



C·CURE 9000 with Wi-Q

User Guide

v3.1

Copyright© Stanley Security 2014.
All rights reserved.

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

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. Please call Stanley Security, Inc at (317) 365-2407 if you see any errors or have any questions. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose, without the express written permission of Stanley Security, Inc.

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

The Stanley Wi-Q Interface, Wi-Q Technology and BEST are registered trademarks of Stanley Security, Inc.

Bonjour is a registered trademark of Apple Inc.

Wi-Spy and MetaGeek are registered trademarks of MetaGeek, LLC.

Microsoft, Windows, CE, and ActiveSync are registered trademarks of Microsoft Corporation.

A85299-B 03/15

FCC Certification

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.

Approved antennas are listed below and antennas not included in this list are strictly prohibited for use with these devices. The required antenna impedance is 50 ohms.

Approved Antennas

Portal Gateway

- HG2402RD-RSF - 2.4GHz Rubber Duck Antenna
- MP24008XFPTNF - 2.4GHz ISM-XF Panel Antenna
- MC2400PTMSMA - 2.4GHz Omni-Directional Antenna

Controller

- Integrated Antenna

IMPORTANT! Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

UM-305 A0

Contents

5	Overview
8	Setup Checklist
9	Hardware Installation
10	Hardware Overview
12	Installing System Hardware
19	Install Portal Gateways (Task 7)
22	Install Door Hardware (Task 8)
23	Signing on Controllers (Task 9)
27	Software Installation
28	Organize Segment Data (Task 3)
29	Prepare Your Computer (Task 4)
41	Install C-CURE Wi-Q Interface Software (Task 5)
61	Software Configuration
62	C-CURE Wi-Q Pane Overview
63	Configuring the Hardware in C-CURE Wi-Q Interface Software (Task 6)
79	Configuring the Software (Task 10)
106	Firmware Updates
111	Troubleshooting
113	Status Flags in the FLAGS Column
115	Update Flags in the PEND Column
117	Glossary

1

Overview

This manual is your guide to the integration of Stanley Wi-Q wireless hardware into your Software House G-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.

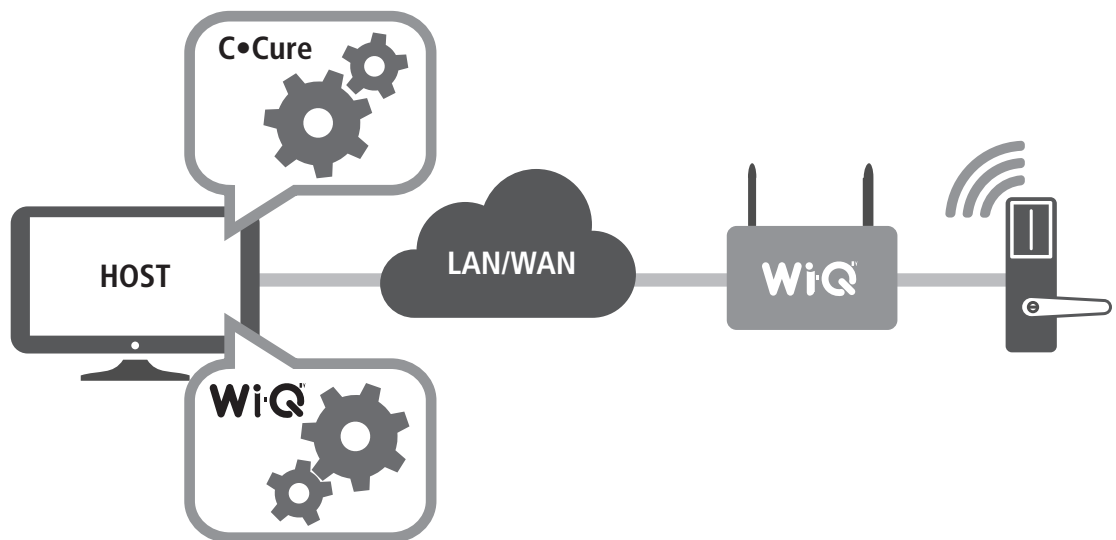
System Overview

A Software House C-CURE 9000 Access System with integrated Wi-Q Technology combines access control software with Portal 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 Portal 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 Portal Gateway

The Portal 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 Portal Gateway recognizes all Wireless Controllers within its antenna range. One Portal 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 Portal Gateway. The Wireless Controller grants user requests according to how they are configured in the C-CURE 9000 Software.

Note The terms "Controller" and "Lockset" 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 a pass code at a Wireless Controller, either using an access card or by entering a code on a keypad. If the controller recognizes the credential from the configured settings downloaded from the Host via the Portal Gateway to the controller, the door opens. The controller also sends regular signals to the portal to let it know that it's working properly. If a controller goes offline, the Host receives a message from the Portal Gateway.

Additional System Configurations

C-CURE 9000 Wi-Q Interface Software supports various system configurations. For example, some locations at your segment may already be hard wired with legacy equipment or additional input or output devices. You can include a Wireless Access Controller that links a hard wired strike and controller with a Portal Gateway. For more information about various applications you can adapt for use with Wi-Q, see "Hardware Overview" on page 10.

Software Overview

C-CURE 9000 provides powerful tools to manage your system. The Wi-Q Interface Software allows you to add Portal Gateways, Controllers and Segment Sign on Credentials to your C-CURE 9000 system. The Wi-Q Interface Software also allows you to send firmware updates to your Portal Gateways and wireless locksets 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 and some at the segment site. It is appropriate to perform some tasks concurrently. For example, you may have someone prepare your computer and install the software concurrently with site plan development and hardware installation. However, you must have the software installed and Portal 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 13.
- Task 2: Position Portal Gateways
See page 16.
- Task 3: Organize Segment Data
See page 28.
- Task 4: Prepare your Computer
See page 29.
- 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 63.
- Task 7: Install Portal Gateways
See page 19.
- Task 8: Install Door Hardware
See page 22.
- Task 9: Signing on Controllers
See page 23.
- 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 Portal Gateways

Task 7 — Install Portal Gateways

Task 8 — Install Door Hardware

Task 9 — Signing on Controllers

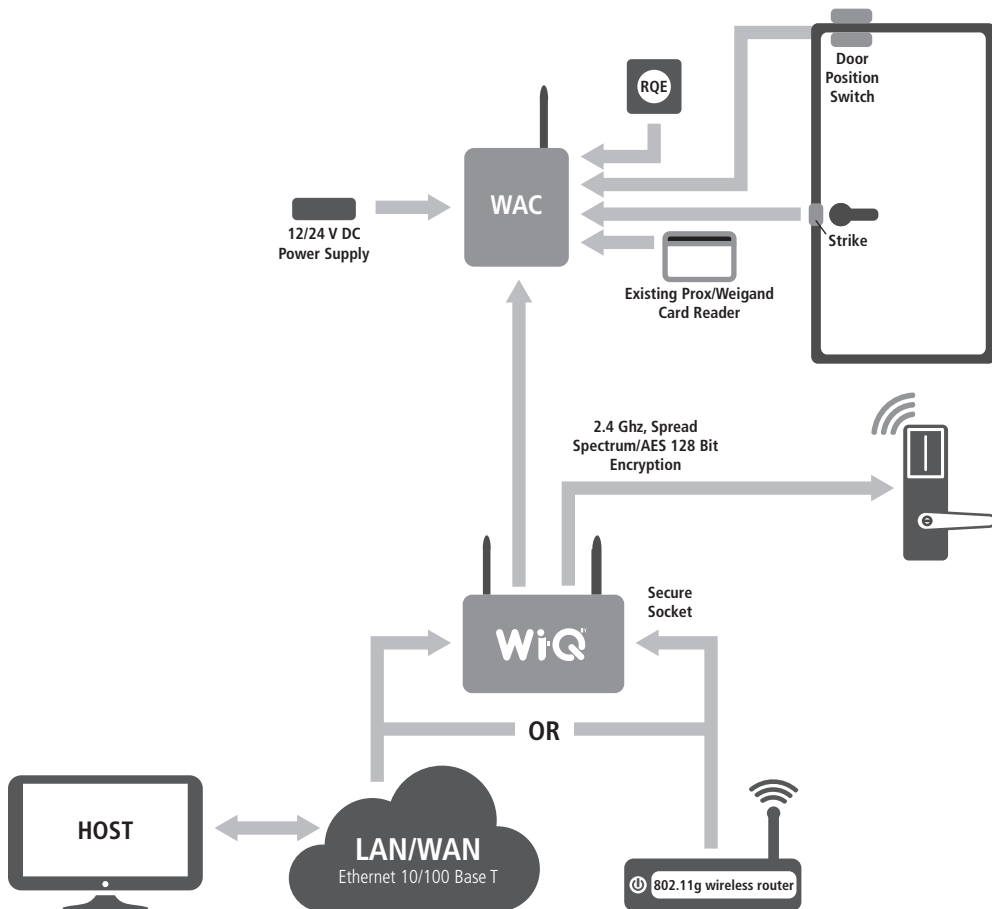
Hardware Overview

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 portals and include various I/O devices.

Note Once Wi-Q Technology locksets 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 23.

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



Portal Gateways

The Wi-Q Portal 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 Portal Gateway recognizes all Wireless Controllers within its antenna range. One Portal Gateway can control up to 64 Wireless Controllers.

Portal 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 Portal Gateway communicates to the Host computer through web services via either Ethernet 10/100 BaseT, approved 802.11 G wireless, or an approved commercial RF carrier-enabling a wireless solution end-to-end. Transmit range from Portal 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 locksets equipped with either keypad, card, or a combination of controller input devices. Door switch monitor, request to exit, and door lock position sensors are included in the locks. 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)
- 18000 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 Portal 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 Stanley representative for a list of compatible controllers.

Antenna Types and Applications

To optimize system performance, it is important to position Portal Gateways to receive maximum signal strength from the Wireless Controllers. Once all door hardware has been installed, you will be ready to position Portal 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 Portal Gateways (Task 2)” on page 16.

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 Portal 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
- Wi-Spy Spectrum Analysis Tool by MetaGeek (or equivalent) to identify the best open channels for your network
- For keypad controllers, you will need the sign-on credential from the Wi-Q Interface Software.
- For magnetic stripe or proximity card readers, you will need the Temporary Operator Card (supplied with the controller) and Sign on Card (supplied in the Wi-Q Interface Software package). You will also need the appropriate magnetic stripe or proximity USB enrollment reader to create a proximity sign-on credential.
- Locksets to be installed on doors, including cores and keys supplied with specific model
- Installation instructions for specific lockset brand and model
- Portal 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 Portal 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 Portal 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 Portal Gateways. You must consider the following:

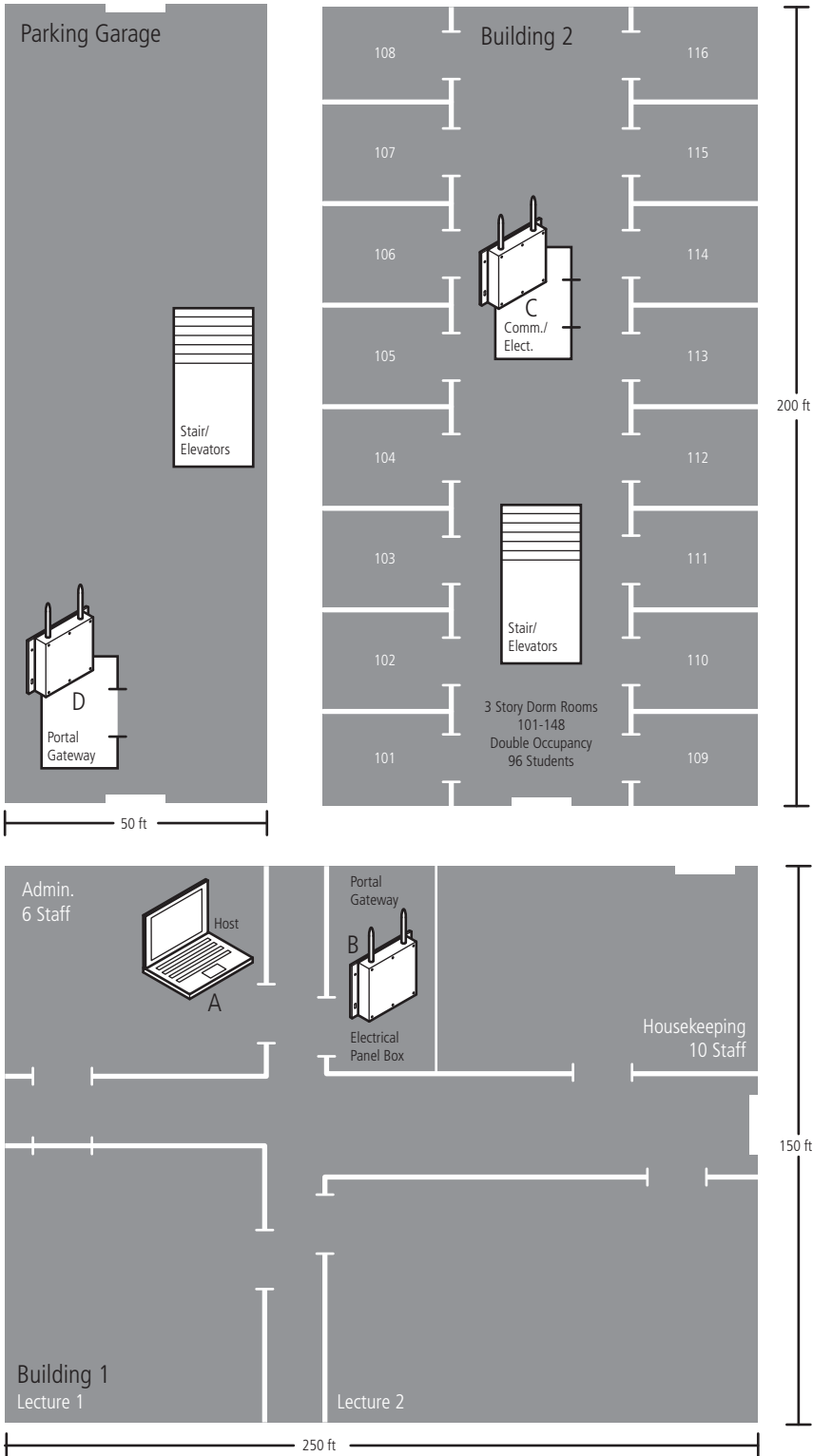
Transmit range from Portal Gateway to controller varies based on building construction. Site characteristics such as reinforced concrete walls could interfere or weaken the signal; open spaces and low interference can increase signal strength.

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

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

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

Figure 3 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 Portal Gateway recognized by the system. We recommend creating a temporary label for each device that includes the MAC address, device name, location, capacity, and type of antenna so that installers on the site will have a reference for installing the correct device in a location.

Interference

Wi-Q Technology transfers information between devices in the form of data packets over the 2.4 GHz ISM band. This band frequency is very heavily used in many devices such as wireless computer networks (802.11 b and g) and cordless phones, which increases the risk of lost packets, that is, packets that do not make it from a controller to a Portal Gateway because of interference. Interference can also reduce controller battery life due to the constant re-broadcasting of packets and lost connections to the portals. To achieve maximum efficiency, 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 Portal Gateway with a directional antenna to extend the transmit range.

Note Actual distances will vary based on building construction.

Position Portal Gateways (Task 2)

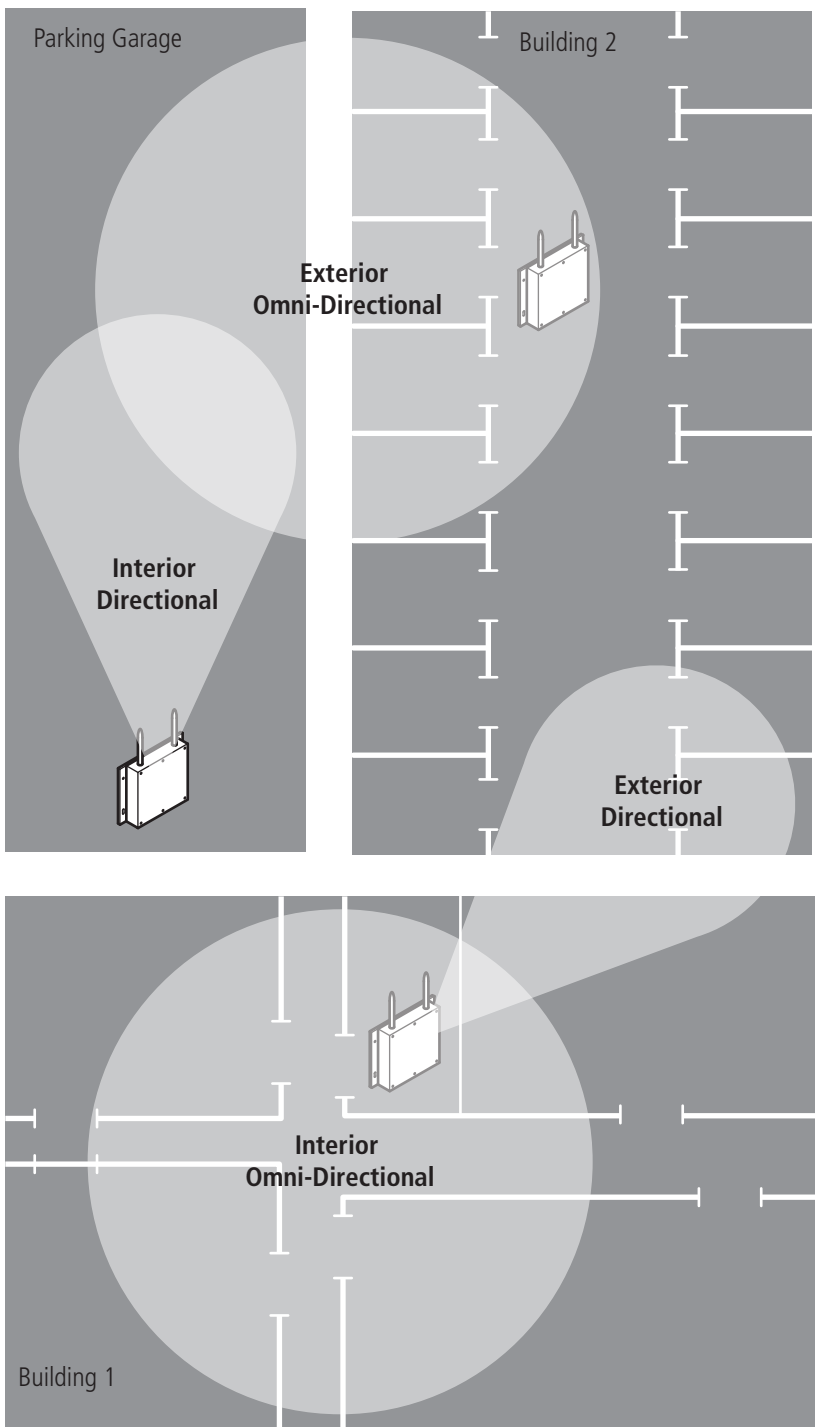
Once all door hardware and controllers have been installed, you are ready to determine the final placement of Portal Gateways using the results from the Wi-Q Technology Site Survey Kit. The Site Survey Kit helps you determine the number and optimum location of Portal Gateways and verify signal strength 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

Portal Gateways must be located where they can receive 12 VDC power from a transformer plugged into a dedicated power source. If this is not possible, ensure they are plugged into a 24/7 power circuit that cannot be turned off at a switch, such as a light switch that might be turned off by a cleaning crew.

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

- Access to Ethernet 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.

Troubleshooting

If you have problems establishing communication using the Wi-Q Technology Site Survey Tool, refer to the following troubleshooting guide:

Troubleshooting (Portal Gateway Communication)	
If...	Then
The green light on the power supply does not turn on.	Firmly press the power cord into the outlet on the outside of the case. Confirm that the other end of the power cord is plugged into a working electrical outlet.
The power supply is on, but the green light on the Portal Gateway does not turn on.	Ensure the power cord is firmly connected to the bottom of the Portal Gateway.
The Stanley Site Survey application freezes after clicking Connect.	Close the application and reconnect the Host PC to the Stanley Site Survey wireless network.
The Stanley Survey network is not listed in the Wireless Network Connection window.	Confirm that the green light on the power supply is on. Ensure the power cord is firmly connected to the bottom of the wireless router (under the foam).
The Stanley Site Survey application is not receiving a signal from a beacon.	Ensure the beacon is powered up. Move the beacon closer to the Stanley Site Survey Kit.
When connecting the battery wires, the beacon does not power up (the blue LED on the circuit board remains off and no confirmation tone sounds).	Disconnect the battery pack wires, wait 10 seconds, and reconnect. If this does not work, replace the battery pack.
The Stanley Site Survey application is not receiving signals from any beacons.	Ensure the Ethernet cord is connected to the wireless router (under the foam). If this does not work, you might need to change the advanced setup options for the application with the assistance of your Stanley Security Solutions representative.

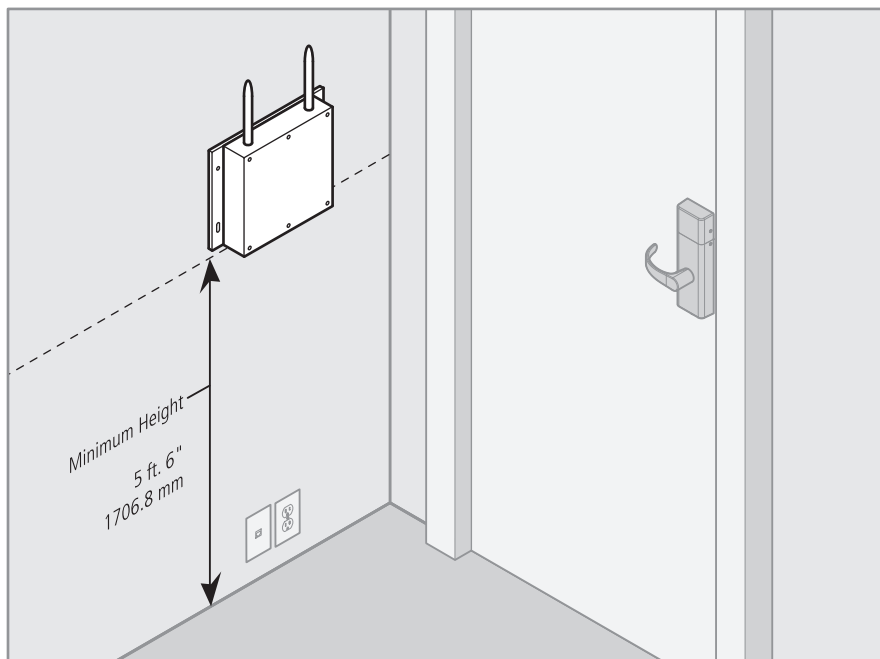
Next steps

When you are satisfied with signal performance, you can proceed to configure Portal Gateways with the C-CURE 9000 Software. See “Configuring the Hardware in C-CURE Wi-Q Interface Software (Task 6)” on page 63.

Install Portal 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 Portal Gateway positioned in a protected area.

Figure 5 Installing a Portal Gateway in a protected area

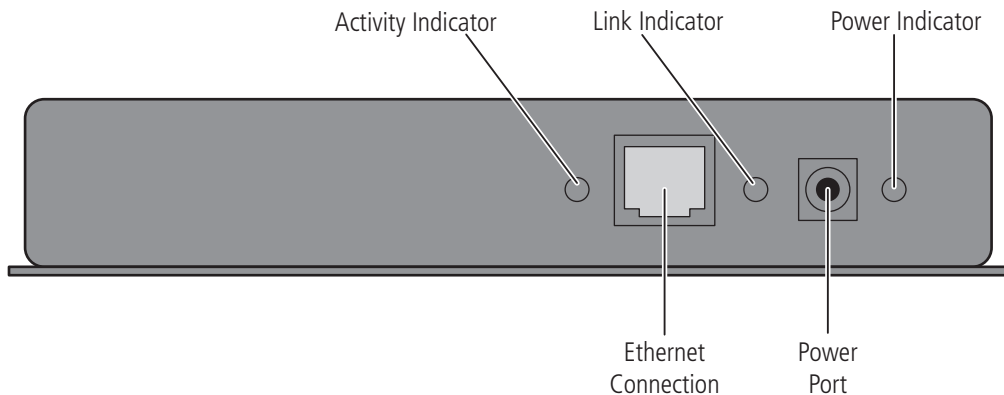


Connecting the Portal Gateway and Verifying Operation

Once the Portal Gateway is installed, connect and verify operation:

- 1 Connect the power supply to the Portal 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 Portal 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 Portal Gateway to Power and Ethernet Connections



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

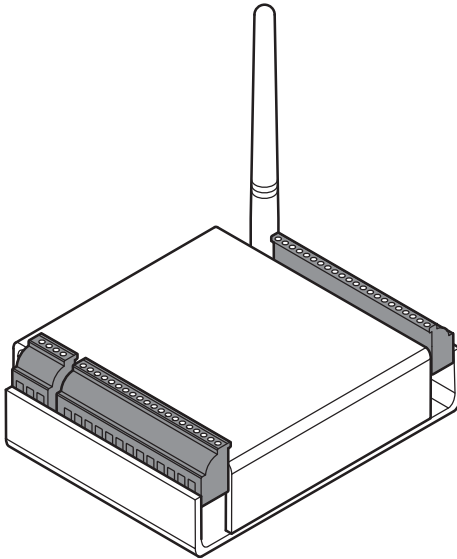
Installing a Wireless Access Controller

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 Stanley 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

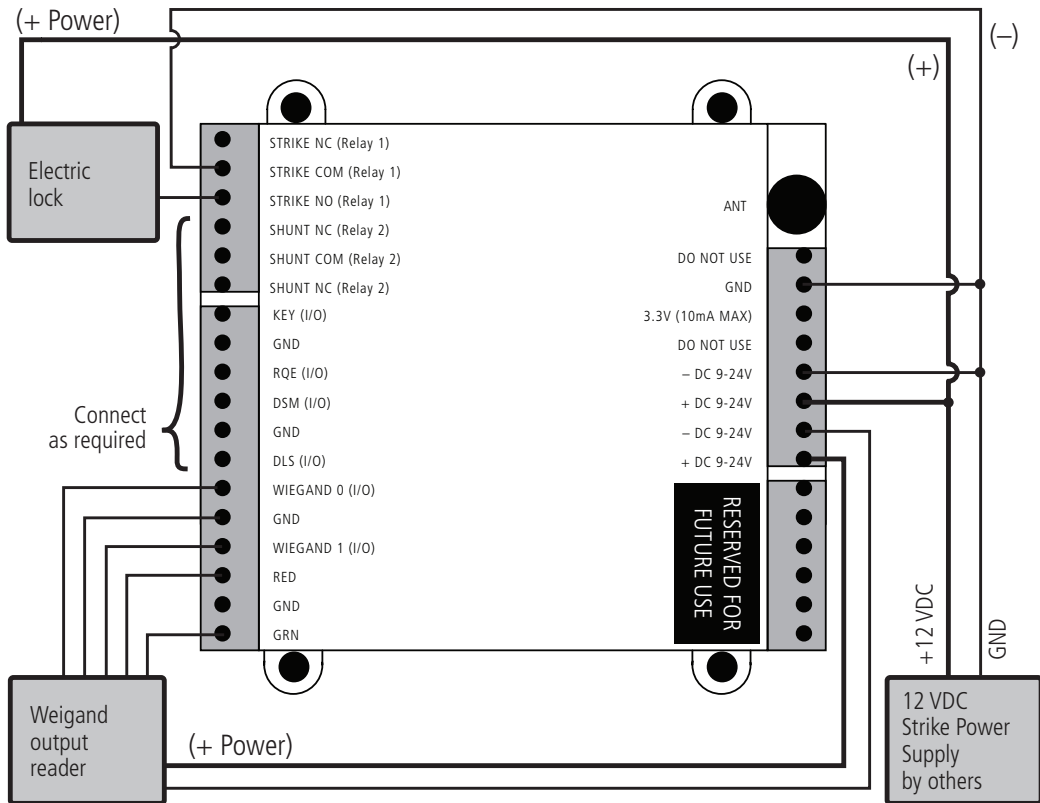
Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

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 Stanley Security Solutions 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 Stanley Wi-Q Technology Best 45HQ Mortise Locks, Best 9KQ Cylindrical Locks and Best EXQ Trim on www.bestaccess.com.

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 Stanley Customer Service for more information.
- Lockset instructions are given for right-hand doors (as determined from outside the door). If you are installing a left-hand door, see the instructions provided with your lockset for hand change instructions.
- If you are installing locksets on unprepared (un-drilled) doors, use the template provided with your specific lockset.

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 Stanley Technical Support at 800-392-5209.

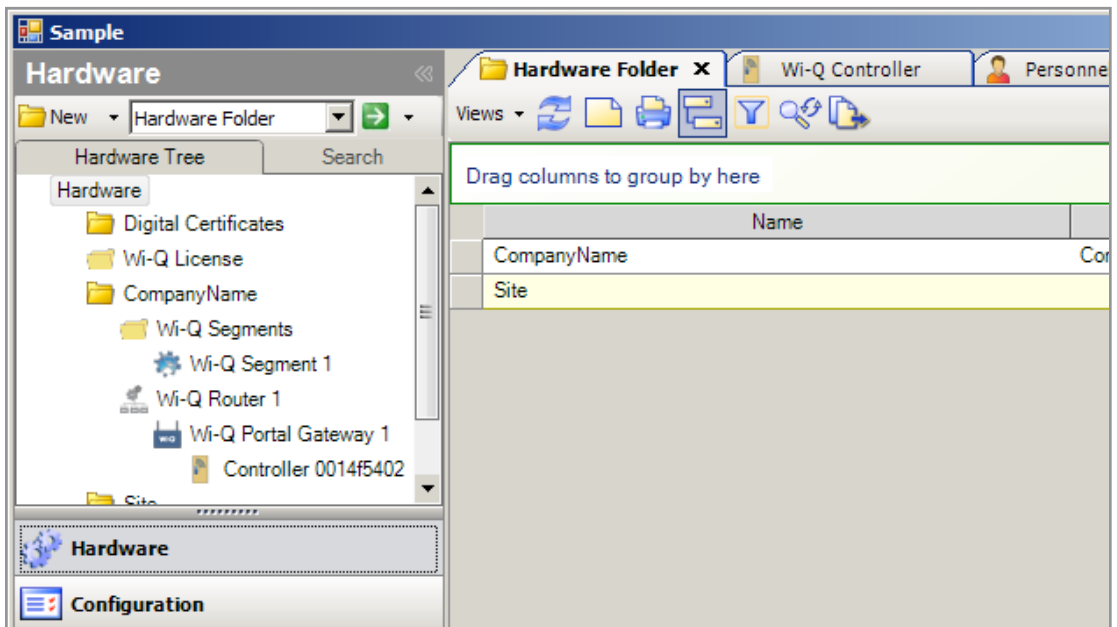
Signing on Controllers (Task 9)

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 portal 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

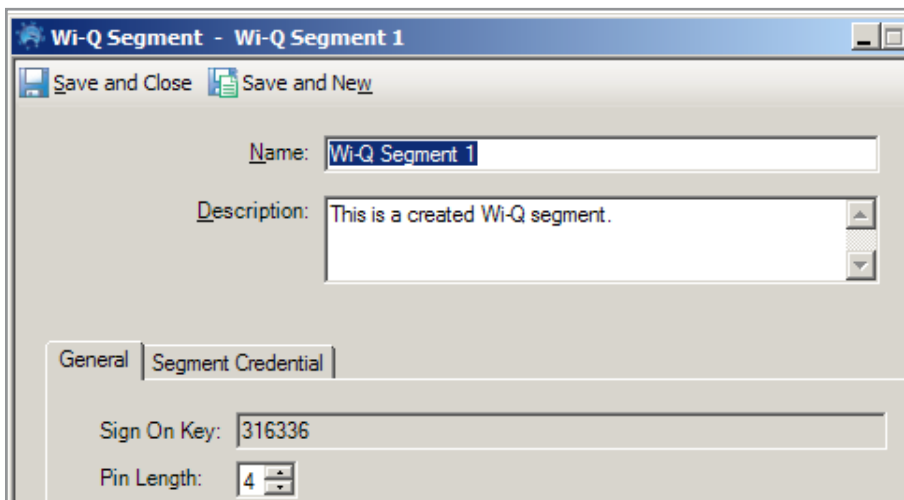
Once you have installed the C-CURE Wi-Q Interface Software and created a segment, a sign on key number is generated for that segment. You will need this number when you return to the site and sign on the controllers. To locate the sign on key number, select the segment to which the controller is to be 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 portal 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 portal gateways in range. The blue light indicates that the controller is communicating with the portal 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.

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 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 portal.

- 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 Portal 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 same as the C-CURE Software. See the "Recommended System Limits" on page 29.
- Configure your Windows Firewall Ports.
- Obtain your Wi-Q Interface Software from Stanley.
- 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.

Recommended System Limits

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

The Wi-Q Interface Software requirements are the same as the C-CURE Software requirements as outlined in the following tables. For additional information, see www.swhouse.com.

Operating System Compatibility

Operating System	Supported Version
Windows 7 Professional (Recommended)	32-bit, 64-bit, SP1 or higher
Windows 7 Enterprise (Recommended)	32-bit, 64-bit, SP1 or higher
Windows 2003 Server Standard	32-bit, SP2 or later
Windows 2003 Server Enterprise	32-bit, SP2 or later
Windows Server 2008 Standard	32-bit, SP1 or later
Windows Server 2008 Enterprise	32-bit, SP1 or later
Windows Server 2008 R2 Standard (Recommended)	64-bit, SP1 or later

Database Compatibility

Database Server Series	Supported Version
SQL Server 2008 R2 Express (Recommended)	10.50.1600.1 RTM (32- and 64-bit)
SQL Server 2008 R2 Standard (Recommended)	10.50.1600.1 (32- and 64-bit)
SQL Server 2008 R2 Enterprise (Recommended)	10.50.1600.1 (32- and 64-bit)
SQL Server 2008 Express	10.0.4000 SP2 (32- and 64-bit)
SQL Server 2008 Standard	10.0.4000 SP2 (32- and 64-bit)
SQL Server 2008 Enterprise	10.0.4000 SP2 (32- and 64-bit)
SQL Server 2005 Express	9.00.4912 SP4 (32-bit)
SQL Server 2005 Standard	9.00.4912 SP4 (32-bit)

Server and Client Compatibility

Note The configuration numbers below correspond to C-CURE 9000 server and client specifications. Windows XP and Windows Vista are not supported for client/Server configuration.

Standalone Server Series L, M, N and Client Workstation

C-CURE 9000 Standalone Server Series L, M, N and Client Workstation	
Recommended Hardware Specifications	
Processor	Intel® 2nd Generation Core i5-2400 or greater (3.1 GHz or greater)
Hard Disk Drives	Dual drives: primary drive = 250 GB (C-CURE 9000 Runtime); secondary drive = 250 GB (data backups)
Drive Speed	7,200 RPM or greater
Memory	4 GB on 32-bit OS; 8 GB on 64-bit OS dedicated to C-CURE 9000
Network Adapter Card	Intel Gigabit ET Quad Port Adapter, Gigabit Ethernet NIC, PCIe x4
DVD Drive	Required
Video Card	Integrated Intel HD Graphics 20007

Standalone Server Series P, Q, R, R+, S and SAS Server Series L, M, N

C-CURE 9000 Standalone Server Series P, Q, R, R+, S and SAS Server Series L, M, N	
Recommended Hardware Specifications	
Processor	Intel Xeon Quad-Core E3-1240 (3.3 GHz or greater)
Hard Disk Drives	Dual drives: primary drive = 300 GB (C-CURE 9000 Runtime) secondary drive = 300 GB (data backups)
Drive Speed	15,000 RPM or greater
Memory	16 GB dedicated to C-CURE 9000
Network Adapter Card	Intel Gigabit ET Quad Port Adapter, Gigabit Ethernet NIC, PCIe x4
DVD Drive	Required
Video Card	Matrox G200eW w/ 8 MB memory

SAS Server Series P, Q, R, R+, S and MAS Server

C-CURE9000 SAS Server Series P, Q, R, R+, S and MAS Server	
Recommended Hardware Specifications	
Processor	Intel® 2nd Generation Core i5-2400 or greater (3.1 GHz or greater)
Hard Disk Drives	Dual drives: primary drive = 250 GB (C-CURE 9000 Runtime); secondary drive = 250 GB (data backups)
Drive Speed	7,200 RPM or greater
Memory	4 GB on 32-bit OS; 8 GB on 64-bit OS dedicated to C-CURE 9000
Network Adapter Card	Intel Gigabit ET Quad Port Adapter, Gigabit Ethernet NIC, PCIe x4
DVD Drive	Required
Video Card	Integrated Intel HD Graphics 20007

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 42 The Router Dialog Box" on page 71. Also, add any configured Wi-Q Portal: "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 44 Portal Dialog Box" on page 73. The following ports must also be enabled:

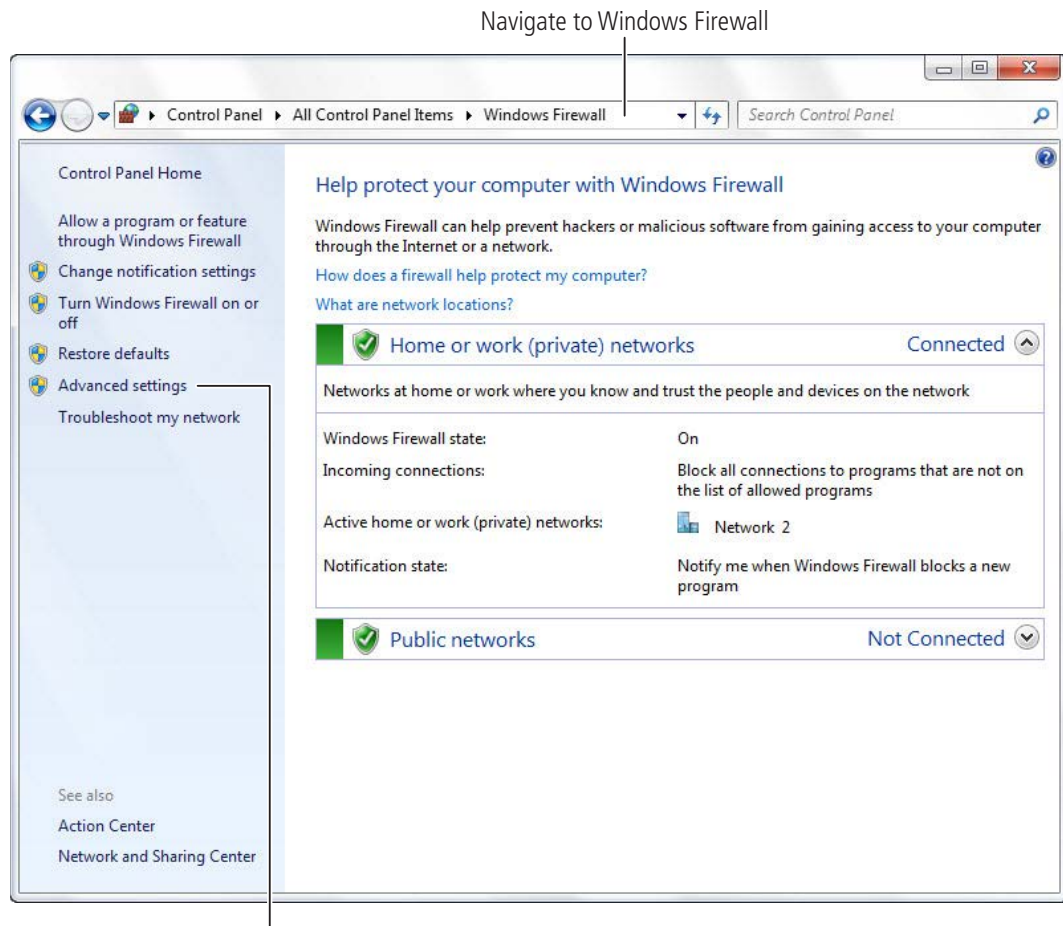
- Port 23
- Port 80
- Port 1433
- Port 1434
- Port 5353
- Port 8000 (default)
- Port 9000
- Port 9001
- Port 11000 (default)

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.

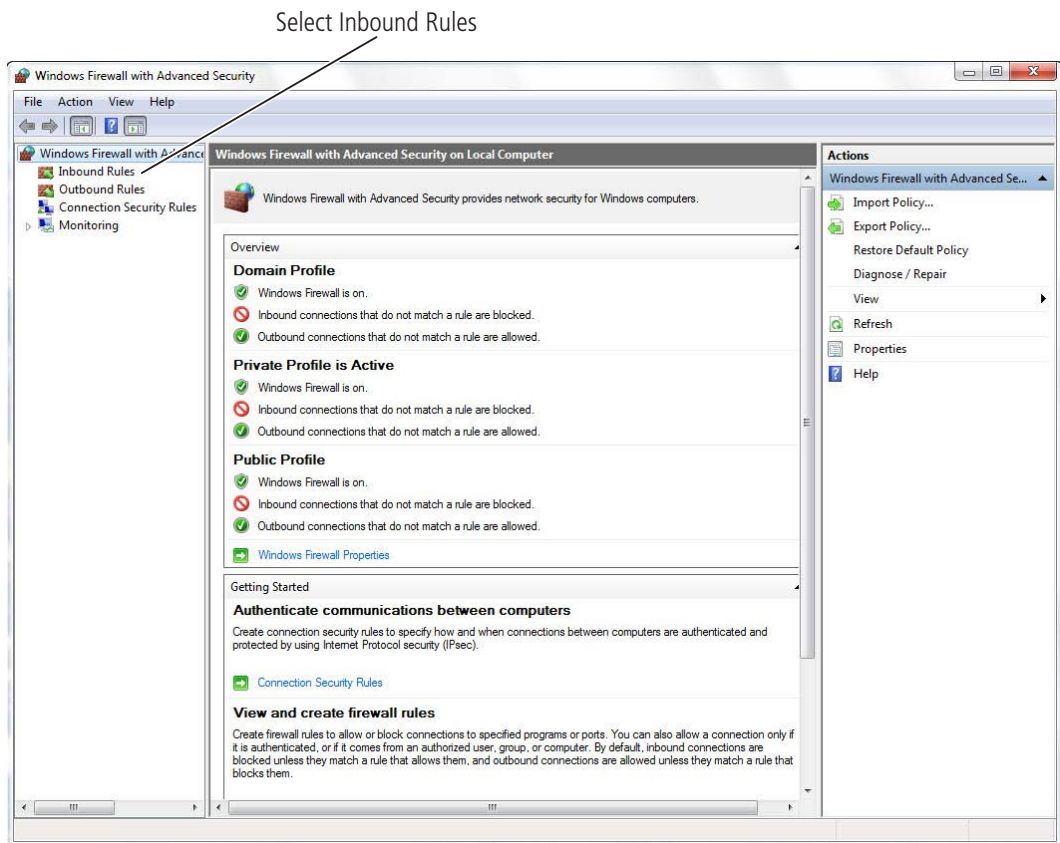
Figure 11 Windows Firewall



Click on Advanced settings

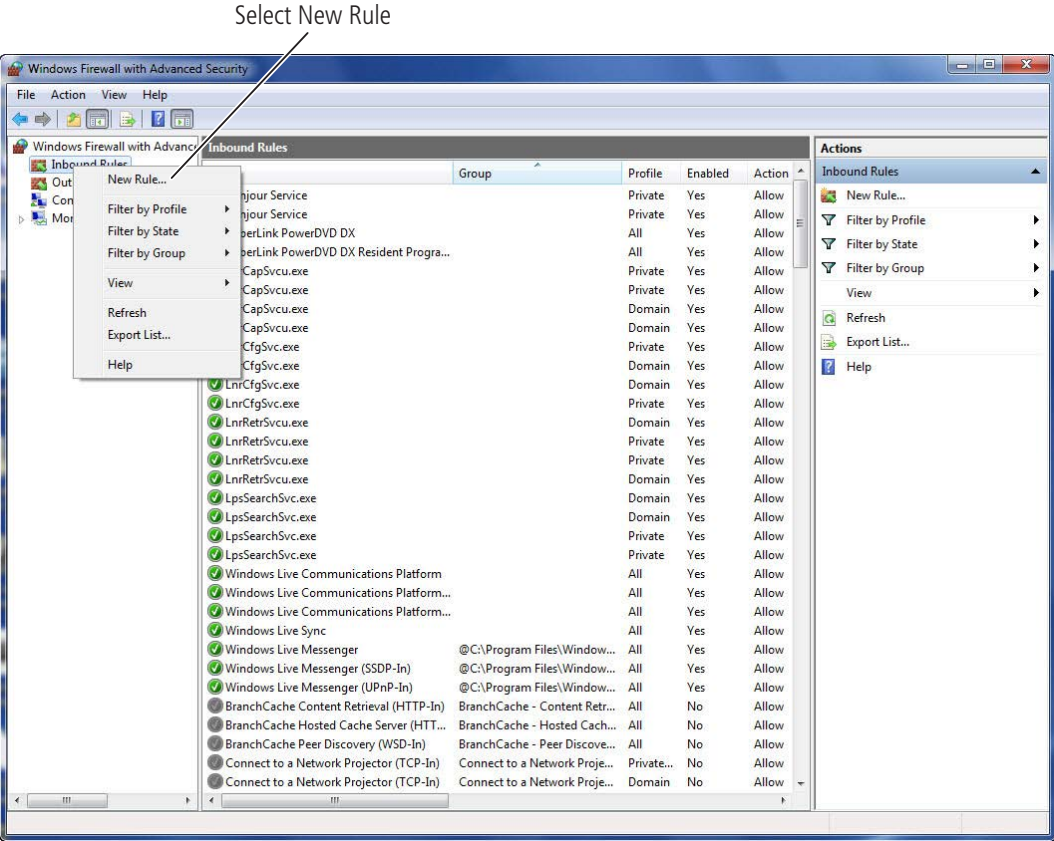
- 1 Navigate to your Windows Firewall settings from your PC's control panel. Then, click on Advanced settings.

Figure 12 Inbound Rules



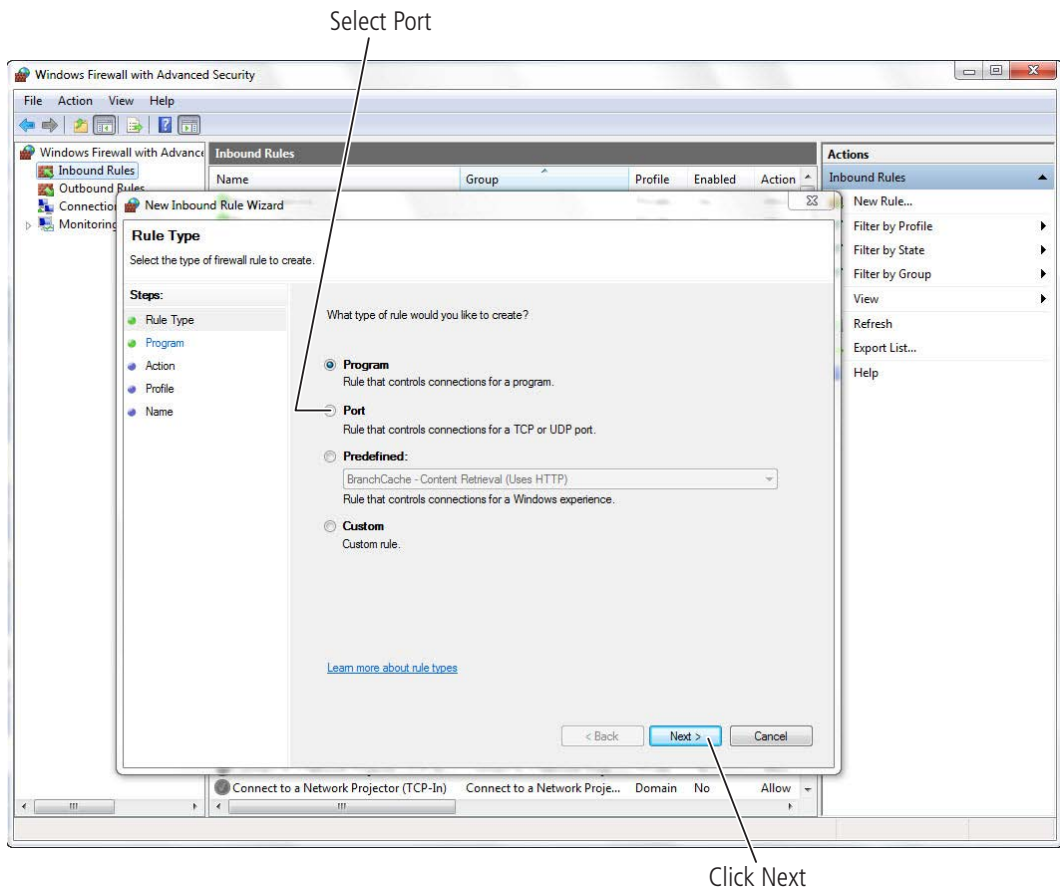
2 Select Inbound Rules.

Figure 13 New Rule



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

Figure 14 Create Port Rule



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

Figure 15 Enter Ports

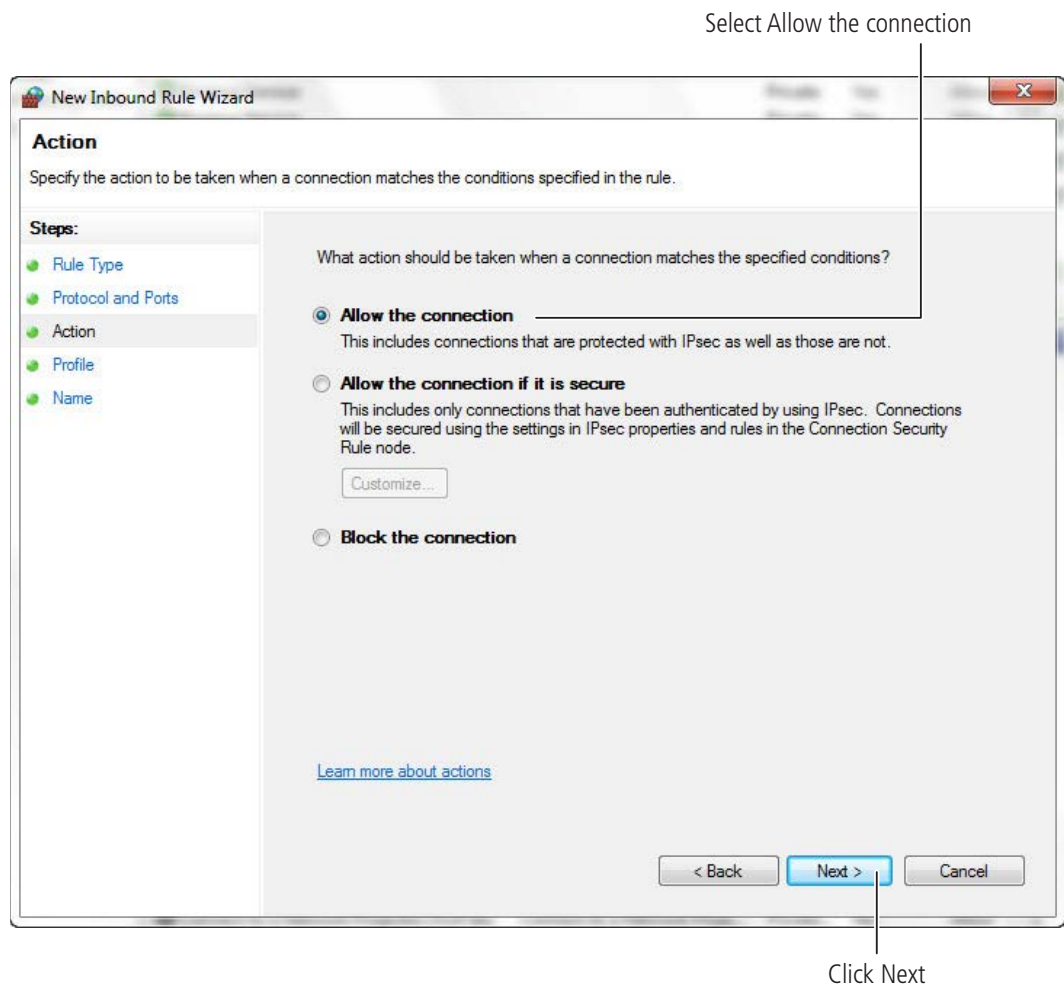
Enter ports: 23, 80, 1443, 1434, 5353, 8000, 9000, 9001, 11000

The screenshot shows the 'New Inbound Rule Wizard' window. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Protocol and Ports' with the instruction 'Specify the protocols and ports to which this rule applies.' On the left, a 'Steps:' pane lists: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions: 'Does this rule apply to TCP or UDP?' with 'TCP' selected, and 'Does this rule apply to all local ports or specific local ports?' with 'Specific local ports:' selected. A text input field is present for specific ports, with an example '80, 443, 5000-5010' shown below it. A link 'Learn more about protocol and ports' is at the bottom left. At the bottom right are buttons for '< Back', 'Next >' (highlighted in blue), and 'Cancel'.

Click Next

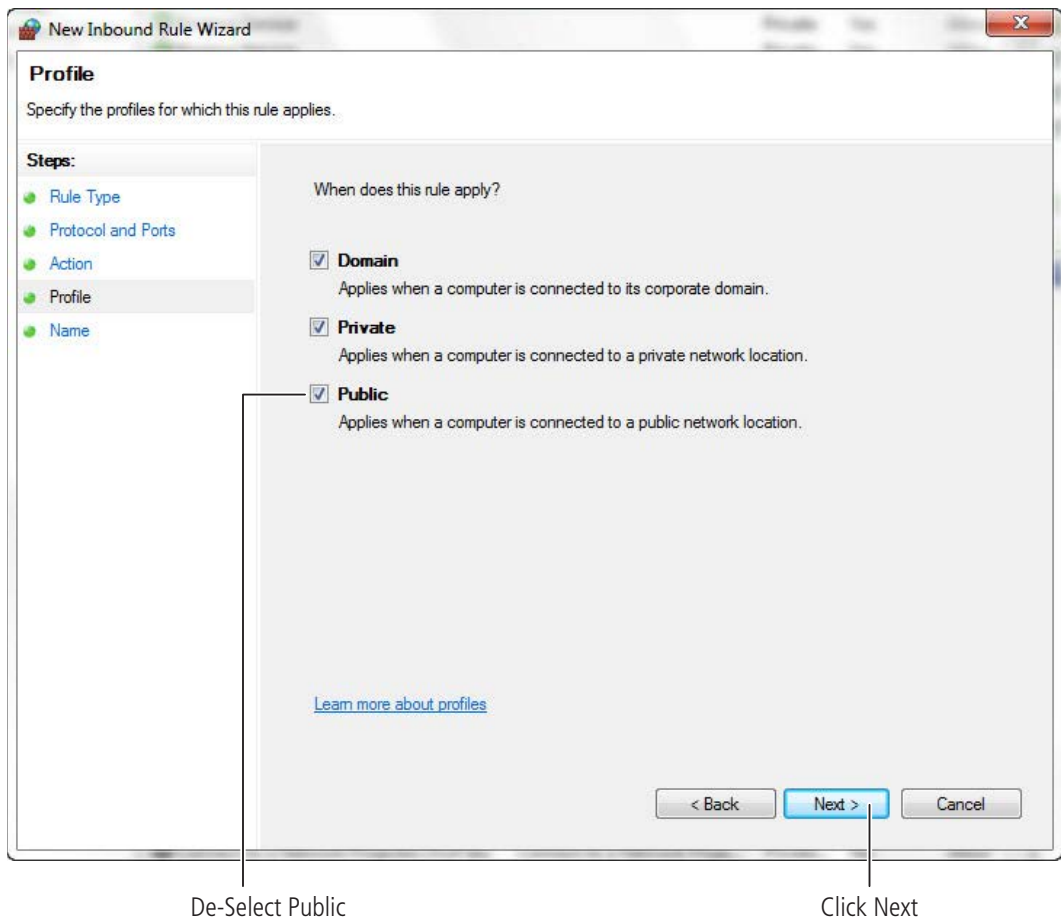
- 5 Enter the following ports into the "Specific local ports" field: 23, 80, 1443, 1434, 8000, 11000, 5353. Then, click Next to continue.

Figure 16 Allow the Connection



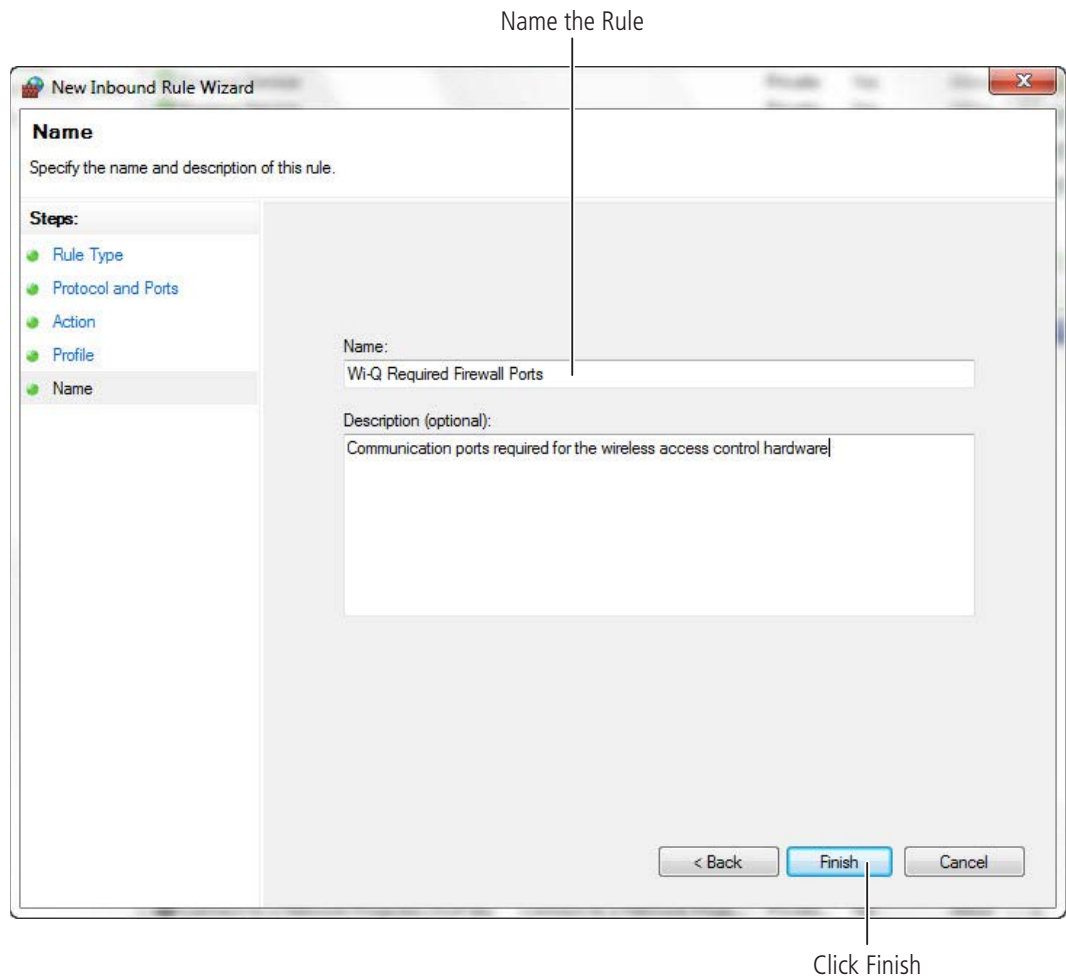
6 Select Allow the connection. Click Next to continue.

Figure 17 De-select Public



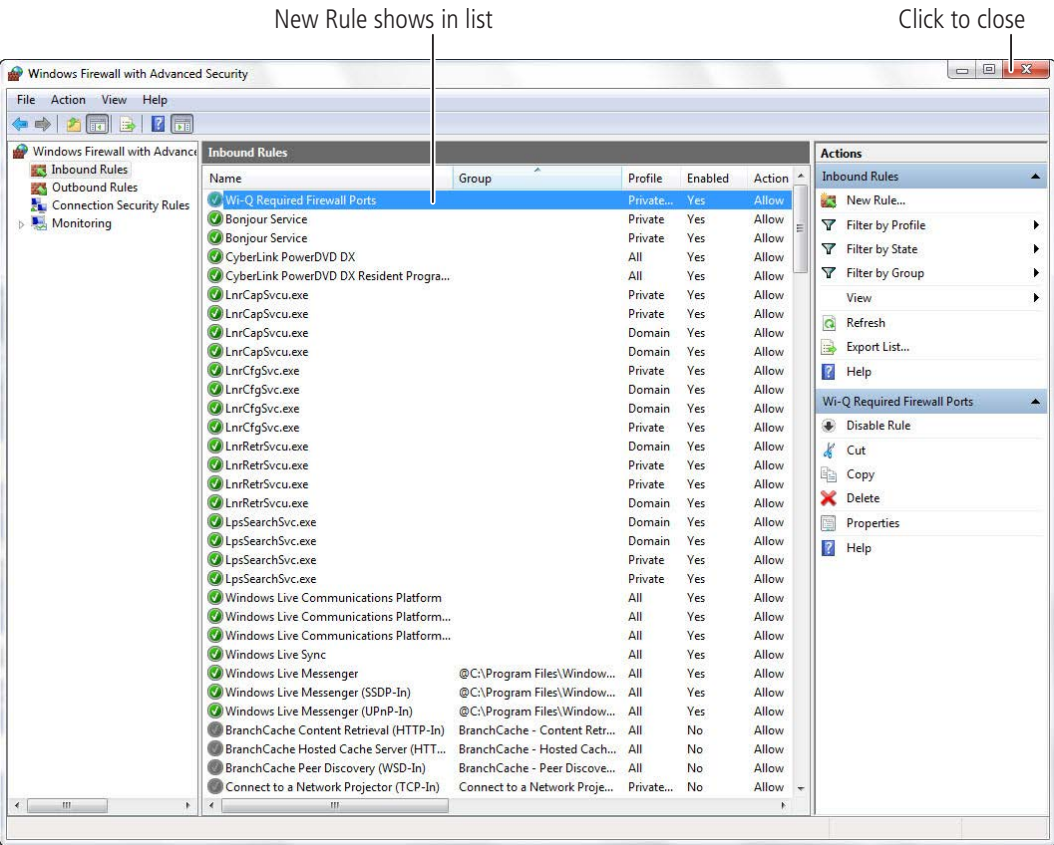
7 De-select the Public option. Click Next.

Figure 18 Name the Rule



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

Figure 19 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 Stanley 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 Portal 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 Portal Configuration Tool** — Provides a list of portal gateways on the network to configure.

The following prerequisites are required:

- .NET Framework 4.0
- 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

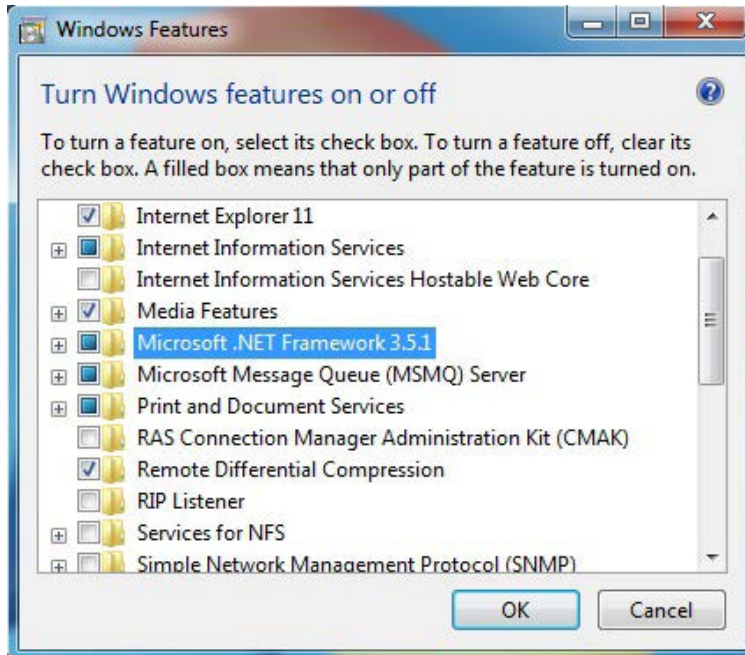
The second installation file packaged along with the Wi-Q Interface Software provides a communication link to the portal gateways.

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 7

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

Figure 20 Turn windows features on or off

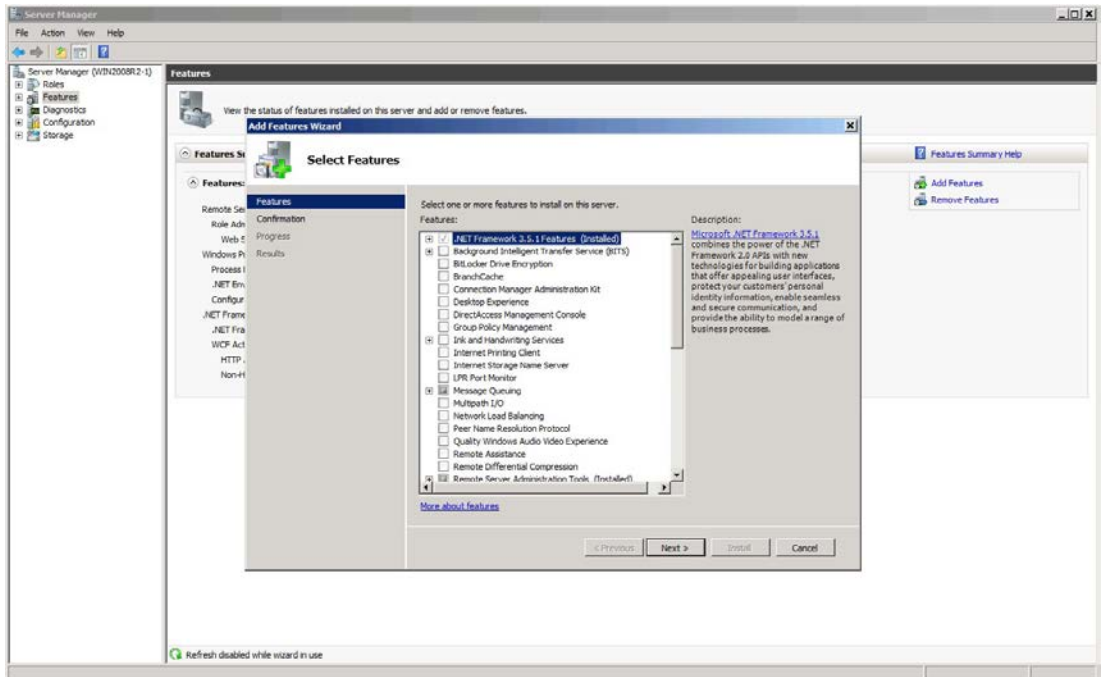


- 2 Check/fill in the check-boxes for Microsoft .NET Framework 3.5.1 and Microsoft Message Queue (MSMQ) Server if they are not already checked/filled in.
- 3 Select OK button to install.

Enabling .NET Framework and Microsoft Message Queuing for Windows Server 2008 R2

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

Figure 21 Add features wizard

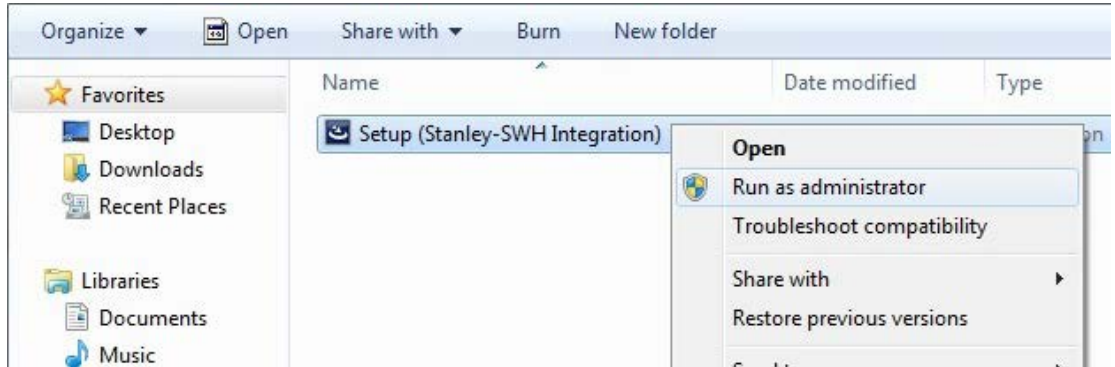


- 2 Select the Features section and, when selectable, select Add Features link.
- 3 Check/fill in the check-boxes for Microsoft .NET Framework 3.5.1 and Microsoft Message Queue (MSMQ) Server if they are not already checked/filled in.
- 4 Select Next button.
- 5 Select Install button for installation to begin.
- 6 Select Close button.

Start the Stanley Wi-Q Integration Installation Wizard

If you have not already done so, download the **Integration Stanley Wi-Q** file from the Stanley Technical Support website or Insert the software disc into your machine's disc reader.

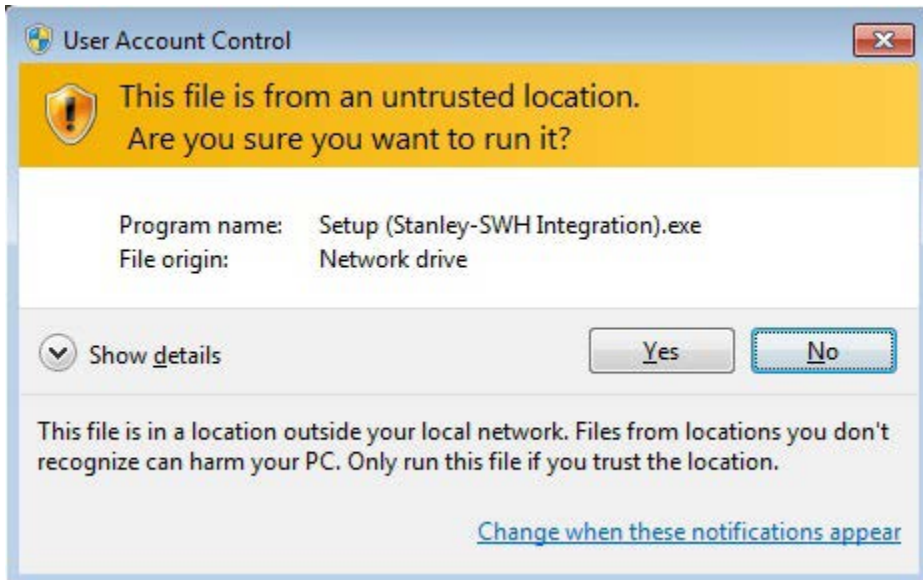
Figure 22 Setup (Wi-Q Router Host)



- 1 Right click the **Integration Stanley Wi-Q.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

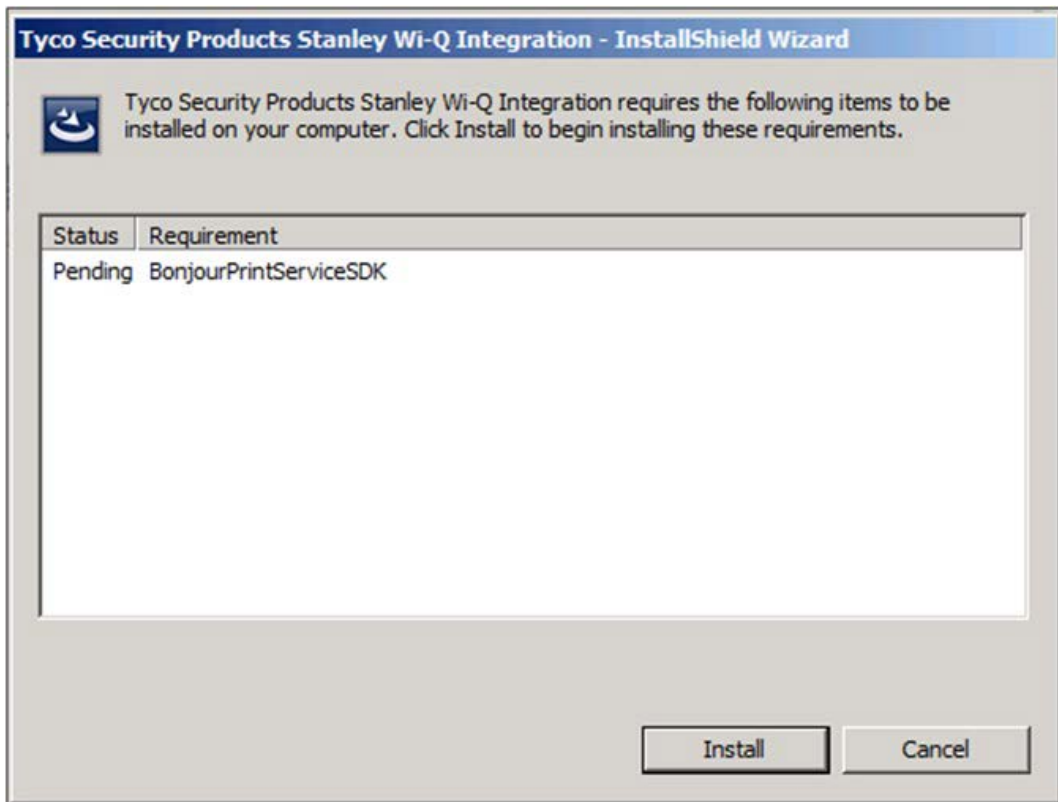
Figure 23 The Bonjour Print Services - InstallShield Wizard



- 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**.

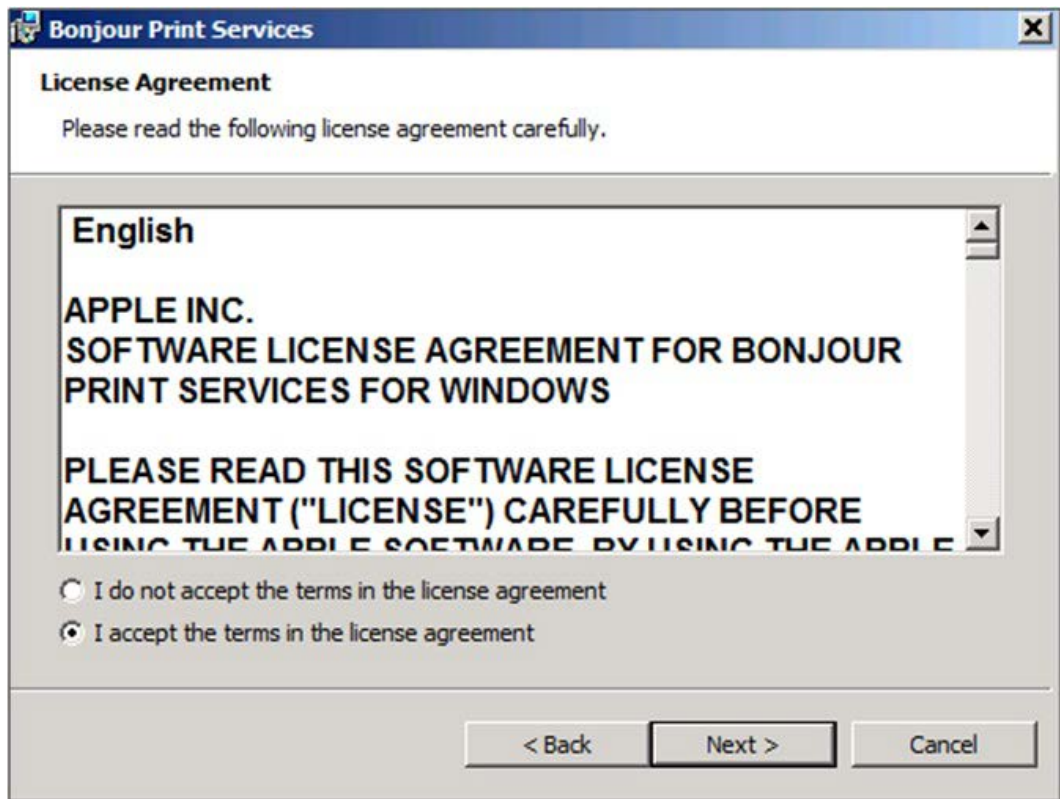
- 2 Select **Next** to continue to the End User License Agreement.

Figure 24 Bonjour End User License Agreement



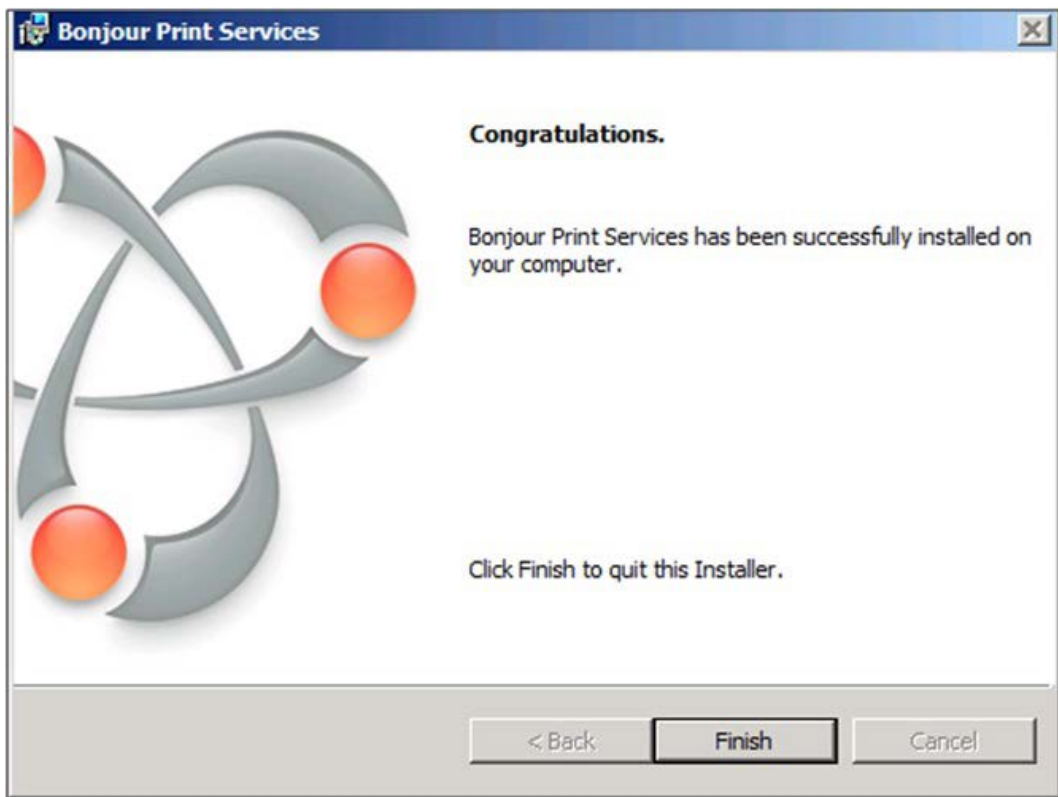
- 3 Read the License Agreement. To continue with the installation, click on "I accept the terms in the license agreement," then press **Next**.

Figure 25 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 26 Finish Installation



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

Installing the Wi-Q Interface Software

Figure 27 The Wi-Q Integration - InstallShield Wizard



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

Figure 28 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 29 Authentication

The screenshot shows a Windows-style dialog box titled "Tyco Security Products Stanley Wi-Q Integration - InstallShield Wizard". The main heading is "Database Server" with the instruction "Select database server and authentication method".

The "Database server that you are installing to:" section features a dropdown menu with "localhost" selected and a "Browse..." button to its right.

The "Connect using:" section has two radio button options: "Windows authentication credentials of current user" (which is selected) and "Server authentication using the Login ID and password below".

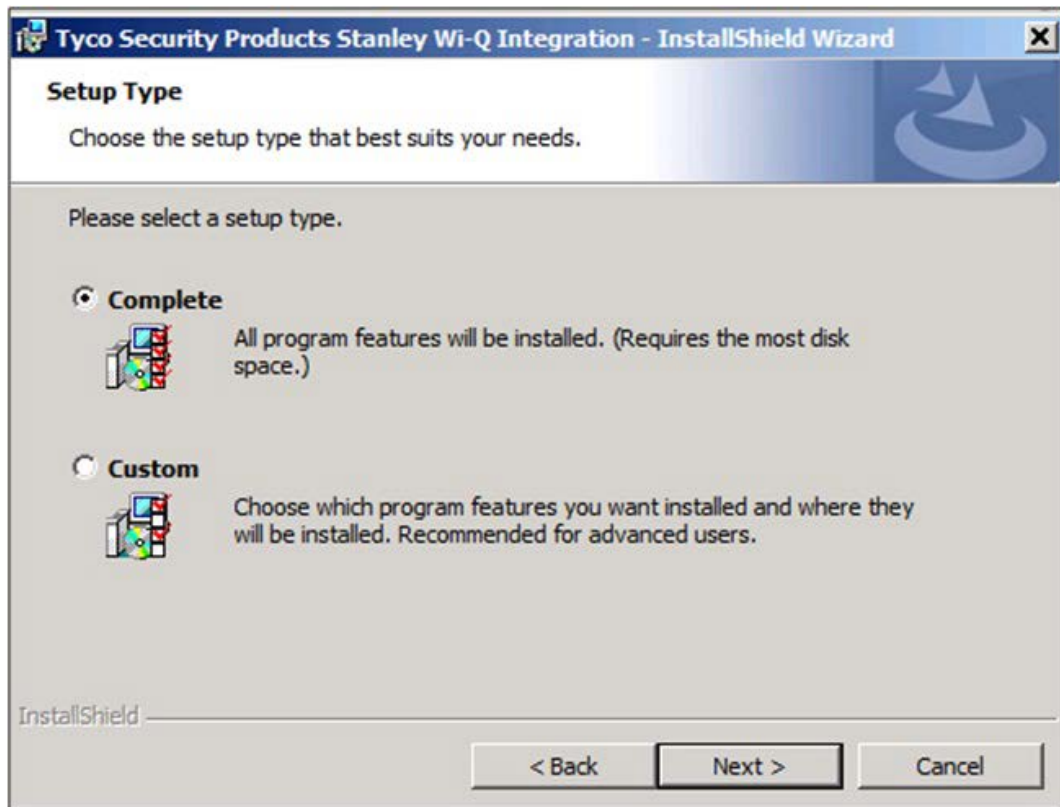
Below the radio buttons are two text input fields: "Login ID:" containing "sa" and "Password:" which is empty.

The "Name of database catalog:" section has a text input field containing "ACVSCORE" and a "Browse..." button to its right.

At the bottom left, the "InstallShield" logo is visible. At the bottom right, there are three buttons: "< Back", "Next >" (highlighted in blue), and "Cancel".

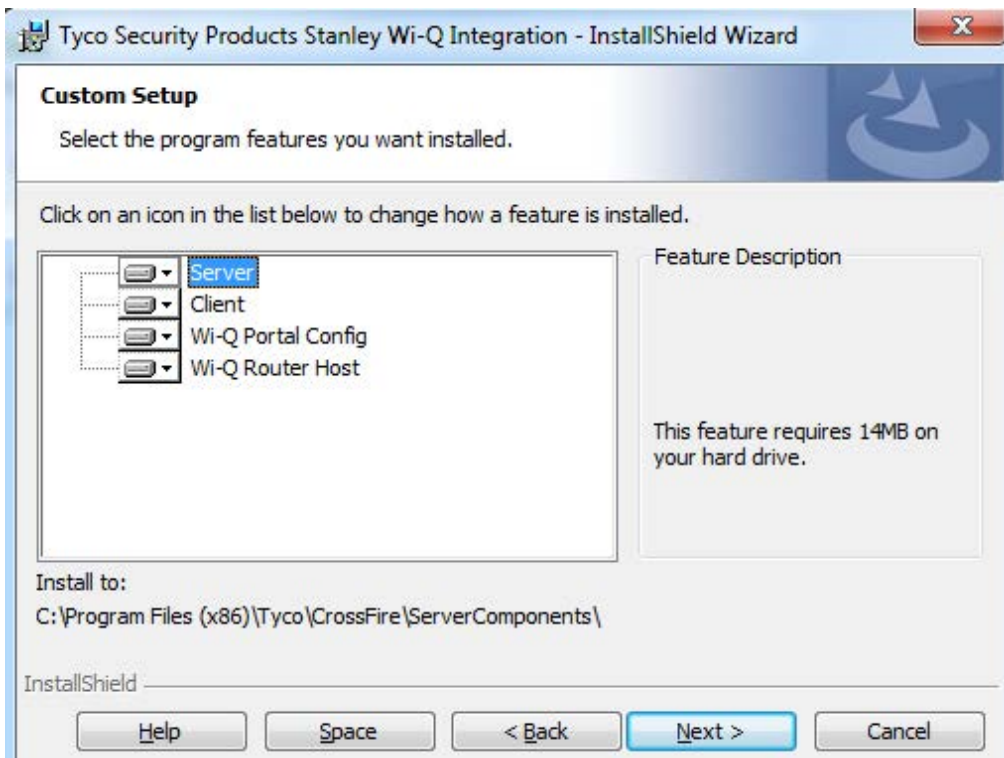
- 3 Select either Windows authentication or enter a Server authentication for the SQL database being used by the current C-Cure system. Select **Next**.

Figure 30 Complete or Custom Installation



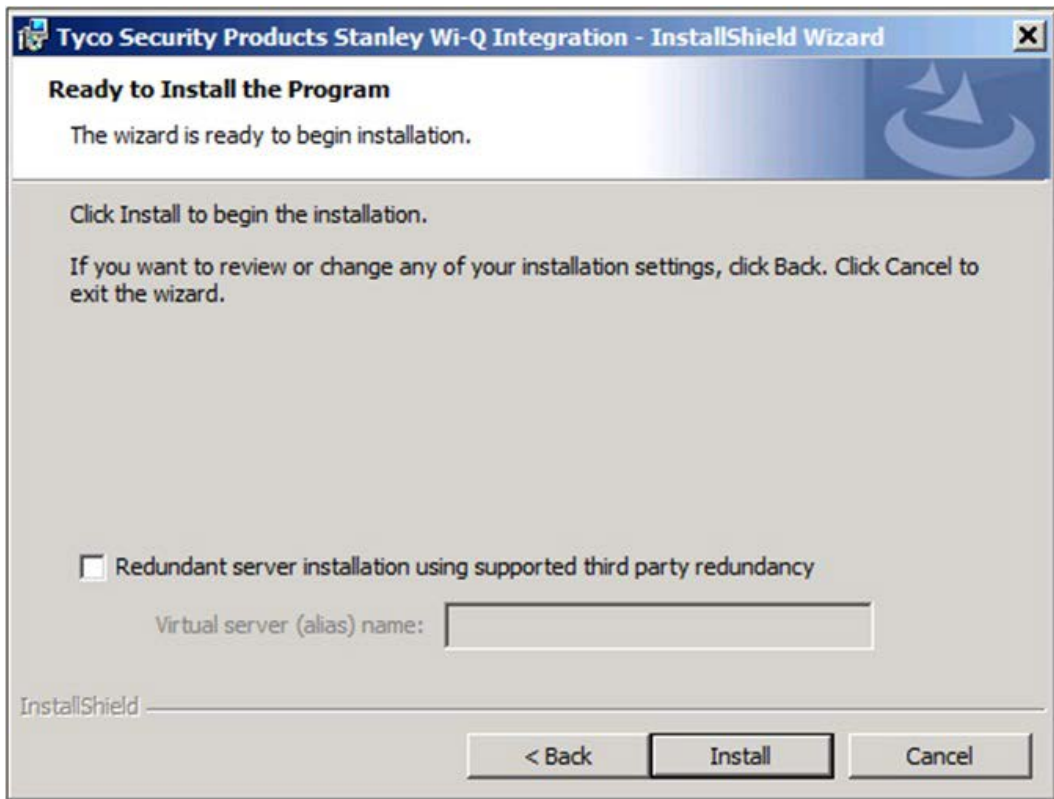
- 4 Select a Complete or Custom Installation and select **Next**.

Figure 31 Custom Installation



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

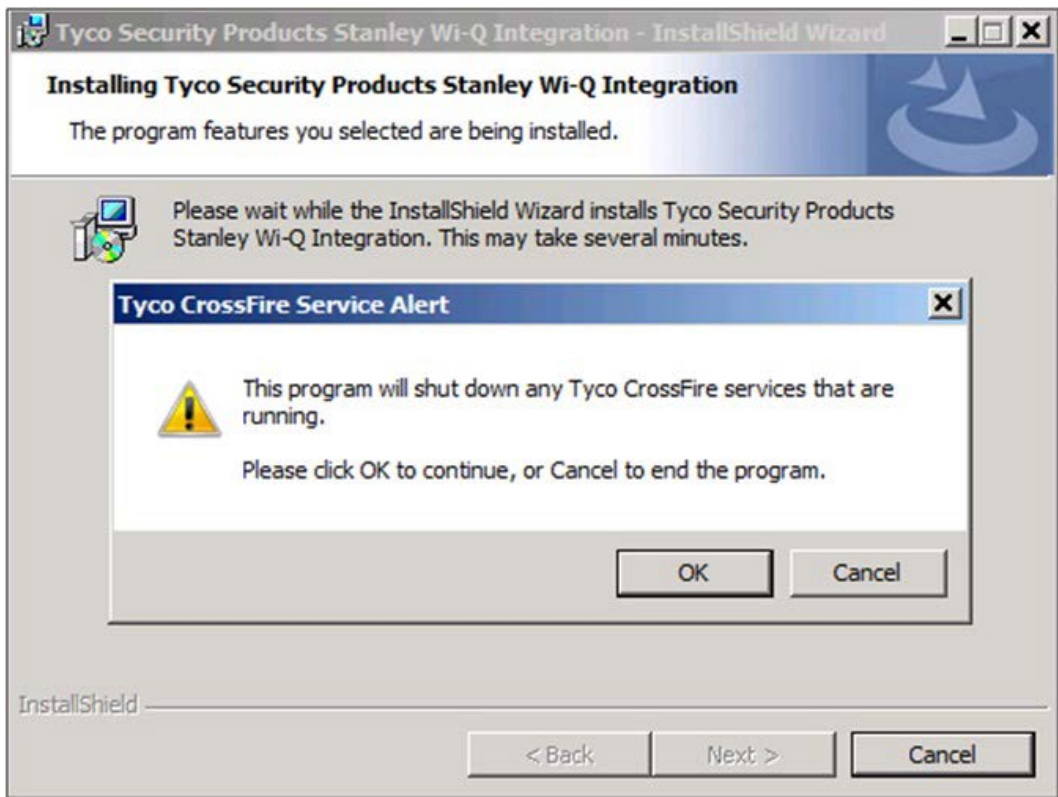
Figure 32 Install the Software



6 Select the **Install** button.

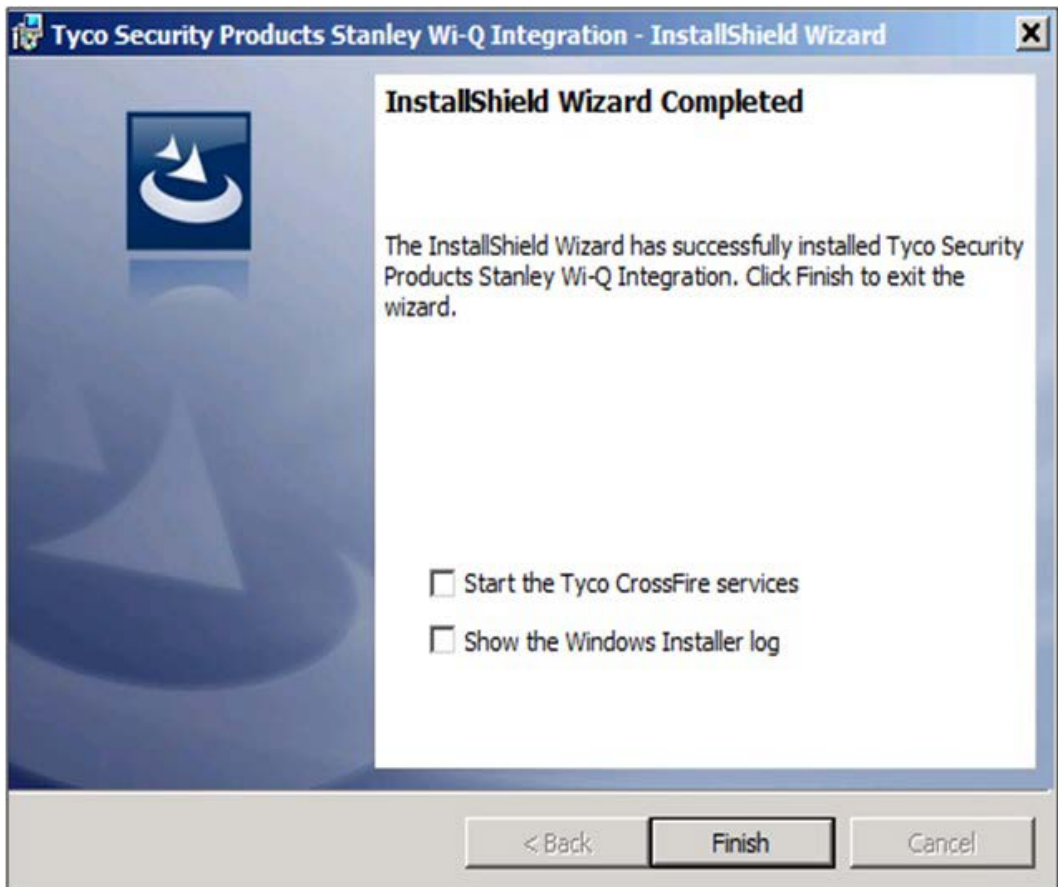
Note A redundant server installation using a third party redundancy option is not supported in Stanley Wi-Q integration with C-Cure. 9000

Figure 33 Stop the CrossFire Services



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

Figure 34 Finishing the Installation



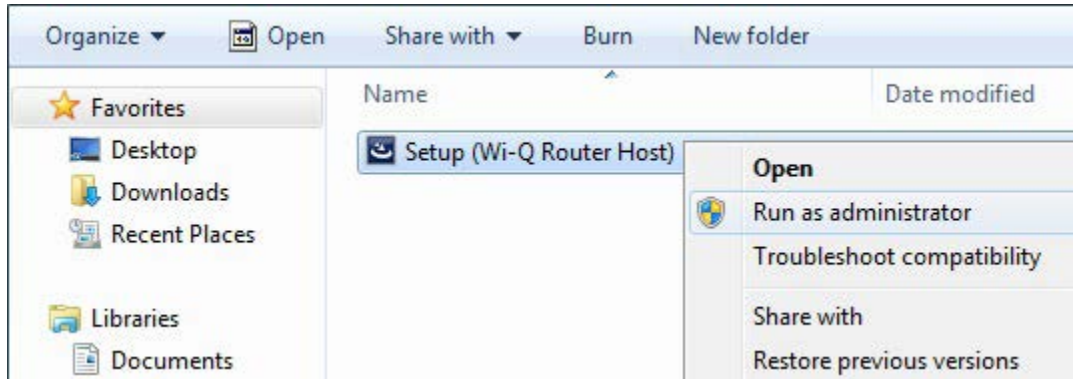
- 8 Choose whether to start the Tyco CrossFire and Stanley Wi-Q Services.
- 9 Choose whether to see the Windows Installer log.
- 10 Select **Finish** to complete the installation.

Wi-Q Router Host Service Installation Steps

(The following steps are for CCure 2.1 or 2.2 when installing the Wi-Q Router Host Service Separate)

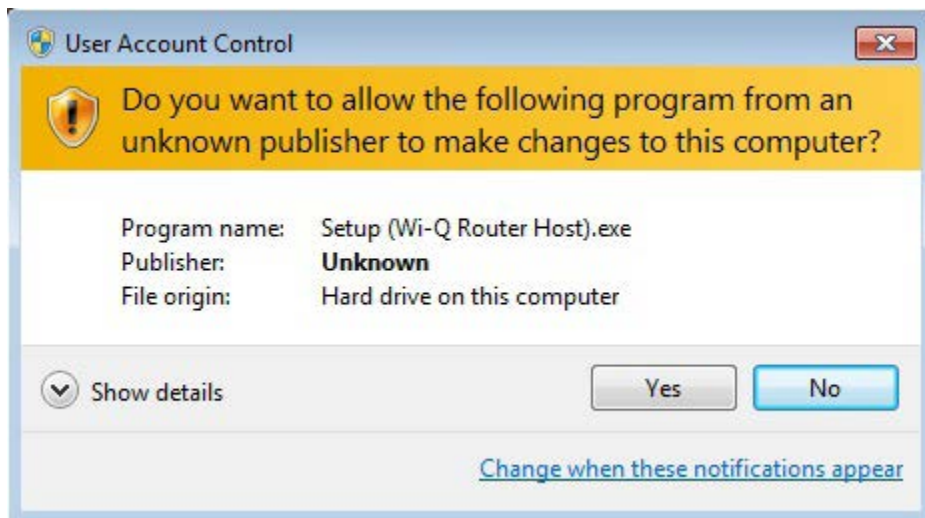
- 1 Right click the Setup (Wi-Q Router Host).exe file and select Run as Administrator.

Figure 35 Setup (Wi-Q Router Host)

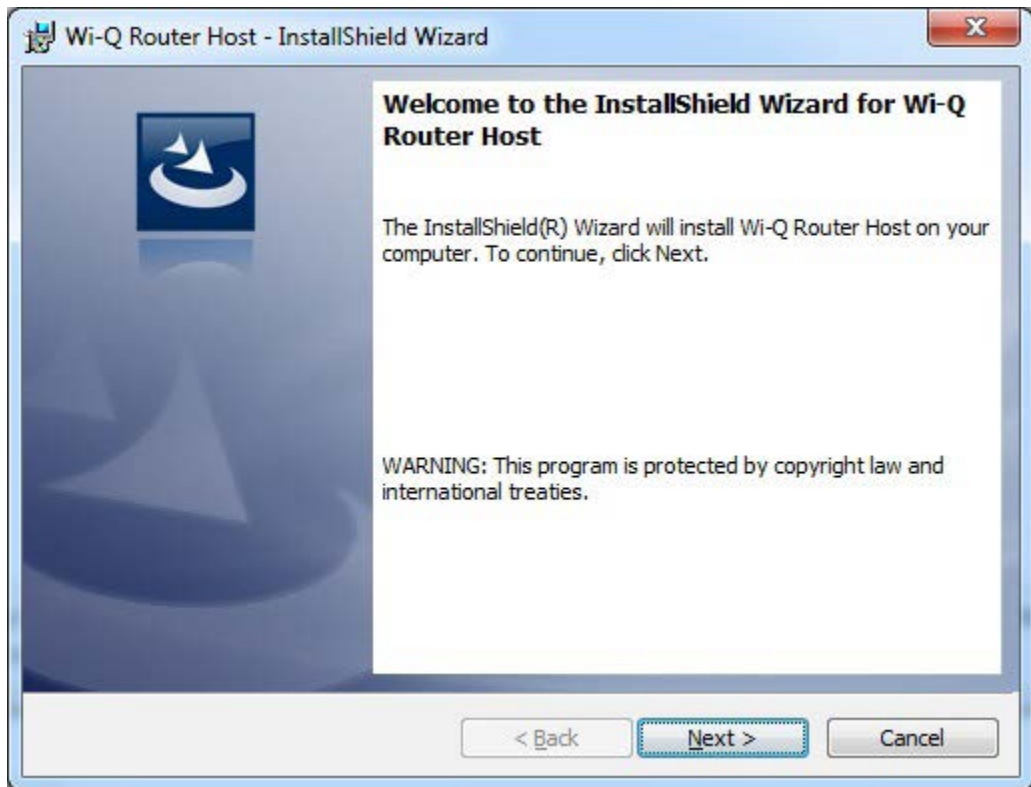


- 2 Select Yes when asked for permission to make changes to the computer.

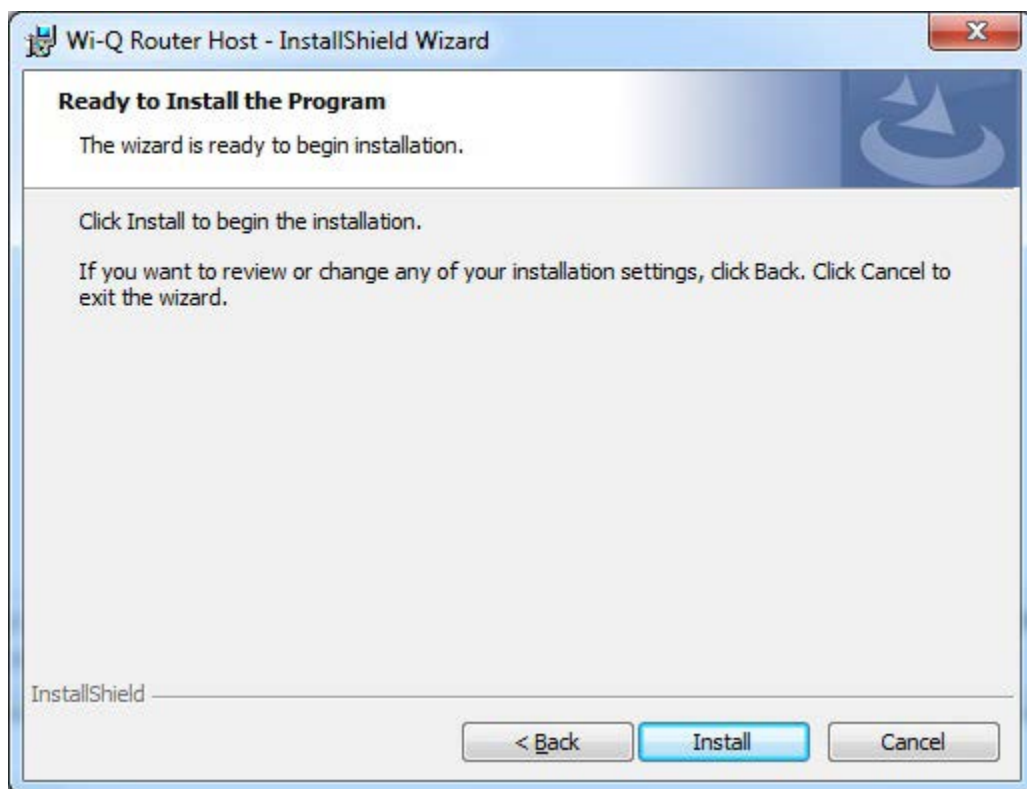
Figure 36 User Account Control



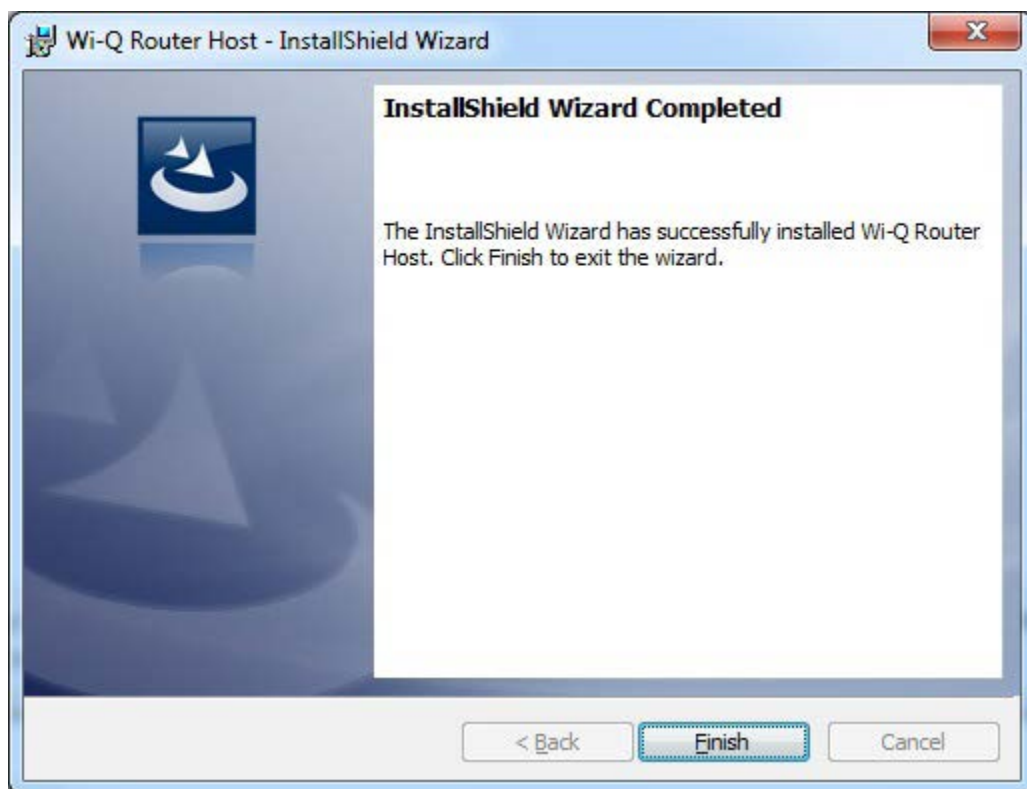
- 3 Select Next to continue to prepare for installation.



- 4 Select Install begin installation.



- 5 Select Finish to complete the installation.



4

Software Configuration

This chapter will guide you through performing the following tasks:

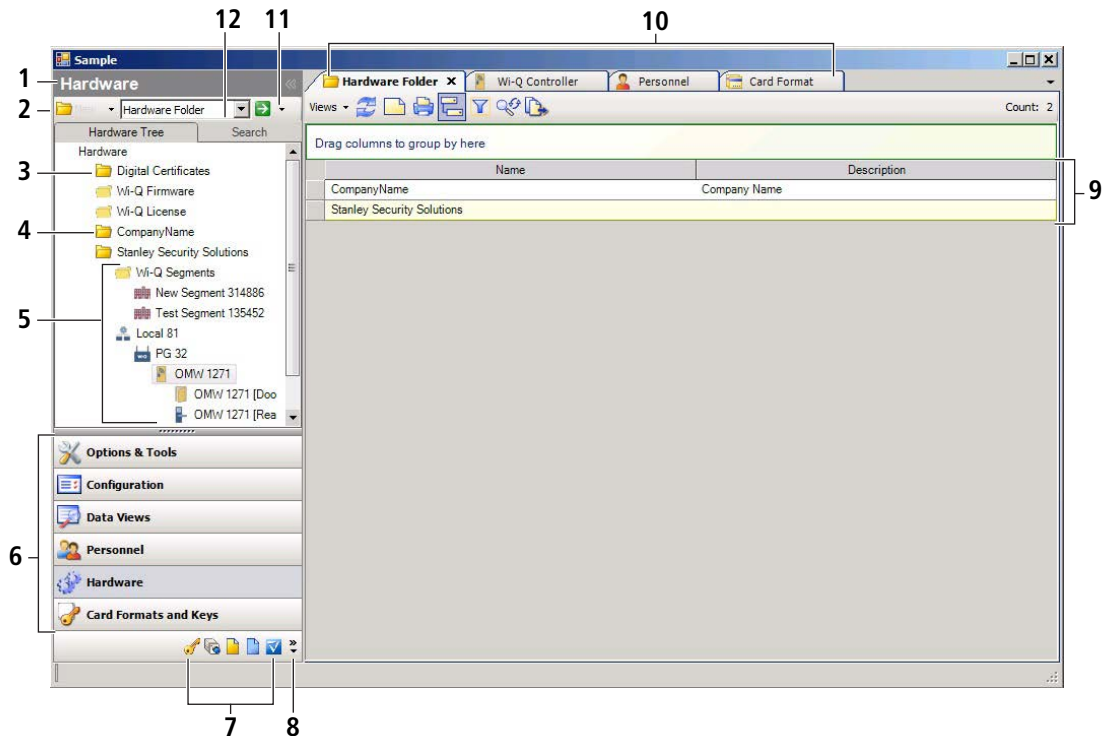
Task 6 — Configure Hardware on Host

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 37.

Figure 37 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 Dock

As the overall window or the Navigation Button Pane is resized and buttons disappear from the bottom of the list, they reappear on the Navigation Button Dock.

8 Navigation Button Pane Options

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

9 View

Displays the results of a search for the item displayed in the Navigation Button Drop-Down List (Item 12).

10 View Tabs

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

11 Search Button

Initiates a search for the item displayed in the Navigation Button Drop-Down List (Item 12) and displays the results in the Dynamic View window.

12 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

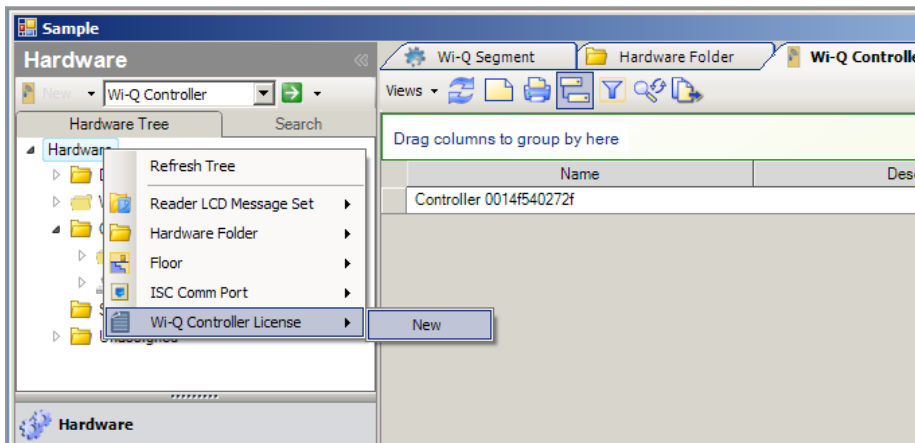
If not already accomplished during the installation of the Wi-Q Interface Software, or to install an upgrade, complete the following steps. Please see www.swhouse.com for contact information regarding controller licenses.

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.

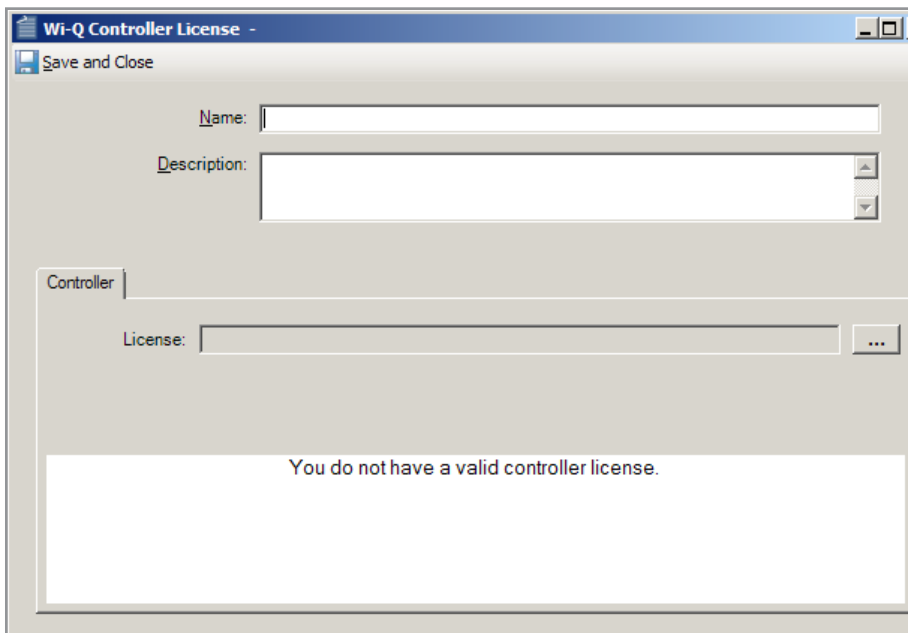
Adding a New Controller License

Figure 38 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 39 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.

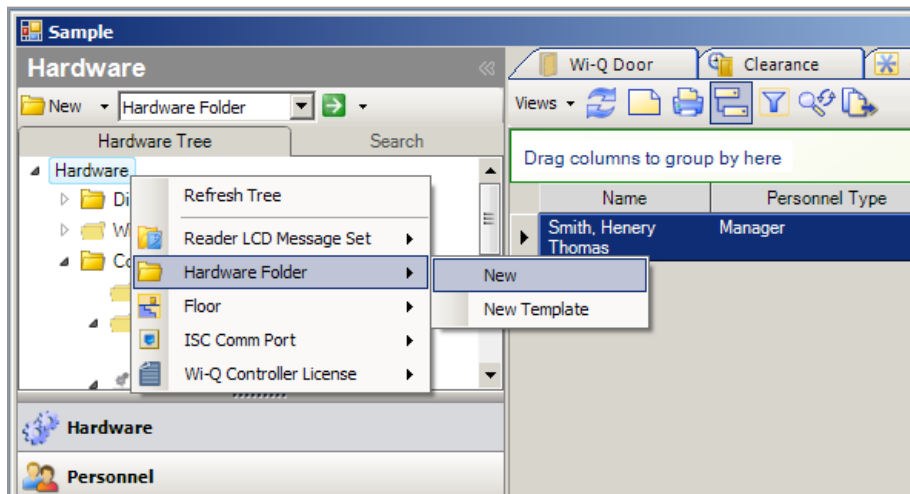
- 5 Click **Save and Close** in the upper left hand corner of the dialog box to finish.

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 40 Creating a Hardware Folder

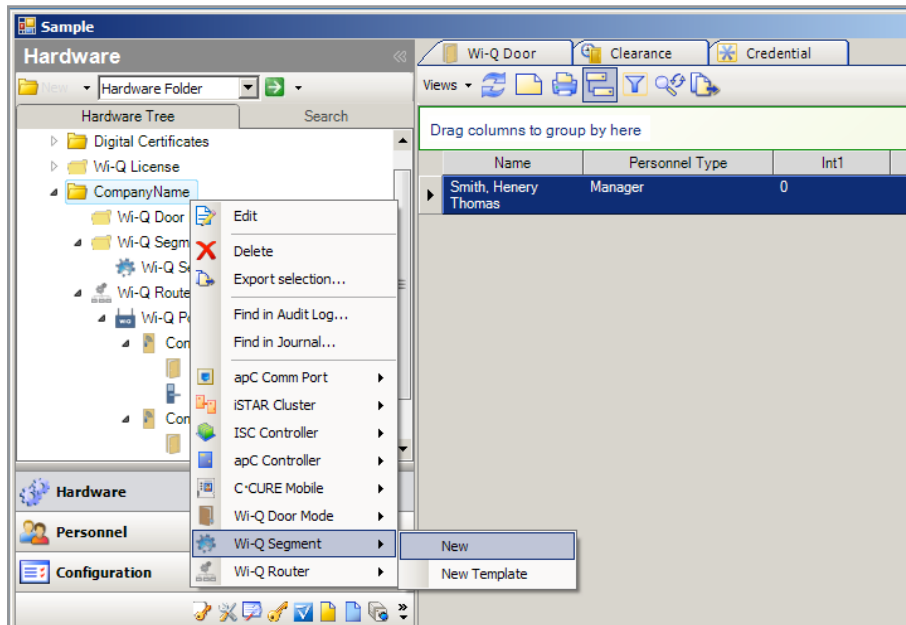


- 1 Click on the Hardware pane in the left column to display the hardware tree in the display panel if it is not already displayed.
- 2 Right click the Hardware heading at the top of the hardware tree and select **Hardware Folder -> New**.
- 3 In the dialog box that appears, name the folder and add an 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 Portal Gateways that can be assigned to one segment, and there are no limitations to the number of segments.

Figure 41 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 42 Wi-Q Segment Dialog Box

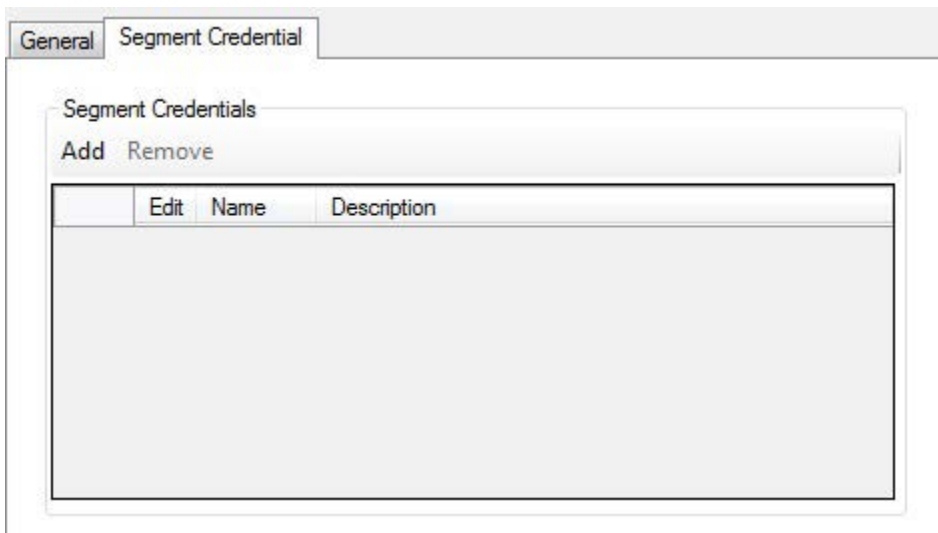
The screenshot shows a window titled "Wi-Q Segment - Test Segment 144438". At the top, there are two buttons: "Save and Close" and "Save and New". Below these are two text input fields: "Name" with the value "Test Segment 144438" and "Description" with the value "This is a create Wi-Q Segment". Below the description field are two tabs: "General" (which is selected) and "Segment Credential". Under the "General" tab, there is a "Sign On Key" field with the value "144438" and a "PIN Length" field with a spinner set to "4". Below these is a "Daylight Savings" section containing a "Time Zone" dropdown menu (set to "(GMT-08:00) Pacific Time (US & Canada)" with an ellipsis button to its right) and four more dropdown menus: "DST Ahead Month" (set to "March"), "DST Ahead Sunday" (set to "Second Sunday"), "DST Back Month" (set to "November"), and "DST Back Sunday" (set to "Last Sunday").

- 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 23). 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

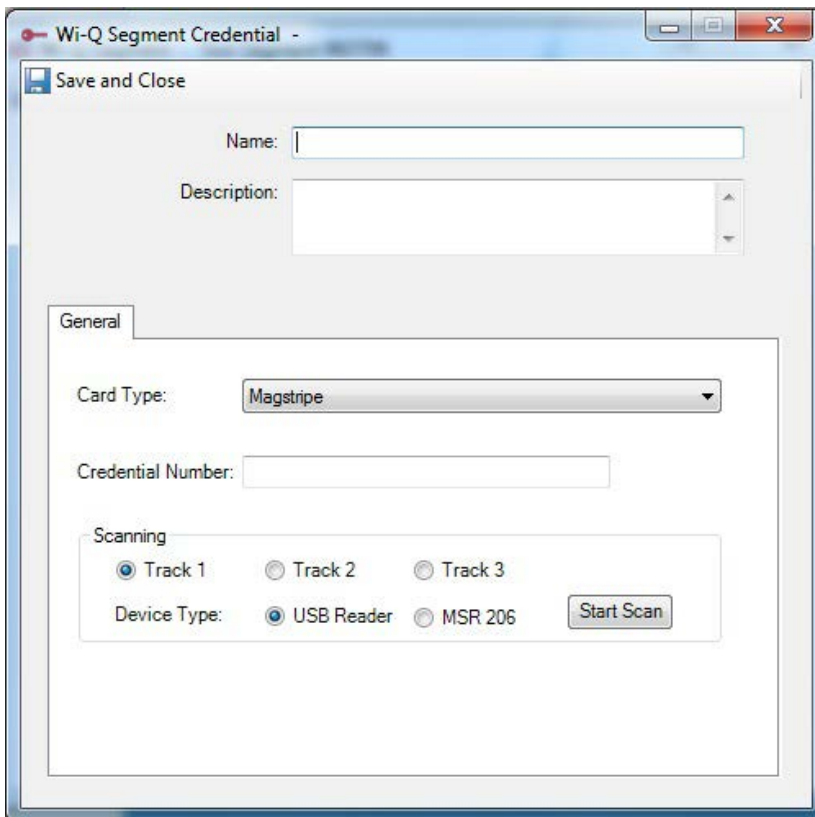
The **Segment Credential** tab allows you to add a Card Sign On Credential so you can use a card to sign on wireless card readers.

Figure 43 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.

Figure 44 Wi-Q Segment Credential Dialog Box



- 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.

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 portal gateway created first. See "Signing on Controllers (Task 9)" on page 23.

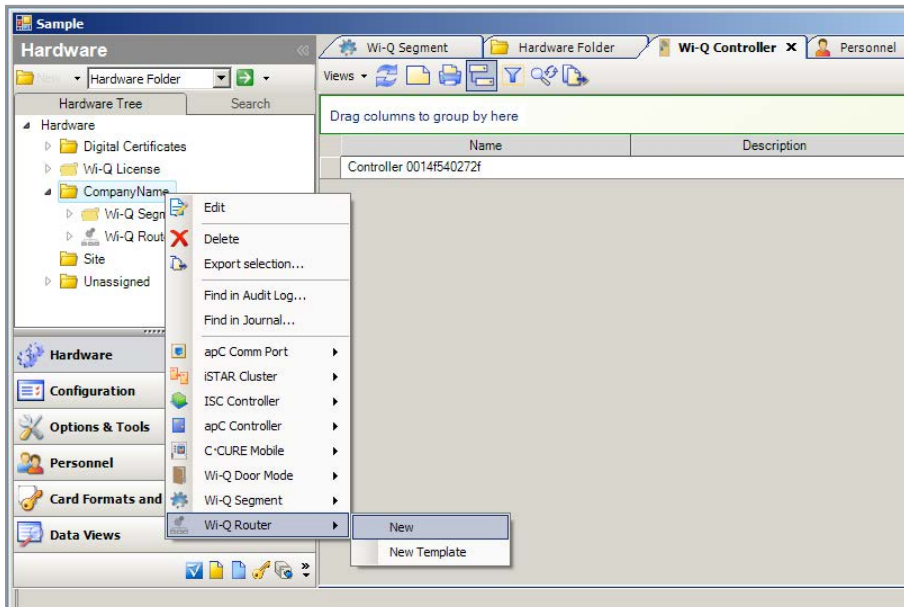
Note The option to delete a segment from the Segment tree becomes available when you right-click the segment from within the tree.

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.

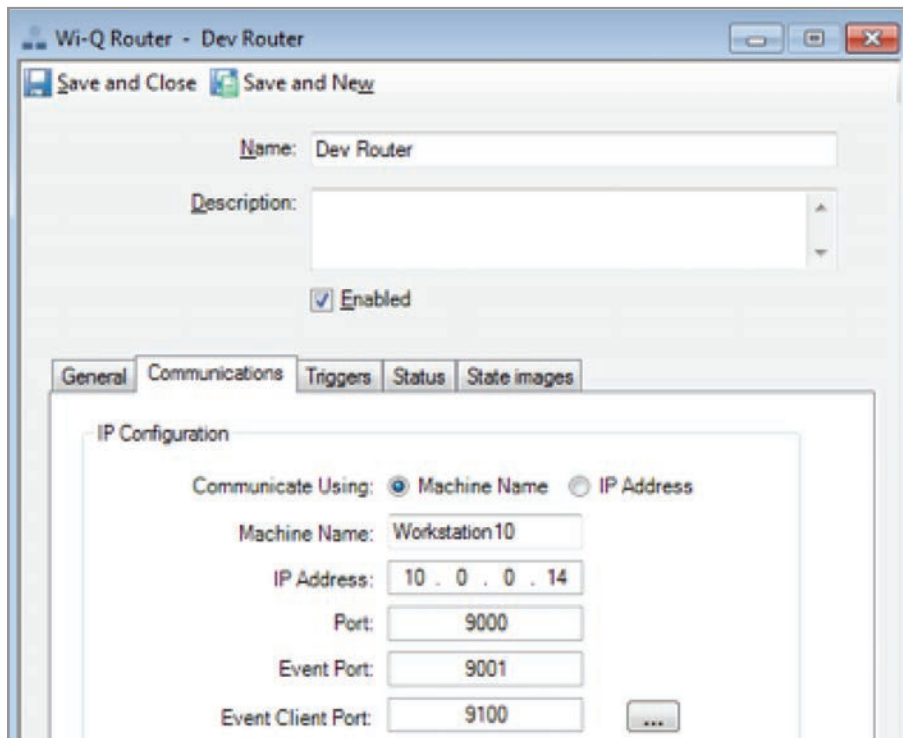
When the router software is installed, the IP address, subnet mask and gateway of the computer should be recorded and provided for use during configuration.

Figure 45 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 46 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.

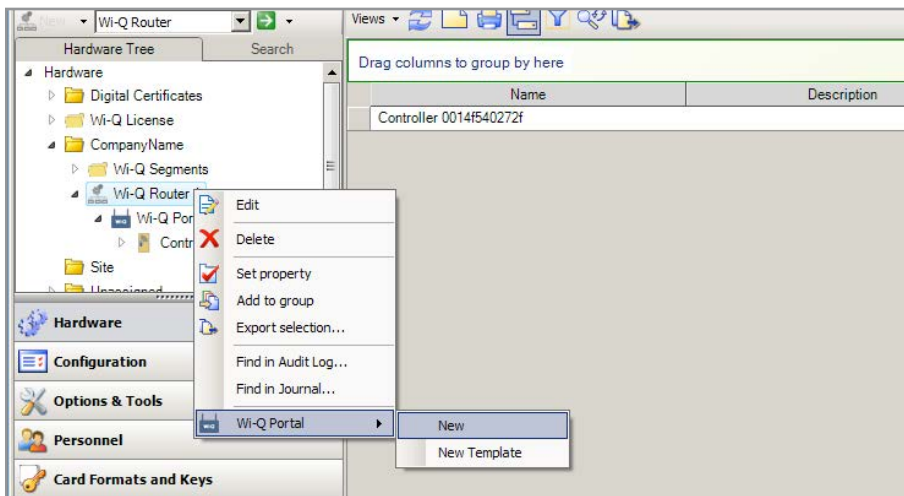
Adding and Configuring Portal Gateways

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

Portals are configured from the factory with an IP address of 192.168.1.200. When configuring a portal gateway, it is best to connect directly to the portal before placing it on the network. This removes the possibility of duplicate IP addresses on the network.

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

Figure 47 Adding a Portal 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 portal to in the hardware tree and select **Wi-Q Portal -> New**.

Figure 48 Portal Dialog Box

Wi-Q Portal - Dev Portal Sim 8000

Save and Close Save and New

Name: Dev Portal Sim 8000

Description:

☒ Enabled

General Communications Segment Journaling Triggers Status State Images

IP Configuration

Communicate Using: ☐ IPv4 ☒ IPv6

IPv4 Address: 10 . 0 . 0 . 14

IPv6 Address: 0004:0003:6666:0004:0005:4546:0045:4564

Portal Service Port: 8000

... ☐ SSL Enabled

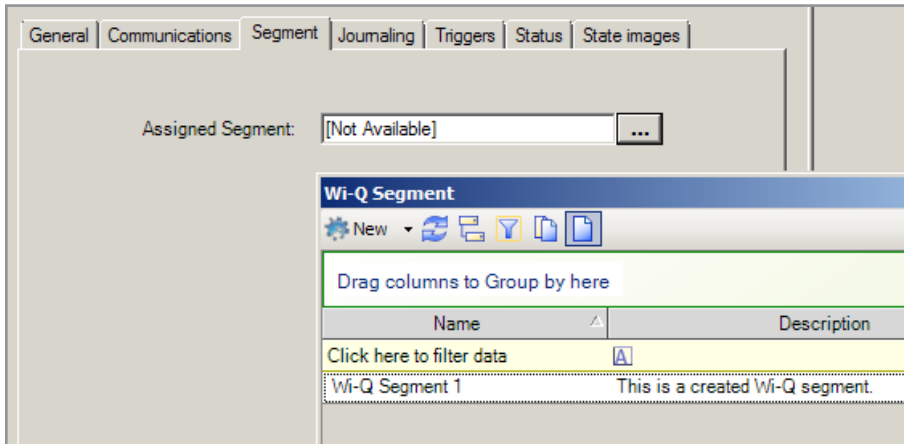
Channels

<input type="checkbox"/> 11	<input type="checkbox"/> 15	<input type="checkbox"/> 19	<input type="checkbox"/> 23
<input type="checkbox"/> 12	<input type="checkbox"/> 16	<input type="checkbox"/> 20	<input type="checkbox"/> 24
<input type="checkbox"/> 13	<input type="checkbox"/> 17	<input type="checkbox"/> 21	<input checked="" type="checkbox"/> 25 (Primary)
<input type="checkbox"/> 14	<input type="checkbox"/> 18	<input type="checkbox"/> 22	<input checked="" type="checkbox"/> 26 (Primary)

- 3 Enter the portal 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 portal. 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 portal with the Portal 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 portal.
- 8 Select the radio channels you wish this portal to use. Each portal has two radios that communicate on separate channels; the default channels are 25 and 26. In an environment with several portals or other

wireless devices in close proximity, alternate channels should be selected. Otherwise they can be left at the default settings.

Figure 49 Assigning a Portal 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 Portal dialog box to finish. The new portal will appear in the hardware tree.

Note When right-clicking on a portal, the following options become available:

- Delete the portal
- Partial download
- Full download of data to the portal
- Reset the portal
- Perform firmware update

Adding and Configuring Wi-Q Controllers

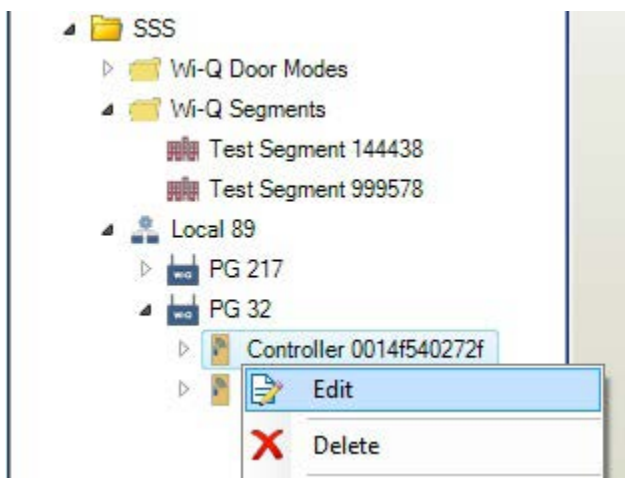
There are 2 options for adding the controllers, Automatic or Manual:

- 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 23.
- 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 router you are assigning the portal to in the hardware tree and select Wi-Q Controller -> New.
 - 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 portal gateways they are assigned to. Now they need to be enabled and configured.

Selecting a Wi-Q Controller

Figure 50 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 portal 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 51 Configuring Wi-Q Controllers - Communications Tab

The screenshot shows a window titled "Wi-Q Controller - Controller 0014f5401321". At the top, there are buttons for "Save and Close" and "Save and New". Below these are fields for "Name" (set to "Controller 0014f5401321") and "Description". A checkbox labeled "Enabled" is checked. Below the fields are tabs for "General", "Communications", "Journaling", "Triggers", "Status", and "State images". The "Communications" tab is active, showing a "Channels" section with a grid of checkboxes for channels 11 through 26. Channels 11-24 are all checked. Channels 25 and 26 are checked and labeled "(Primary)". Below the channels is a "Beacon" section with "Beacon Time (seconds)" set to 60 and "Beacon Offline Count" set to 5.

Wi-Q Controller - Controller 0014f5401321

Save and Close Save and New

Name: Controller 0014f5401321

Description:

☒ Enabled

General Communications Journaling Triggers Status State images

Channels

<input checked="" type="checkbox"/> 11	<input checked="" type="checkbox"/> 15	<input checked="" type="checkbox"/> 19	<input checked="" type="checkbox"/> 23
<input checked="" type="checkbox"/> 12	<input checked="" type="checkbox"/> 16	<input checked="" type="checkbox"/> 20	<input checked="" type="checkbox"/> 24
<input checked="" type="checkbox"/> 13	<input checked="" type="checkbox"/> 17	<input checked="" type="checkbox"/> 21	<input checked="" type="checkbox"/> 25 (Primary)
<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 18	<input checked="" type="checkbox"/> 22	<input checked="" type="checkbox"/> 26 (Primary)

Beacon

Beacon Time (seconds): 60

Beacon Offline Count: 5

- 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 80.

- 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 portal gateway. Once a controller has found a portal 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 portal gateway.
- 3 The Beacon Time is how often (in seconds) the controller turns on its radio and exchanges messages with its portal 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 portal gateway to time-out its efforts to establish contact with the controller, after which the portal 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 52 Configuring Wi-Q Controllers - Journaling Tab

The screenshot shows the 'Journaling' tab selected in a configuration window. The window has several tabs: 'General', 'Communications', 'Journaling' (active), 'Triggers', 'Status', and 'State images'. The 'Journaling' tab contains two main sections: 'Statistics' and 'Transactions'. In the 'Statistics' section, there is a checkbox labeled 'Journal Statistics Messages:' which is currently unchecked. To its right is the word 'Enabled'. Below this is a text box labeled 'Statistics Update Interval (Seconds):' with the value '86400' entered. In the 'Transactions' section, there is a single button labeled 'Configure'.

- 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 53 Configuring Wi-Q Controllers - Transactions Dialog Box

Ty ID	Transaction Type	Transaction	Priority
0	Alarm Cleared	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1	Entry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	Attempt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Set Access Level	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Low Battery Shutdown	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Motor Fault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Request To Exit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Door Open Too Long	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Door Latch Open	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Forced Entry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Connect Attempt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons: Select All Transactions, Select All Priorities, Clear All Transactions, Clear All Priorities, OK, Cancel

- 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.

Additional Right Click Options for Items in the Hardware Tree

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 portals or controllers are associated with it.
- Portal -> Delete — Allows a portal to be deleted if no controllers are associated with it.
- Portal -> Partial Download — Sends a partial download of data to a portal.
- Portal -> Full Download — Sends a full download of data to a portal.
- Portal -> Reset — Resets a portal.
- Portal -> Firmware Update — Updates firmware.
- Router -> Delete — Allows a router to be deleted if no portals are associated with it.
- Router -> View Network Portals — Displays the Wi-Q Portals that are on the network.
- 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 Portal.
- Controller -> Firmware Update — Updates firmware.
- 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.

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.

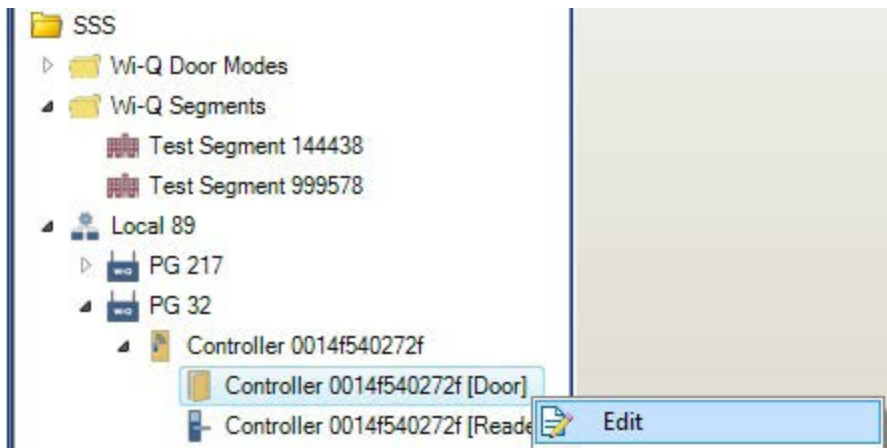
You will also find information about Firmware Updates in the C-CURE Wi-Q Interface Configuration Tool. Finally, you will be provided with a term comparison chart of events/transactions that are viewable in C-CURE Wi-Q Alarm Monitoring and the Controllers tab of C-CURE Wi-Q software.

Configuring the Wi-Q Doors and Readers

G-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 54 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 55 Timing

The screenshot shows a software window titled "Wi-Q Door - WDC 272f [Door]". Inside the window, there is a "Save and Close" button at the top left. Below it, there are two text input fields: "Name:" with the value "WDC 272f [Door]" and "Description:" which is empty. Below these fields is a tabbed interface with five tabs: "General", "Timing", "Modes", "Groups", and "Triggers". The "Timing" tab is currently selected. Under the "Timing" tab, there are four spin box controls, each with a label and a numerical value: "Unlock Time (seconds):" with a value of 3, "Shunt Time (seconds):" with a value of 3, "Unlock Delay (seconds):" with a value of 0, and "Shunt Delay (seconds):" with a value of 0.

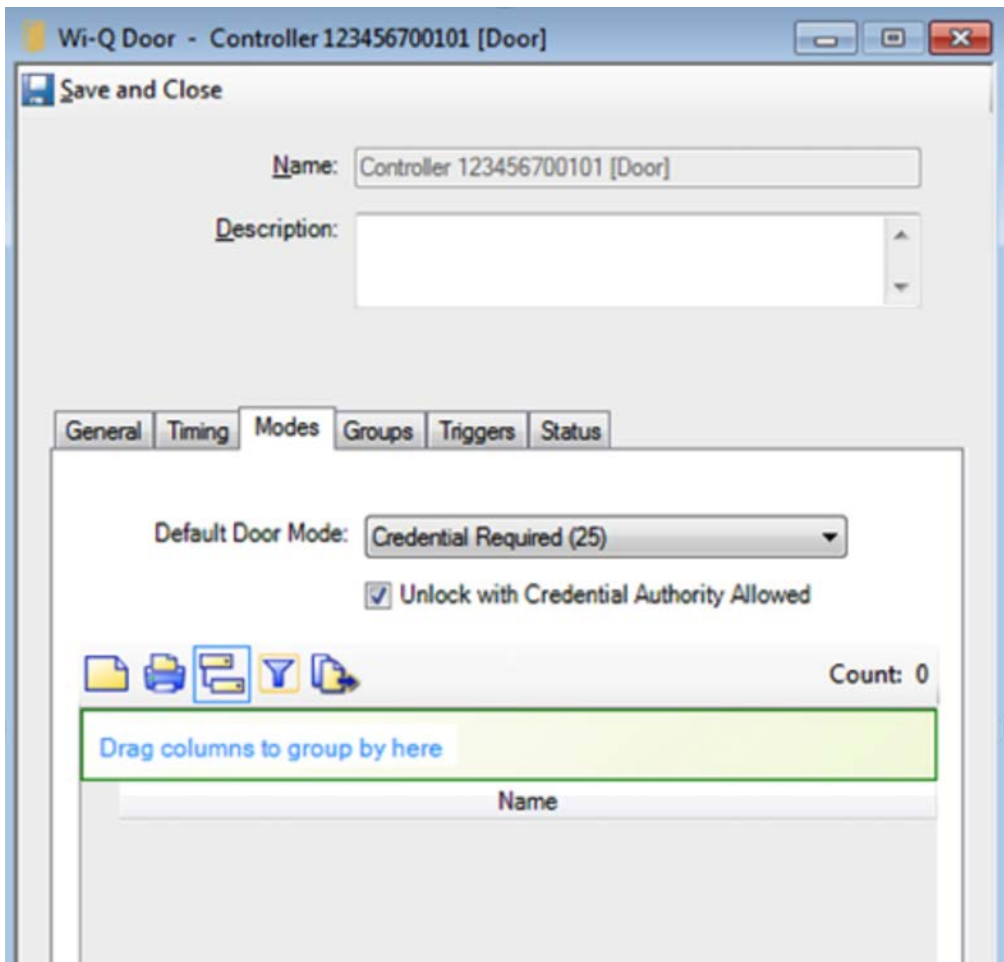
3 Click the **Timing** Tab.

4 Enter values for the following fields:

- Operate Time — 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.
- Operate 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 56 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.

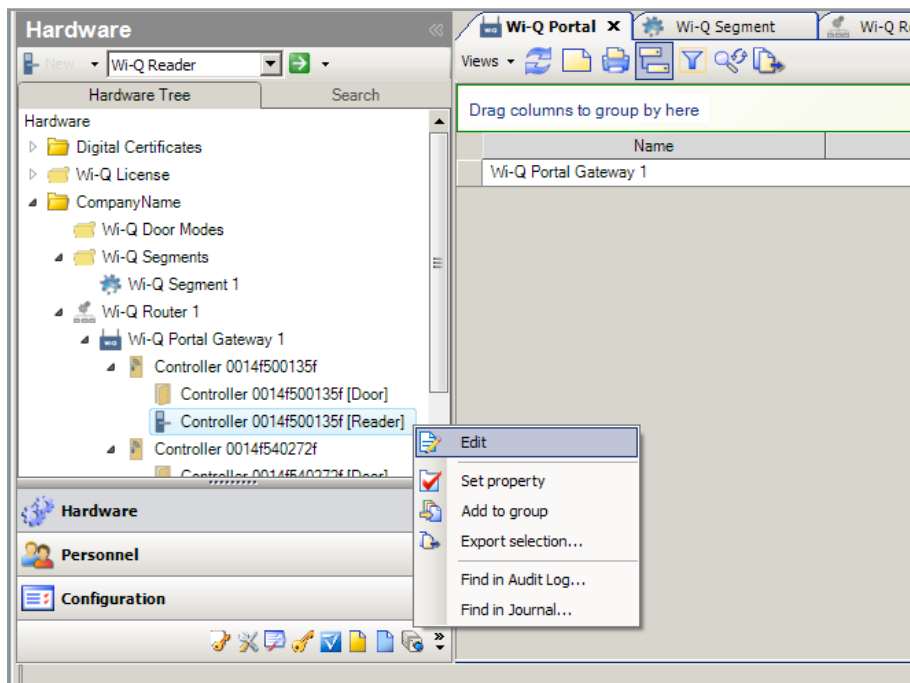
- General Tab — This tab shows the controller associated with the door and can not be changed.
- Groups Tab — Displays the groups that this door belongs to.
- Triggers Tab — Assigns an action if certain events are detected. You must select "Wi-Q Override Access Level" under "Action" to generate Wi-Q 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	Card ID 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.
5	Unlock with Credential	Any credential (card or keypad) will unlock the door and it will stay unlocked.
0	Unlock	The door is unlocked, anyone can open it.

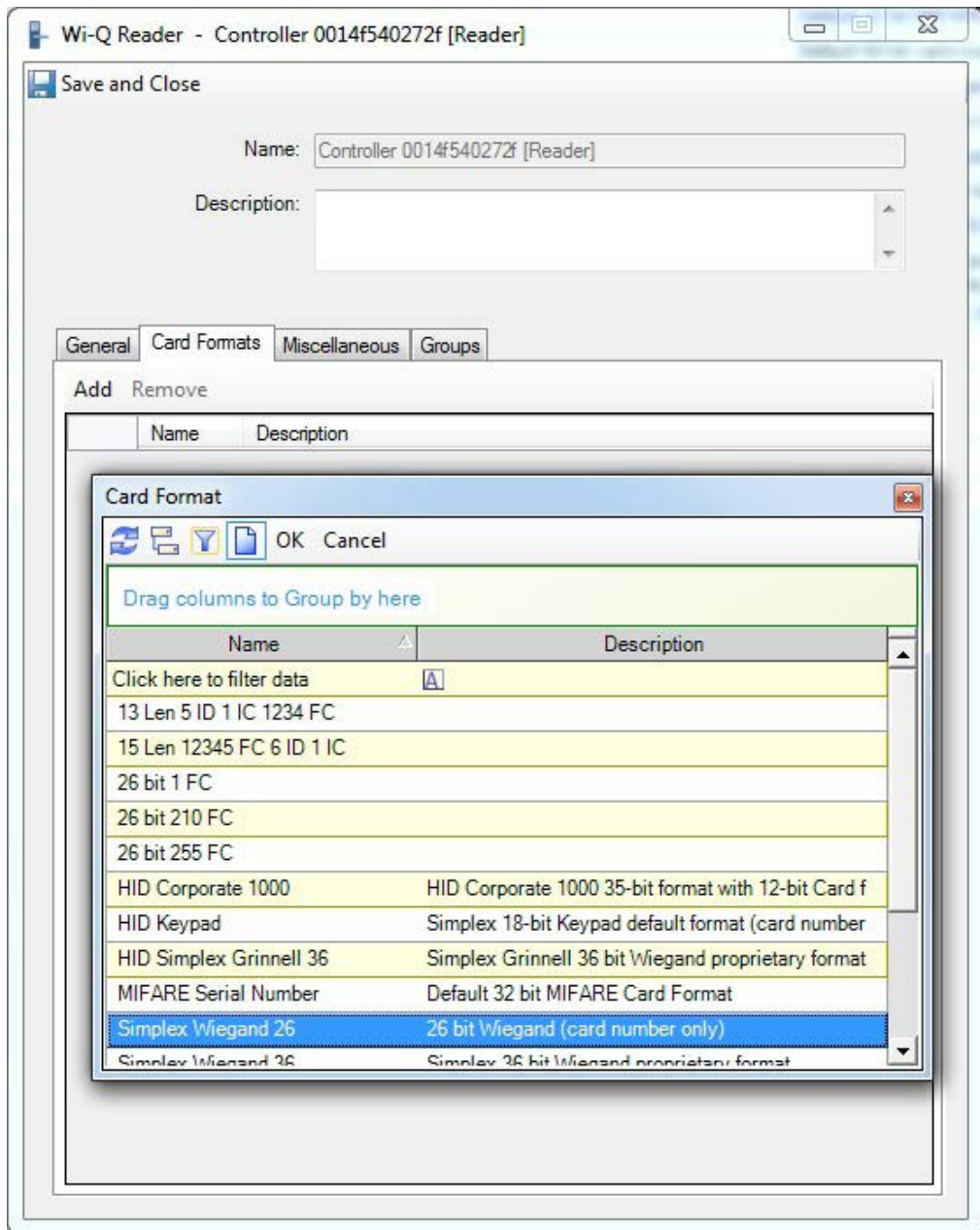
Selecting and Configuring a Wi-Q Reader

Figure 57 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 58 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.

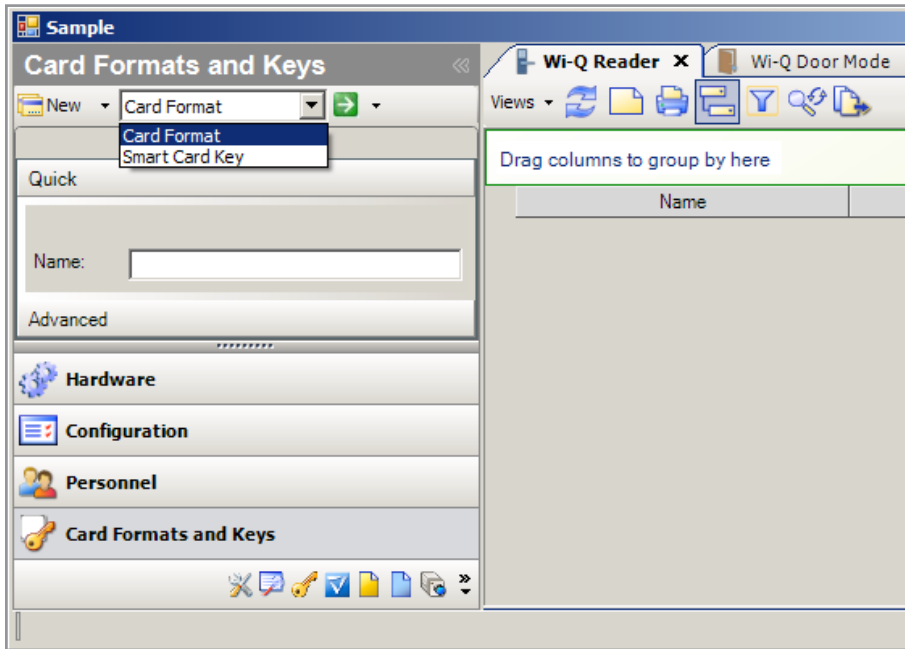
The following additional tabs are available, but no configuration changes are required at this time. See www.swhouse.com for more information.

- 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 59 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 60 Creating a Magnetic Card Format - General Tab

The screenshot shows the 'Card Format (Template)' dialog box with the 'General' tab selected. At the top, there are input fields for 'Name' and 'Description'. Below these, the 'General' tab is active, showing a 'Card Format Description' section. In this section, the 'CHUID Format' is set to 'Card Only' with an ellipsis button to its right. Below this, the 'Data Length' is set to '15'. There are two radio buttons: 'Magnetic' (which is selected) and 'Wiegand / Proximity'. At the bottom, there is a 'Reverse Swipe Setting' section with five radio buttons: 'Read as Normal Swipe' (selected), 'Read as Dupress', 'Ignore Reverse Swipe (ISC only)', 'Reverse Swipe is Not Allowed', and 'Must Always Use Reverse Swipe (ISTAR only)'.

- 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 61 Creating a Magnetic Card format - Format Tab

Card Format (Template) -

Save and Close

Name:

Description:

General | Format Fields

Card Data Fields

Field Type	Start Position	Length	End Position	Values
Card facility code	2	5	6	12345
Card Number	7	6	12	
Issue code	13	1	13	

Card facility code
Card Number
Card status
Expiration date
Fixed data
Issue code
Site code
Unknown

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 62 Creating a Proximity Card Format - General Tab

The screenshot shows a software window titled "Card Format (Creating from Wiegand 26 Template) -". It has a menu bar with "Save and Close" and "Save and New". Below the menu bar are two text input fields: "Name:" and "Description:". The "Description:" field contains the text "Template for Standard Wiegand 26 format with Facility Code". Below these fields are two tabs: "General" (selected) and "Format Fields". The "General" tab contains a section titled "Card Format Description" which includes a "CHUID Format:" dropdown menu set to "Card Only" with an ellipsis button to its right. Below this is a "Data Length:" field set to "26". To the right of the "Data Length" field are two radio buttons: "Magnetic" (unselected) and "Wiegand / Proximity" (selected). Below these is a section titled "Reverse Swipe Setting" with five radio buttons: "Read as Normal Swipe" (selected), "Read as Dupress", "Ignore Reverse Swipe (ISC only)", "Reverse Swipe is Not Allowed", and "Must Always Use Reverse Swipe (iSTAR only)".

- 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 63 Creating a Proximity Card format - Format Tab

Card Format (Creating from Wiegand 26 Template) -

Save and Close Save and New

Name:

Description:

General Format Fields

Card Data Fields

Add Remove

	Field Type	Start Position	Length	End Position	Complement	Encoding	Values
▶	Card facility code	2	8	9	<input type="checkbox"/>	Binary	<input type="text"/> ...
	Card Number	10	16	25	<input type="checkbox"/>	Binary	<input type="text"/>

Parity Fields

Add Remove

Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

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.

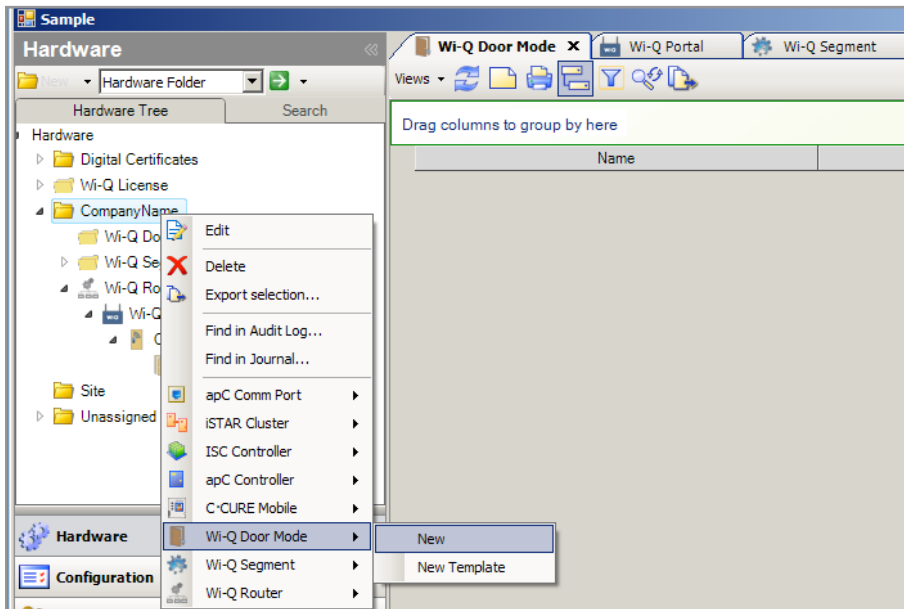
11 Click the **Add** button to list additional data fields and then enter their start positions, length and end positions (and default values if applicable).

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.

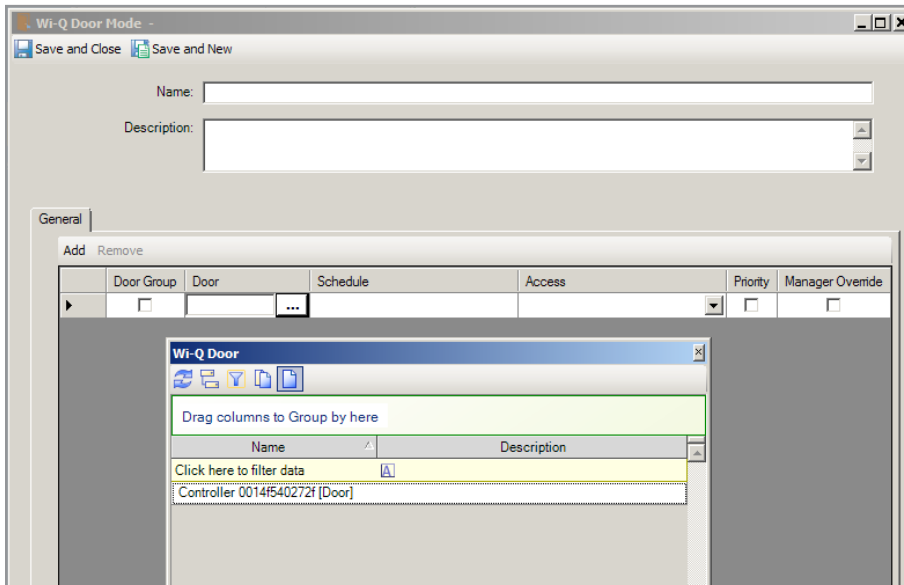
Adding Wi-Q Door Modes

Figure 64 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 65 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 11 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	Card ID 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.
5	Unlock with Credential	Any credential (card or keypad) will unlock the door and it will stay unlocked.
0	Unlock	The door is unlocked, anyone can open it.

Configuring Events with Wi-Q Hardware

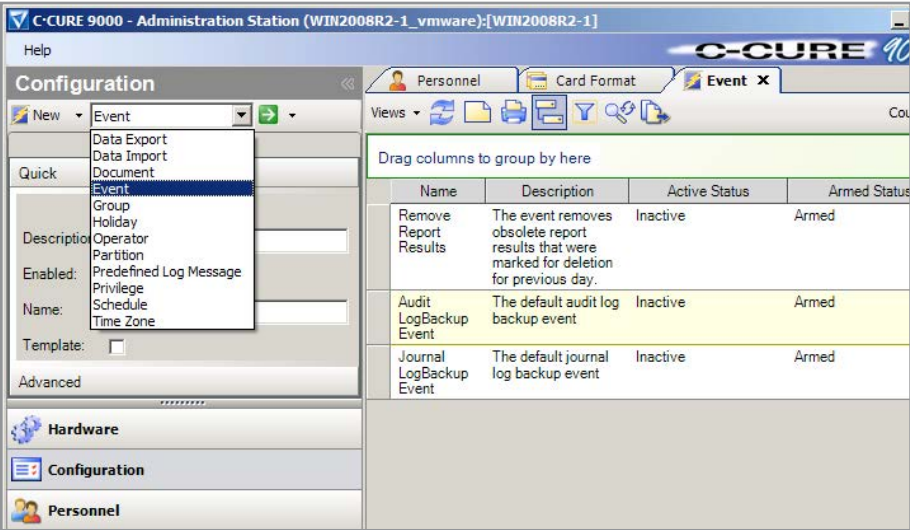
The default Event Actions in C-Cure are not supported by Wi-Q Hardware. A Wi-Q specific Action, named "Wi-Q Override Access Level", has been added to the list of selectable Actions when creating an Event. This allows Triggers to, upon activation, override the current door mode of a Wi-Q door.

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.

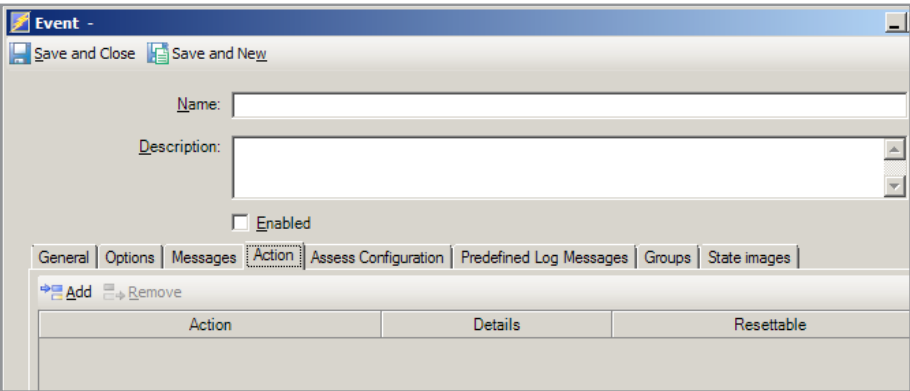
Note Every other part of events and triggers work the same as in C-CURE.

Figure 66 Adding an Event for use with the Wi-Q Hardware



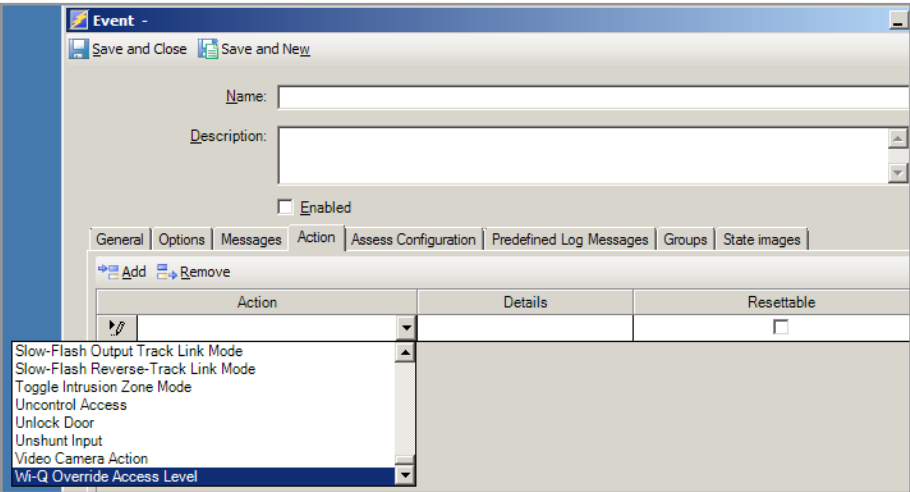
- 1 Click on the **Configuration** button in the left column.
- 2 Select **Event** from the Configuration drop down menu at the top and click the **New** button to the left.

Figure 67 New Event Dialog Box



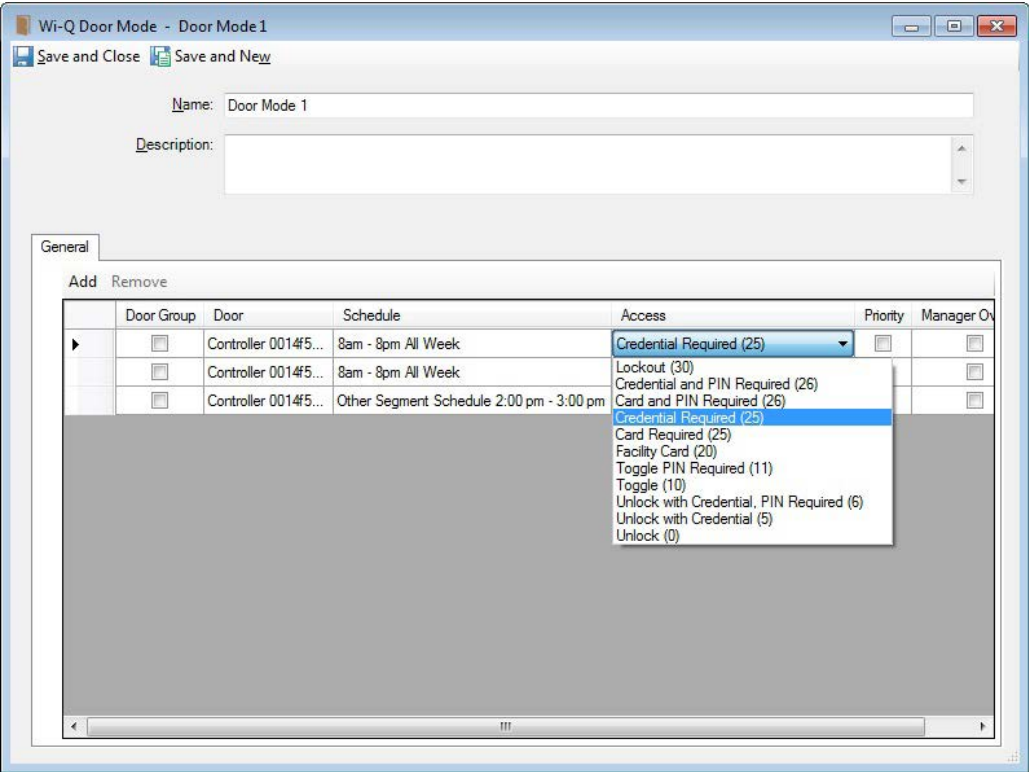
- 3 Enter the event name and description.
- 4 Click the **Enabled** check box to allow communications.
- 5 Click the **Action** tab.

Figure 68 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 69 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 priority level from the **Override Door Mode** drop down menu.

Adding Programmer and Manager to the Personnel Types

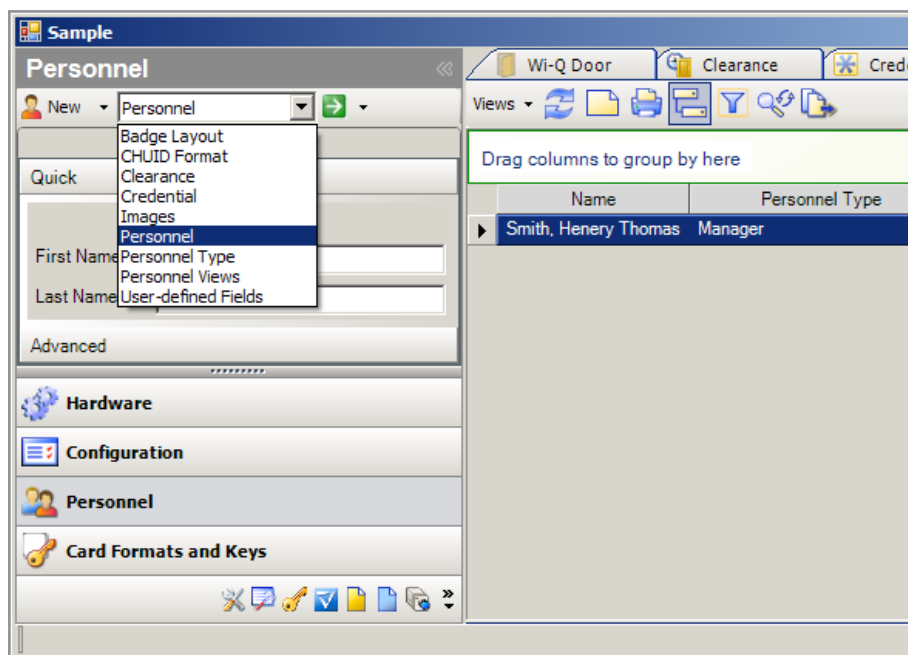
In order to make personnel managers or programmers, they must be added to either the Managers or Programmers group, which were created during the Wi-Q Interface Software installation.

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 Unlck 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 70 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 71 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 not 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 72 The Personnel Dialog Box - Credentials Tab

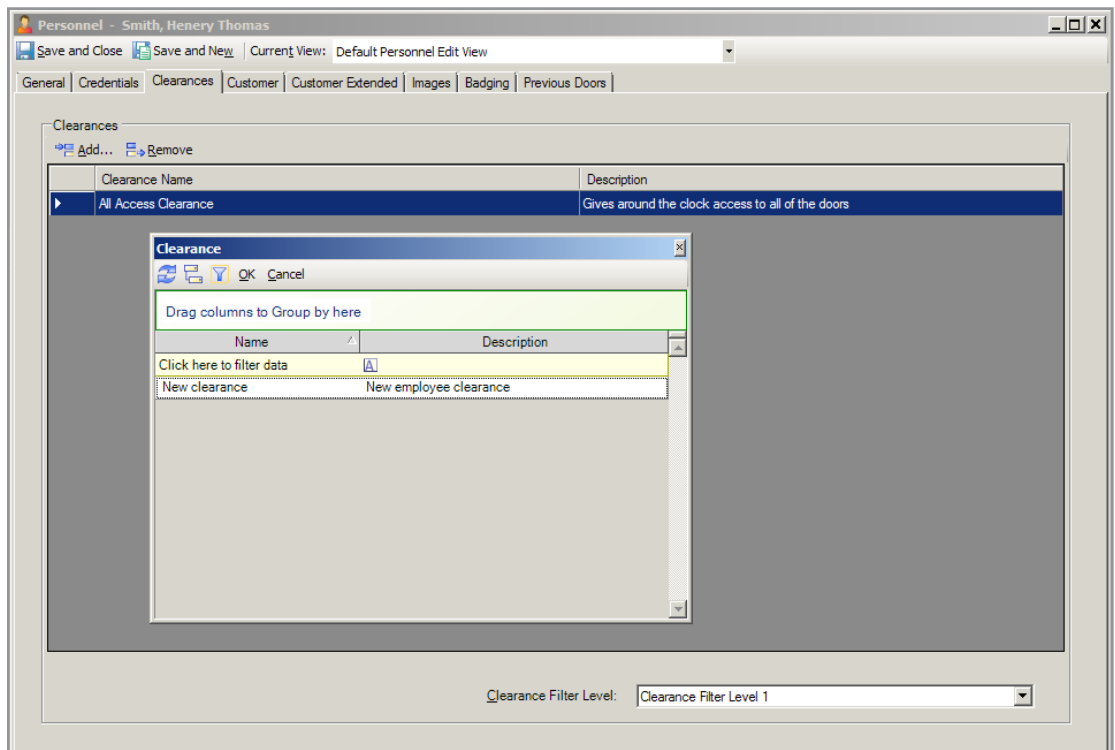
- 1 Click the Add Card Access button above the Credential List box at the top and enter the card number in the Card Number field. It will automatically fill in the Card Number field in the Standard Fields box when you move to a new field.
- 2 Enter the Facility Code and the Issue Code in the Standard 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 104. 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 **Credentials** tab.

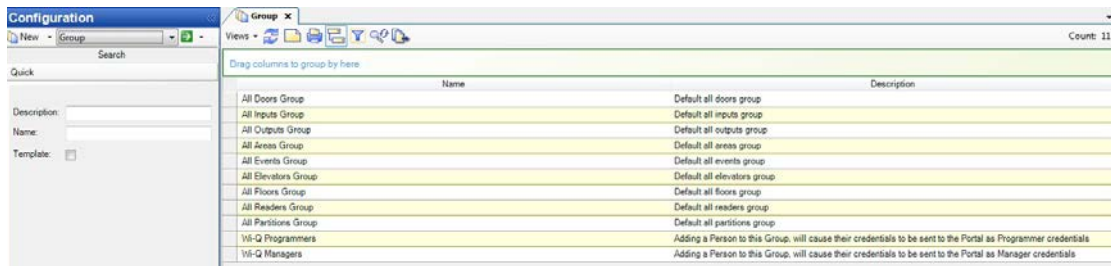
Figure 73 Personnel Dialog Box - Clearances Tab



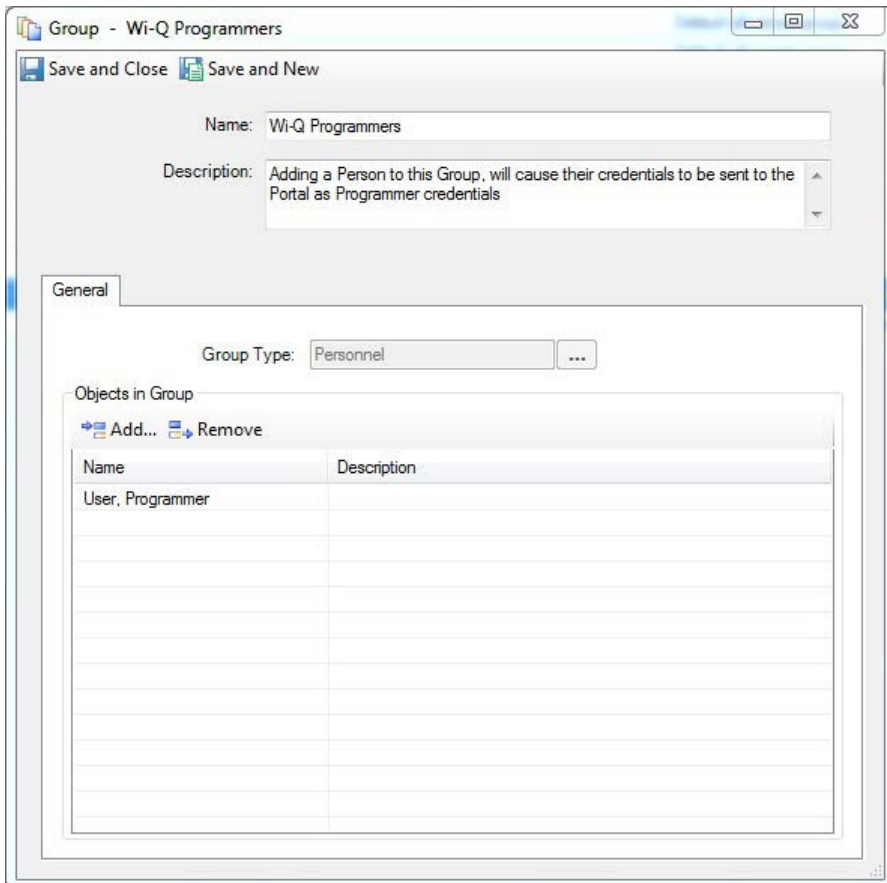
- 6 Click the **Add ...** button below the Clearances box to display the Clearance dialog box.
- 7 Select the clearances to assign to this user. Shift-click or Alt.-click to select multiple clearances.
- 8 Click the **OK** button in the header of the Clearance dialog box. The dialog box will close and 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.



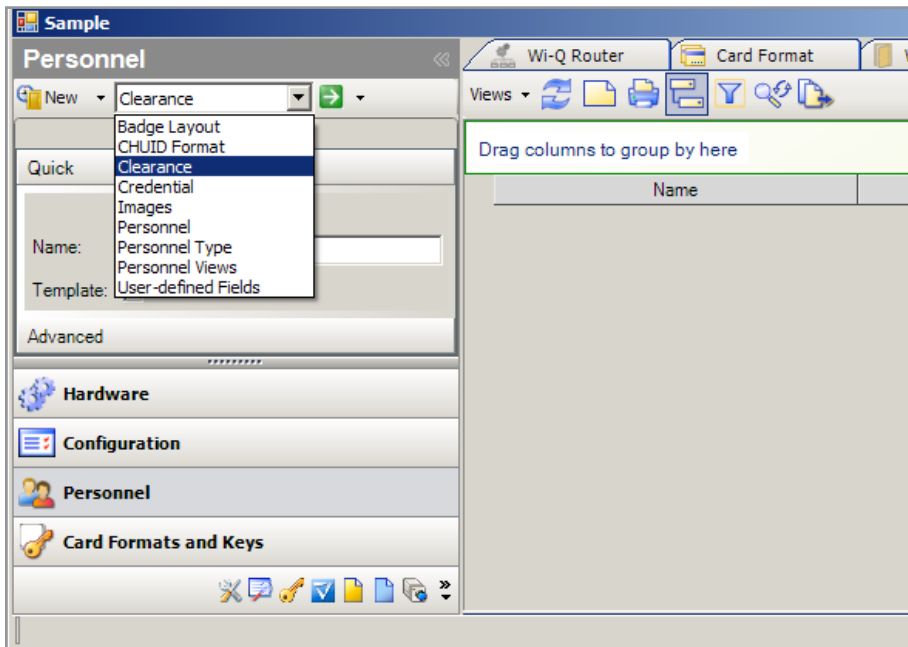
- 2 Select Group from the drop down menu and click the green arrow button.
- 3 Edit the Wi-Q Programmers/Wi-Q Managers Group to add the personnel to the group.



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

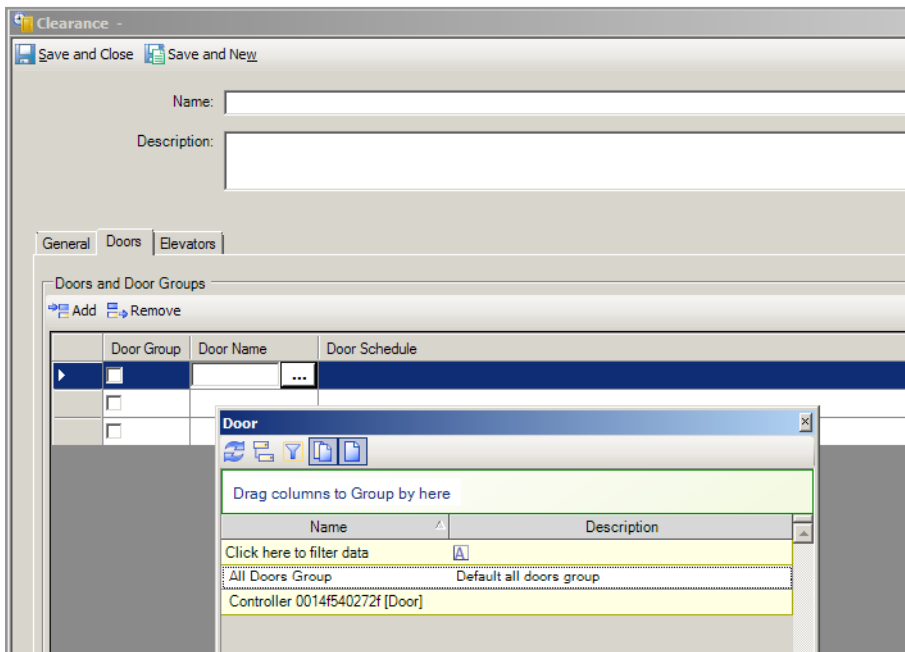
Creating Clearances

Figure 74 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 75 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.
- 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.

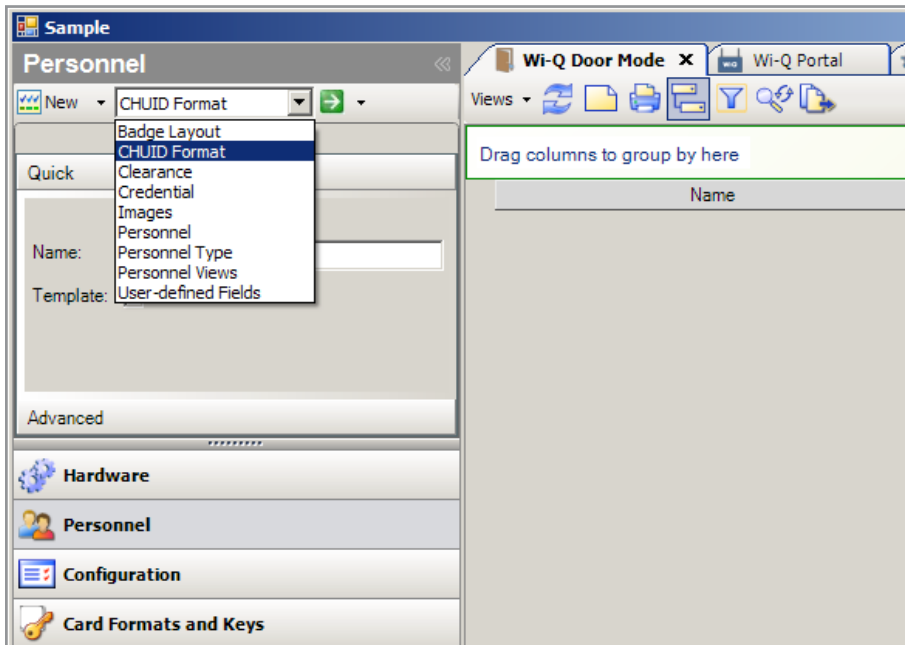
- 8 Click in the Schedule field and then click the Ellipsis button that appears to the right, to get the Schedule dialog box.
- 9 Select a schedule from the list. The dialog box will close and the schedule name will be filled into the Door Schedule field.
- 10 Click the **Add** button again to include 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 76 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 New button to the left.

Figure 77 Enabling Keypad Credential

CHUID Format -

Save and Close Create Copy

Name:

Description: The description of th

☐ Enabled

General

CHUID Length:

CHUID Format Type:

☐ Use this format to decipher unknown CHUIDs in Journal

CHUID Fields

Add Remove Validate Fields Move up Move Down

Id	Field Name	Length	Start Position
----	------------	--------	----------------

- 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.

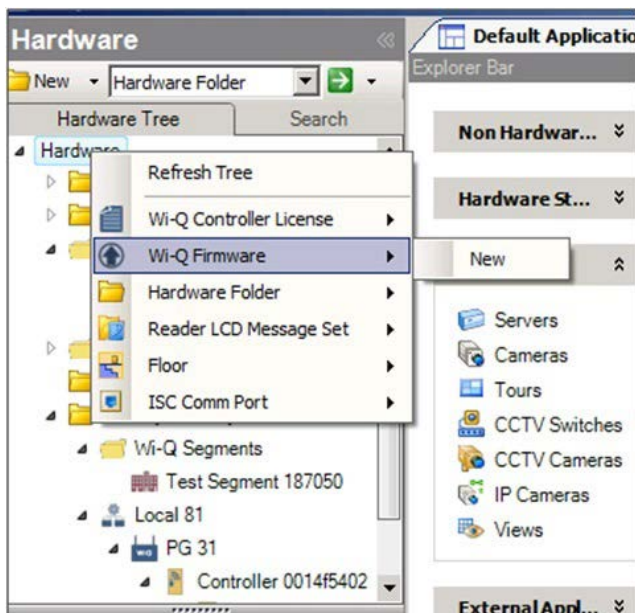
Firmware Updates

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 78 New Wi-Q Firmware



- 4 Enter name and description.

Figure 79 Wi-Q Firmware

Wi-Q Firmware - WAC 3.00.040

Save and Close

Name: WAC 3.00.040

Description: WAC Firmware version 3.00.040

Firmware

Firmware File: \\IND-Jessica\Share Folder\WAC\WAC_BIN_V03_00_040\WAC_BIN_V03_00_040\W... ..

Version: 3.00.040 Device Type: WAC

- 5 Select a firmware file.

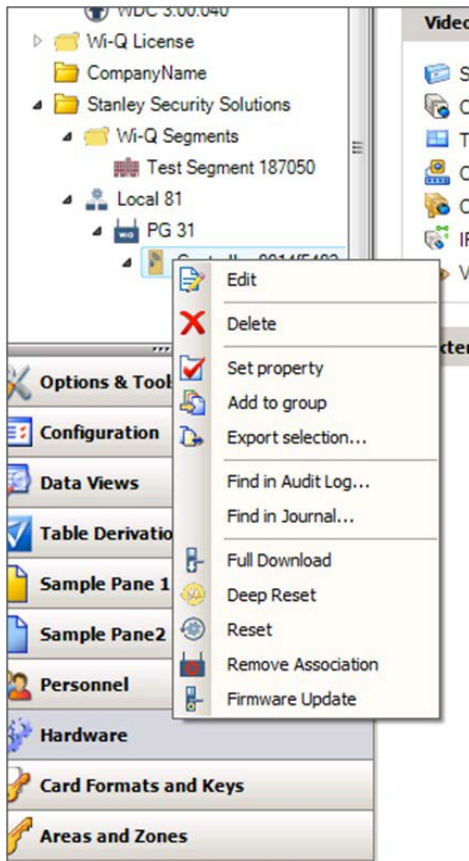
- 6 Select Save and Close.

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.

Download the Firmware

- 1 In the hardware tree, right-click an enabled controller or portal gateway.

Figure 80 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 81 Controller Firmware

Name: Controller Firmware

Description: Displays Firmware Download Information

General

View type: Wi-Q Controller

Query:

☐ Make default view ☐ Display in card view

☒ Show toolbar ☒ Enable context menu

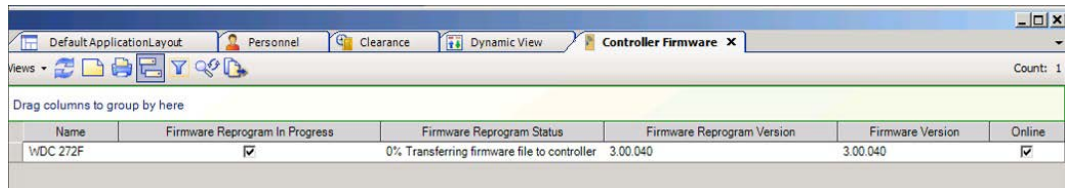
Add Remove Up Down

Column property	Hidden	Justification	Foreground color	Header font	Sort	Editable	Initially group
Name	<input checked="" type="checkbox"/>	Left	Black		None	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firmware Reprogram In Progress	<input type="checkbox"/>		Black		None	<input type="checkbox"/>	<input type="checkbox"/>
Firmware Reprogram Status	<input type="checkbox"/>	Left	Black		None	<input type="checkbox"/>	<input type="checkbox"/>
Firmware Reprogram Version	<input type="checkbox"/>	Left	Black		None	<input type="checkbox"/>	<input type="checkbox"/>
Firmware Version	<input type="checkbox"/>	Left	Black		None	<input type="checkbox"/>	<input type="checkbox"/>
Online	<input type="checkbox"/>		Black		None	<input type="checkbox"/>	<input type="checkbox"/>

- 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 82 Controller Firmware



The screenshot shows a software window titled "Controller Firmware". It has a menu bar with "Default ApplicationLayout", "Personnel", "Clearance", "Dynamic View", and "Controller Firmware x". Below the menu bar is a toolbar with icons for file operations and a search icon. A "Views" dropdown menu is on the left, and a "Count: 1" indicator is on the right. The main area contains a table with the following data:

Name	Firmware Reprogram In Progress	Firmware Reprogram Status	Firmware Reprogram Version	Firmware Version	Online
WDC 272F	<input checked="" type="checkbox"/>	0% Transferring firmware file to controller	3.00.040	3.00.040	<input checked="" type="checkbox"/>

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

5

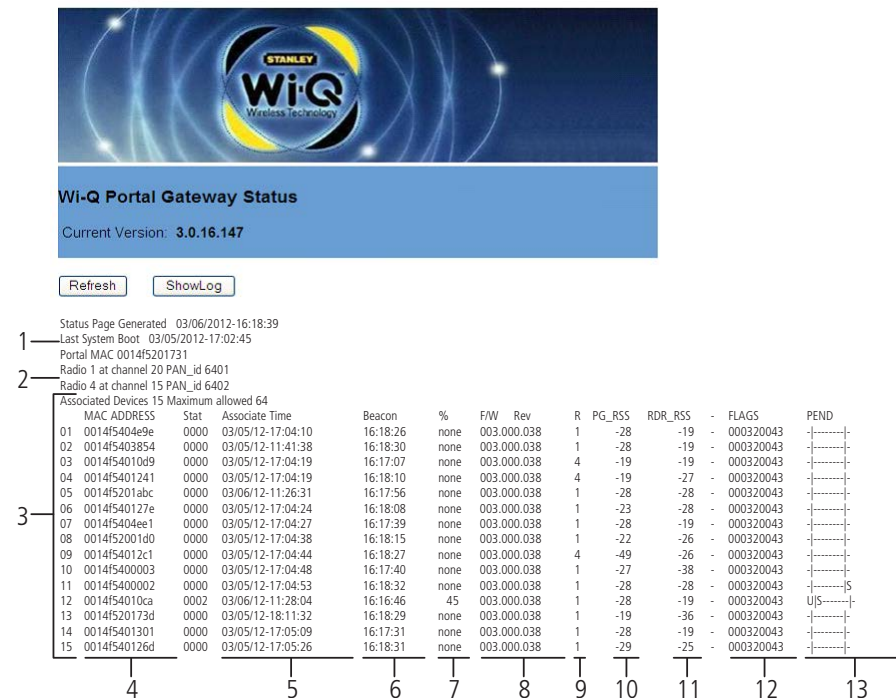
Troubleshooting

This section provides an overview on the Portal Gateway status webpage. You can access the status webpage for a specific Portal Gateway in one of three ways and your browser will display the status of your Portal Gateway and associated devices. See Figure 83.

- Inside the Wi-Q Portal Configuration Tool, select Scan. Locate the desired Portal in the list and click on its hyperlink. See Figure 83 on page 112.
- Type your desired Portal's IP address directly into your internet browser.
- Right click on Router and select View Network Portals. Click on selected IP address.

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

Figure 83 Portal Gateway Status Webpage



The Portal Gateway Status webpage provides the following information:

- 1 **Last System Boot**
Last time Portal Gateway was reset or rebooted.
- 2 **Radio and Channel**
Shows the channel associated with each radio in the Portal.
- 3 **Associated Devices List**
Shows which devices are associated with the Portal.
- 4 **MAC Address**
Column shows the MAC Address of each associated device.
- 5 **Associate Time**
Column shows the time that the Controller last associated with the Portal.
- 6 **Beacon**
Column shows the time of the last Controller beacon.
- 7 **%**
Column shows progress percentage of pending operations.
- 8 **F/W Rev**
Column shows the firmware version number of associated Controller.

9 R

Column shows which radio the Controller is connecting to in the Portal Gateway. Radio 1 is on the right side of the Portal. Radio 4 is on the left side of the Portal.

10 PG_RSS

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

11 RDR_RSS

Column shows the signal strength of the Portal 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 PEND

Column shows the abbreviation of the message currently in operation.

Status Flags in the FLAGS Column

The following is a list of the bits in the FLAGS column and their corresponding Portal Gateway status flags and definitions (Figure 83, item 12).

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

Bit			Portal 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

Figure 84 is a section of the Associated Devices listed in Figure 83. Notice that items 11 and 12 have letters U and S in the PEND column. These letters are update flags, and they stand for controller information that is being updated. The placement of the update flags within the column denotes update status.

Figure 84 PEND Column Codes

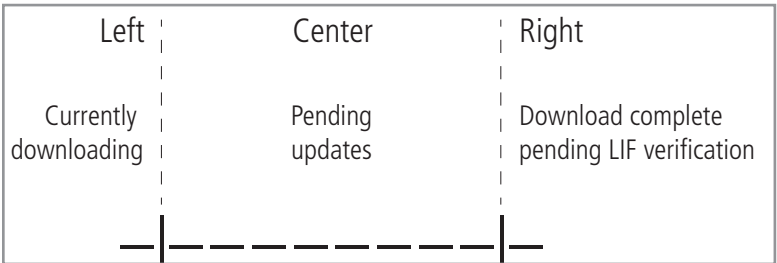
Associated Devices 15 Maximum allowed 64														
	MAC ADDRESS	Stat	Associate Time	Beacon	%	F/W	Rev	R	PG_RSS	RDR_RSS	-	FLAGS	PEND	
01	0014f5404e9e	0000	03/05/12-17:04:10	16:18:26	none	003.000.038		1	-28	-19	-	000300043	- -----	
11	0014f5400002	0000	03/05/12-17:04:53	16:18:32	none	003.000.038		1	-28	-28	-	000300043	- ----- S	
12	0014f54010ca	0002	03/06/12-11:28:04	16:16:46	45	003.000.038		1	-28	-19	-	000300043	U S-----	
13	0014f520173d	0000	03/05/12-18:11:32	16:18:29	none	003.000.038		1	-19	-36	-	000300043	- -----	
14	0014f5401301	0000	03/05/12-17:05:09	16:17:31	none	003.000.038		1	-28	-19	-	000300043	- -----	
15	0014f540126d	0000	03/05/12-17:05:26	16:18:31	none	003.000.038		1	-29	-25	-	000300043	- -----	

The following is a list of the Update Flags that may be visible in PEND column.

PEND Column Update Flags	
S	Segment (PIN length, DST times)
C	Card Formats
L	Controller configuration (beacon time, channels, transaction masks, etc.)
U	Users
T	Timezone Intervals
I	WAC I/O
F	Firmware
P	Ping (missing LIF data after association or update)

Figure 85 shows the significance of update flag placement between the dividing lines in each entry of the PEND column.

Figure 85 Update Flag Placement in PEND Column



Item 11 in Figure 84 shows that the Controller's Segment download is complete pending LIF verification.

Item 12 in Figure 84 shows that the Controller's Users are currently downloading, with 45% complete, and the Controller's segment update is pending.

Note Only one update flag will be positioned at the left or right, but it is possible for more than one flag at a time to be in the center of an entry in the PEND column.

Glossary

This Glossary contains only Stanley 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 assigned to a badge ID for the purpose of granting access through a reader or readers during a specified time.
activation/deactivation date	The date that a credential becomes active or expires.
badge	The credential or token that carries a cardholder's data.
badge ID	Part of the access control information that is encoded to a token. This information, usually numerical, is unique to a particular credential holder.
card format	The way that data is arranged and ordered on the card.
cardholder	An individual who is issued a particular credential.
chassis type	The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.
communication server	The server application designed to provide network services to access panels, readers, PCs and PDAs.
credential	A physical token, usually a card or fob, encoded with access control information.
cylindrical	Lock chassis that installs into a circular bore in the door.
directional antenna	An antenna type optimized to focus signal from point-to-point over longer distances and through obstacles.
ethernet	The most common networking standard in the world, formally known as IEEE 802.3.
exit hardware	Lock chassis type that supports exit hardware trim lock.
extended unlock	The extra period of time the lock will unlock when an authorized credential with extended unlock privileges is presented.
guest	A feature that enables you to add and delete cardholders to and from a lock without having to go out to a lock to reprogram it.
Host	the computer on which Wi-Q Interface Software is installed and set up to integrate portal 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.
portal gateway	The Portal 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 portals, and ultimately to a segment in the Software.
site survey kit	The Wi-Q Site Survey Kit tool is used to determine optimum Portal 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.

