click Options



Configuring the Software (Task 10)

In this section, you will find additional notes for configuring C·CURE Wi-Q Doors and Readers, Card Formats, Door Modes, adding the programmer and manager options, creating personnel credential and assigning clearances.

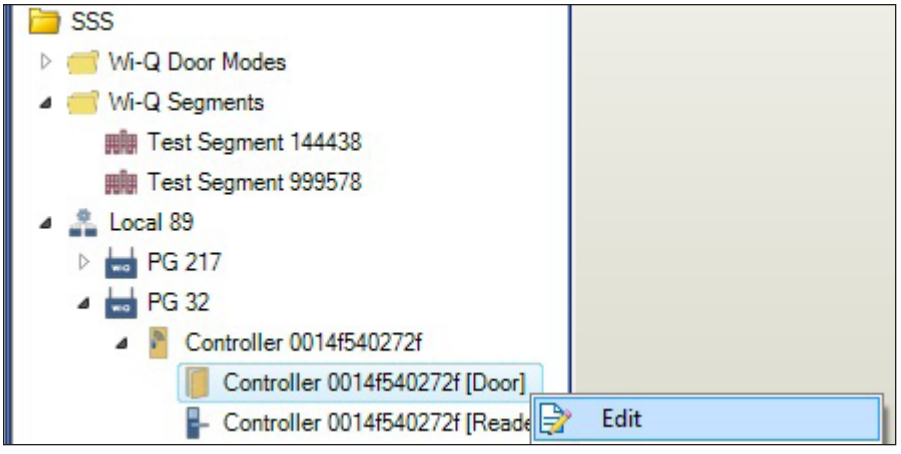
You will also find information about Firmware Updates in the C·CURE Wi-Q Interface Configuration Tool. Finally, you will be provided with a term comparison chart of events/transactions that are viewable in C·CURE Wi-Q Alarm Monitoring and the Controllers tab of C·CURE Wi-Q software.

Configuring the Wi-Q Doors and Readers

C·CURE hardware has 3 separate components; a controller, a door and a reader. The Wi-Q hardware, on the other hand, combines these components into a single unit. When a Wi-Q controller is signed on, the software automatically creates a door and a reader component under the parent controller for configuration purposes.

Selecting and Configuring a Wi-Q Door

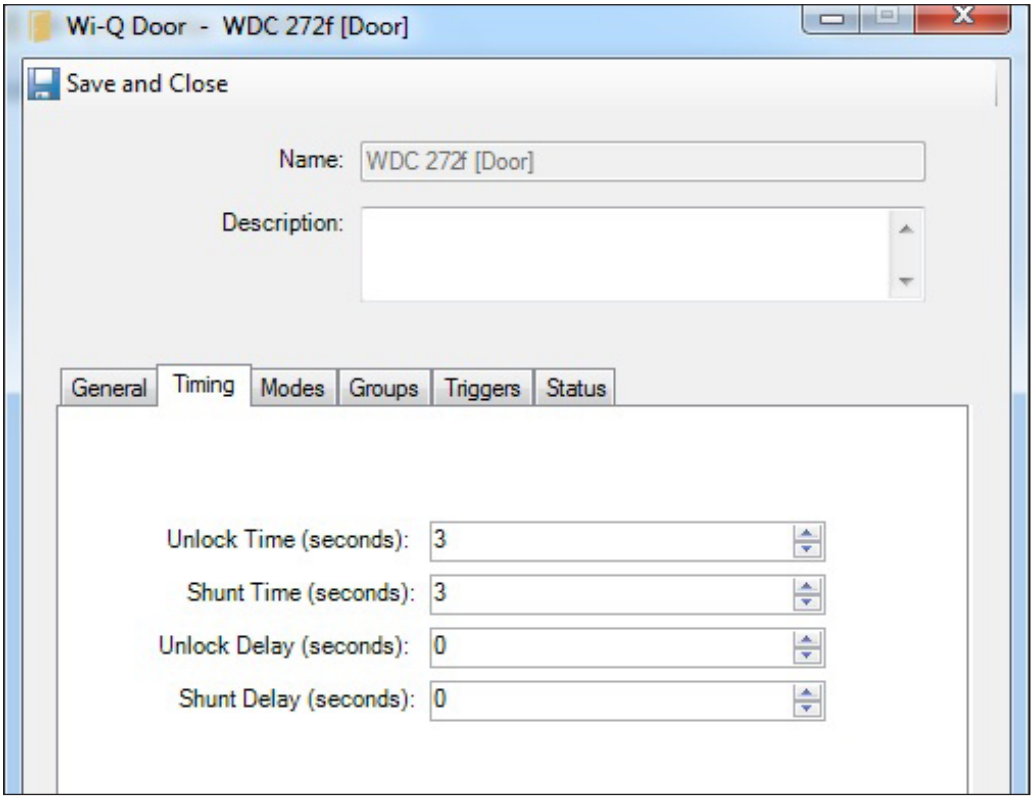
Figure 62 Selecting a Wi-Q Door



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel and expand the folders, as required, to see the door component under its associated controller.

2 Right click the door controller you are configuring and select **Edit**, or double click the controller icon.

Figure 63 Timing



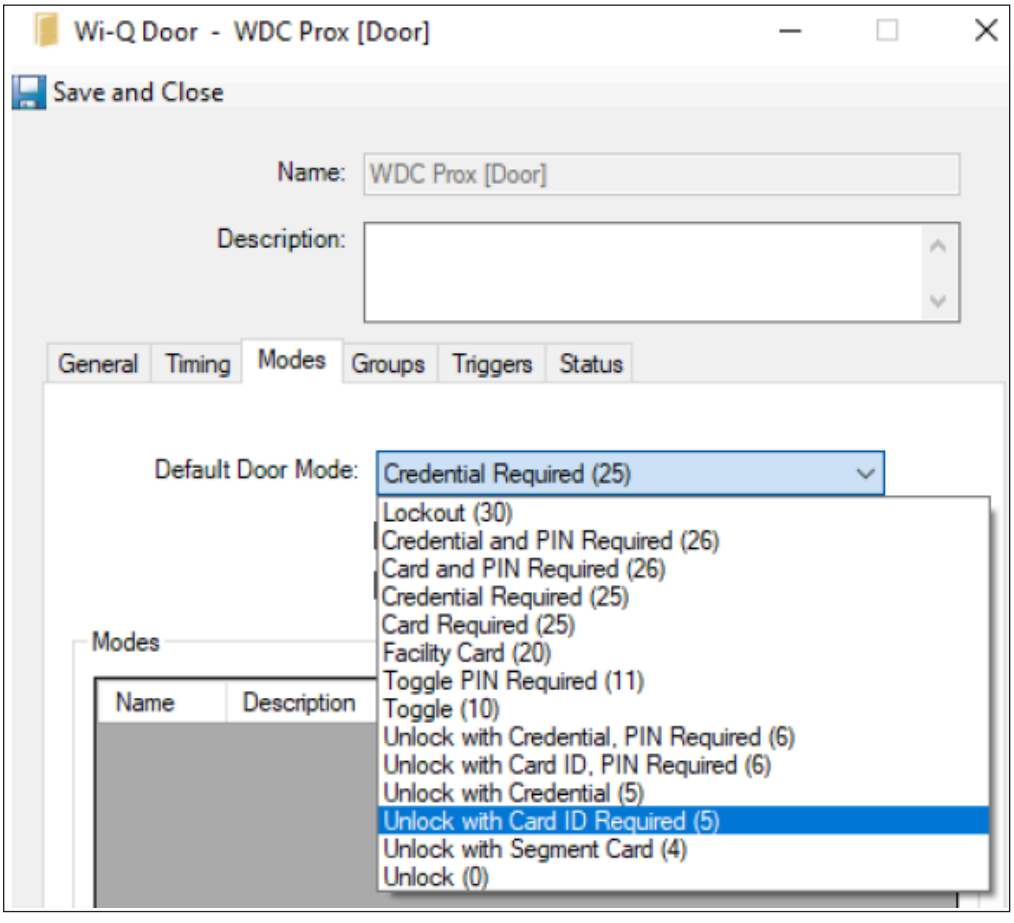
3 Click the **Timing** Tab.

4 Enter values for the following fields:

- UnlockTime — The length of time the latch stays unlocked regardless of door position. The default is 3 seconds.
- Shunt Time — The length of time, after the latch opens, that you have to close the door before door open events are generated. The default is 3 seconds. Increasing this allows more time to move through the door, say if you were using a wheel chair or moving objects.
- Unlock Delay — The length of time between the door recognizing a valid entry and when the latch actually unlocks. Optional. Using a value here will allow time to get to a door if the keypad/reader were located at a distance from the door, say at the foot of a ramp, or if a guard needs to visually verify the user before the door opens.
- Shunt Delay — The length of time until the Shunt Delay starts.

5 Click the **Modes** Tab.

Figure 64 Configuring a Wi-Q Door - Modes Tab



6 Select the desired default door mode from the drop down list. This will be the default door mode when no schedule is active at the door. ID Required is the initial default setting. See the table - "Door Mode Priority Levels" on page 83 for an explanation of the available door modes.

It is the default door mode when a clearance schedule is active, but no door mode is active at the door. The Unlock with Credential Authority Allowed will be configured at the Wi-Q Door level.

The following additional tabs are available, but no configuration changes are required at this time. See www.swhouse.com for more information.

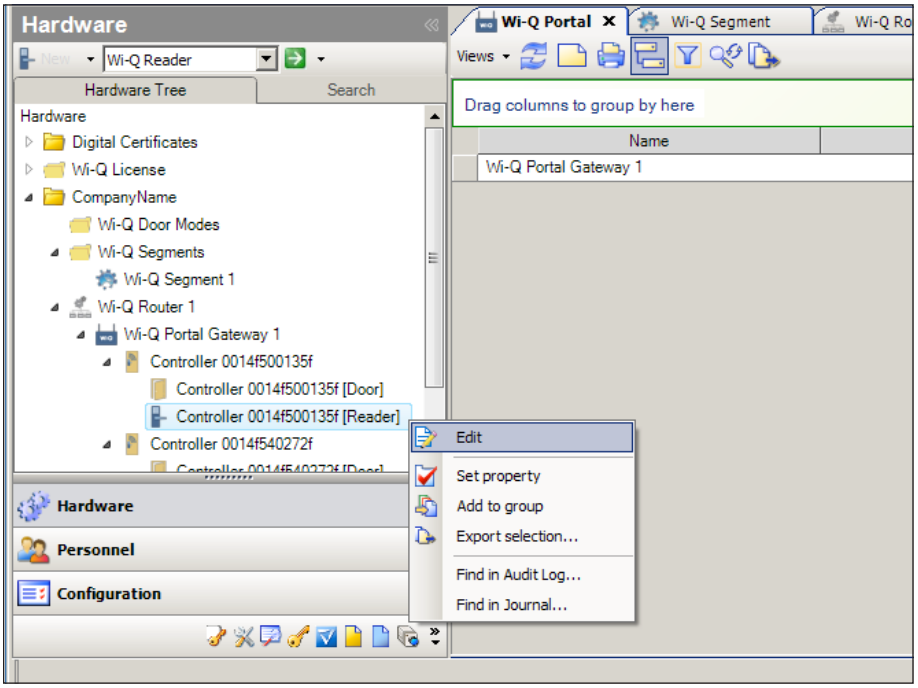
- General Tab — This tab shows the controller associated with the door and can not be changed.
- Groups Tab — Displays the groups that this door belongs to.
- Triggers Tab — Assigns an action if certain events are detected. You must select "Wi-Q Override Access Level" under "Action" to generate Wi-Q options.
- Status Tab — Shows the current status of the door and can not be changed.

7 Click **Save and Close** in the upper left hand corner of the Wi-Q Door dialog box to finish.

Door Mode Priority Levels		
Priority	**Mode**	**What it does ...**
30	Lockout	Only users with special permissions are granted access, such as a manager or programmer. The most secure level, used to lock-down a facility.
26	Credential and PIN Required	After using an credential (card or keypad), a PIN must be entered in the keypad to validate it.
26	Card ID and Pin Required	Only accepts a card, and a PIN must be entered in the keypad to validate it.
25	Credential Required	Accepts card or keypad to validate the credential.
25	Card Required	Locks out the keypad and only accepts a card.
20	Facility Card	Only looks for a facility code on a card without regard to the assigned user.
11	Toggle, PIN Required	Each use of any valid ID will toggle the door between lock and unlock, and a PIN must be entered in the keypad to validate the ID.
10	Toggle	Each use of any valid ID will toggle the door between lock and unlock.
6	Unlock with Credential, Pin Required	Any credential (card or keypad) will unlock the door and it will stay unlocked, and a PIN must be entered in the keypad to validate the credential.
6	Unlock with Card ID and PIN Required	Only accepts a card, and a PIN must be entered in the keypad to unlock the door and it will stay unlocked.
5	Unlock with Credential	Any credential (card or keypad) will unlock the door and it will stay unlocked.
5	Unlock with Card ID Required	Accepts only cards to unlock the door and it stay unlocked.
0	Unlock	The door is unlocked, anyone can open it.

Selecting and Configuring a Wi-Q Reader

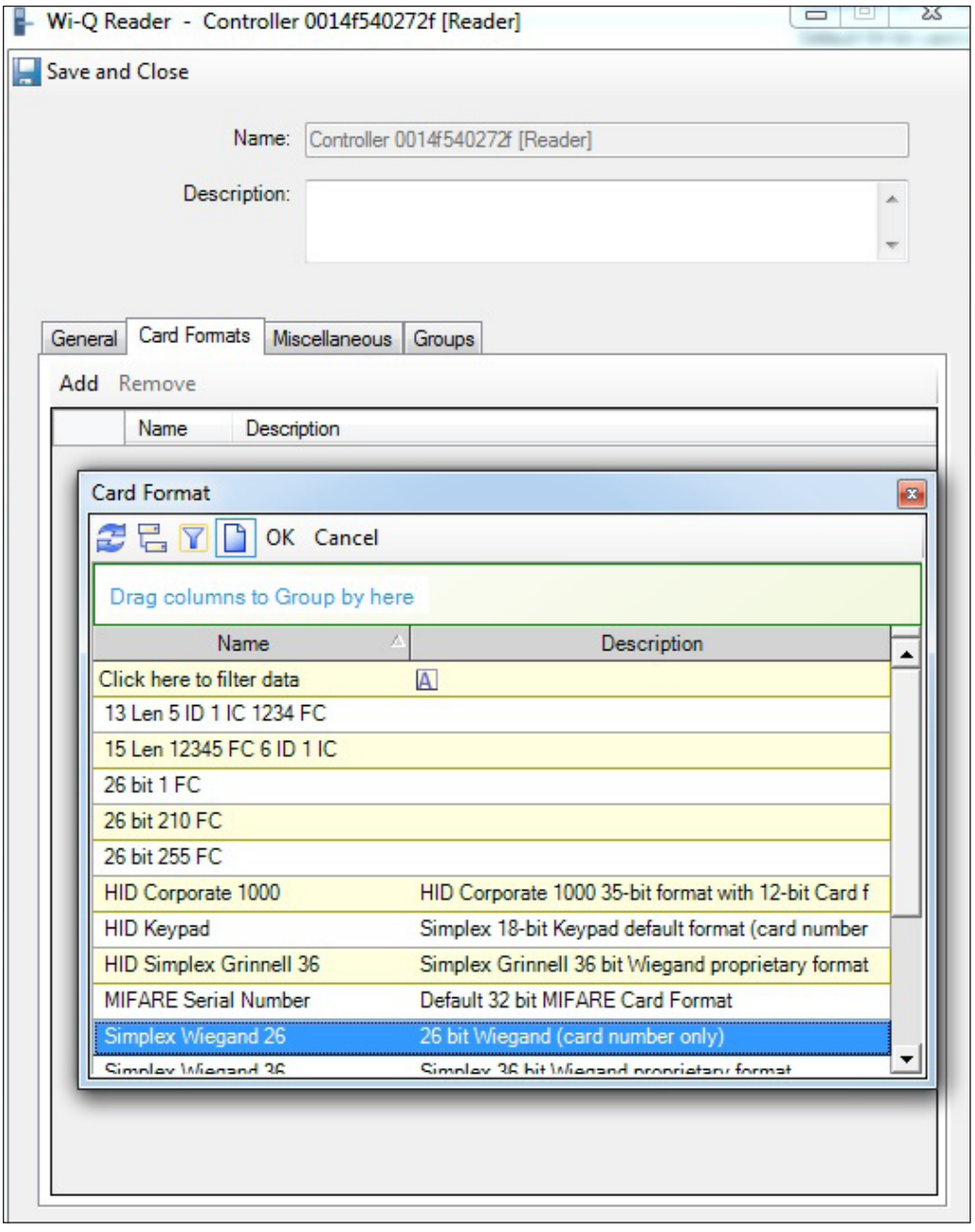
Figure 65 Selecting a Wi-Q Reader



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel and expand the folders, as required, to see the reader component under its associated controller.

2 Right click the door reader you are configuring and select **Edit**, or double click the reader icon.

Figure 66 Configuring a Wi-Q Door Reader



3 Click the **Card Format** tab and click the **Add** button to display the Card Format Dialog Box.

4 Select a previously defined card format from the list. More than one format may be selected by Alt.-clicking the desired formats.

Note Maximum number of card formats that can be entered into the reader is 7.

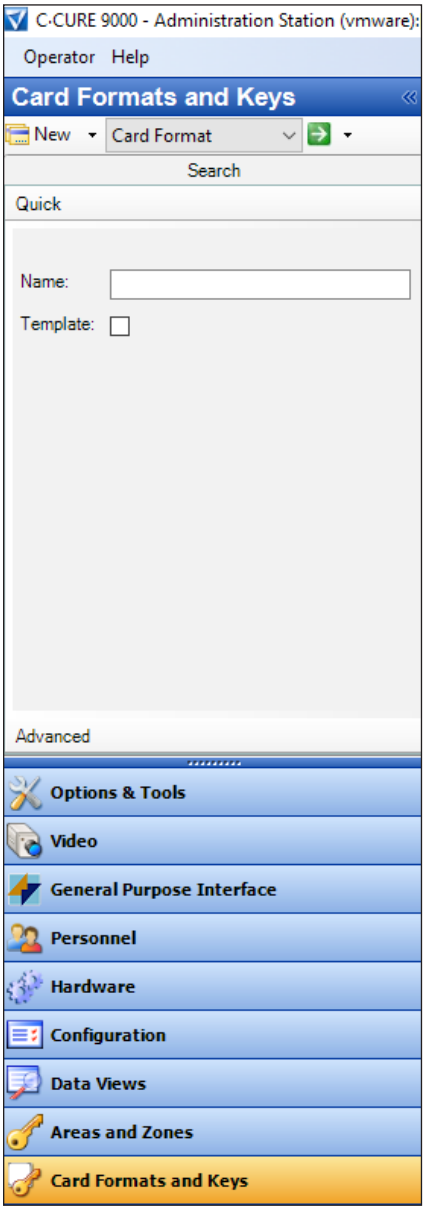
The following additional tabs are available, but no configuration changes are required at this time. See www.swhouse.com for more information.

- General Tab — This tab shows the controller associated with the reader and can not be changed.
- Miscellaneous — Displays information about the Wiegand device if selected. Only applies to WAC hardware types.
- Groups Tab — Displays the groups that this reader belongs to.

5 Click **Save and Close** in the upper left hand corner of the Wi-Q Reader dialog box to finish.

Selecting and Configuring a Card Format

Figure 67 Selecting the Card Format Dialog Box

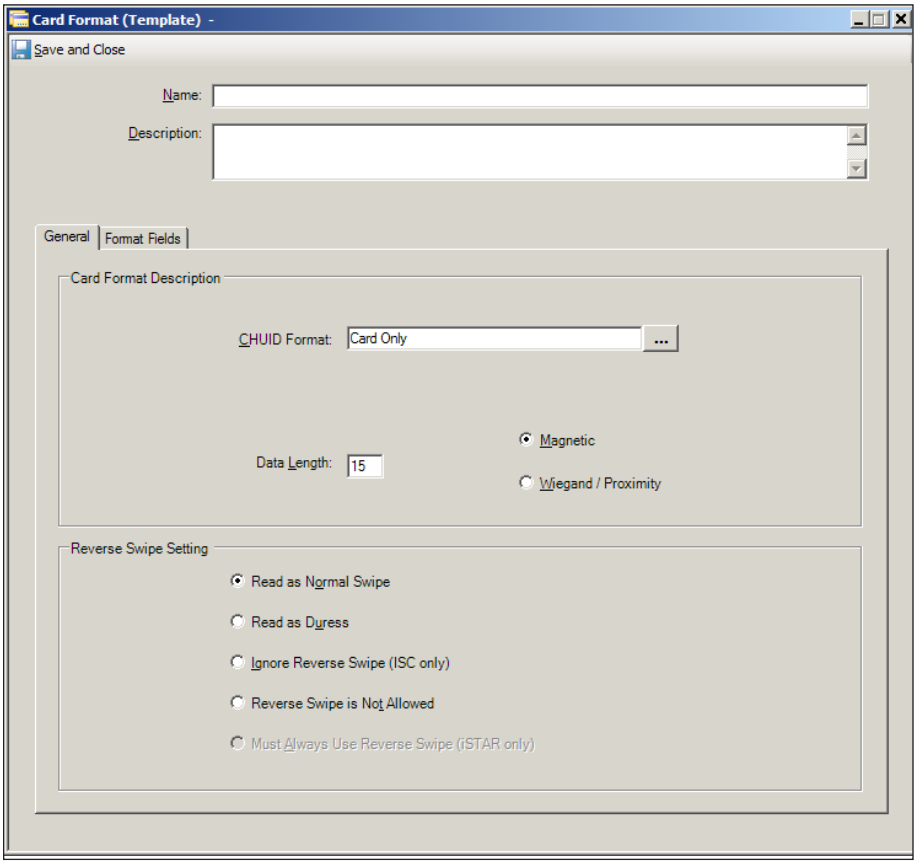


1 Click on the Card Formats and Keys button in the left column and select **Card Format** from the drop-down menu at the top.

2 Click the **New** button next to the drop-down menu and select the desired named template. If there are no named templates in the list, you must first select **New -> Template** to create and save at least one named template.

Creating a Magnetic Card Format

Figure 68 Creating a Magnetic Card Format - General Tab



1 Enter the card format name and description.

2 Click the **General** tab.

3 Select the Ellipsis button to the right of the CHUID Format box and select **Card Only**. This applies to all Wi-Q readers that accepts cards.

4 Click the Magnetic card type radio button.

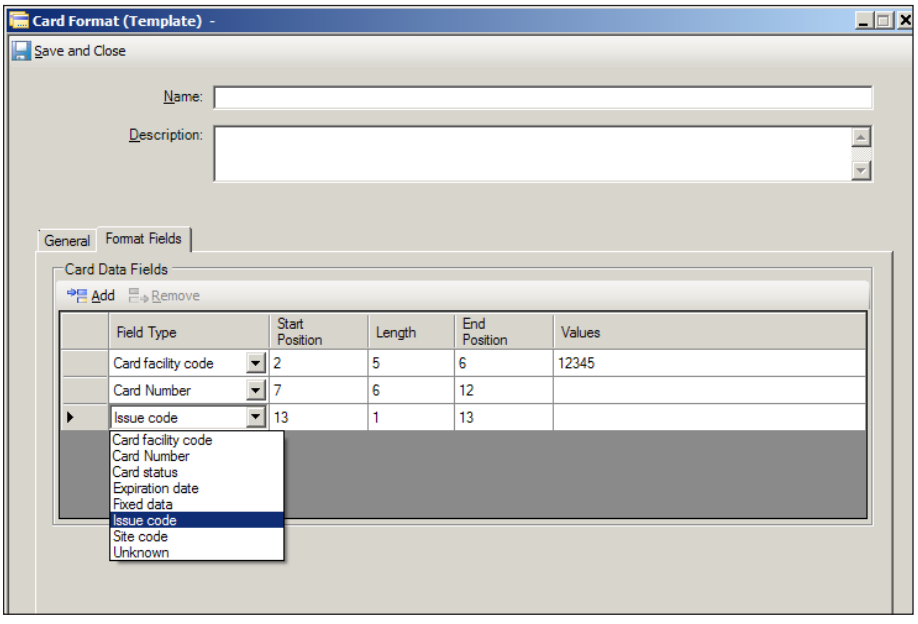
5 Enter the total length of the data on the card including any format characters.

Note On magnetic cards the data format has 3 invisible characters, a start character at the beginning, with an end character and a check sum at the end. These 3 extra characters must be included in the data length. So if the data fields add up to 12 characters long, the data length would be 15.

6 A reverse swipe is not supported in the Wi-Q hardware, so the reverse swipe settings can be ignored.

7 Click the **Format** tab.

Figure 69 Creating a Magnetic Card format - Format Tab



8 Click the **Add** button for a new data field and select the Field Type from the drop down menu.

9 Enter the start position, length of the data field, and the end position.

Note The card format has an invisible start character at the beginning in position 1, so the start position of the first field is 2.

10 If a default value needs to be entered, double click in the values data field and an Ellipsis button will appear to the right of it. Clicking this button will bring up a Values dialog box. Enter a single value in the dialog box list and save. The value will appear in the Values column. In this example a facility code of 12345 is entered.

Note Wi-Q only supports a single value in the Values data field.

11 Click the **Add** button to list additional data fields and then enter their start positions, length and end positions (and default values if applicable).

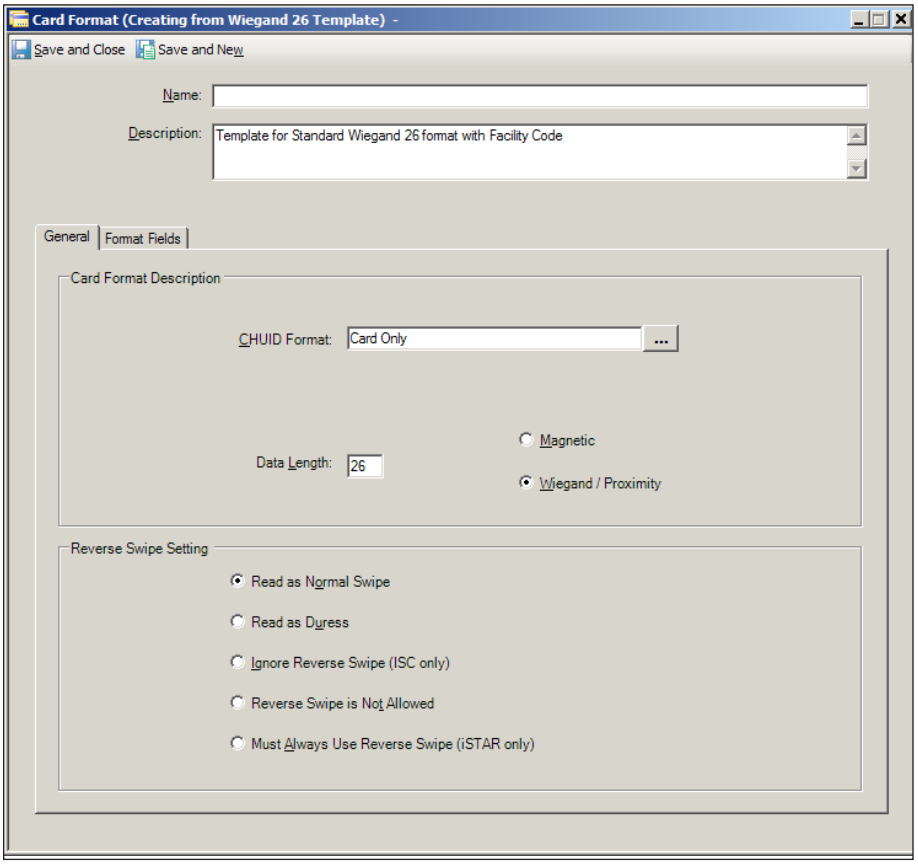
Note The Wi-Q controllers only use the Facility Code, Card Number and Issue Code data fields. Any additional data is ignored by the controllers.

Note The end position of the last data field must be at least 2 less than the total data length entered in the general tab to allow for the end and the check sum characters.

12 Click **Save and Close** in the upper left hand corner of the Card Format dialog box to finish.

Creating a Proximity Card Format

Figure 70 Creating a Proximity Card Format - General Tab



1 Enter the card format name and description.

2 Click the **General** tab.

3 Select the Ellipsis button to the right of the CHUID Format box and select **Card Only**. This applies to all Wi-Q readers that accepts cards.

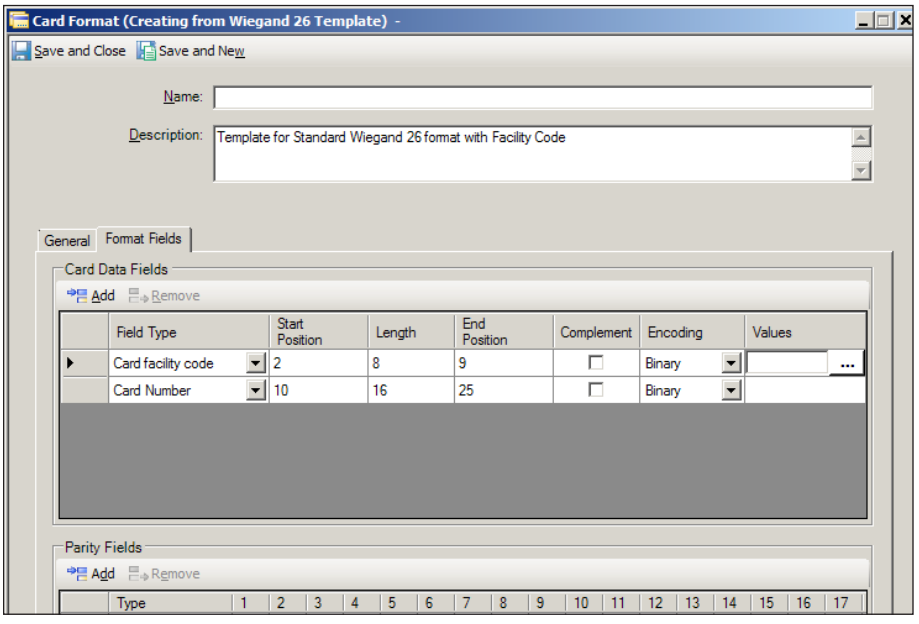
4 Click the Wiegand/Proximity card type radio button.

5 Enter the total length of the data on the card in bits.

6 A reverse swipe is not applicable to a Proximity card, so the reverse swipe settings can be ignored.

7 Click the **Format** tab.

Figure 71 Creating a Proximity Card format - Format Tab



8 Click the **Add** button for a new data field and select the Field Type from the drop down menu.

9 Enter the start position, length of the data field, and the end position.

Note On Proximity cards, the start position of the first field is 2.

10 If a default value needs to be entered, double click in the values data field and an Ellipsis button will appear to the right of it. Clicking this button will bring up a Values dialog box. Enter a single value in the dialog box list and save. The value will appear in the Values column.

Note Wi-Q only supports a single value in the Values data field.

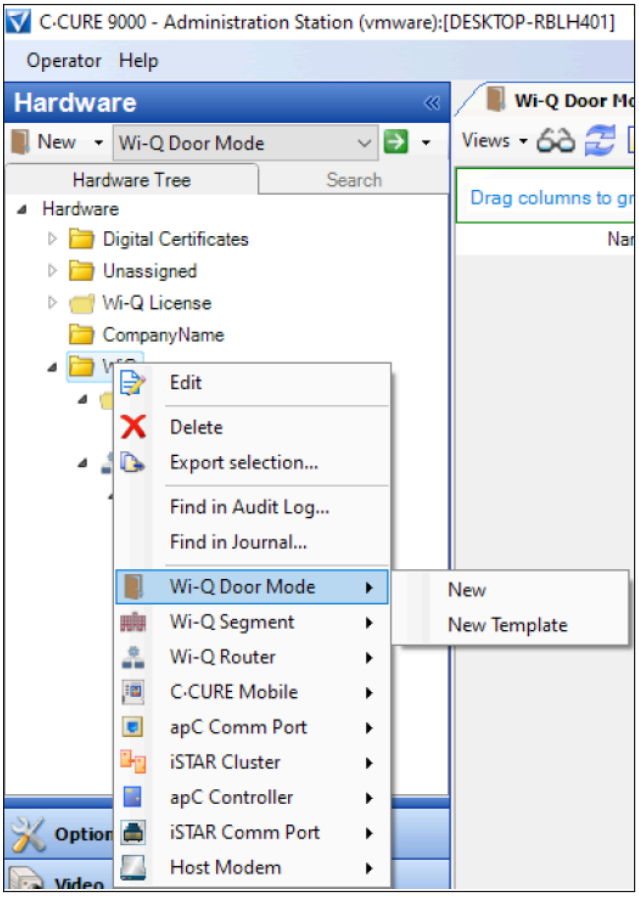
11 Click the **Add** button to list additional data fields and then enter their start positions, length and end positions (and default values if applicable).

Note The Wi-Q controllers only use the Facility Code, Card Number and Issue Code data fields. Any additional data is ignored by the controllers.

12 Click **Save and Close** in the upper left hand corner of the Card Format dialog box to finish.

Adding Wi-Q Door Modes

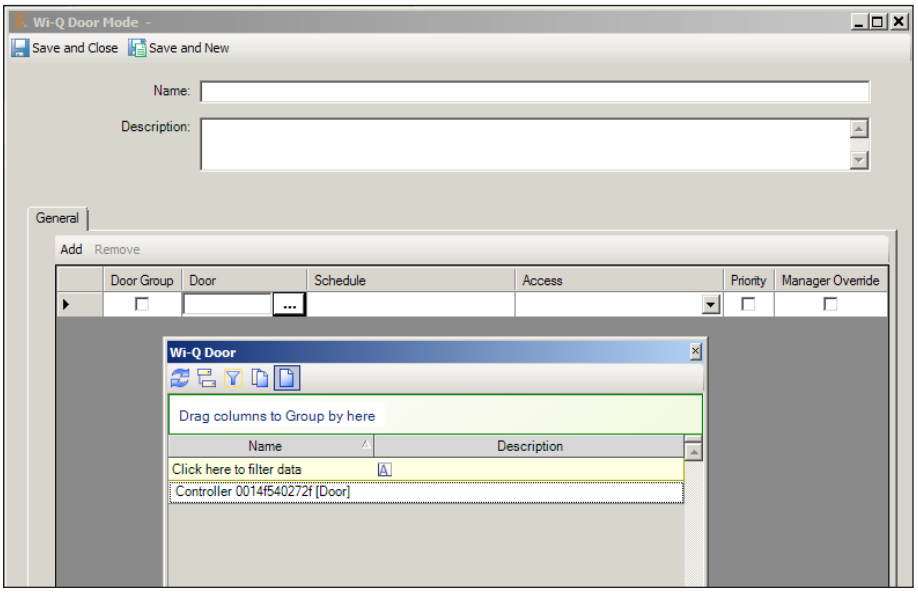
Figure 72 Adding a New Wi-Q Door Mode.



1 Click on the Hardware pane in the left column to display the hardware tree in the display panel if it is not already displayed.

2 Right click the Hardware folder in the hardware tree (In this example it is named CompanyName) and select **Wi-Q Door Mode -> New.** A new Wi-Q door modes folder is created under the Hardware folder and a Door Mode dialog box appears.

Figure 73 Assigning a Wi-Q Door Mode



1 Enter the door mode name and description.

2 Click the **Add** button to enter a new row of door mode data fields.

3 Select the Door field, pause, and then click again. Click the drop down button that appears to the right of the field and select a door from the list of signed on doors in the dialog box that appears.

4 Select the Schedule field, pause, and then click again. Click the Ellipsis button that appears to the right of the field and select a schedule from the list in the dialog box that appears. Schedules are basically blocks of time.

Note To create schedules, see the appropriate C·CURE 9000 Manual on www.swhouse.com.

5 Select the Access field, pause, and then click again. Click the Ellipsis button that appears to the right of the field. From the list in the dialog box that appears, select the Door Mode that applies to the selected schedule. The drop down menu will close and the selected mode will be filled into the Access field.

6 If desired, select the Priority check box to increase the priority level of this access door mode as described in "Door Mode Priority Levels" on page 94.

7 Select the Manager override check box to give managers all access privileges.

Note During the highest priority door mode — Lockout, only a programmer's credential is granted access. By checking Manager override, the same level of access is granted to credentials designated as managers.

Note Personnel must be added to the Programmer or Manager group to enable this option.

Door Mode Priority Levels

There are 13 door modes and each is ranked by a priority level from 30 (most secure) to zero (least secure). If the door has been mistakenly or intentionally set with overlapping schedules with different door modes, the door will be set to the door mode with the highest priority level.

If the priority check box has been selected for a given door mode, it then goes to the top of the list and becomes the highest priority level. If multiple door modes have their priority check boxes selected, they all go to the top of the list and are sorted among themselves according to their original priority rankings. You can think of checking the priority check box as adding 30 to a door mode's original level of priority. If a level 6 door mode is checked as priority, you can think of it as a level 36 and would now be the highest priority, but if later a level 11 is checked as priority, it becomes a level 41 and is now the highest level over the level 36 and so on. A level 10 checked would become a level 40 and be ranked between the two.

Door Mode Priority Levels		
Priority	**Mode**	**What it does ...**
30	Lockout	Only users with special permissions are granted access, such as a manager or programmer. The most secure level, used to lock-down a facility.
26	Credential and PIN Required	After using an credential (card or keypad), a PIN must be entered in the keypad to validate it.
26	Card ID and Pin Required	Only accepts a card, and a PIN must be entered in the keypad to validate it.
25	Credential Required	Accepts card or keypad to validate the credential.
25	Card Required	Locks out the keypad and only accepts a card.
20	Facility Card	Only looks for a facility code on a card without regard to the assigned user.
11	Toggle, PIN Required	Each use of any valid ID will toggle the door between lock and unlock, and a PIN must be entered in the keypad to validate the ID.
10	Toggle	Each use of any valid ID will toggle the door between lock and unlock.
6	Unlock with Credential and Pin Required	Any credential (card or keypad) will unlock the door and it will stay unlocked, and a PIN must be entered in the keypad to validate the credential.
6	Unlock with Card ID and PIN Required	Only accepts a card, and a PIN must be entered in the keypad to unlock the door and it will stay unlocked.
5	Unlock with Credential	Any credential (card or keypad) will unlock the door and it will stay unlocked.
5	Unlock with Card ID Required	Accepts only cards to unlock the door and it stay unlocked.
0	Unlock	The door is unlocked, anyone can open it.

Configuring Events with Wi-Q Hardware

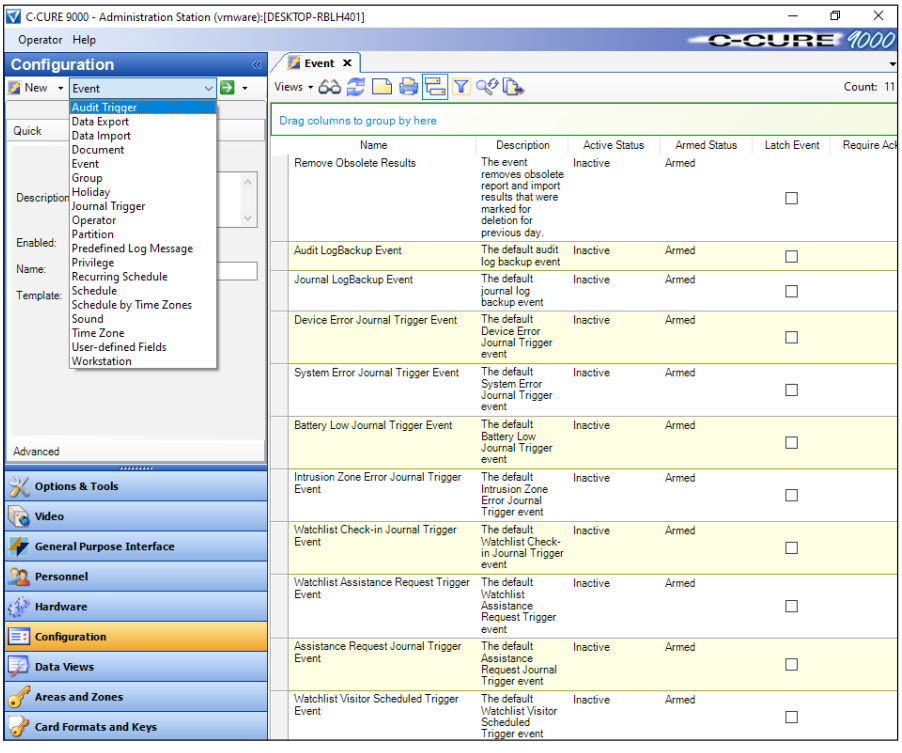
The default Event Actions in C-Cure are not supported by Wi-Q Hardware. A Wi-Q specific Action, named "Wi-Q Override Access Level", has been added to the list of selectable Actions when creating an Event. This allows Triggers to, upon activation, override the current door mode of a Wi-Q door.

Note Wi-Q devices are visible and selectable for default C-Cure Actions, such as Momentary Unlock Door, however, as stated above, these Actions will not function if a Wi-Q device is selected.

Note The use of Triggers has remained unchanged, and can be configured to perform any Action that follows the previously stated restrictions.

Note Every other part of events and triggers work the same as in C·CURE.

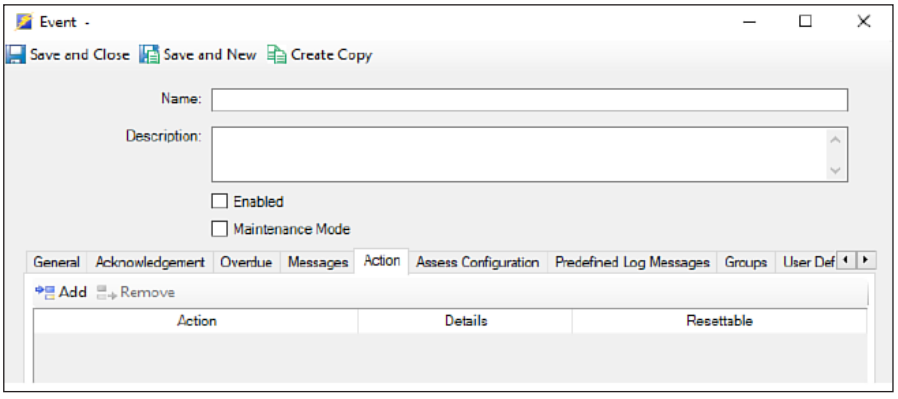
Figure 74 Adding an Event for use with the Wi-Q Hardware



1 Click on the **Configuration** button in the left column.

2 Select **Event** from the Configuration drop down menu at the top and click the **New** button to the left.

Figure 75 New Event Dialog Box

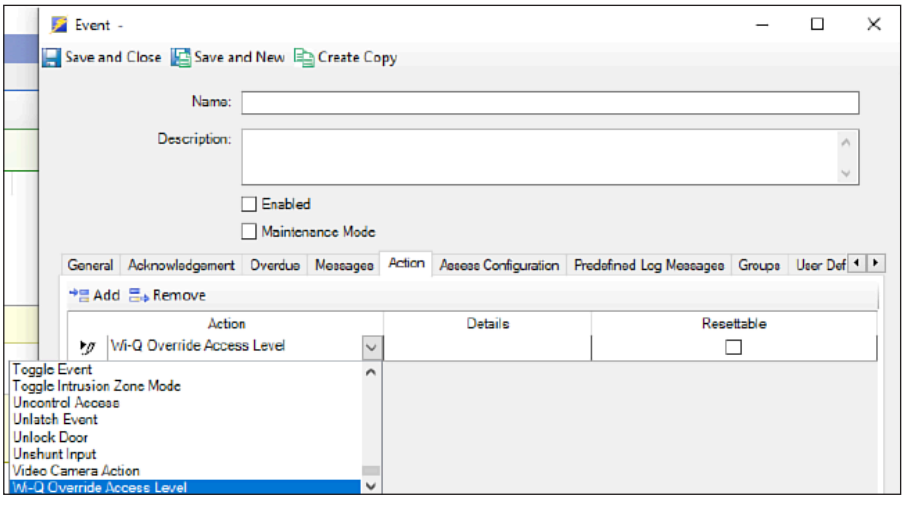


3 Enter the event name and description.

4 Click the **Enabled** check box to allow communications.

5 Click the **Action** tab.

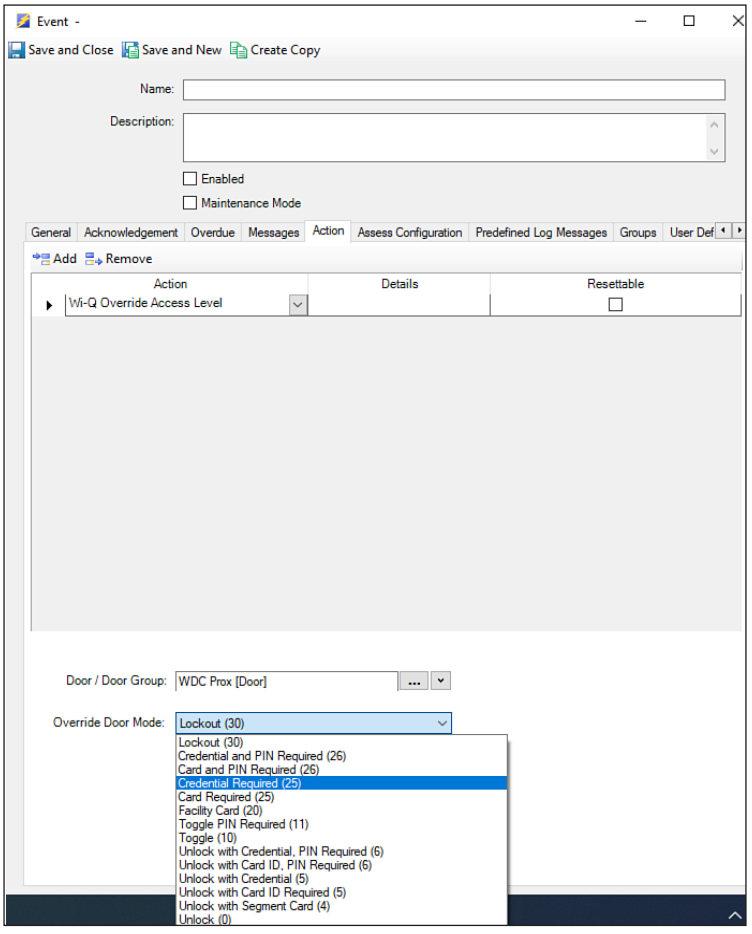
Figure 76 Event Dialog Box - Action Tab



6 Click the **Add** button to add a new event row.

7 Select **Wi-Q Override Access Level** from the Action column drop down menu and the Door / Door Group and Override Door Mode fields will appear at the bottom of the dialog box.

Figure 77 Event Dialog Box - Override Door Mode



8 Click the **Ellipsis** button next to Door / Door Group field and select the desired door or door group from the dialog box that appears.

9 Select a new **Door mode priority level** from the **Override Door Mode** drop down menu.

Adding Programmer and Manager to the Personnel Types

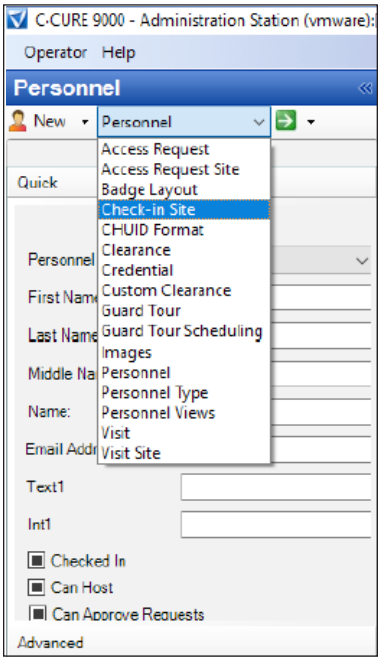
In order to make personnel managers or programmers, they must be added to either the Managers or Programmers group, which were created during the Wi-Q Interface Software installation.

Adding Unlock with Credential, Passage Mode, and Deadbolt Authority to the Personnel Types

In order to give personnel Unlock with ID and/or Passage Mode Authority, they must be added to the Unlock with Credential and/or Passage Mode Authority groups, which were created during the Wi-Q Interface Software installation.

Wi-Q Considerations when Creating Personnel Credentials

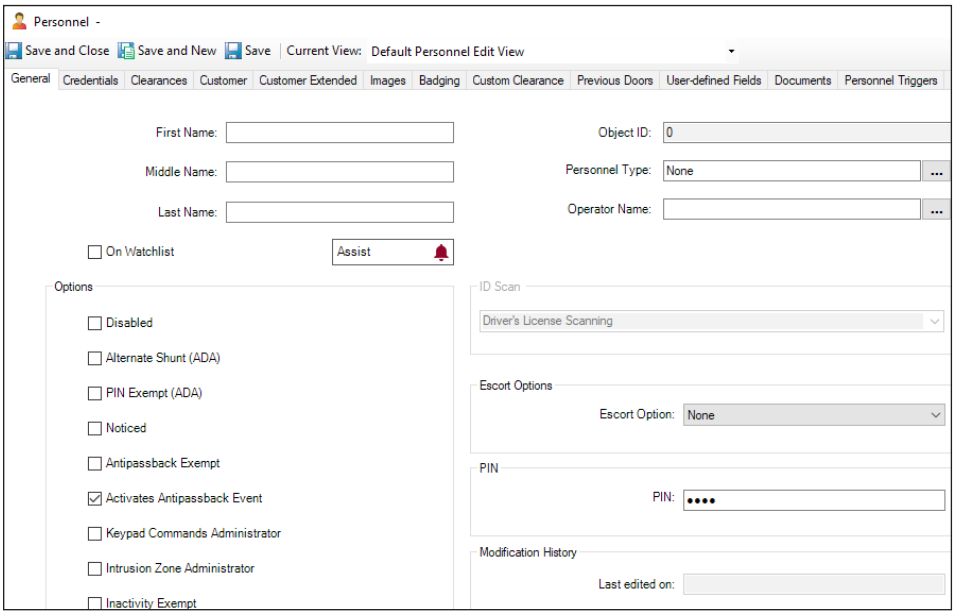
Figure 78 Selecting the Personnel Dialog Box



1 Click on the Personnel button in the left column.

2 Select **Personnel** from the Personnel drop down menu at the top and click the **New** button to the left.

Figure 79 Personnel Dialog Box - General Tab



1 Click the **General** tab.

2 Fill in the users personal information.

3 In the Personnel Type field click the Ellipsis button and select the personnel type.

4 In the Operator field click the Ellipsis button and select the operator name if applicable.

5 Enter a PIN (Personnel Identification Number), if one is to be assigned, to authenticate a card (or keypad) entry ID using a keypad. Only assign a PIN here if your readers have keypads. The PIN is not shown as it is entered, but when moving to another field, a dialog box appears to confirm the PIN.

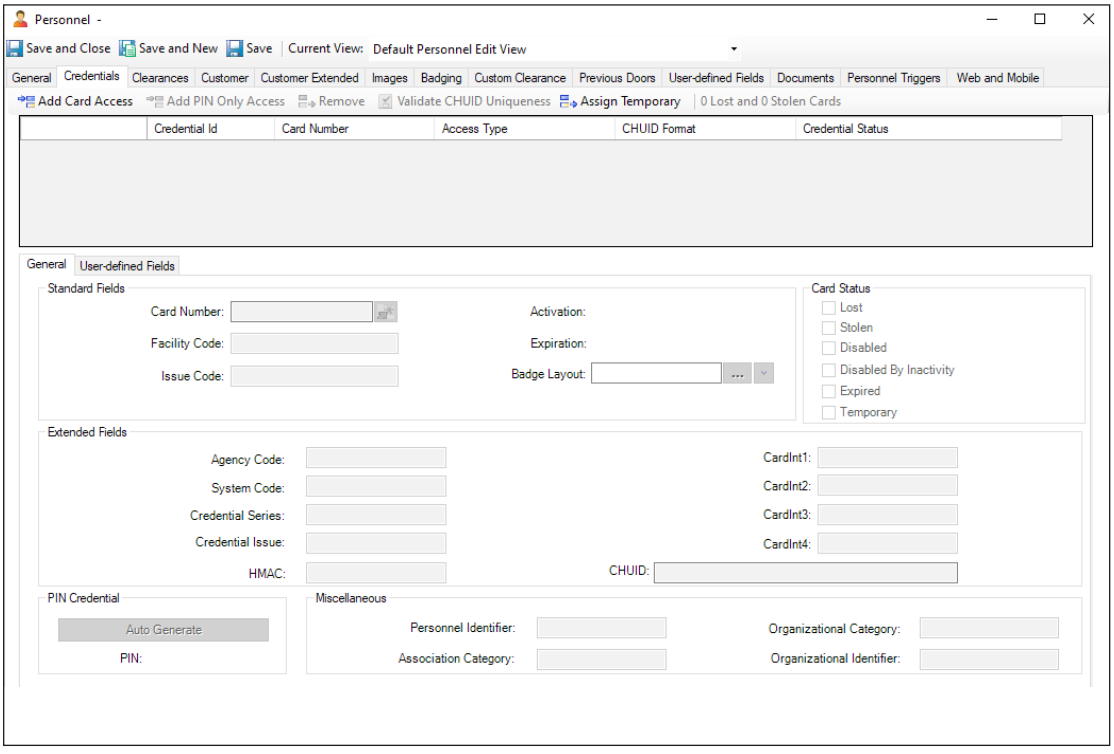
6 The following are options that are supported:

- General tab->Options box->Disabled (disables user)
- General tab->Options box->Alternate Shunt (if this is checked, the OverrideOperateTime and OverrideShuntTime will be set to the values defined in the Interface.dll.config file)
- General tab->PIN (used for pin value if general pin is being used)
- Credentials tab->Card Number, Issue Code, Expiration (translated to Wi-Q)
- Credentials tab->Card Status Lost, Stolen, Disabled (removes user)
- Credentials tab->PIN Credential (used if not general pin used)
- Credentials tab->Access Type (only Card Access and PIN Only)
- All of the Clearances tab.

For more information on options and the PIN, see the appropriate C·CURE 9000 Manual on www.swhouse.com.

7 Click the **Credentials** tab.

Figure 80 The Personnel Dialog Box - Credentials Tab



1 Click the Add Card Access button above the Credential List box at the top and enter the card number in the Card Number field. It will automatically fill in the Card Number field in the Standard Fields box when you move to a new field.

2 Enter the Facility Code and the Issue Code in the Standard Fields box. The card number, facility code and issue code are the data contained on the card.

3 Click the Add Card Access button above the Credential List box at the top to add more cards.

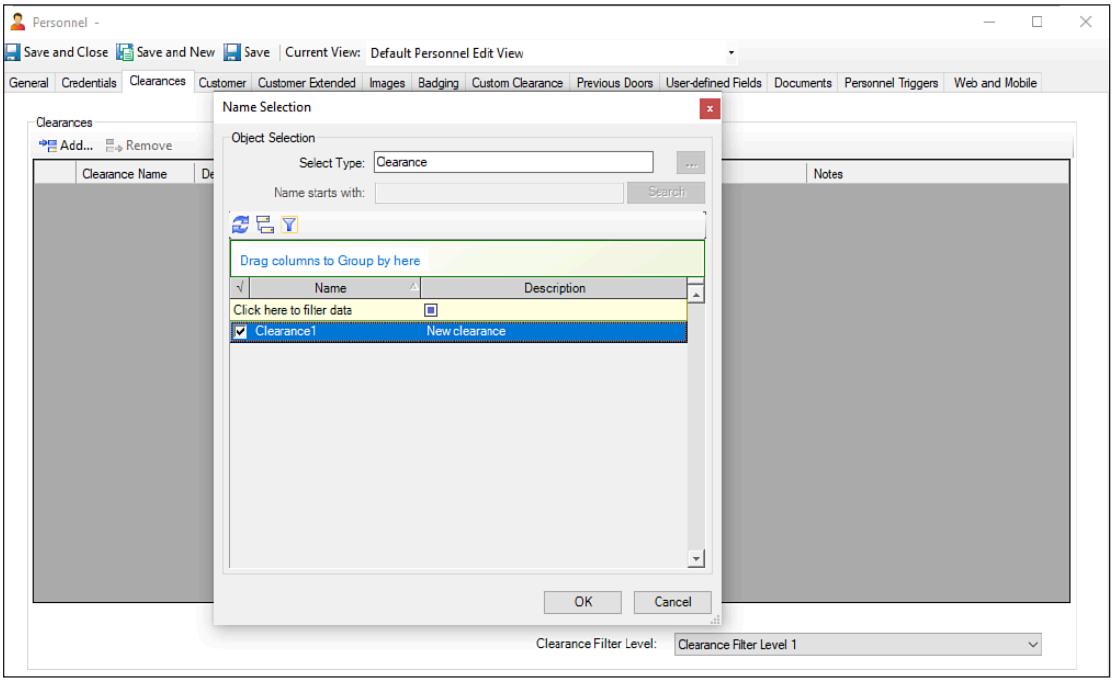
4 To use a keypad entry, click the Add PIN Only Access button above the Credential List box at the top and click the Auto Generate button in the PIN Credential box in the lower left corner. This generates the keypad PIN credential, where the PIN under the General tab is the authentication PIN for either a card or keypad entry.

Note Wi-Q only supports one keypad PIN credential.

Note The **Add PIN Only Access** buttons and **Auto Generate** button are only available when enabled in the C·CURE 9000 software. See "Enabling Keypads for Wi-Q in C·CURE 9000" on page 105. See the appropriate C·CURE 9000 Manual on www.swhouse.com for information on the other fields in the Personnel dialog box.

5 Click the Clearances tab.

Figure 81 Personnel Dialog Box - Clearances Tab



6 Click the **Add ...** button below the Clearances box to display the Clearance dialog box.

7 Select the clearances to assign to this user. Shift-click or Alt.-click to select multiple clearances.

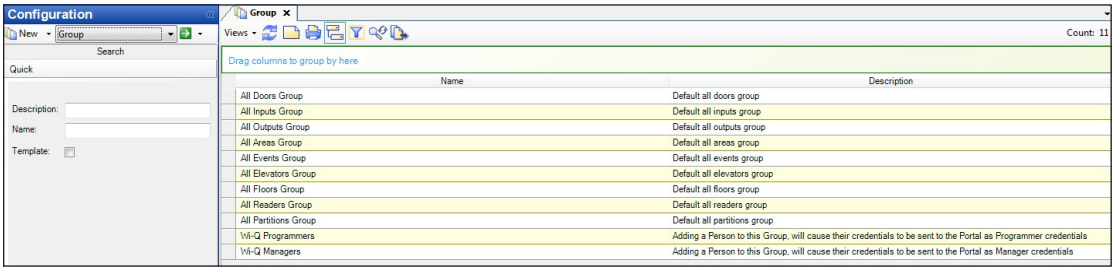
8 Click the **OK** button in the header of the Clearance dialog box. The dialog box will close and the assigned clearances will appear as a list in the clearances box.

9 Click **Save and Close** in the upper left hand corner of the Personnel dialog box to finish.

Adding the Programmer and Manager Personnel Types

1 Select the Configuration Navigation pane.

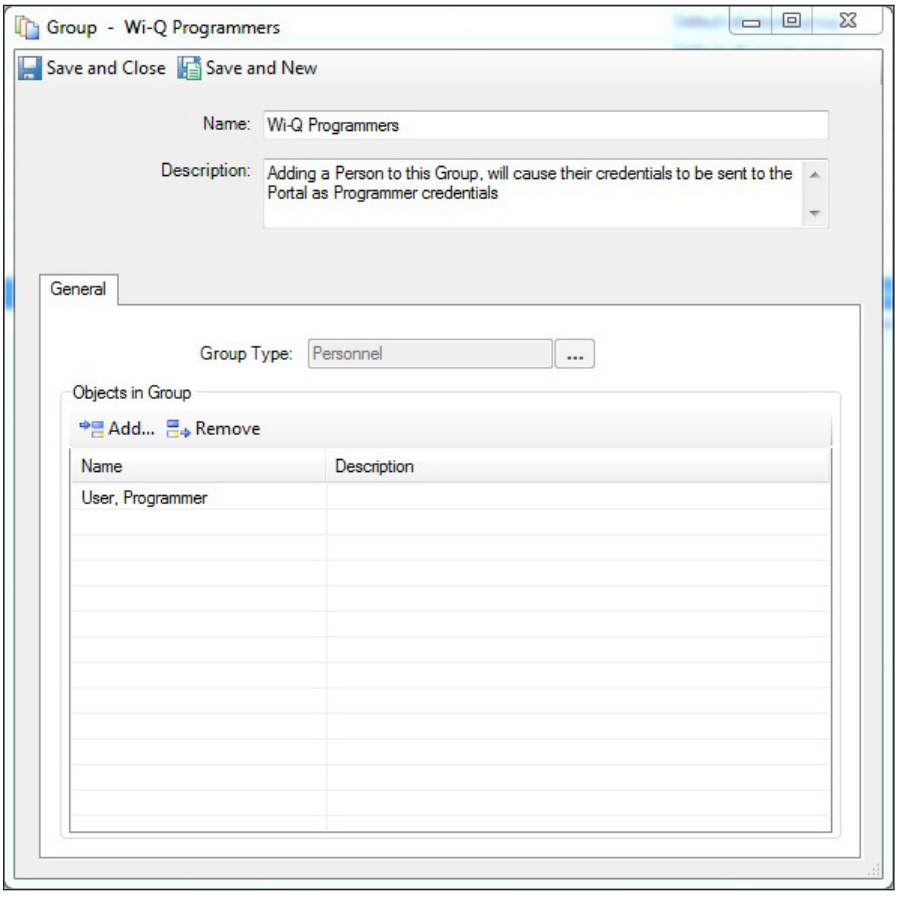
Figure 82 Selecting the Configuraion Navigation Pane



2 Select Group from the drop down menu and click the green arrow button.

3 Edit the Wi-Q Programmers/Wi-Q Managers Group to add the personnel to the group.

Figure 83 Edit Wi-Q Programmers/Wi-Q Managers Group

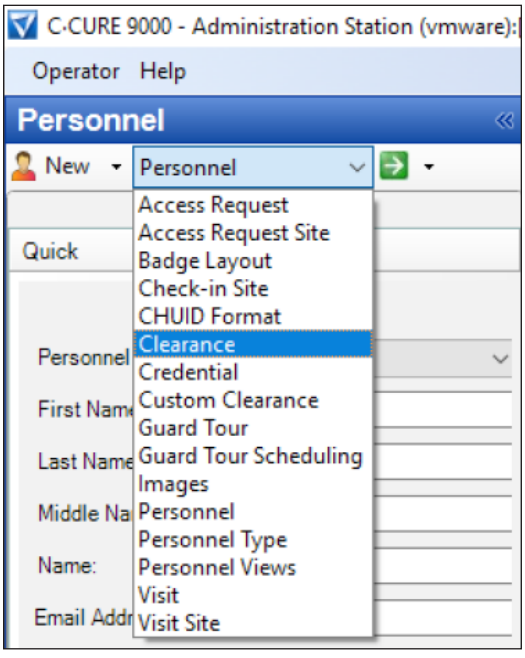


4 Select the Add button and select the personnel to be made a Programmer/Manager.

5 Select the Save and Close button.

Creating Clearances

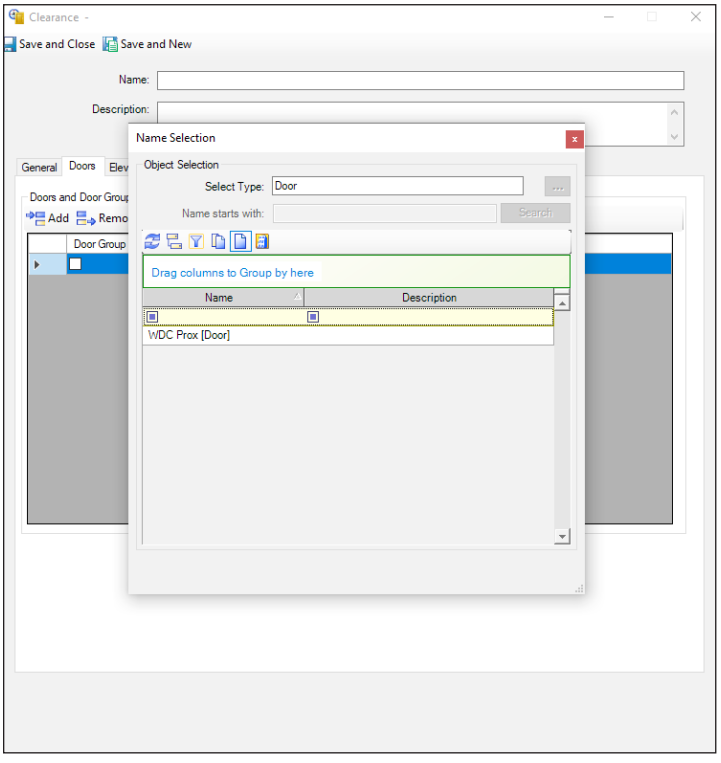
Figure 84 Selecting the Clearances Dialog Box



1 Click on the Personnel button in the left column.

2 Select **Clearance** from the Personnel drop down menu at the top and click the **New** button to the left.

Figure 85 The Clearances Dialog Box - Doors Tab



3 Enter the clearance name and a description.

4 Click the **Doors** tab.

5 Click the **Add** button at the top of the Doors and Door Group box to add a door.

6 Click in the Door Name field and then click the Ellipsis button that appears to the right, to display the Door dialog box. (This step is required only during editing an existing Door in the Door Name field.)

7 Select an individual door or a door group from the list. The dialog box will close and the door name will be filled into the Door Name field, and if it is a group, the Door Group check box is checked.

Note Click the icon depicting two pages in the top header of the Door dialog box to display the door groups in the list. The icon depicting a single page toggles between showing groups and single items.

8 Click in the Schedule field and then click the Ellipsis button that appears to the right, to get the Schedule dialog box. (This step is required only during editing an existing Schedule in the Door Schedule field.)

9 Select a schedule from the list. The dialog box will close and the schedule name will be filled into the Door Schedule field.

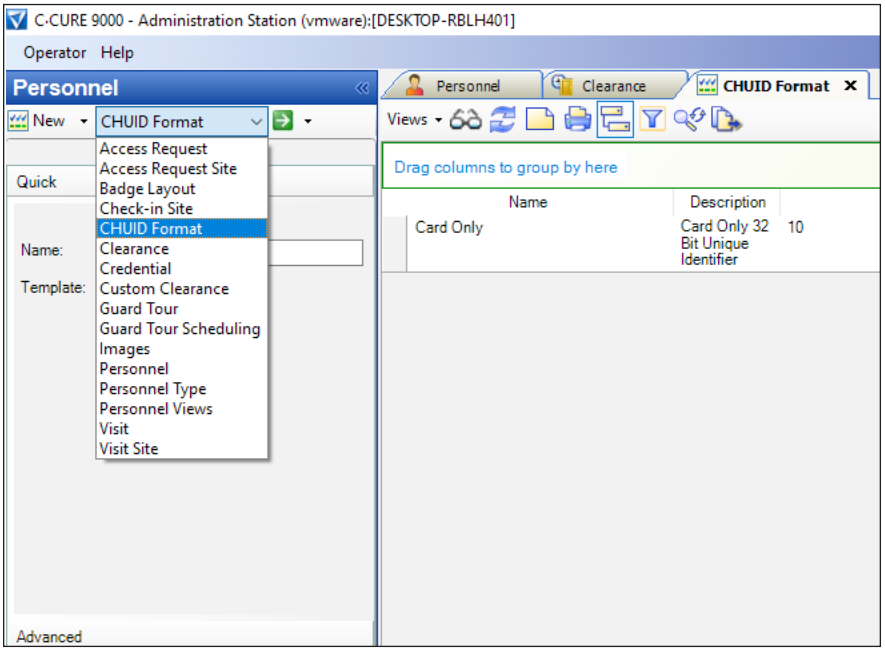
10 Click the **Add** button again to include additional doors and proceed with steps 4 through 7. Click the **Add** button as many times as needed, but it is more efficient if door groups have been created. See

Groups in the appropriate C·CURE 9000 Manual on www.swhouse.com for information on creating door groups.

11 Click **Save and Close** in the upper left hand corner of the dialog box to finish.

Enabling Keypads for Wi-Q in C·CURE 9000

Figure 86 Selecting the CHUID Format



1 Click on the Personnel navigation pane in the left column.

2 Select CHUID Format from the Personnel drop down menu at the top and click the Down arrow next to New button and select PIN Only Template.

Figure 87 Selecting the CHUID Format

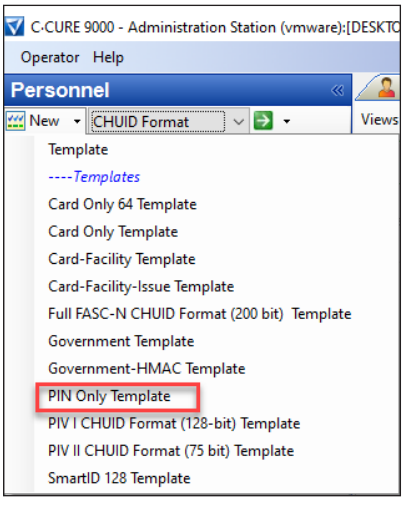
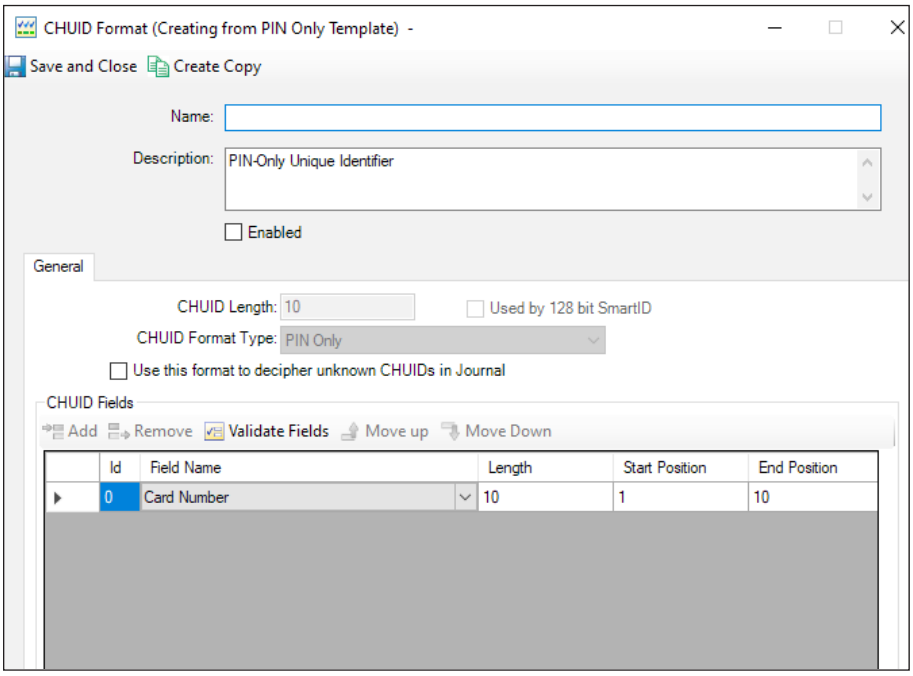


Figure 88 Enabling Keypad Credential



3 Enter "Wi-Q Keypad Credential" in Name field.

4 Enter "Keypad Credential" in Description field.

5 Check the **Enabled** check box.

6 Click **Save and Close** in the upper left hand corner of the dialog box to finish.

Note Both the Keypad Credential length and length of a PIN on the General tab of the Personnel configuration form are set by the PIN Length value in the System Variables. They will always be the same. This value can be viewed, but not changed on the Segment configuration form. If the PIN Length in System Variables is ever reduced in value, keypad credentials will not function until a full download is performed by the user or a new Keypad Credential is generated for the user in the Personal Configuration form.

Firmware Updates

Firmware updates will be sent to you periodically by Stanley Technical Support. These files should be stored locally. Please complete the following steps using the locally stored file:

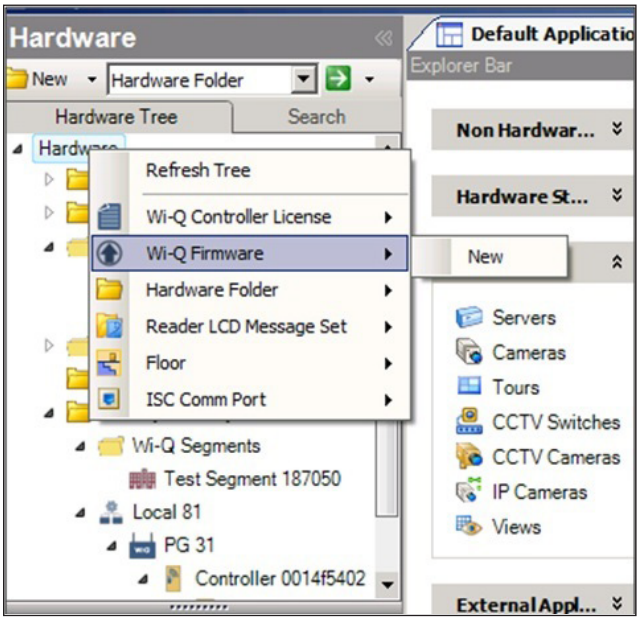
Adding Firmware Files to the Interface

1 Navigate to the Hardware Pane.

2 Right click the root of the Hardware Tree.

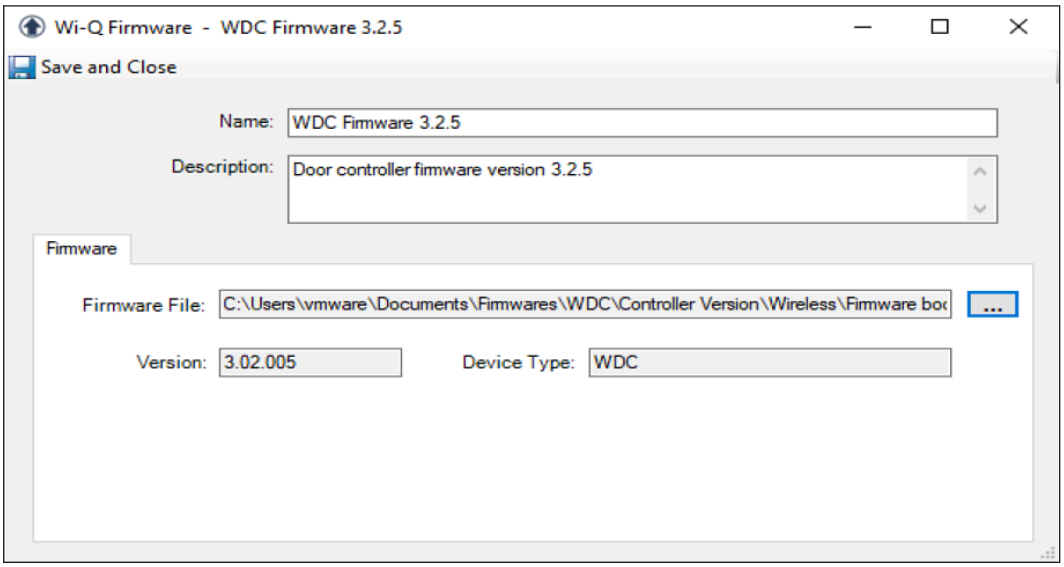
3 Select Wi-Q Firmware -> New.

Figure 89 New Wi-Q Firmware



4 Enter name and description.

Figure 90 Wi-Q Firmware

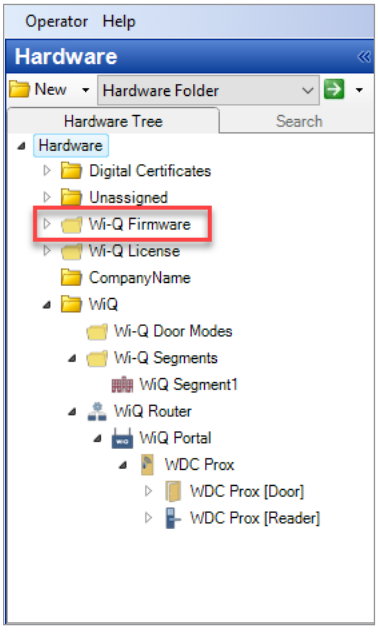


5 Click on Ellipsis button to open the Windows Explorer. Select the firmware file to be uploaded and click Open button.

6 Select Save and Close.

Note After the first firmware file is created, a new folder called Wi-Q Firmware will be added to the Hardware tree, and all firmware files in the interface will stored here.

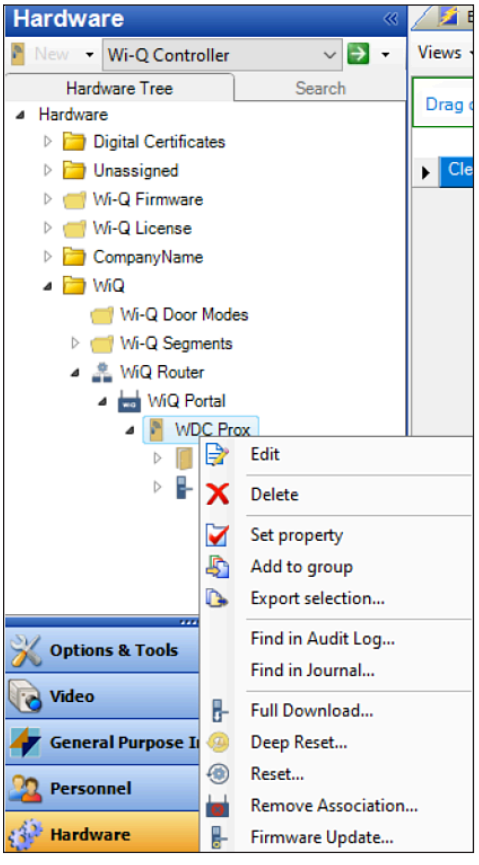
Figure 91 Wi-Q Firmware



Download the Firmware

1 In the hardware tree, right-click an enabled controller or Wi-Q Gateway.

Figure 92 Hardware Tree



2 Choose Firmware Update and select the firmware file to download from the list of compatible files.

3 The device will reset upon completion of the firmware download.

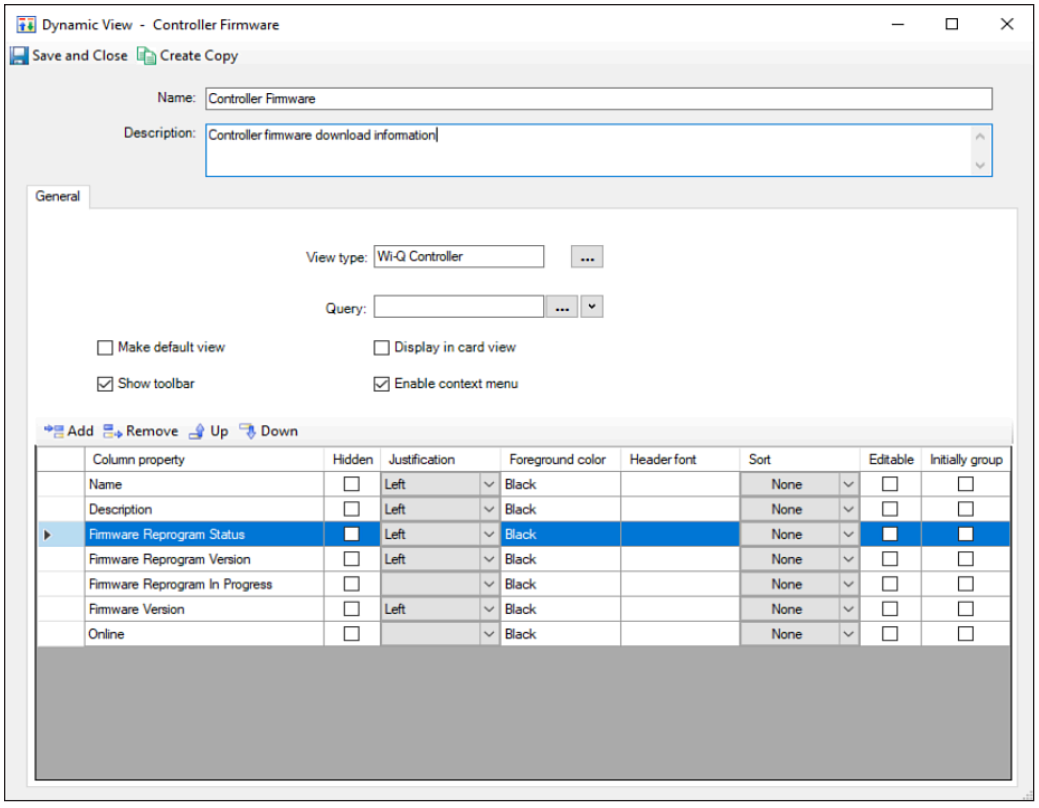
Viewing the Firmware Download

1 Navigate to the Data Views Pane.

2 Select Dynamic View from the drop down menu.

3 Select Dynamic View from the drop-down menu at the top and click the New button to the left.

Figure 93 Controller Firmware



4 Name this dynamic view 'Controller Firmware' with a description of 'Displays Firmware Download Information for Wi-Q Controllers.

5 Select the View type to be Wi-Q Controller.

6 Select the Add button.

7 Choose the Column property to be Name.

8 Continue to add the following column properties:

- Firmware Reprogram In Progress
- Firmware Reprogram Status
- Firmware Reprogram Version
- Firmware Version
- Online

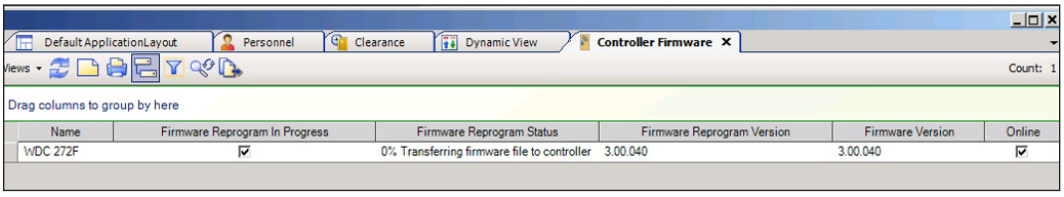
9 Select the formatting for each of the columns.

10 Select Save and Close when finished.

11 Double click the new Dynamic view (or right-click it and select View).

12 You may view the entire status of the firmware download as it occurs. Ensure that, when complete, the Firmware Version and the Firmware Reprogram Version are the same.

Figure 94 Controller Firmware



Note These steps can be repeated for the Wi-Q Portal view type with appropriate name and description changes in order to observe a Wi-Q Gateway firmware reprogram.

5
Troubleshooting

This section provides an overview on the Wi-Q Gateway status webpage. You can access the status webpage for a specific Wi-Q Gateway in one of three ways and your browser will display the status of your Wi-Q Gateway and associated devices. See Figure 95.

Launch the Portal Configuration tool and the list of Wi-Q Gateways online are displayed. Select the hyperlink to open the webpage. See Figure 95.

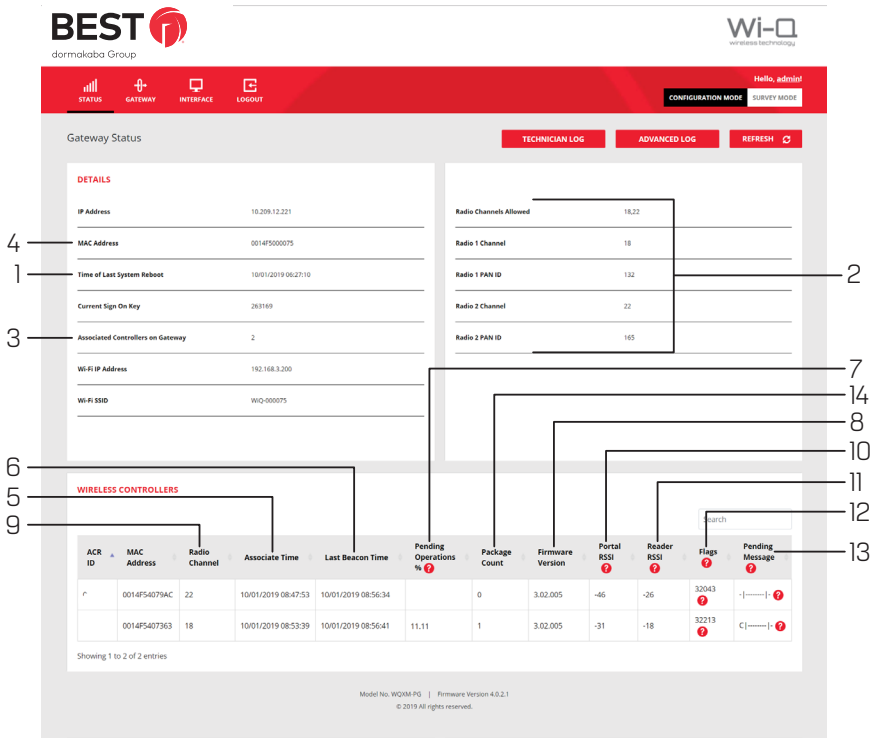
Note This will be supported in upcoming releases. Please connect to WQXM-PG gateway Wi-Fi to get the LAN IP address of the gateway.

- Type your desired Wi-Q Gateway's IP address directly into your internet browser.
- Right click on Router and select View Network Portals. Click on selected IP address.

Note This will be supported in upcoming releases.

Note For all C·CURE 9000 troubleshooting, see www.swhouse.com for contact information.

Figure 95 Wi-Q Gateway Status Webpage



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 channels allowed and channels assigned to Radios.

3 a) Associated Controllers on Gateway (Details section)

Number of associated controllers.

b) Wireless Controllers

Shows the details of the associated controllers.

4 MAC Address

MAC Address of 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 packages 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 definitions.

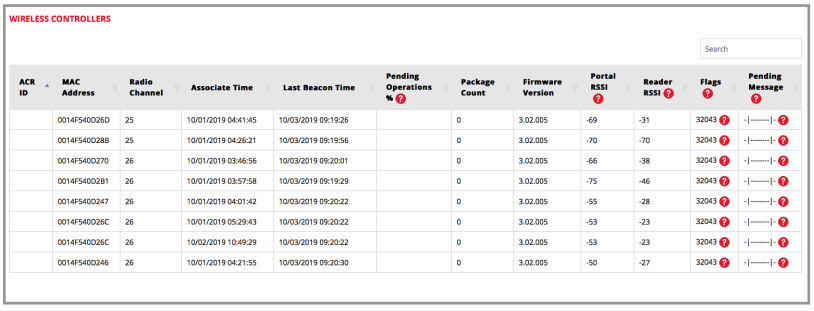
Note The typical Wi-Q device status code is 00032043. This is the example used in the chart below.

Bit			Wi-Q Gateway Status Flag	Definition
Right END	**3**	**Bit 0**	CONTROLLER_IS_ASSOCIATED	Set when the Controller is first associated with the Portal.
		Bit 1	CONTROLLER_IS_VALID	Set during association, after the Portal receives a beacon from the Controller.
		Bit 2	CONTROLLER_CONFIG_REQUIRED	Set during association, cleared by Portal Communication Service after Controller configuration.
		Bit 3	CONTROLLER_ASSOC_PENDING_ LIF	Set during association to indicate that Portal requires LIF (Lock Information Frame) data.
	4	Bit 4	CONTROLLER_BEGIN_ TRANSMISSION	Set when Portal first transmits data to the Controller.
		Bit 5	CONTROLLER_DEEP_RESET_ PENDING	Portal 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 Portal.
		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 is a list of the associated Wi-Q Controllers and their attributes.

Figure 96 Wi-Q Gateway Status Webpage



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

- **ACR ID** – The Reader ID when the Wi-Q Gateway 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 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)

Glossary

This Glossary contains only dormakaba (BEST Access Systems) Wi-Q Terms. See www.swhouse.com for the appropriate C·CURE 9000 Manual for a listing of C·CURE terms.

access level	An access control relationship made between a reader or readers and a time zone or time zones. An access level is assbadge ID for the purpose of granting access through a reader or readers during a specified time.
activation/deactivation date	The date that a credential becomes active or expires.
badge	The credential or token that carries a cardholder's data.
badge ID	Part of the access control information that is encoded to a token. This information, usually numerical, is unique to a particular credential holder.
card format	The way that data is arranged and ordered on the card.
cardholder	An individual who is issued a particular credential.
chassis type	The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.
communication server	The server application designed to provide network services to access panels, readers, PCs and PDAs.
credential	A physical token, usually a card or fob, encoded with access control information.
cylindrical	Lock chassis that installs into a circular bore in the door.
directional antenna	An antenna type optimized to focus signal from point-to-point over longer distances and through obstacles.
ethernet	The most common networking standard in the world, formally known as IEEE 802.3.
exit hardware	Lock chassis type that supports exit hardware trim lock.
extended unlock	The extra period of time the lock will unlock when an authorized credential with extended unlock privileges is presented.
guest	A feature that enables you to add and delete cardholders to and from a lock without having to go out to a lock to reprogram it.
Host	the computer on which Wi-Q Interface Software is installed and set up to integrate Wi-Q Gateways and readers into.
IP address	The numeric address (like 192.168.1.1) that identifies each device in a TCP/IP network. input A hardware connection point used for status reporting of a particular sensor.
issue code	Part of the access control information contained on a credential that allows reuse of the badge ID when a credential is lost, damaged, or stolen. Usually one or two digits in length, this code increments forward when creating a new credential. Access is granted only when the badge ID and the issue code match the current database information.

MAC address	The Media Access Control number (MAC). A unique, 12-digit number assigned by the manufacturer of a network device.
mortise	A lock chassis that installs into a mortised cavity in the edge of a door.
omni-directional antenna	An antenna type optimized to provide signal coverage in all directions.
packet	A discrete chunk of data, being transferred on a TCP/IP or other addressable network.
Wi-Q Gateway	The Wi-Q Gateway is a wireless device connected to the Host computer through a secure IP address to transfer data signals from wireless reader locks to and from the Host computer.
request to exit	A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation.
segment code	Part of the access control information that can be encoded to a credential. This information, usually numerical, is unique to a group of credentials. Usually this feature is used to authenticate a credential to a particular organization.
sign-on key	Number generated within Wi-Q Interface Software to establish the connection between the readers and the Wi-Q Gateways, and ultimately to a segment in the Software.
site survey kit	The Wi-Q Site Survey Kit tool is 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.
timezone	A defined range of time for assignment to various access control activities. A time zone may be applied to a reader or readers when creating an access level, to a reader to change the mode of operation, to a relay to activate and deactivate, to an input to mask and unmask, and a host of other operations. Dual access The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening. unlock duration The time that the lock momentarily unlocks. Use limit A configuration limiting a credential to a defined number of uses.
Wi-Q Technology	Provides efficient, online access control decisions at the door.
wireless access controller	Wireless access controller provides additional capability to connect stand-alone controllers and locks.
wireless controller	The wireless lockset that controls user access at the door and grants user requests according to how they are configured in your Wireless Access Software.