



STANLEY® Wi-Q™ ACCESS MANAGEMENT SYSTEM  
USER GUIDE

v3.1

**STANLEY**  
**OMNILOCK®**

Copyright ©2012 Stanley Security Solutions, Inc.  
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 Solutions, Inc. at (317) 849-2250 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 Solutions, 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 AMS and Wi-Q Technology are registered trademarks of Stanley Security Solutions, 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.

T85202/Rev E August 2015

## FCC/IC Certification

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

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

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

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) this device must accept any interference, including any interference that may cause undesired operation of the device.

Cet appareil est conforme à la norme RSS Industrie Canada exempt de licence. Son fonctionnement est soumis aux deux conditions suivantes: (1) cet appareil ne doit pas provoquer d'interférences et (2) cet appareil doit accepter toute interférence, y compris les interférences pouvant causer un mauvais fonctionnement du dispositif.

This Class [B] digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe [B] respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Warning! Changes or modifications not expressly approved by {Applicant name} could void the user's authority to operate the equipment. Approved antennas are listed below and antennas not included in this list are strictly prohibited for use with these devices. 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
- BS2400XL3 - 2.4GHz Outdoor 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.

## Contents

<b>1</b>	<b>Overview</b>	
	System Overview .....	7
	Setup Checklist .....	12
<b>2</b>	<b>Hardware Installation</b>	
	Hardware Overview .....	13
	Installing System Hardware .....	16
	Install Portal Gateways (Task 8).....	24
	Install Door Hardware (Task 9).....	28
<b>3</b>	<b>Software Installation</b>	
	Prepare Your Computer (Task 3) .....	33
	Gather and Organize Segment Data (Task 4).....	43
	Install Software (Task 5).....	45
<b>4</b>	<b>Configuring Segments, Portal Gateways and Controllers</b>	
	Create Your Segment (Task 6) .....	63
	Add and Configure Portal Gateways (Task 7).....	67
	Sign on and Configure Controllers (Task 10).....	84
<b>5</b>	<b>Configure AMS Software (Task 11)</b>	
	Associations .....	96
	Credential Settings.....	108

	<b>Daylight Saving Settings</b> .....	<b>116</b>
	<b>I/O</b> .....	<b>116</b>
	<b>Misc</b> .....	<b>120</b>
	<b>PIN Settings</b> .....	<b>120</b>
	<b>Adding Users to the Segment</b> .....	<b>121</b>
	<b>Portal and Reader Control and Messaging</b> .....	<b>134</b>
	<b>Configuring Timezones</b> .....	<b>137</b>
<b>6</b>	<b>Using and Managing the System</b>	
	<b>Wi-Q AMS Configurator</b> .....	<b>145</b>
	<b>System Administrator</b> .....	<b>166</b>
	<b>Backing Up and Restoring Your AMS Database</b> .....	<b>174</b>
	<b>Firmware Updates</b> .....	<b>178</b>
	<b>Transactions Monitor</b> .....	<b>181</b>
	<b>Statistics Monitor</b> .....	<b>191</b>
	<b>Reports</b> .....	<b>199</b>
<b>7</b>	<b>Advanced Troubleshooting</b>	
	<b>Status Flags in the FLAGS Column</b> .....	<b>211</b>
	<b>Update Flags in the PEND Column</b> .....	<b>212</b>
<b>A</b>	<b>Glossary</b> .....	<b>214</b>
<b>B</b>	<b>Lock installation</b> .....	<b>220</b>

# 1 Overview

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

The information is presented in a linear manner, describing each tab, feature and application in the system. However, tasks to install hardware and software and configure the system for the first time do not necessarily progress in a linear manner. You will find a Set Up Checklist at the end of this section and in the Getting Started Guide to take you through the initial setup and configuration tasks in a logical sequence.

If you have not yet read through the Wi-Q AMS Getting Started Guide, it is a good idea to do so before beginning any installation and setup. The Getting Started Guide presents the big picture in just a few pages and will help you identify problems and create solutions as you work your way through hardware installation and setup, software configuration, and system operation. If you are unfamiliar with the terms used in wireless technology, you may want to refer to the Glossary included in this manual as Appendix A.

## **System Overview**

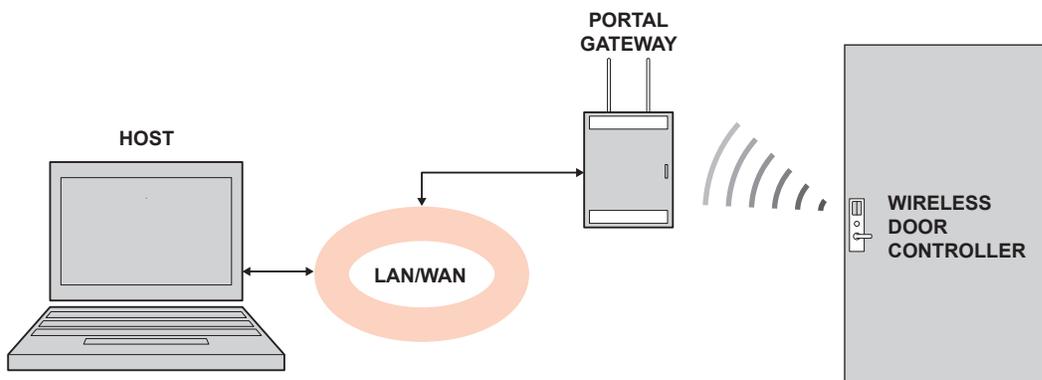
The Stanley Wi-Q Access Management System (Wi-Q AMS) integrates powerful access management software with Portal Gateways, Wireless Access

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

## Basic Hardware Components

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

Figure 1 Four Basic Components



### The Host Computer

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

### The Portal Gateway

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

### Wireless Controllers

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

### ***Wi-Q***

- Wireless Access Controller
- Wireless Door Controller

### ***Omnilock***

- Single Door Controller
- Omnilock Reader

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

### **Basic Operation**

The system works very simply. A user enters a pass code at a controller, either using an access card or by entering a code on a keypad. If the controller recognizes the credential from the configured settings downloaded from the Host via the Portal Gateway to the controller, the door opens. The controller also sends regular signals (beacons) 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**

Wi-Q AMS supports various system configurations. For example, some locations at your segment may already be hard-wired with legacy equipment or additional input or output devices. You can also use a Wireless Access Controller, hard-wired to a controller and strike, and wirelessly communicate back to a Portal Gateway.

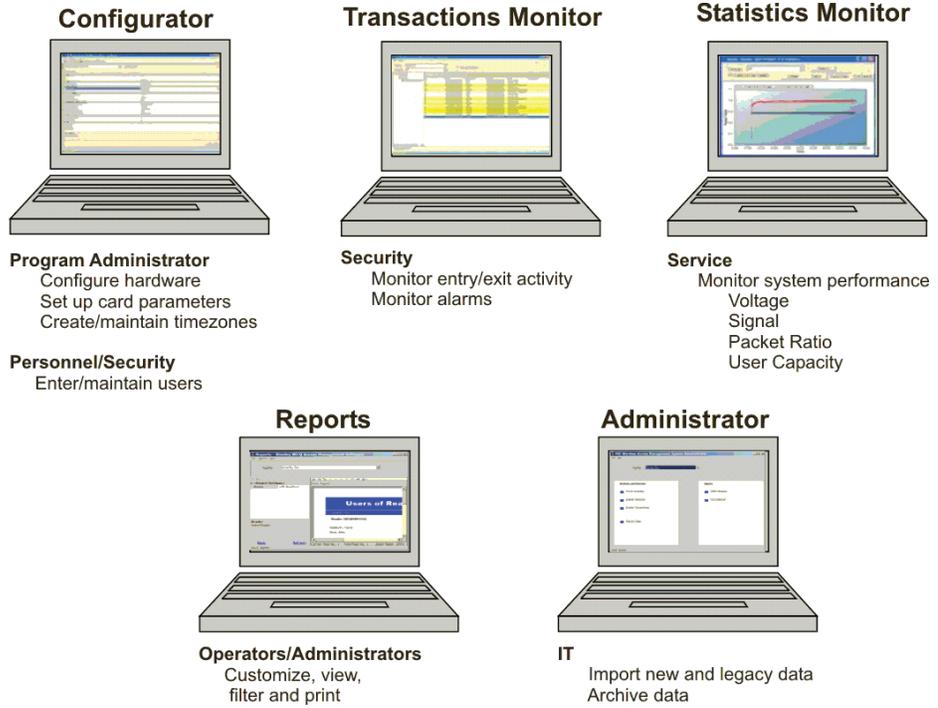
For more information about various applications you can adapt for use with Wi-Q AMS, see “Hardware Overview” on page 13.

## **Software Overview**

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

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

Figure 2 Five Applications



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

## Setup Checklist

Wi-Q AMS is set up in eleven basic tasks. Completing these tasks will ensure you get your system up and running as quickly and efficiently as possible.

Some tasks are performed at the Host computer and some at the segment site. It is appropriate to perform some tasks concurrently, for example, you may have someone prepare your computer and install the software concurrently with site plan development and hardware installation. However, you must have the software installed and 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 this User Guide.

- Task 1: Develop a Site Plan, page 17.
- Task 2: Position Portal Gateways, page 21.
- Task 3: Prepare your Computer, page 33.
- Task 4: Gather and Organize Segment Data, page 43.
- Task 5: Install Software, page 45.
- Task 6: Create your Segment, page 63.
- Task 7: Add and Configure Portal Gateways, page 67.
- Task 8: Install Portal Gateways, page 24.
- Task 9: Install Door Hardware, page 28.
- Task 10: Sign On and Configure Controllers, page 84.
- Task 11: Configure AMS Software, page 96.

## 2 Hardware Installation

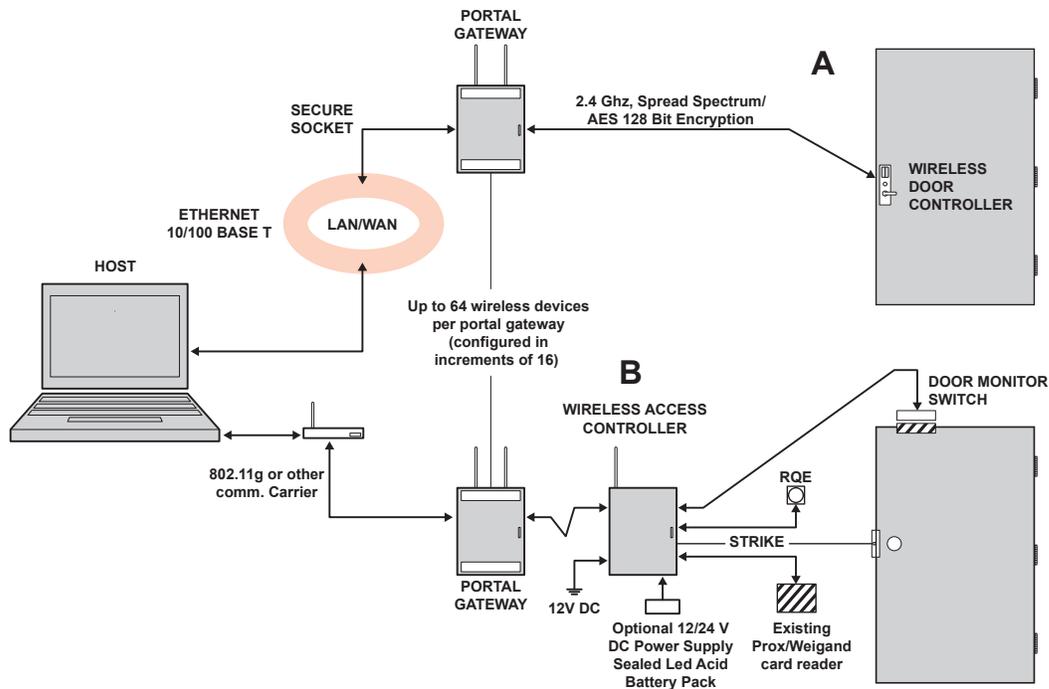
### Hardware Overview

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

**Note** Once Wireless Controllers are installed, you will need to sign them on to AMS software. Therefore, it is appropriate to install the software before or concurrent with hardware installation. For more information, see “Sign on and Configure Controllers (Task 10)” on page 84.

Figure 3 is a block diagram showing various configurations. Wi-Q AMS supports all Wireless Controllers via Portal Gateways (A); and existing Prox/Wiegand, RQE, door strike, and door monitor switch configurations (B). Configuration types are briefly described in the following paragraphs. Full installation instructions are provided in the following sections.

Figure 3 Example System Configurations



## Portal Gateways

The Stanley 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 be upgraded to 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. All communications between Wireless Controllers and Portal Gateways can be further backed up by “redundant” Portal Gateways each with capacity for up to 64 Wireless Controllers.

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

## Wireless Controllers

Wi-Q AMS software is designed to operate with Wi-Q Technology Best 45HQ mortise and Best 9KQ Cylindrical locksets equipped with either keypad, card, or a combination of controller input devices. Wi-Q AMS software is also designed to work with Omnilock 9KOM cylindrical and 45KOM mortise locksets. Door switch monitor, request to exit, and door lock position sensors are included in the locks. Wi-Q and Omnilock Controllers support a broad range of Controller technologies:

- Card or Keypad ID with PINs
- Magnetic Stripe, Prox, MIFARE (card number only)
- 512 Timezones (per Segment)
- 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 Portal Gateways using Wireless Access Controllers. You can also use this device to connect other I/O devices to the system. About the size of a standard double-gang box electrical box, these controllers operate on standard 12V DC or an optional 12/24 V DC power supply, sealed, lead acid battery pack. They seamlessly integrate existing door hardware into the Wi-Q AMS system, supporting Wiegand-compatible keypad Controller inputs. Check with your 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 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 and Omnilock Technology support two antenna types: Omni-directional, designed to provide coverage in all directions; and Directional antennas that focus the signal from point-to-point over longer distances and through obstacles. For more information, see Position Portal Gateways (Task 2).

## Installing System Hardware

Wi-Q AMS is designed to operate with Stanley Wi-Q and Omnilock Controllers and Portal Gateways. Detailed installation instructions are provided in the following sections and in the lock instructions provided with the hardware which are included as Appendices to this manual.

### What you will need

- Engineering drawings or segment map
- Wi-Q Technology Site Survey Kit
- Wi-Spy Spectrum Analysis Tool by MetaGeek (or equivalent) to identify the best open channels for your network
- For Keypad Controllers, you will need the sign-on credential from the Wi-Q AMS software
- For magnetic stripe or proximity card controllers, you will need the Programmer ID cards supplied in the software package. You will also need the appropriate magnetic stripe or proximity USB enrollment controller to create a proximity sign-on credential.
- Locksets to be installed on doors, including cores and keys supplied with specific model.
- Installation instructions for specific lockset brand and model.
- 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 in your lock)
- Phillips-head and flat-head screw drivers
- Access to the Host, a networked workstation, or wireless laptop computer.

### **Develop a Site Plan (Task 1)**

Before installing 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:

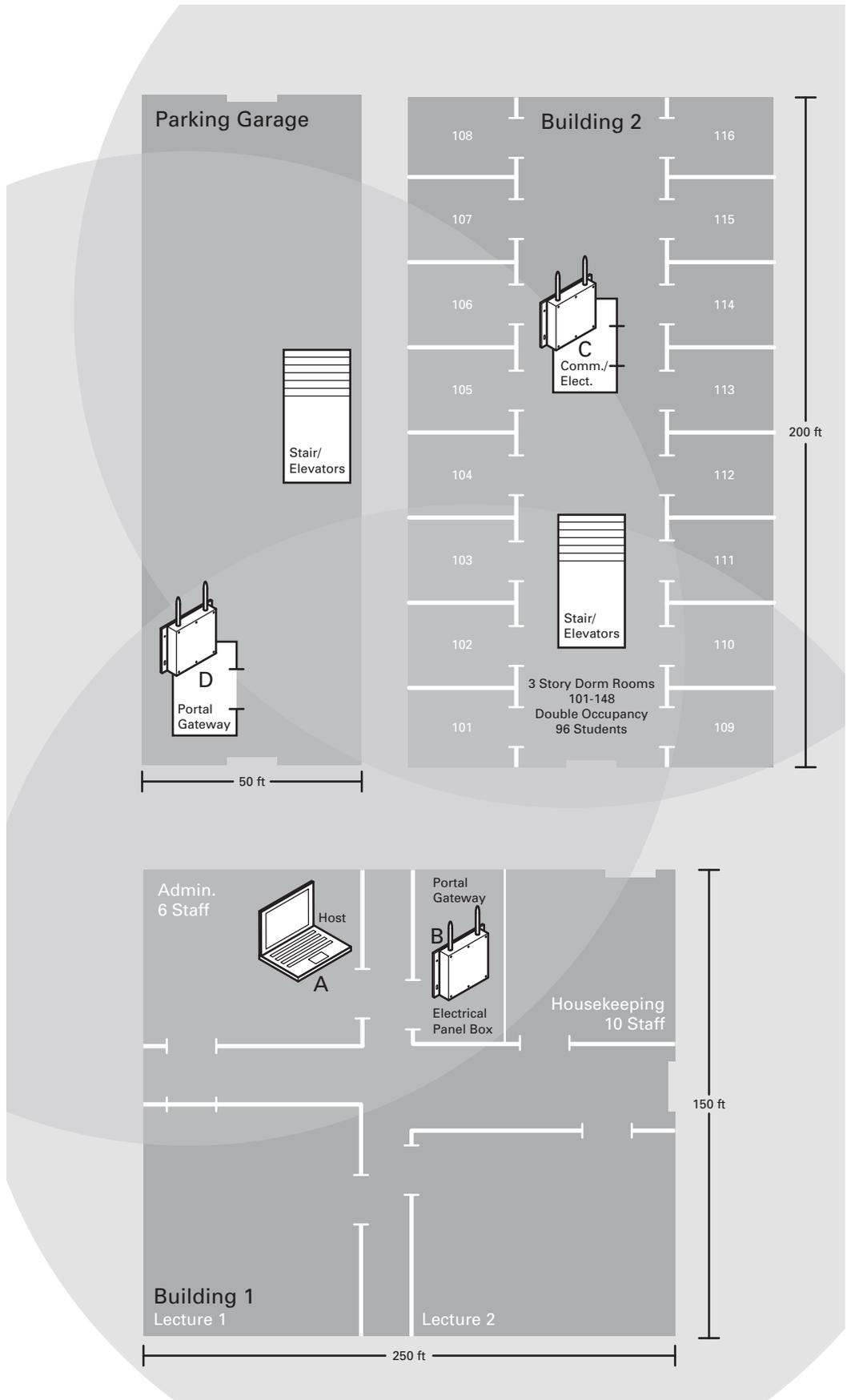
Transmit range from Portal Gateway to controller varies based on building construction. Site characteristics such as reinforced concrete walls could interfere or weaken the signal; open spaces and low interference can increase signal strength.

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

Figure 4 shows a typical site configuration. The Host (A) is located in Building 1. The Building 1 Portal Gateway (B) is located near the electrical panel in the communications/electronics room. This Portal Gateway will collect transactions from the 12 controllers in Building 1. As you can see by the gray circle representing the Portal's range, it also extends to the entrance of Building 2 and the Parking Garage. This provides redundant coverage of those areas should either of the other Portals go off line.

The Building 2 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 4 Sample site installation plan



## Plotting the Plan

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

## Device Identification

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

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

When you move on to configure the Host computer, it is essential to have a list identifying each controller lock and 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.

## Redundancy

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

## Interference

Wi-Q and Omnilock Technology transfers information between devices in the form of data packets over the 2.4 GHz ISM band. This band frequency is very heavily used in many devices such as wireless computer networks (802.11 b and g) and cordless phones, which increases the risk of lost packets, that is, packets that do not make it from a controller to a 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 in AMS, this frequency range must be managed effectively. Therefore, the installer must know the positions and channels of all the 2.4 GHz wireless devices in the segment and ensure channels are assigned to each device so that there is minimum frequency overlap with adjacent or nearby devices.

### **Extended Range**

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

**Note** Actual distances will vary based on building construction.

### **Position Portal Gateways (Task 2)**

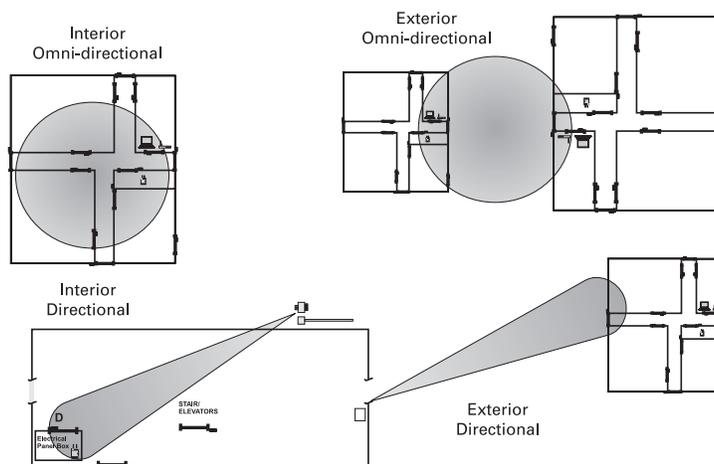
Once all door hardware and controllers have been installed, you are ready to determine the final placement of Portal Gateways using the results from the Wi-Q Technology Site Survey Kit. The Site Survey Kit helps you determine the number and optimum location of Portal Gateways and verify signal strength 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 and Omnilock Technology provide two antenna types: Omni-directional, designed to provide coverage in all directions; and Directional antennas that focus the signal from point-to-point over longer distances and through obstacles. If you have trouble verifying signals, you may need to consider some antenna type options. Figure 5 shows two available antenna types.

Figure 5 Selecting the antenna type that best suits your needs.



## 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 in to 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** Actual distances 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:

<b>If...</b>	<b>Then</b>
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 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.

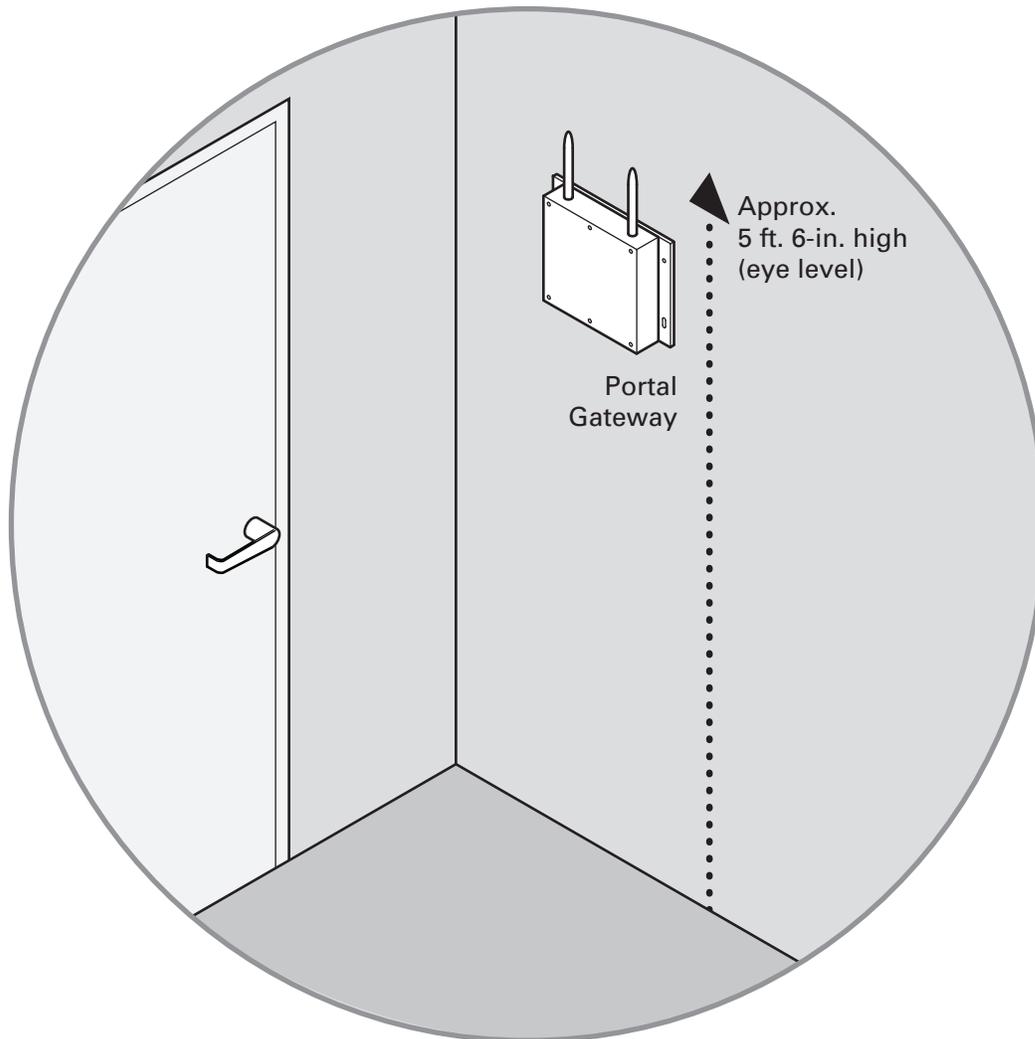
## Next steps

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

## Install Portal Gateways (Task 8)

The most common installation site is inside an existing protected area such as a locked room or other secure enclosure, or above ceiling level. If you are installing inside a dealer-supplied locked enclosure, refer to the instructions provided with that equipment. Figure 6 shows a Portal Gateway positioned in a protected area.

Figure 6 Installing a Portal Gateway in a protected area.



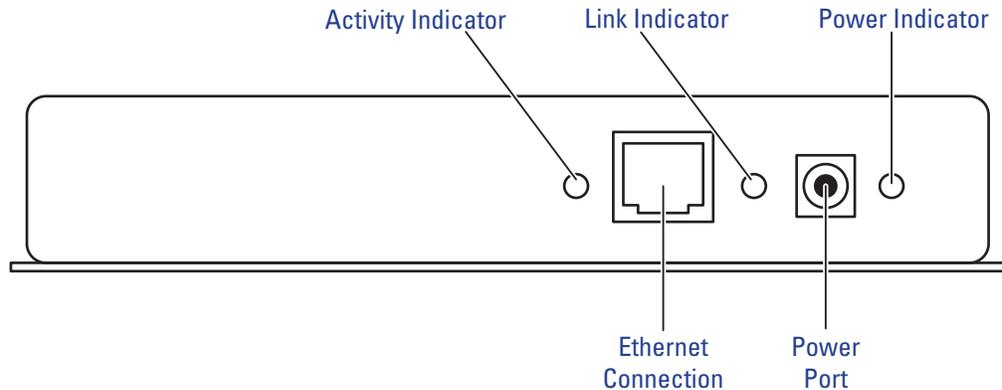
### Connecting the Portal Gateway and Verifying Operation

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 7.

- 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 7 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.

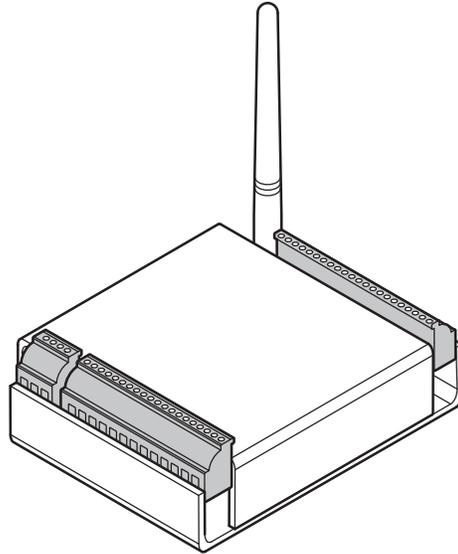
## Installing a Wireless Access Controller

The Wi-Q Technology Wireless Access Controller (WAC) provides an optional, cost effective way to retrofit an existing hard-wired application, or where the installed controller may be obsolete or unable to handle additional controller inputs. It supports Wiegand-compatible keypad Controllers and is configured and monitored in Wi-Q AMS the same as a standard controller.

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

Using the Wireless Access Controller (Figure 8), 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 8 Wireless Access Controller.



### Installation

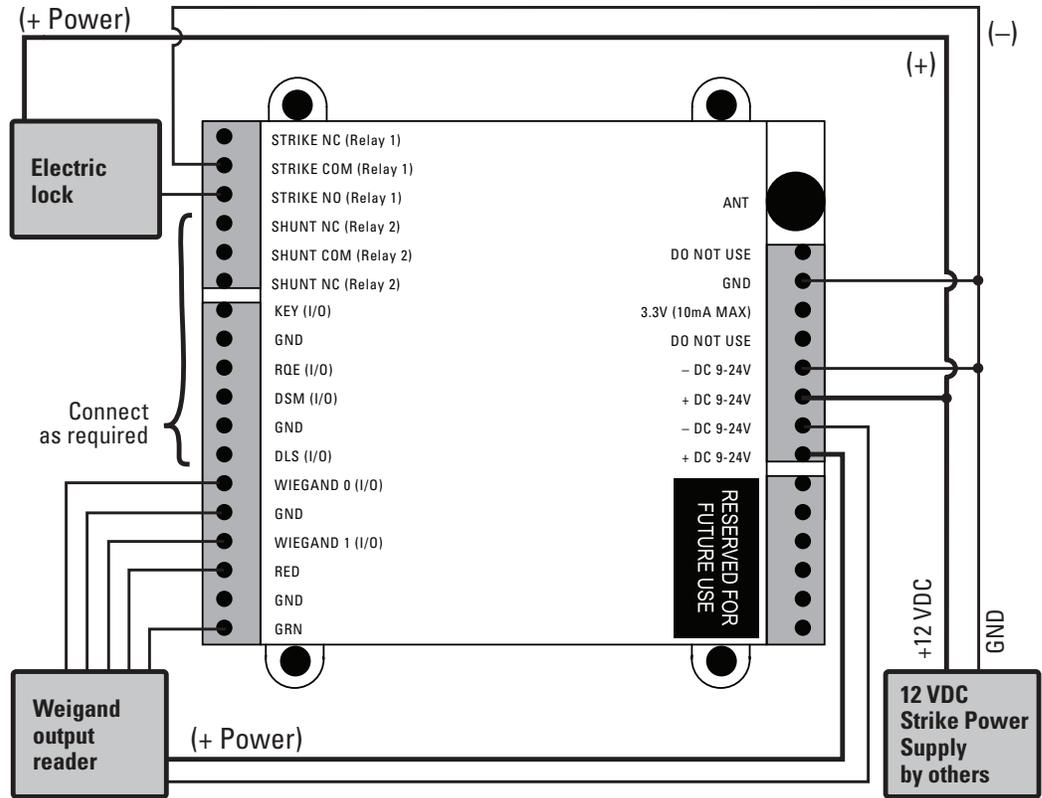
Specific installation methods are dependent on the device type and configuration of the system; therefore, the WAC should be installed by a trained technician using the instructions provided with the controller.

***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 (WAC) can be installed with its own 12 VDC power supply or slaved to the existing installation. Figure 9 is a wiring diagram illustrating both configurations.

Figure 9 Connecting devices to a WAC



Once the WAC is installed and all points connected, it will be recognized by Wi-Q AMS as a 'Controller' in the system. For more information about configuring the WAC in the software, see "I/O" on page 116.

## Install Door Hardware (Task 9)

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

### Before You Begin

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

- Record device MAC address before installing device. You will need this when configuring the controller in the software.
- Wi-Q and Omnilock Technology locks will work from -31°F to 151°F.

**Note** Extreme heat will cause a reduction in wireless signal strength and can cause a loss of connectivity while the heat remains.

**Note** Alkaline batteries cease to operate if they reach a temperature of -20°F.

- Wi-Q and Omnilock Controllers are designed for use on 1-3/4-inch doors. If you need to install on non-standard doors, contact 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.

Please refer to the Appendices or the instructions provided with your particular lock to complete these steps. Once this is done, check controller operation as described in the following paragraphs.

## Check Controller Operation

Verify controller operation using the steps appropriate for your controller type (Magnetic Card or keypad). If the system does not operate properly, see Troubleshooting, at the end of the section.

### Magnetic Card Check

If your system has a magnetic card controller (mag card), default Programmer ID cards are supplied with the software. You will need these cards when you are ready to sign on the controllers.

#### To perform a magnetic stripe card verification:

- 1 Determine if the magnetic card type is Track 2 or Track 3.
- 2 Select the default Programmer ID card that matches the type for your magnetic card controller.
- 3 Insert and remove the magnetic card. The magnetic stripe on the card should be aligned with the 'V' mark by the card slot. The lights on the top of the Controller will flash green once and unlock, then during the open delay time, it will flash green five times. Once this occurs, the card controller light will flash red and lock.
- 4 While unlocked, check for proper lock operation.

### Keypad Check

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

- 1 At the keypad, enter the default Programmer ID, 1234#. The green light on top of the card controller will flash once and the lock will unlock, then during the open delay time, it will flash green five times. Once this occurs, the controller red light will flash and the lock will relock.
- 2 While unlocked, check for proper lock operation.

## Troubleshooting mortise and cylindrical locks

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

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

## Troubleshooting EXQ Exit Hardware trim

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

LEDs	Sounder	You should...
Single red flash	—	Use the card at a moderate speed.
Red flashes	3 short tones	Use the temporary operator card provided with the lock or Perform a door reset to restore to the factory default settings (the lock may already be associated (programmed)).
Green flashes	—	Check the motor connection.
Alternating red and green flashes	—	Check the motor connection.
—	—	Check the battery connection.

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

Once you have installed and tested your Controllers, you are ready to sign them on in your system. To do this, Wi-Q AMS software must be installed on your Host computer. At a minimum, you will need to create your Segment and add your Portal Gateways to the Segment Tree before you can sign on the Controllers. See "Add and Configure Portal Gateways (Task 7)" on page 67. Once that is done you can return to the site and sign on the controllers. See "Sign on and Configure Controllers (Task 10)" on page 84.

## Verify Signal Strength, Voltage and Packet Radio

If you used the Wi-Q Technology Site Survey Kit, you have already verified basic controller signal strength. Once the controllers are signed on, you can use the Statistics Monitor application to further measure controller performance, including controller voltage (battery level), and the packet ratio (the number of packets received vs the number of packets sent) of the controller. For more information about the Statistics Monitor application, see “Statistics Monitor” on page 191.

## 3 Software Installation

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

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

The following setup tasks are covered in this section:

Task 3 — Prepare your Computer

Task 4 — Gather and Organize Segment Data

Task 5 — Install Wi-Q AMS Software

## Prepare Your Computer (Task 3)

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

### Recommended System Limits

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

Hardware Configuration	Parameter			
	Config 1	Config 2*	Config 3*	Config 4*
<b>CPU Speed</b>	1 cores @ 3GHz	2 cores @ 3GHz	4 cores @ 3GHz	8 cores @ 3GHz x 2 machines (SQL server & communication server)
<b>RAM</b>	1 GB	4 GB	4 GB	8 GB
<b>Hard Disk</b>	40 GB	40 GB	40 GB	100 GB
<b>OS</b>	Windows 7 Pro, Ultimate & Enterprise SP1 (x32 & x64) Windows 8.1 Pro & Enterprise (x32 & x64)	Windows 7 Pro, Ultimate & Enterprise SP1 x64 Windows 8.1 Pro & Enterprise x64	Windows Server 2008 R2 Standard & Enterprise SP1 x64 Windows Server 2012 Standard & R2 Standard x64	Windows Server 2008 R2 Standard & Enterprise SP1 x64 Windows Server 2012 Standard & R2 Standard x64
<b>SQL Version</b>	SQL 2008 Express (x32 & x64) SQL 2012 Express (x32 & x64)	SQL 2008 R1 SP3 x64 SQL 2008 R2 SP2 x64 SQL 2012 R1 SP1 x64	SQL 2008 R1 SP3 x64 SQL 2008 R2 SP2 x64 SQL 2012 R1 SP1 x64	SQL 2008 R1 SP3 x64 SQL 2008 R2 SP2 x64 SQL 2012 R1 SP1 x64
<b>Portal Gateways</b>	50	100	250	1000
<b>Devices</b>	300	1000	3000	10000
<b>Users</b>	1000	5000	10000	50000
<b>Segments</b>	1	1	1	1
<b>Ethernet</b>	1000 Base T	1000 Base T	1000 Base T	1000 Base T

\* — requires tuning of system parameters during installation by Stanley Security Solutions Technical Support

## **Configure Windows Firewall Ports**

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

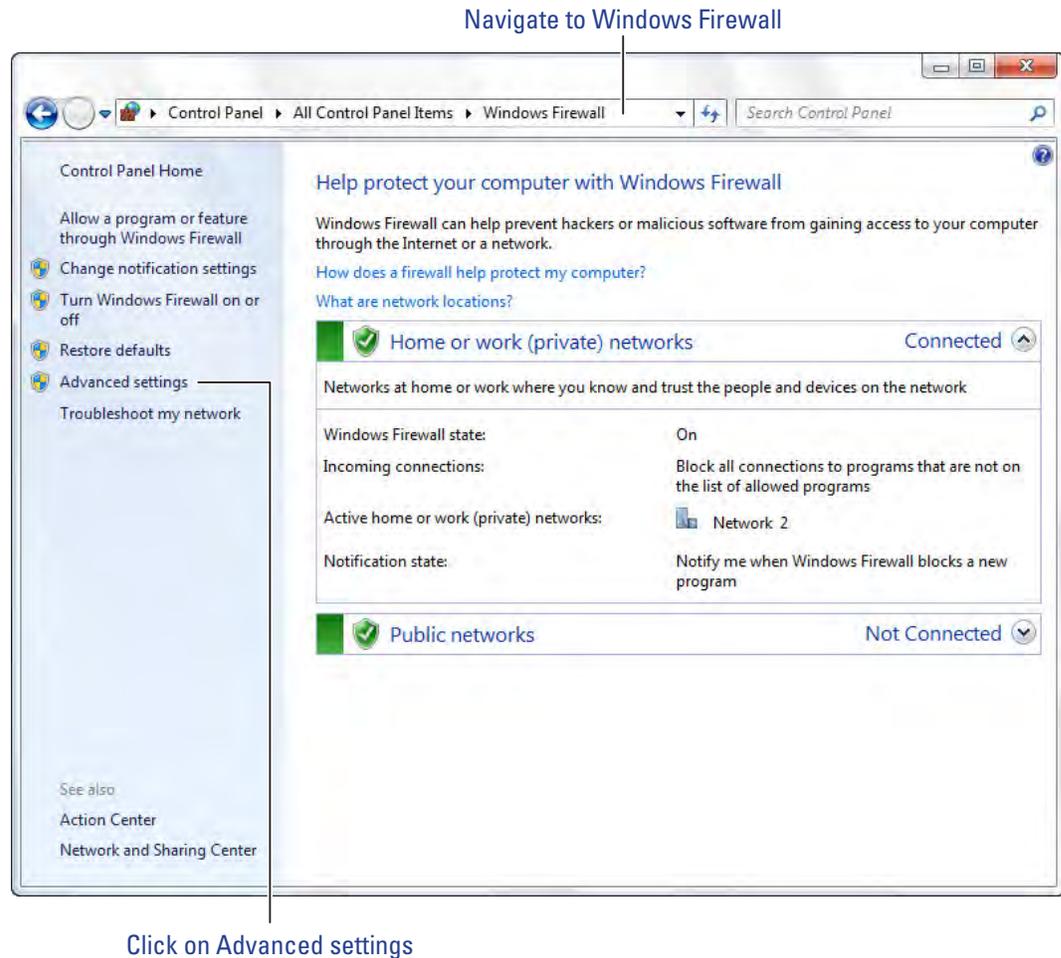
- Port 23
- Port 80
- Port 1433
- Port 1434
- Port 8000
- Port 11000
- Port 5353

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

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

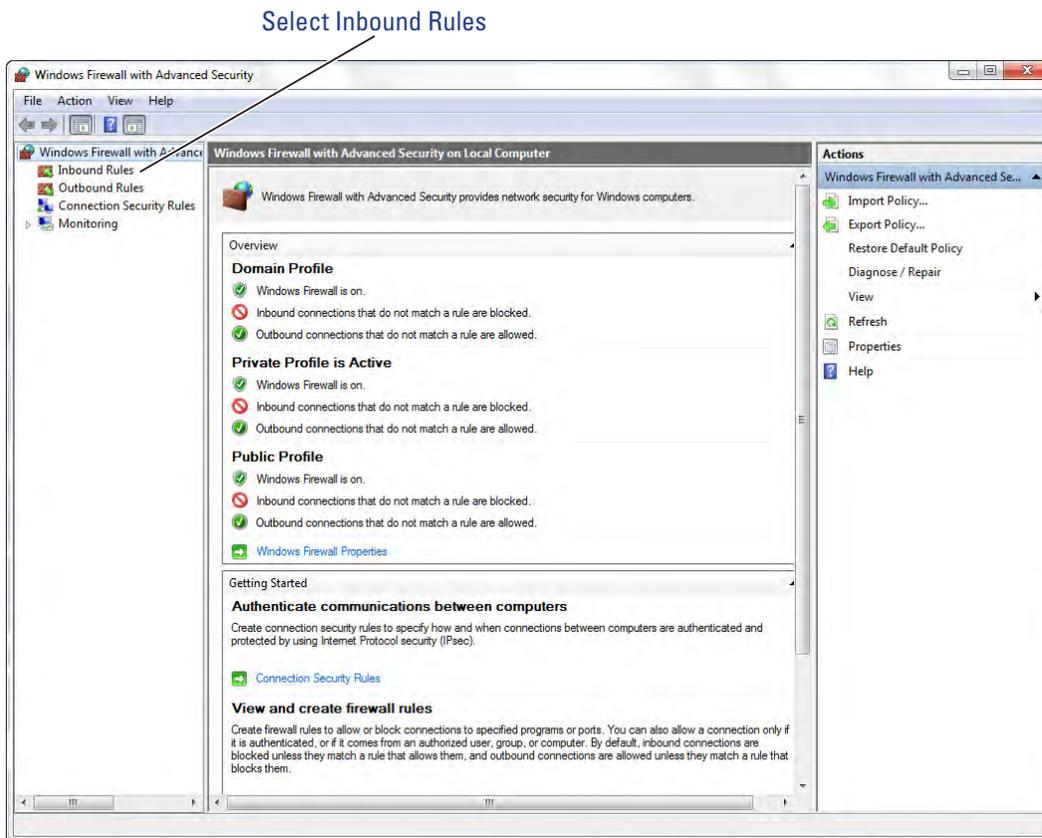
- 1 Navigate to your Windows Firewall settings from your PC's control panel. See Figure 10. Then, click on Advanced settings.

Figure 10 Windows Firewall



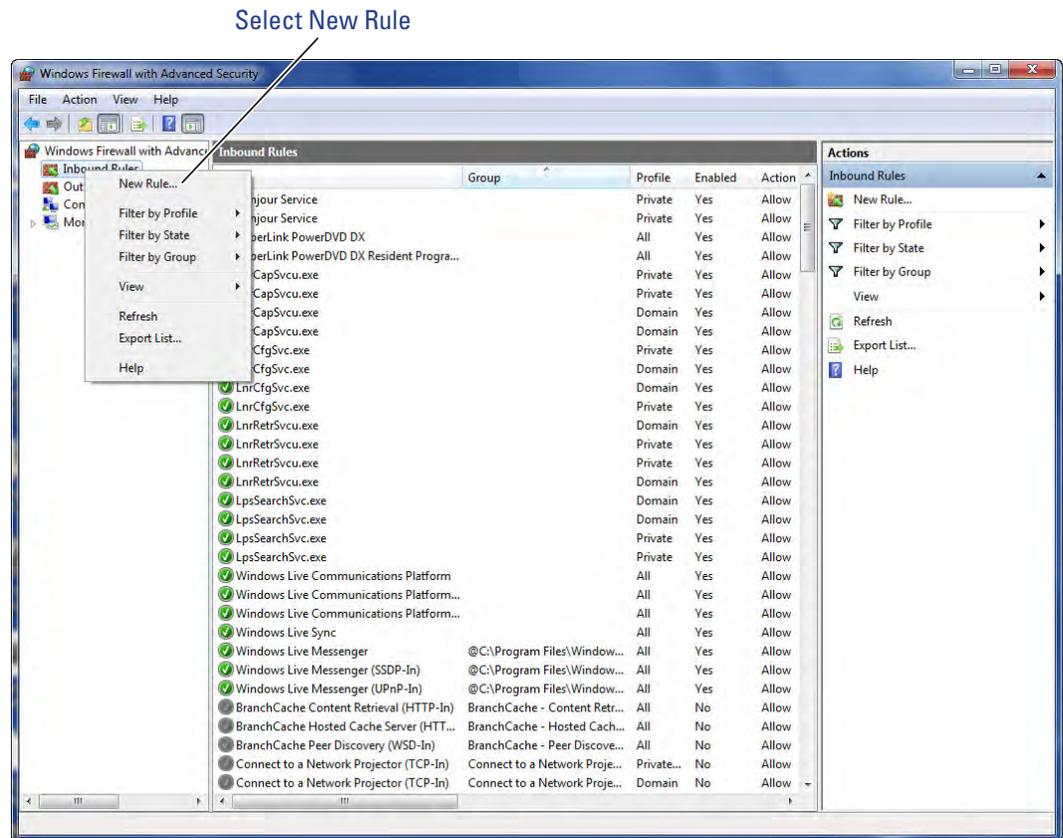
## 2 Select Inbound Rules.

Figure 11 Inbound Rules



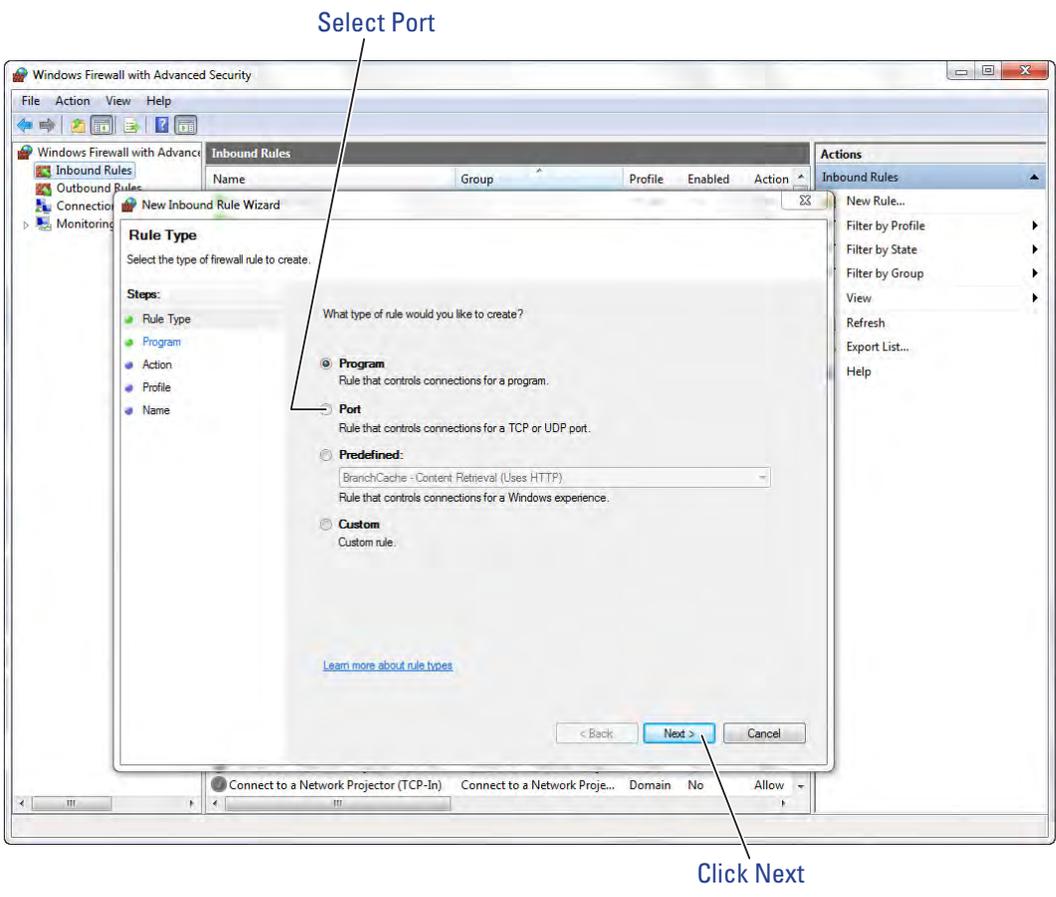
- 3 Right click on Inbound Rules to open an option menu. Select New Rule from the menu.

Figure 12 New Rule



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

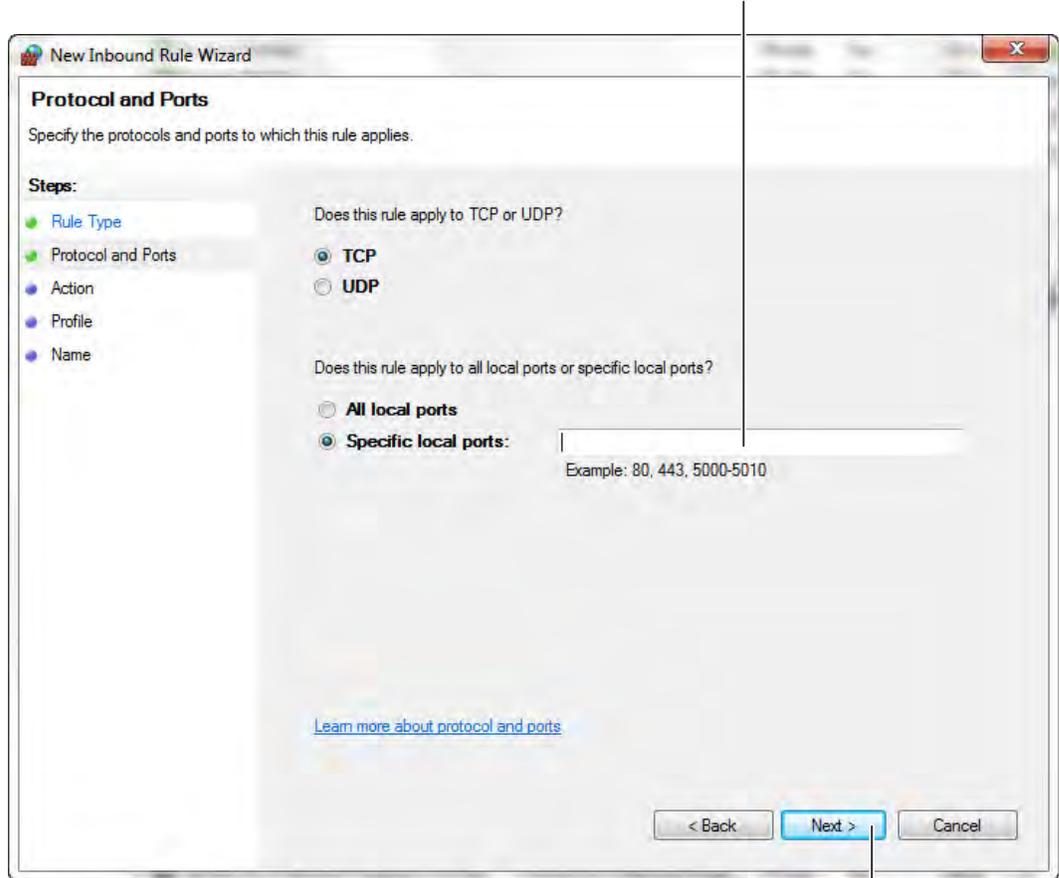
Figure 13 Create Port Rule



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

Figure 14 Enter Ports

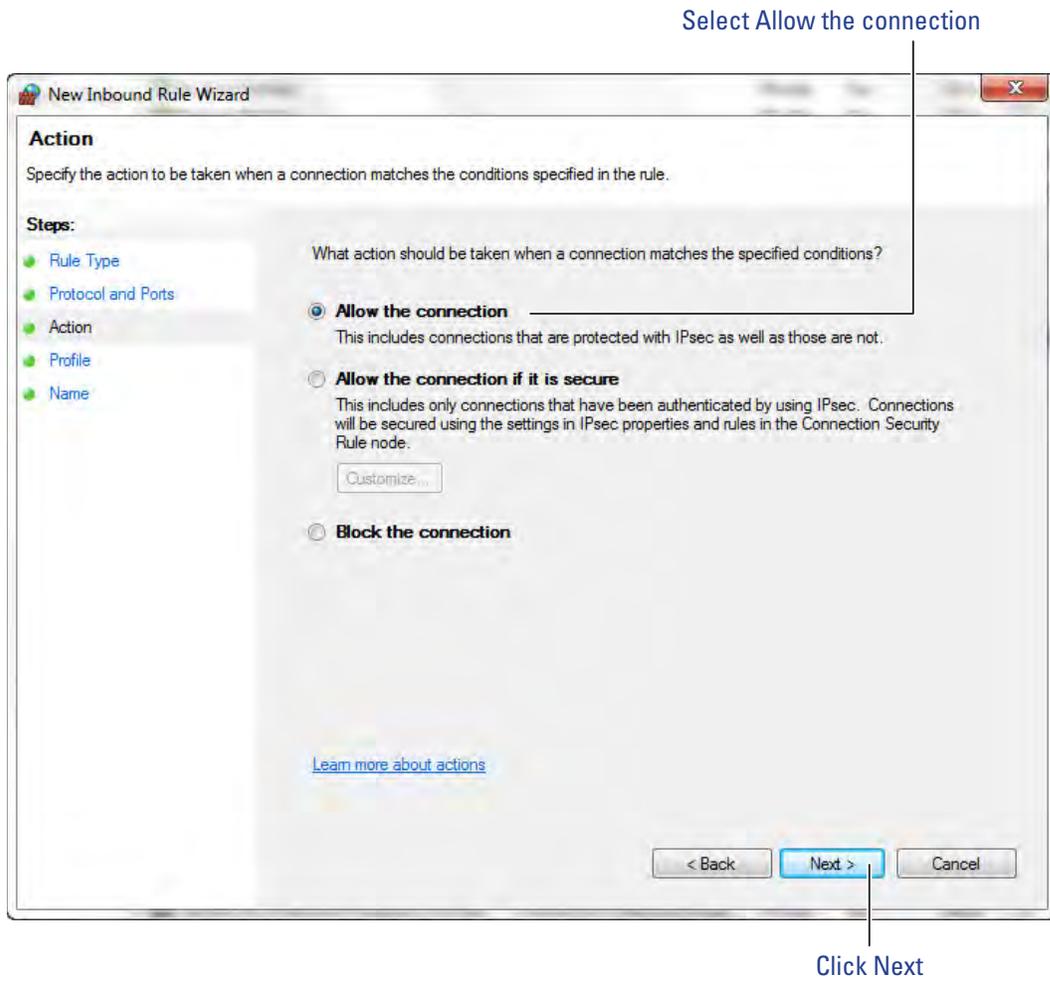
Enter ports: 23, 80, 1443, 1434, 8000, 11000, 5353



Click Next

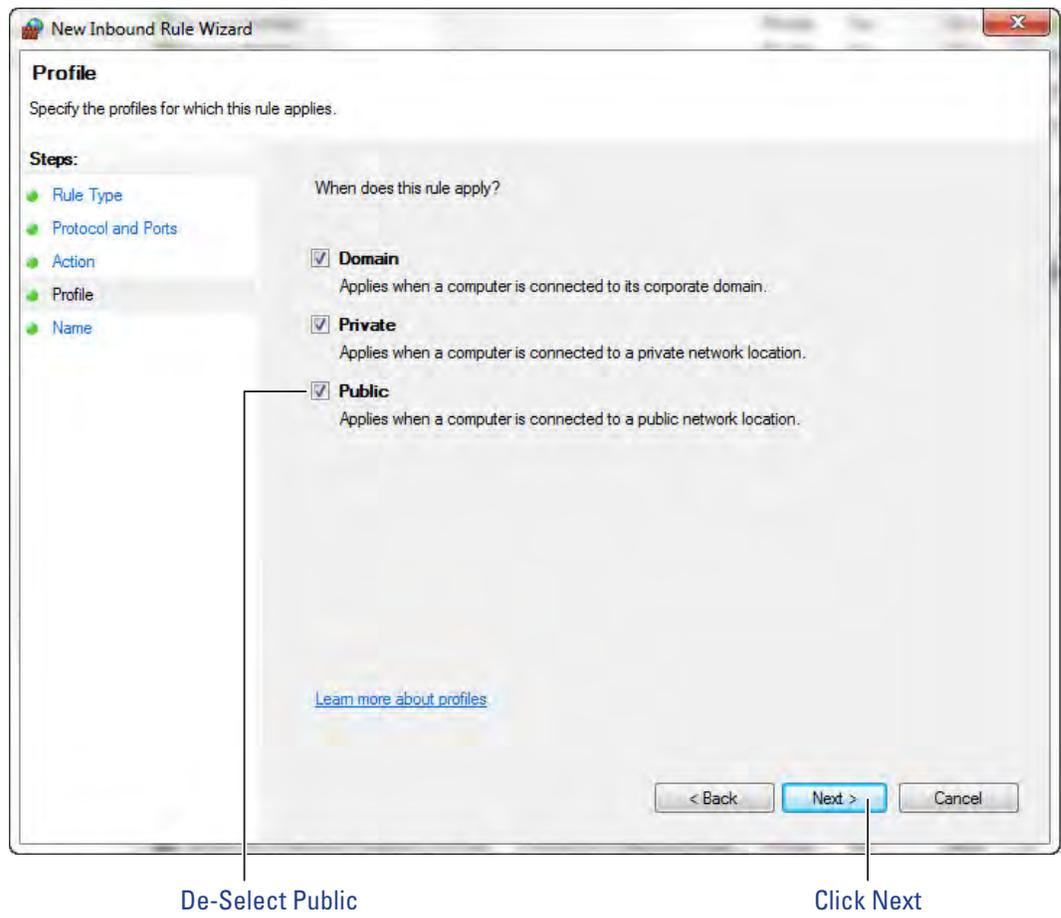
6 Select Allow the connection. Click Next to continue. See Figure 15.

Figure 15 Allow the Connection



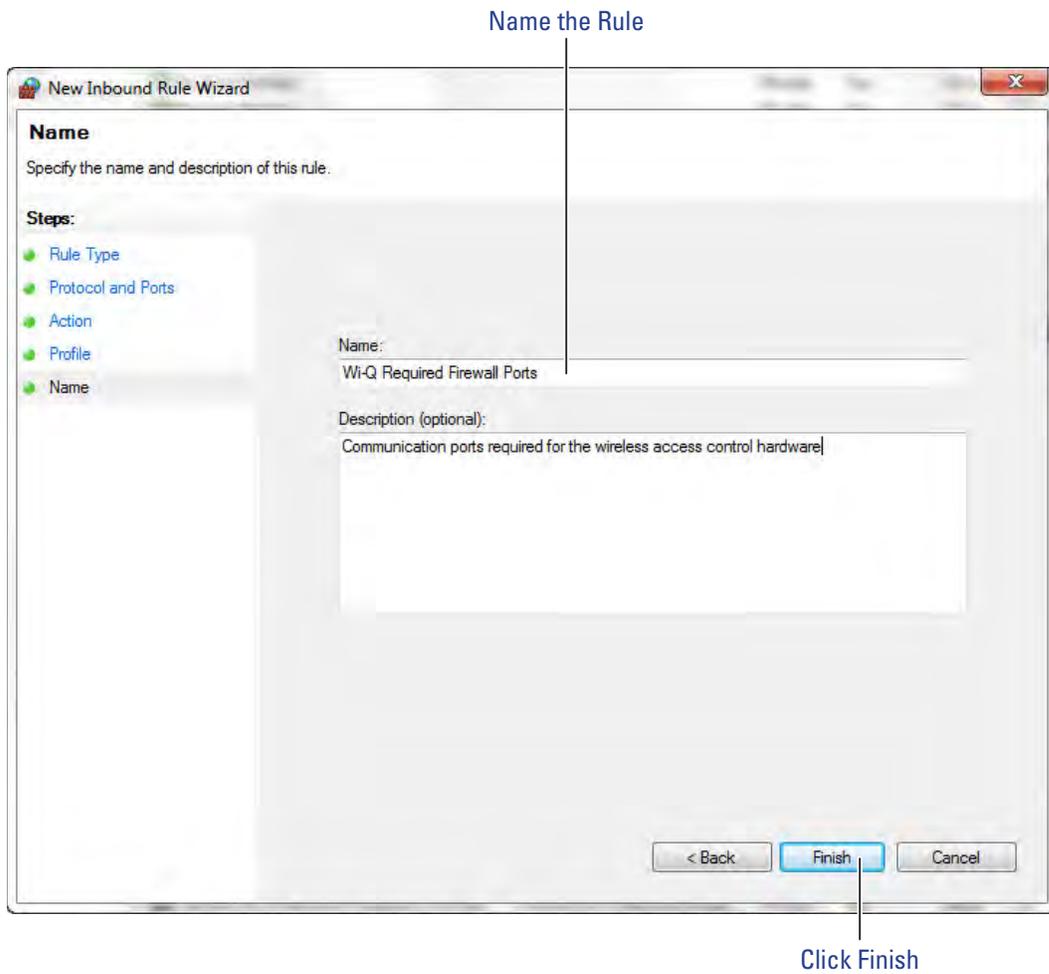
## 7 De-select the Public option. Click Next.

Figure 16 De-select Public



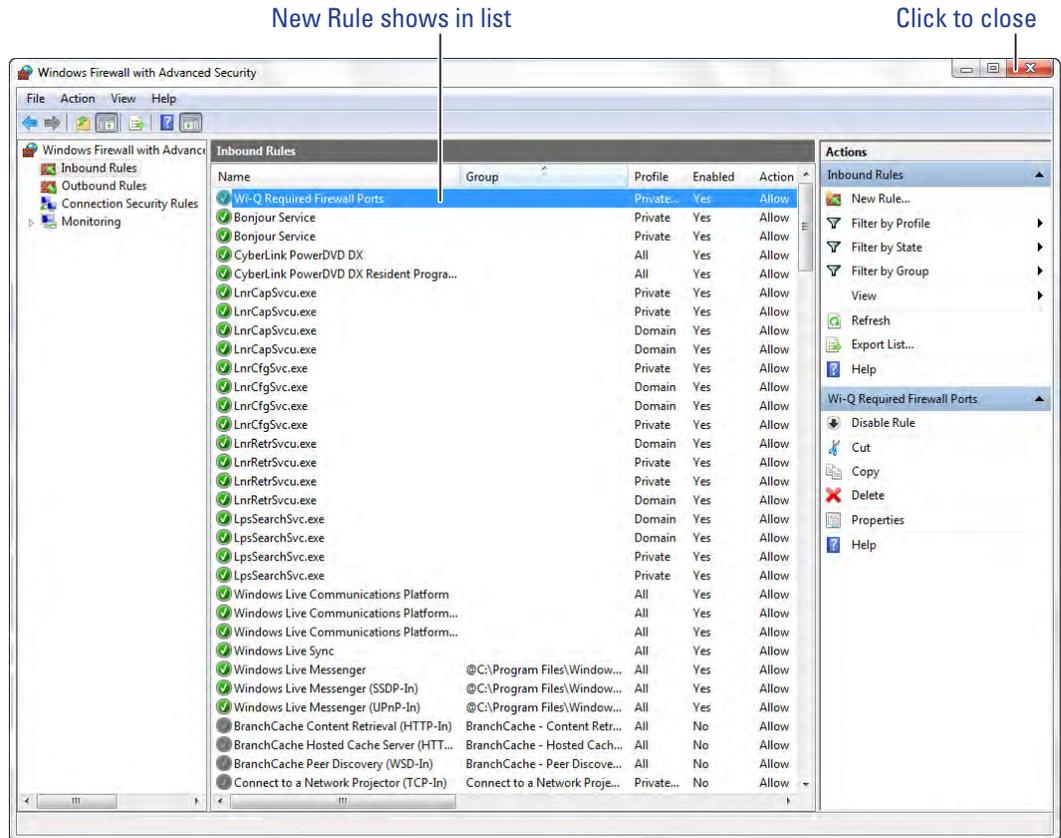
- 8 Give the new rule a name that can be easily identified by an administrator. Once finished, click Finish. See Figure 17.

Figure 17 Name the Rule



9 The new rule now appears in the list. The Firewall Settings module may now be closed. See Figure 18.

Figure 18 Inbound Rules List



## Gather and Organize Segment Data (Task 4)

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

### Device Information

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

## User Information

You will also need to gather the names of users, define their access requirements, organize user and timezone groups, and decide how you will use other features configurable within AMS.

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

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

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

## Importing Data

Do you have an existing database that already contains much of the information you need? It is likely you can modify a version and import it into AMS using the program's System Administrator feature. If you have a large organization, this will save you time and reduce data entry error. See "Importing Data from a Legacy OFM Database" on page 170.

## Install Software (Task 5)

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

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

If...	Then
If you plan to use a secure socket layer (SSL) connection (connecting via the internet)	A valid certificate must be obtained from a certificate authority for IIS. See your Network Administrator.
You plan to use a basic authentication	A local administrator user account, login, and password must be generated for the system to log into. (Instructions are presented in Portal Gateway Setup, Setup tab, Host Access Settings.)
You plan to use certificate mapping	A client certificate file must be generated. See your Network Administrator.

### Beginning Installation

- 1 If you have not already done so, download the Wi-Q AMS Software from the Stanley Technical Support website

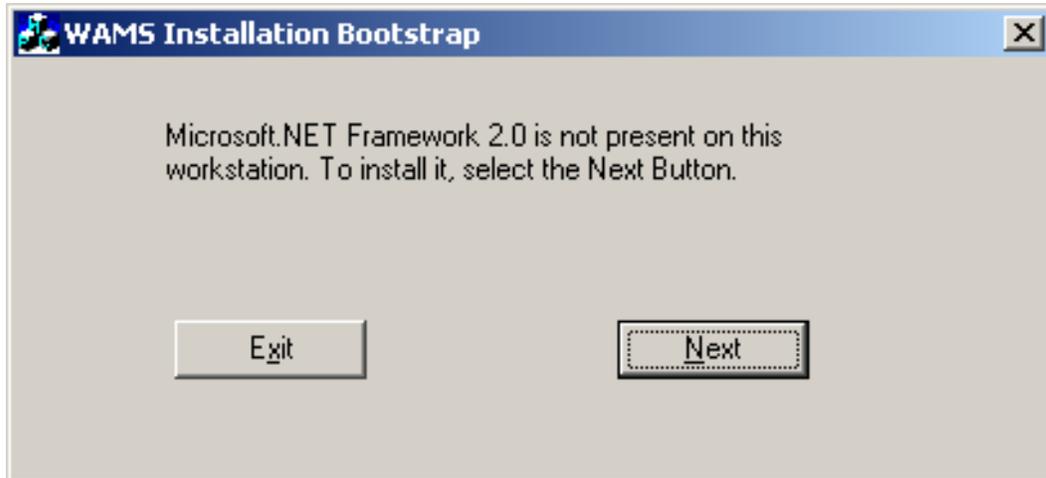
**or**

Insert the software disc into your machine's disc reader.

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

- 2 Click on the .exe file that contains "Bootstrap"  
(Example: WiQBootstrap.exe).
- 3 Wi-Q AMS Setup checks your workstation for any missing prerequisites, such as Microsoft.NET Framework. If the following dialog box opens, click Next. If not, proceed to Step 4.

Figure 19 Installation Bootstrap



- a The Microsoft .NET Framework Setup wizard welcome screen opens. Click Next to continue.
- b Read the End-User License Agreement. To continue with the installation, click the checkbox at the bottom. Then click Install. The installation may take a few minutes.
- c When the installation is complete, click Finish.

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

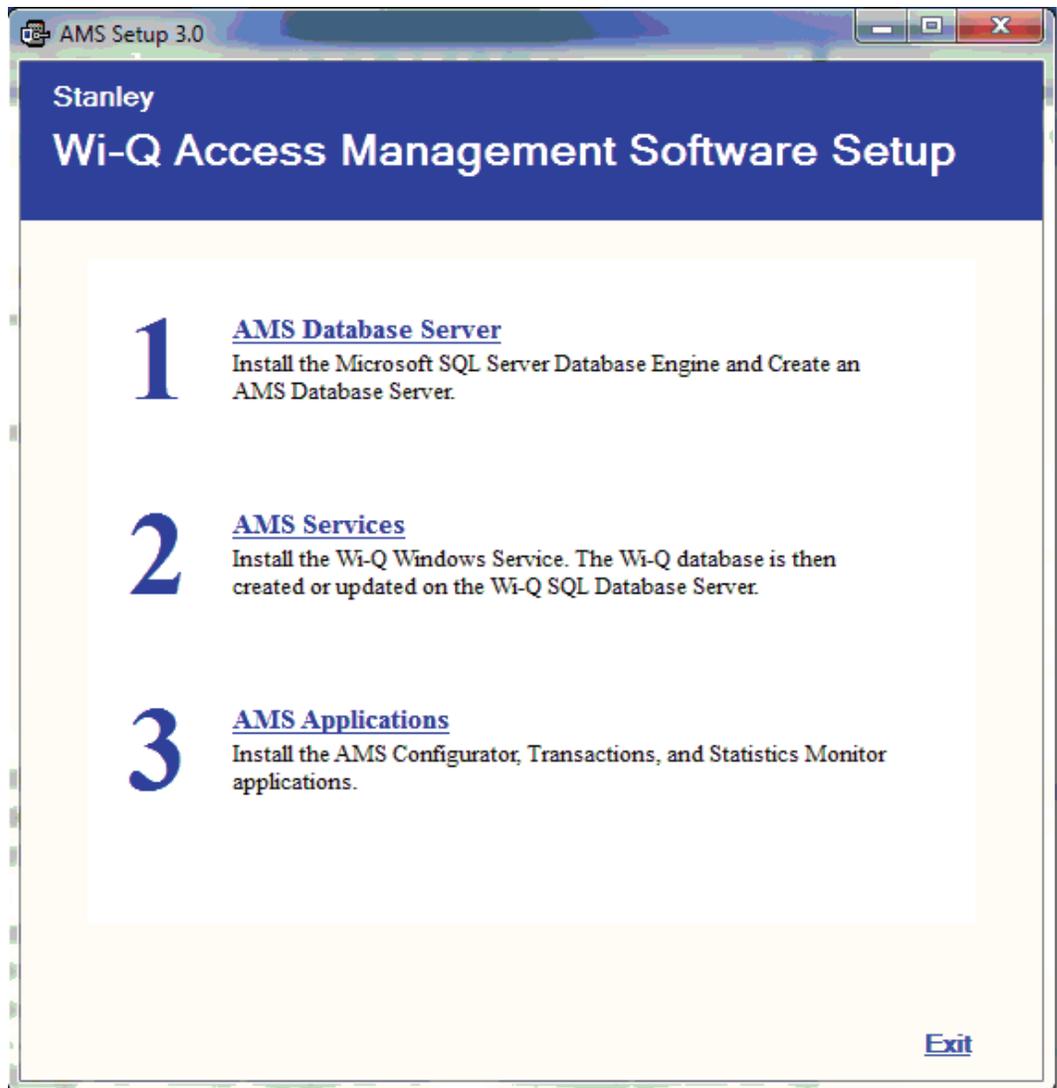
- d After rebooting your machine, click the "Bootstrap" .exe file again.

- 4 The AMS Setup Main page opens, Figure 20. It is important to perform the steps in the sequence presented.

**Note** You may wish to install the services and database on one machine (such as the Host) and the AMS Applications only at other machines. This can be done by selecting the appropriate application from the System Setup windows.

**Note** The screen shots in this User Guide are from a Stanley Wi-Q AMS system.

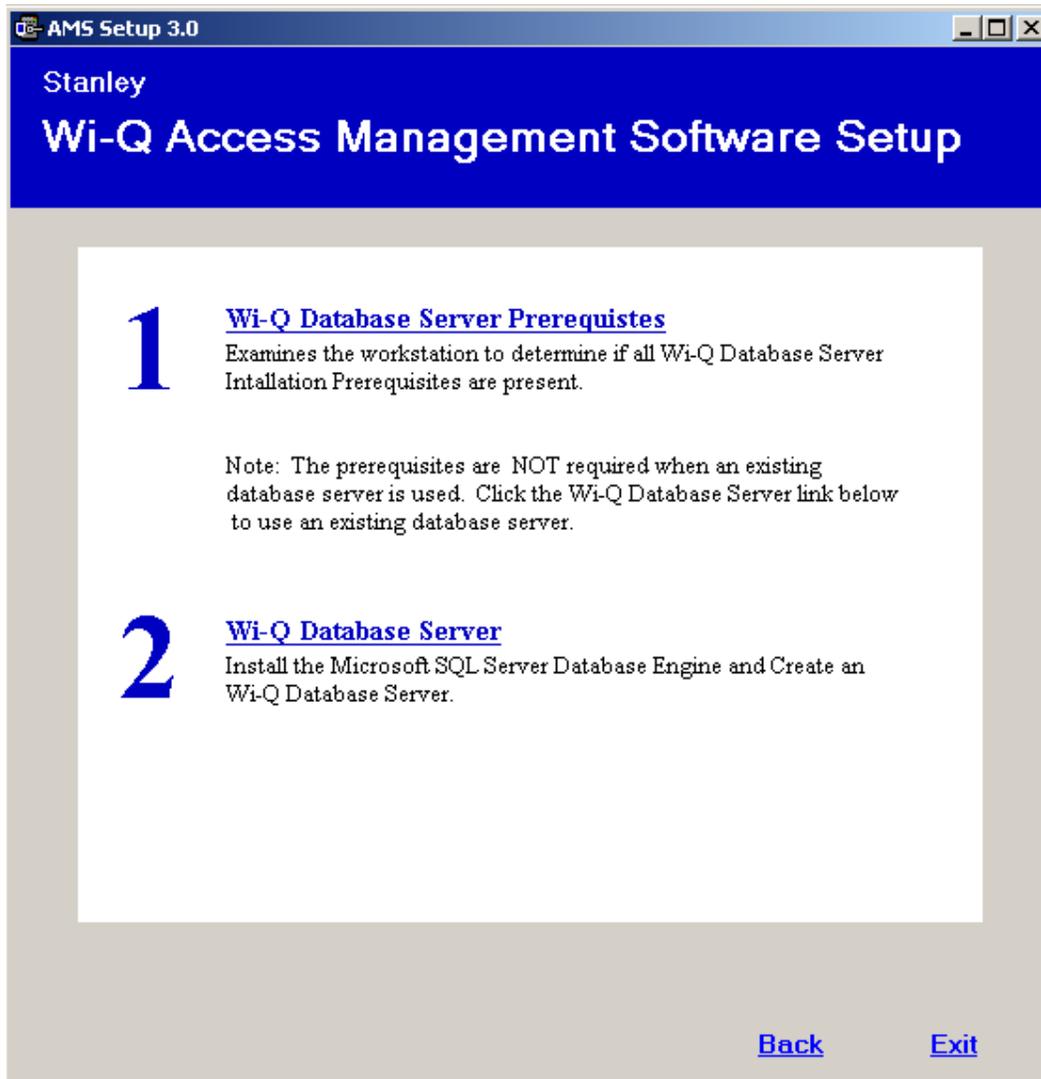
Figure 20 AMS Setup



## Step 1

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

Figure 21 Database Server Prerequisites



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

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

- 3 Once all the prerequisites have been installed, click the link on the main setup screen to install the AMS Database Server.
- 4 The Database Server System Definition dialog box opens. Choose whether to install the server on a local machine or within an existing SQL Server instance. If you choose to install on a local machine, decide whether to use the default password or define a new password. If you choose to install within an existing server, enter the instance name and associated user name and password. Then click Finish.

Figure 22 Database Server System Definition

**Database Server System Definition**

Define the Database and System Administrator (sa) Password.

Install OSI instance on local machine

Use Default Password (osi)

Define Password

Enter Password:

Retype Password:

Install within existing SQLSERVER instance

Instance Name:   
*Ex: APACHE-GY3H1\OSI*

User Name:

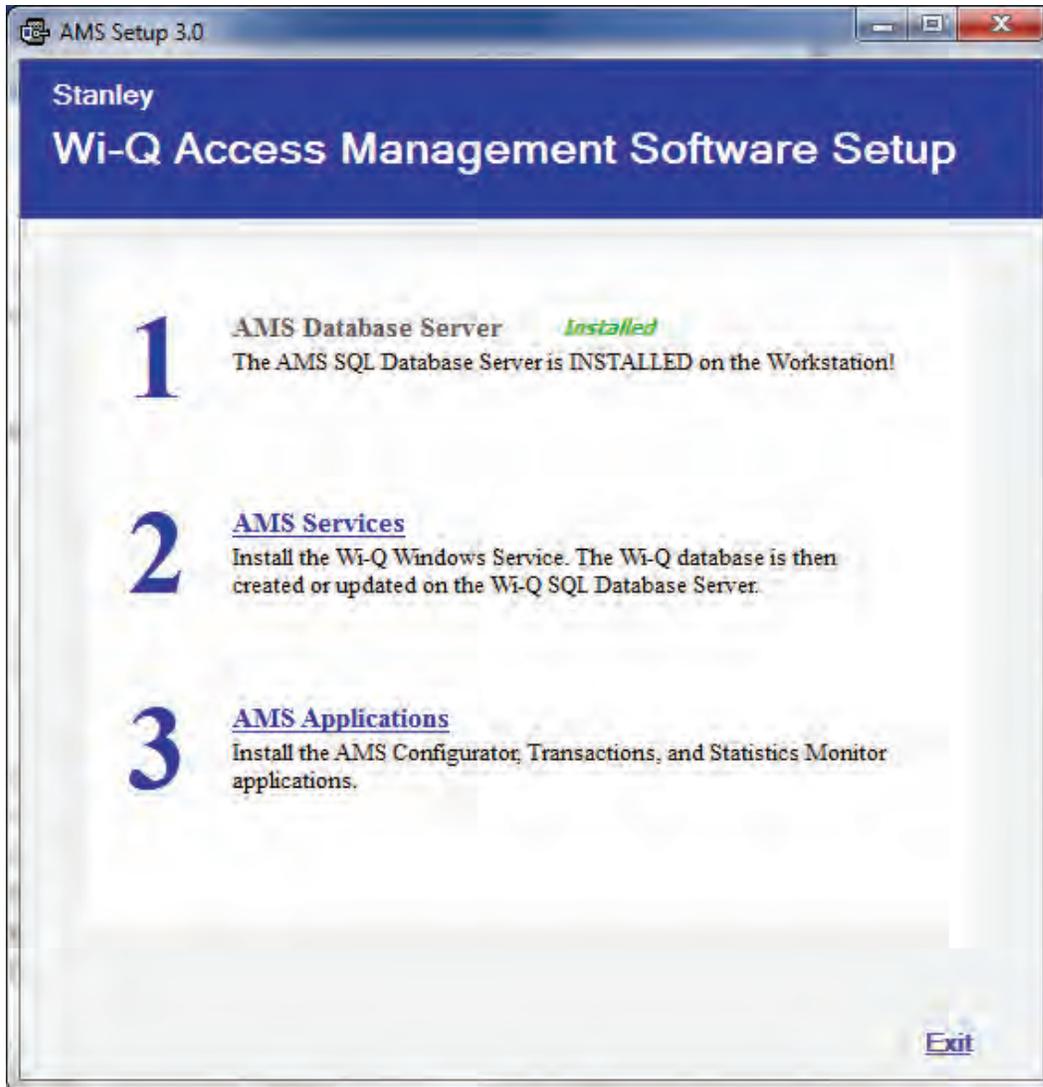
Password:

Cancel Finish

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

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

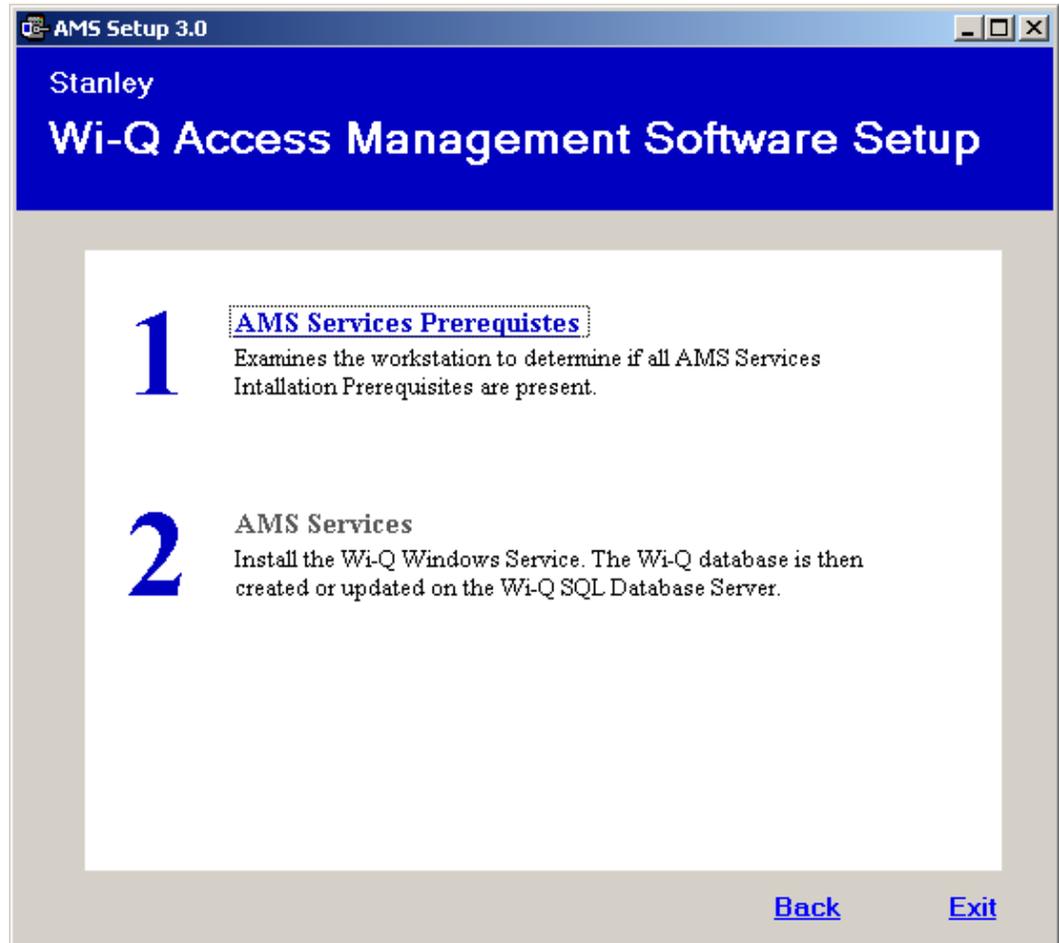
Figure 23 AMS Database Server Successfully Installed



## Step 2

- 1 On the Setup main page, click the AMS Services link.
- 2 If a similar dialog box opens with a link to install Prerequisites, click the link. See Figure 24.

Figure 24 Install Prerequisites



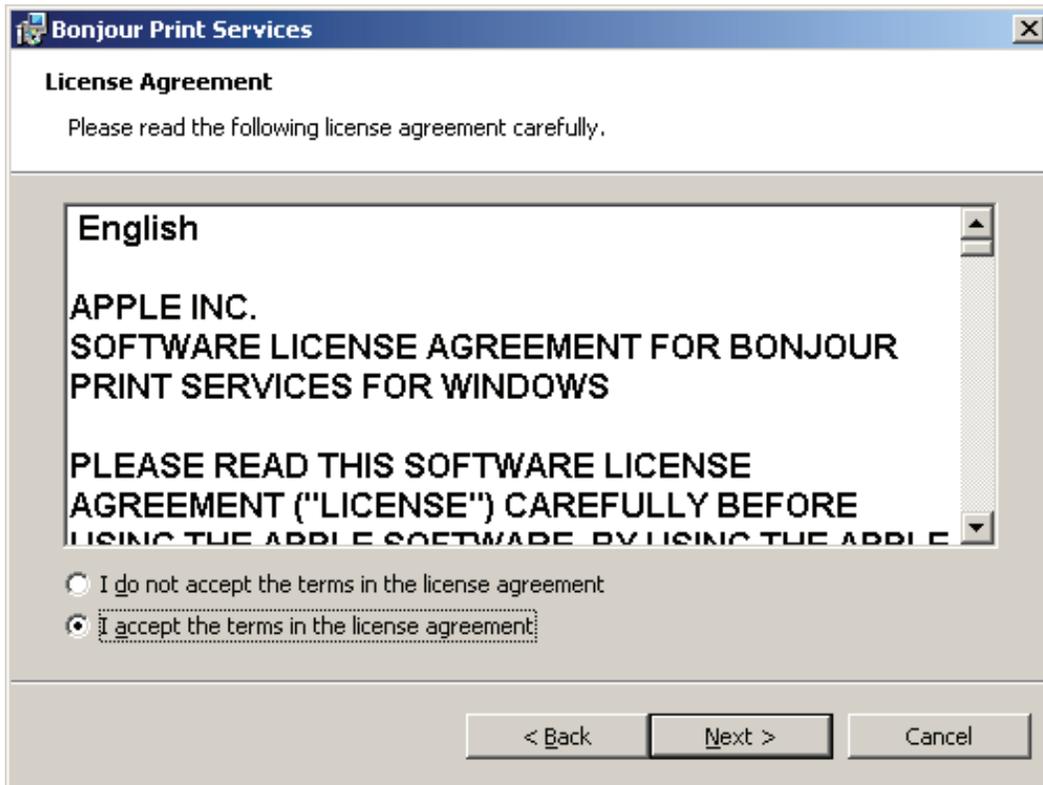
- a You may be prompted to install Apple® Bonjour®. Bonjour networking technology is used by the Portal Configuration Tool to locate and list all Portal Gateways on the network. Click the link to begin installing Bonjour.
- b The Bonjour Print Services window opens. Click Next to continue.

Figure 25 Bonjour Print Services Installer



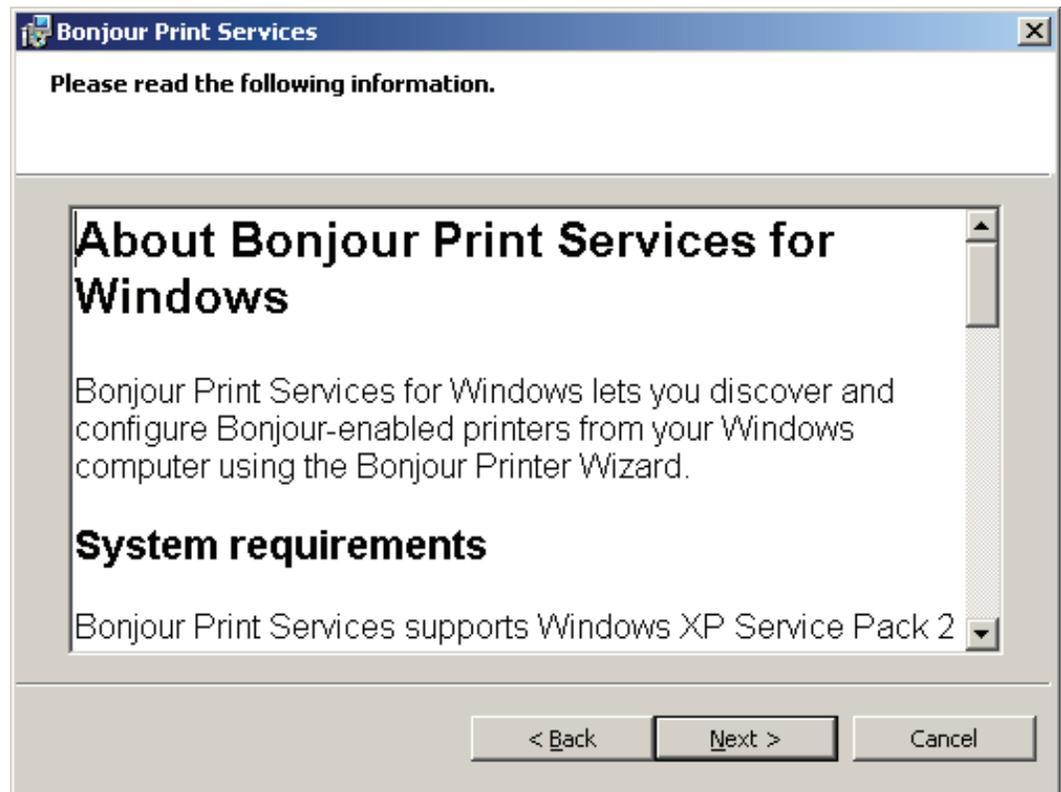
- c Read the License Agreement. To continue with the installation, click on "I accept the terms in the license agreement," then press Next.

Figure 26 Bonjour Print Services License Agreement



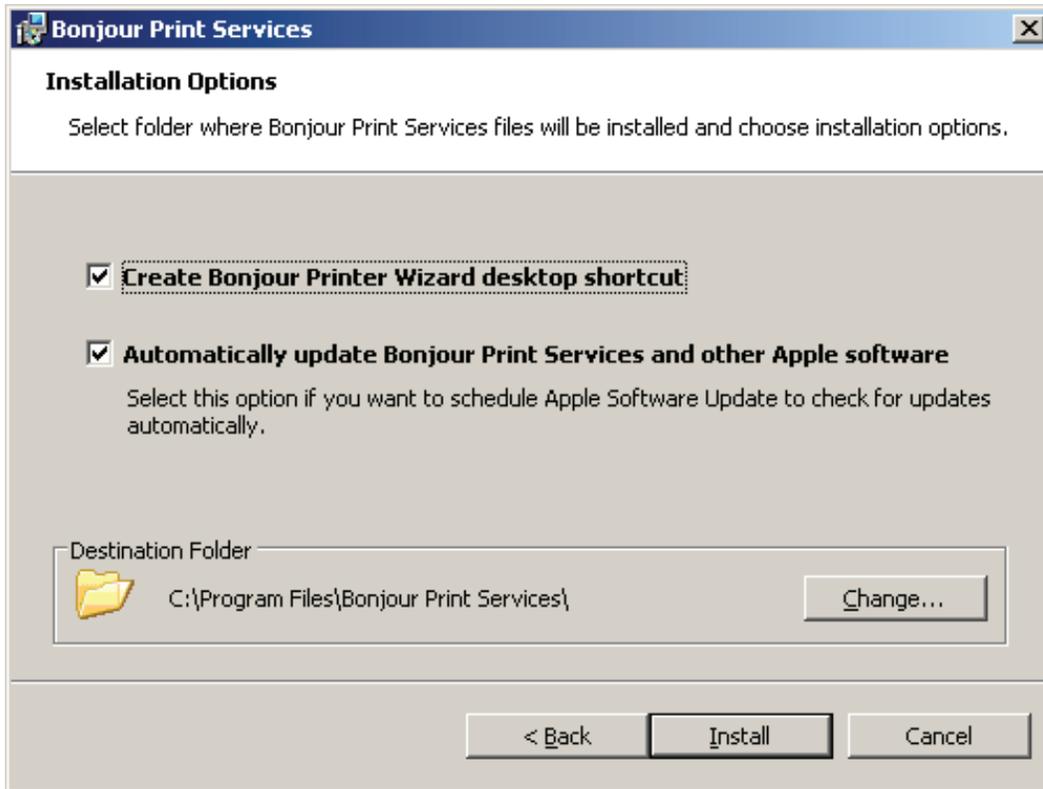
- d Read the information about Bonjour Print Services. Then press Next.

Figure 27 Bonjour Print Services Information



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

Figure 28 Bonjour Installation Options



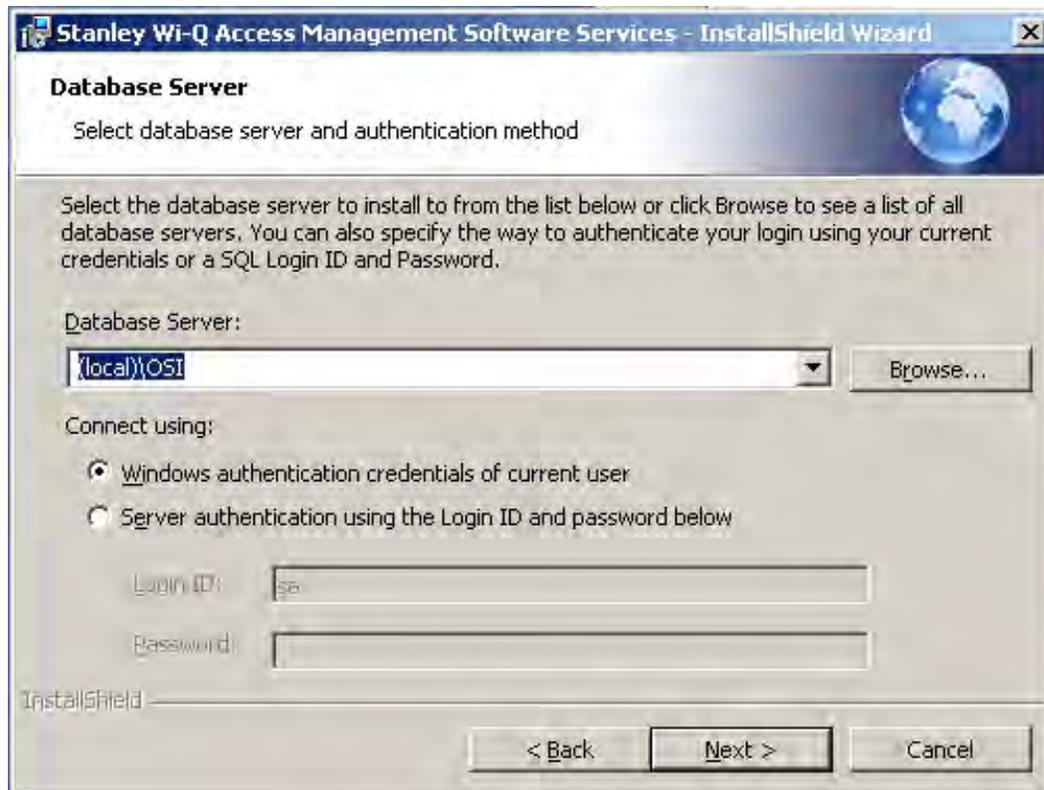
- f Once the Bonjour Print Services Installation is complete, press Finish.

Figure 29 Bonjour Print Services Installation Complete



- 3 Click on AMS Services to install the Wi-Q/Omnilock Windows Service and create a database.
- 4 Click Next to continue past the Welcome page.
- 5 On the Database Server dialog box, browse to your database server and select your connection method. In the Connect Using section, choose your connection method. If you choose Server authentication, provide the Login ID and Password for the server. See Figure 30

Figure 30 InstallShield Wizard Database Server



- 6 In the Setup Type dialog box (Figure 31), select a Complete or Custom install. Selecting Complete will run installations for the Database, Communication Service, Portal Config App and Wi-Q/Omnilock Service. Selecting Custom will allow you to choose which components to install. Once you've made your selection, press Next to continue.

Figure 31 Setup Type

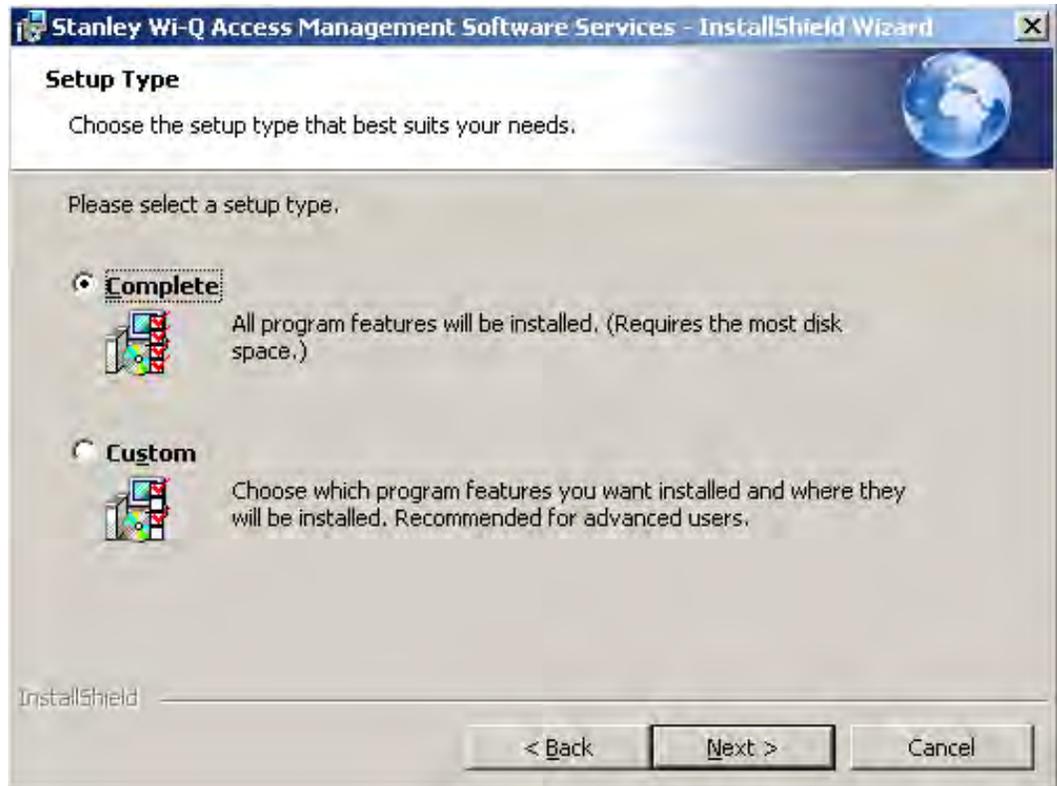
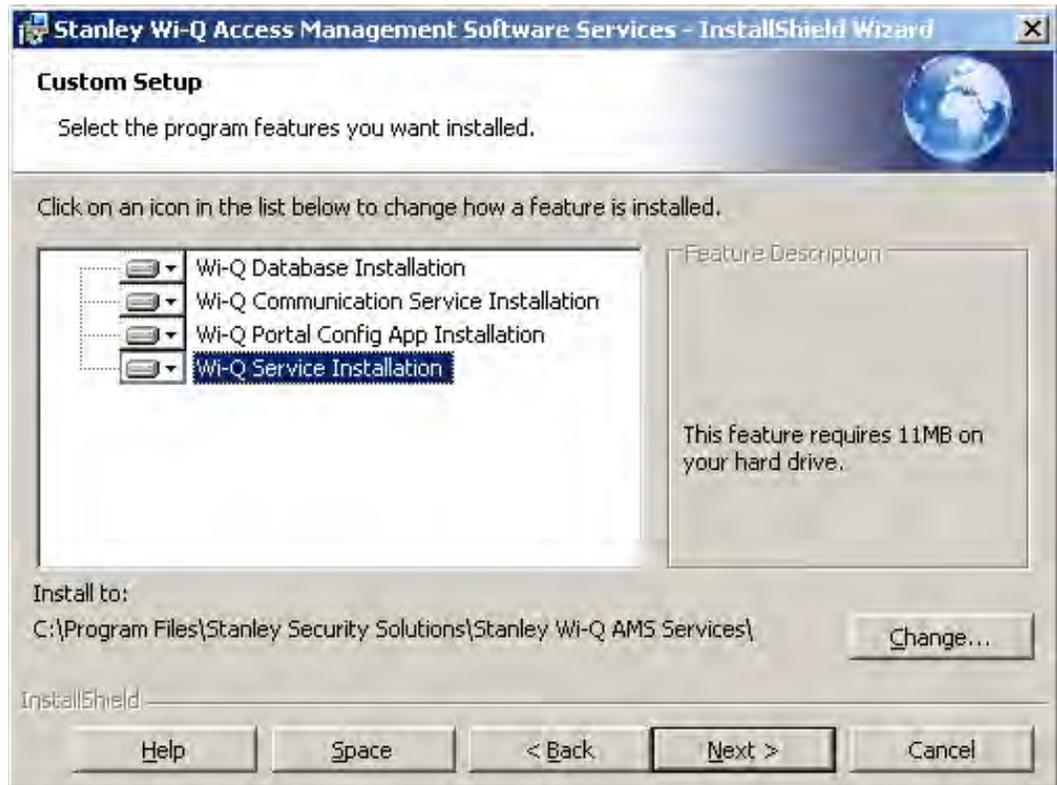


Figure 32 shows the installation components available in a Custom Setup.

Figure 32 Custom Setup



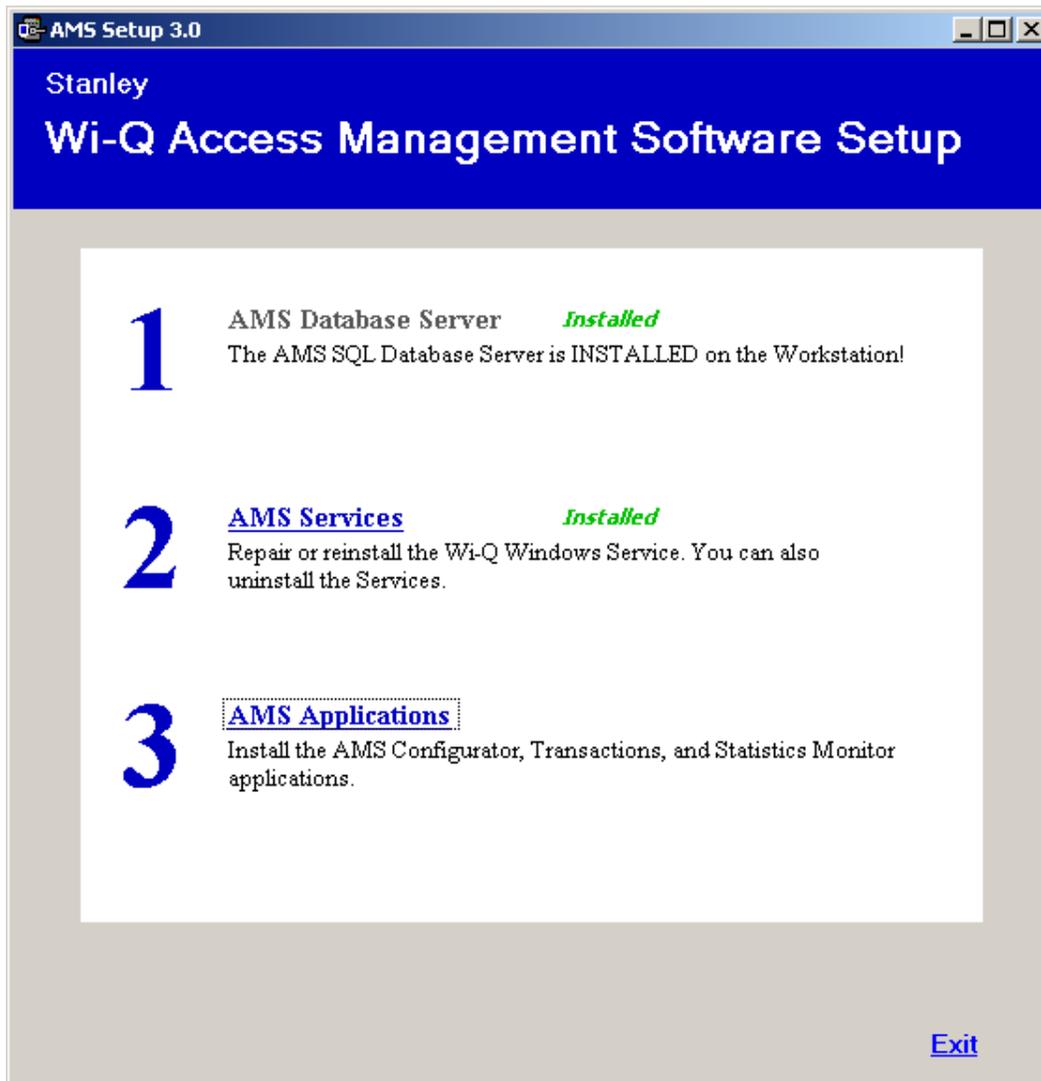
Clicking on the icons to the left of each component will bring up installation options. If you decide on a Custom Setup, you must select an installation option for each component. Then click Next to continue.

- 7 The wizard is now ready to begin installation. Click Install.
- 8 Once the installation is complete, click Finish.

### Step 3

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

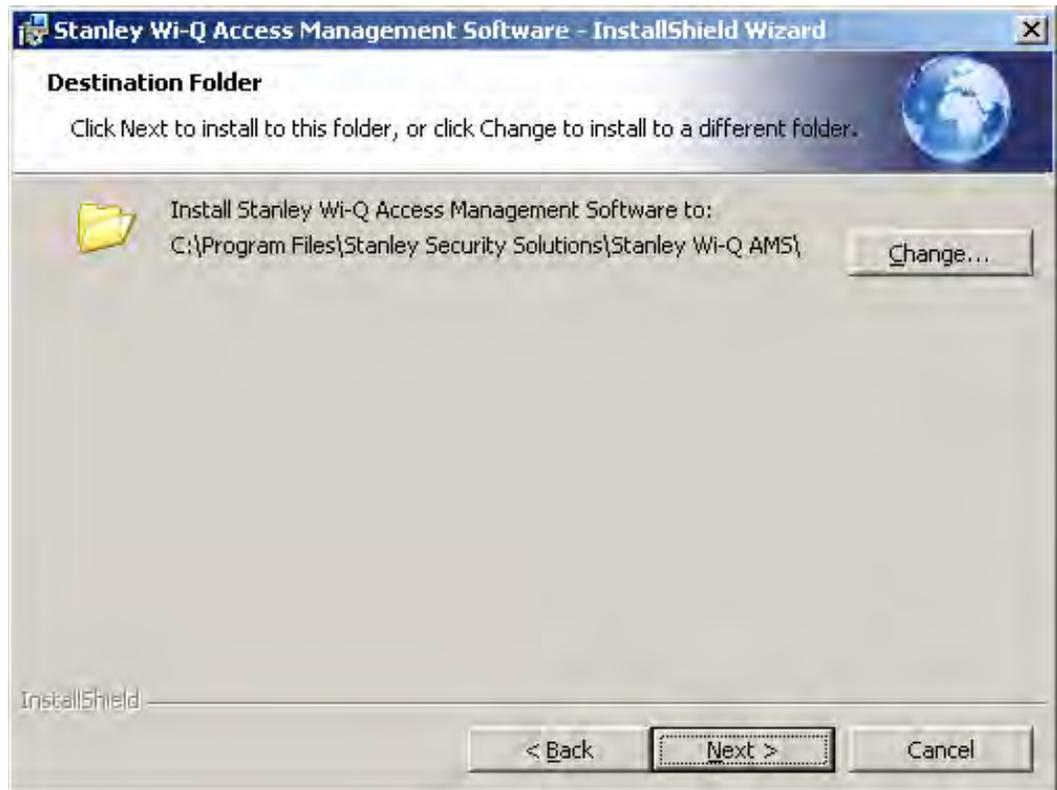
Figure 33 Install AMS Applications



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

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

Figure 34 Destination Folder



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

Figure 35 shows the installation components available in a Custom Setup.

Figure 35 Custom Setup

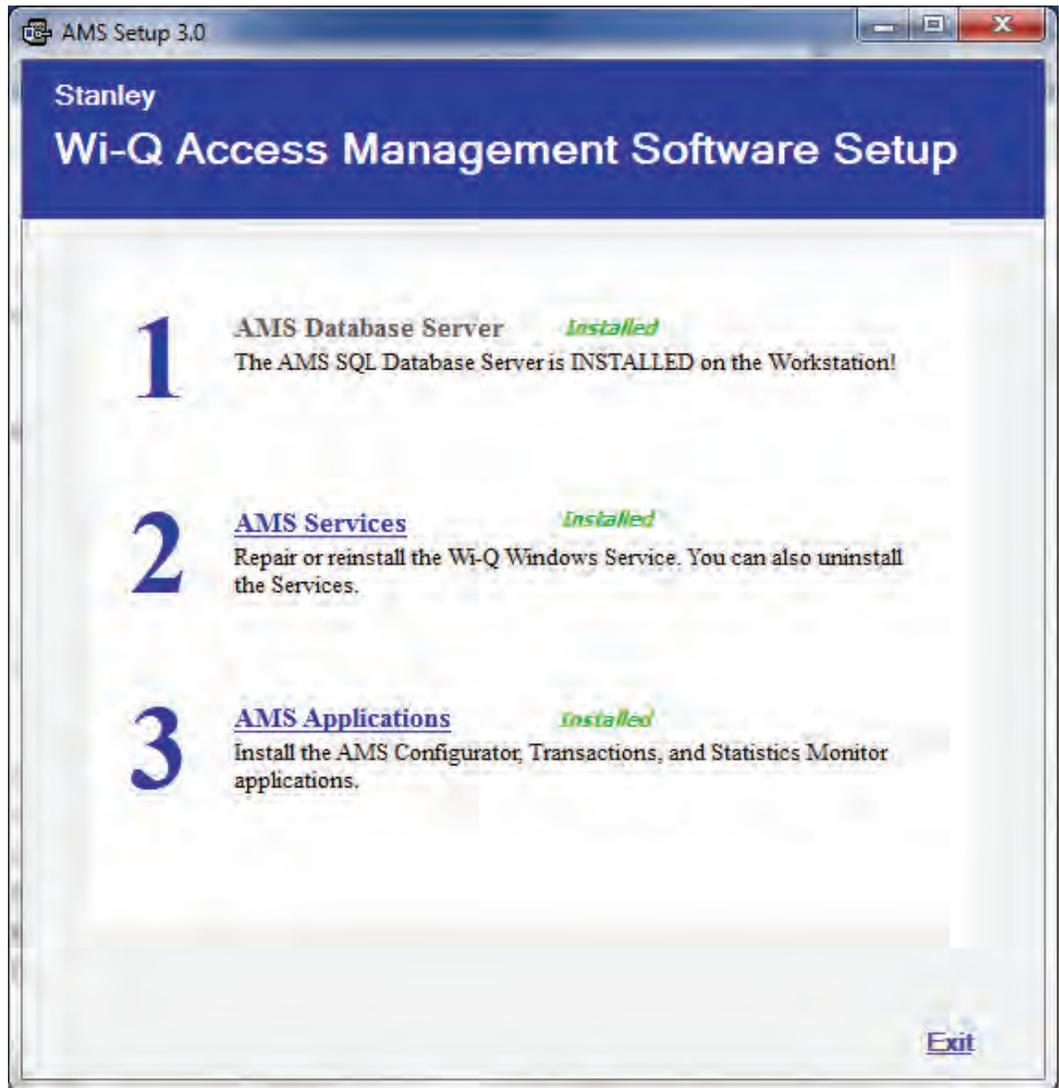


Clicking on the icons to the left of each component will bring up installation options. If you decide on a Custom Setup, you must select an installation option for each component. Then click Next to continue.

- 5 The wizard is now ready to begin installation. Click Install.
- 6 Once the installation is complete, click Finish.

The installation of all three components is now complete.

Figure 36 Successful System Setup



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

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

## 4 Configuring Segments, Portal Gateways and Controllers

This chapter contains detailed steps to perform the following tasks:

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

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

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

## Create Your Segment (Task 6)

It is important to give some thought to how you will go about configuring a segment in AMS. If you have not already done so, it may be helpful to review the Getting Started Guide.

### Logging in to Configurator

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

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

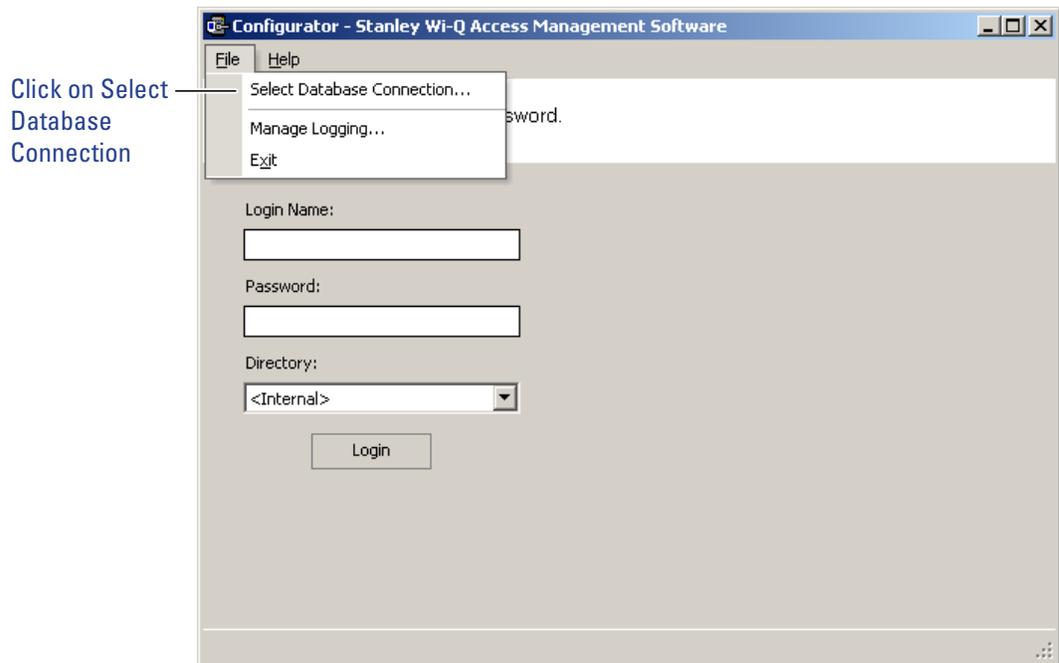
### Selecting the Database Connection

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

#### *To select a database on a different computer*

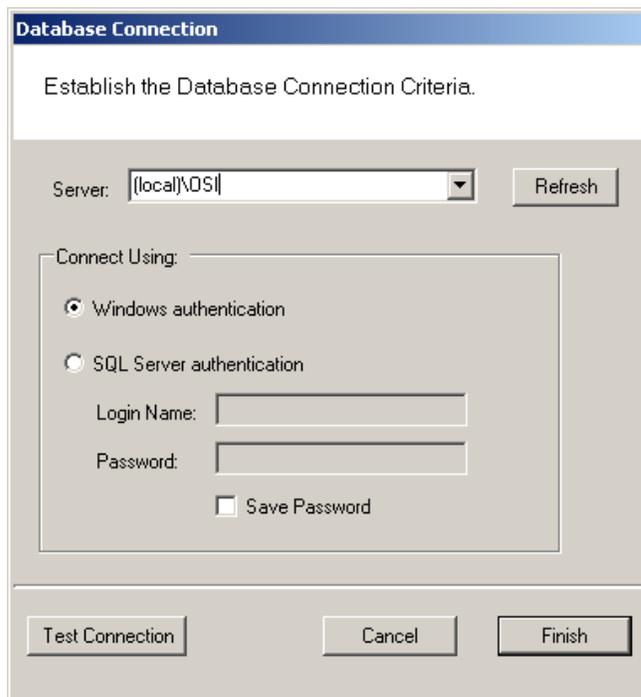
- 1 From the File menu, select Select database connection from the drop-down list.

Figure 37 Select Database Connection



The Database Connection dialog box opens. See Figure 38.

Figure 38 Database Connection Window



- 2 In the Server field, select the server location from the drop-down list.
- 3 Under Connect Using, select either Windows authentication or SQL Server authentication. If you select SQL Server, enter the login name and password for that server.
- 4 Click Test Connection.
- 5 Click Finish. You are ready to login to AMS using your desired database.

### **Login Information**

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

Login: Admin

Password: Admin

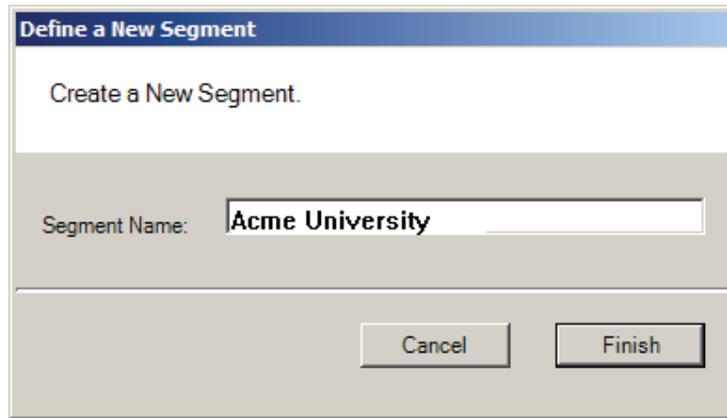
- 1 Enter the Login Name and Password.
- 2 Select Login. You are ready to start setting up your new segment.

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

## Define a New Segment

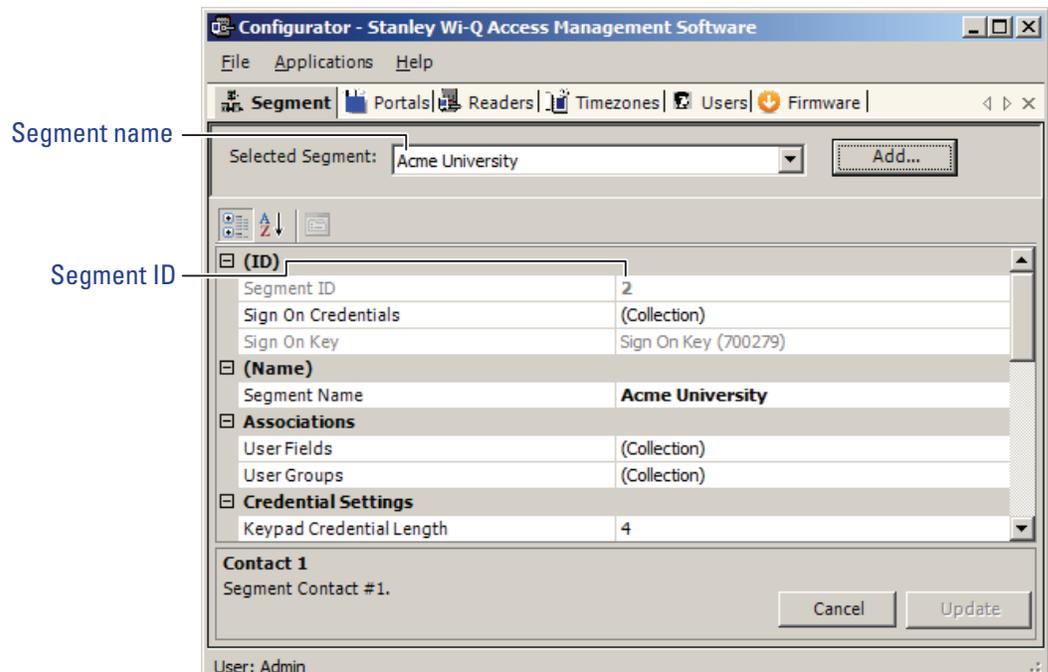
- 1 In the Segment Name box, enter a unique name for your segment.

Figure 39 Define a New Segment



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

Figure 40 Identifying the Segment name and ID



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

## To change the Password

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

Figure 41 Set Password of User



The image shows a dialog box titled "Set Password of User (Admin)". The dialog contains the following elements:

- Title bar: "Set Password of User (Admin)"
- Message: "Set the User Password."
- Input fields:
  - "Enter Current Password:"
  - "Enter New Password:"
  - "Retype New Password:"
- Buttons: "Cancel" and "Finish"

- 2 Enter the new password
- 3 Retype the new password.
- 4 Select Finish.

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

## Add and Configure Portal Gateways (Task 7)

Portal Gateways can now be added and configured within the software. 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.

You can change the IP address of your Portals with the Portal Configuration Module.

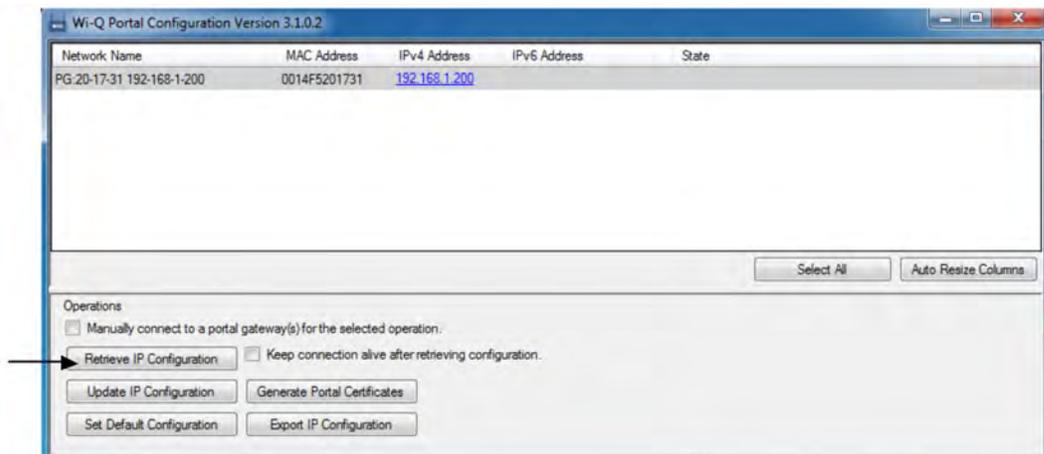
**Note** All Portal Gateway IP address must be unique across the entire system.

### Configuring a Portal Gateway with the Portal Configuration Module

Perform the following steps to change your Portal Gateway's IP address.

- 1 Connect the Portal Gateway to the Host either over the network or directly via crossover Ethernet cable (recommended). For more information on connecting a Portal Gateway, see "Connecting the Portal Gateway and Verifying Operation" on page 24.
- 2 Open the Portal Configuration module (Start Menu>Stanley Security Solutions>Stanley Wi-Q AMS Tools).
- 3 Portals available on the network will automatically be listed in the Portal Configuration module.

Figure 42 Portal Gateways Available on the Network



- 4 Select a portal from the list.
- 5 At this point, you may change the IP address from the factory setting to one from the range you've created. Click on Update IP Configuration to update the selected portal.
- 6 Select IPv4 and/or IPv6 and enter the IP address.
- 7 You may need to adjust the SubNet Mask/Network Destination and Gateway to match your network. Consult your network administrator for details.
- 8 If you wish to generate a SSL certificate for a more secure connection, click on the SSL Enabled checkbox, then click OK.

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

Figure 43 Update IP Configuration

The screenshot shows a dialog box titled "Update IP Configuration". It has two main sections: "IPv4 Configuration" and "IPv6 Configuration".

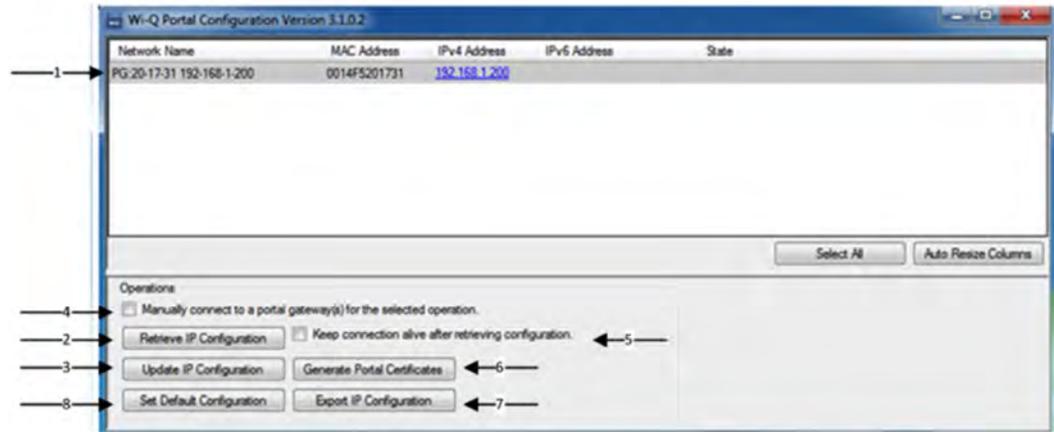
- IPv4 Configuration:** This section is checked. It contains the following fields:
  - IP Address: 192.168.1.200
  - Subnet Mask: 255.255.255.0
  - Gateway: 192.168.1.20
  - Portal Service Port: 8000
  - Portal Config Service Port: 11000
  - SSL Enabled:
- IPv6 Configuration:** This section is unchecked. It contains the following fields:
  - IP Address: : : : : : : :
  - Network Destination: : : : : : : :
  - Gateway: : : : : : : :
  - Portal Service Port: 0
  - Portal Config Service Port: 0
  - SSL Enabled:

At the bottom of the dialog are "OK" and "Cancel" buttons. Each configuration section also has a "Fill Default" button.

## Portal Configuration Features and Functions

Review this section for additional information regarding the Portal Configuration window. See Figure 44.

Figure 44 Portal Configuration Window



### 1 Portals on the Network grid

Provides a list of Portal Gateways on the network. It shows the status of the last operation performed, the portal network name, a hyperlink that opens the corresponding status page, portal MAC address and portal IP configuration data.

### 2 Retrieve IP Configuration Scan

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

### 3 Update IP Configuration

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

### 4 Manual Connection

When checked, allows a portal to be configured by IP address. Some net-

works do not allow port 5353 to be open, which is required by the application when scanning for portals. This allows manual connection to the portal so the portal can be configured. You must click on Update IP Configuration after selecting this box.

#### **5 Keep Connection Alive Checkbox**

Allows the connection with the portal to continue, otherwise a reboot will occur after the action selected.

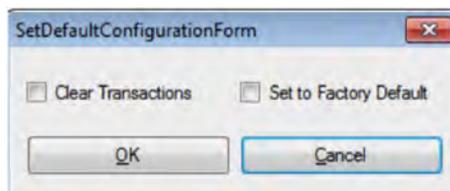
#### **6 Generate Portal Certificates**

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

#### **7 Export Portal IP Configuration**

Exports the portal IP configuration for the selected portals.

### **Set Default Configuration**



#### **Clear Transactions**

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

#### **Set Back to Factory Default**

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

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

## **Adding Portal Gateways to AMS**

Portals can be added to your system in two ways:

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

## Adding Portal Gateways One at a Time

Refer to Figure 45.

- 1 In the Configurator application, click the Portals Tab.
- 2 Click Add and the Configure New Portal Gateway screen opens.
- 3 In the Workstation field, select the location of your server.
- 4 Enter the name and description of the Portal Gateway.

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

- 5 Enter the IP address of the Portal Gateway. You will need to get IP addresses from your network administrator.
- 6 Enter the port.

Figure 45 Configure New Portal Gateway screen

Tom's Test Segment	
PG200	
Virtual Portal Test	
IPV6 Portal Test	

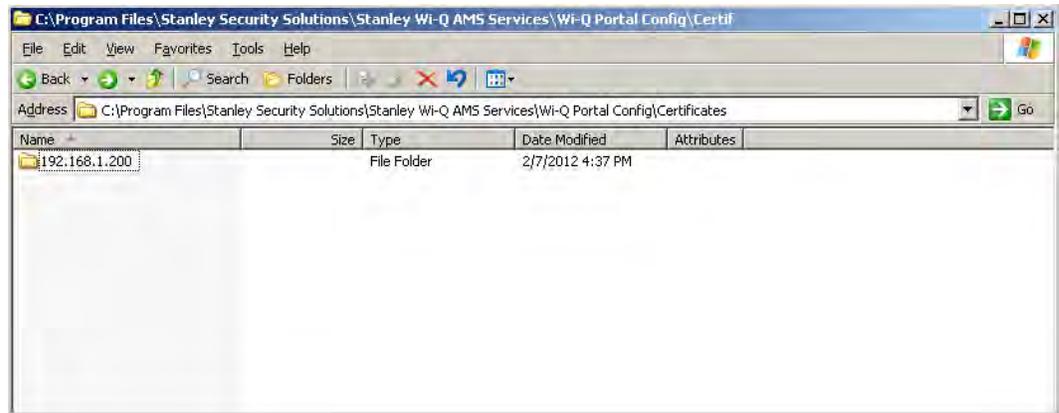
Configure New Portal Gateway	
<b>(Address)</b>	
MAC Address	Waiting for Sync
Workstation	WIN-FL6P3DQ7V15
<b>(Name)</b>	
Portal Name	IPV6 Portal Test
Description	IPV6 Portal Test
<b>(Portal Connection)</b>	
IP Address Used	2001:0db8:0000:0000:0000:ff00:0042:8329
IPv4 Address	192.168.1.201
IPv6 Address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

- 7 Click the ellipsis button next to the Channels field and select at least two channels that the Portal Gateway will use to communicate. Check with your network administrator to make sure the channels are available.

- 8 Click the ellipsis button next to the Update Interval field. Here you can set how often the system will update the Portal Gateway with changes you've made to users, readers, timezones, and other functional changes to the database.
- 9 Click the ellipsis button next to the Transactions field to select which, if any, Portal Gateway transactions you want to enable and which you want to make a 'priority.' Priority transactions will be uploaded immediately rather than waiting for the next 'update interval' that was set in the field above. Two transactions are available:
  - Portal Firmware Update
  - Portal Radio Start Failed

If you click on Select All, a dialog box window will ask you to confirm your choice and it will also ask if you would like to enable priorities as well.
- 10 If you generated SSL certificates within the Portal Configuration module, you may browse to your Portal Gateway's certificate by clicking on the ellipsis button next to the SSL Certificate field. The Certificate can be found in your Program Files at the path shown below (Figure 46). The file is located within a folder named for the Portal Gateway's IP address. Select the file with the .pfx extension, and click Open.

Figure 46 Path to Certificate File



- 11 Click Finish.

The Portal(s) you have added will now be visible in the Segment Tree. See "Viewing the Segment Tree" on page 79. You can check the operational status of your Portal(s) by clicking on the top folder within your Segment Tree.

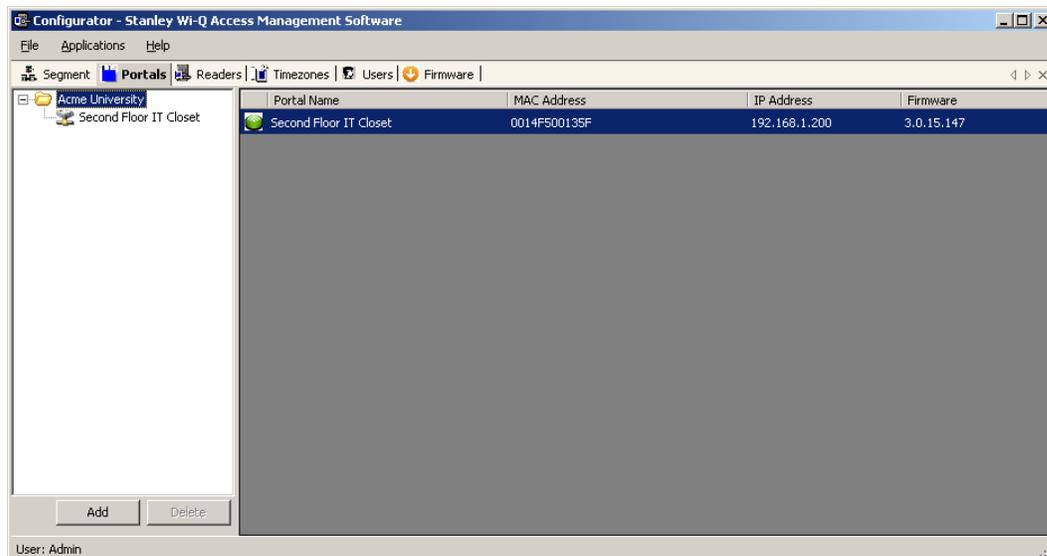
## Portal Gateway Operational Status

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

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

If your Portal Gateways have blue down arrow icons, restart your Communication Server. See “Restarting your Communication Server”. After you restart your Communication Server, your Portal Gateway status icons should change to green circles, indicating that the devices are online. See Figure 47.

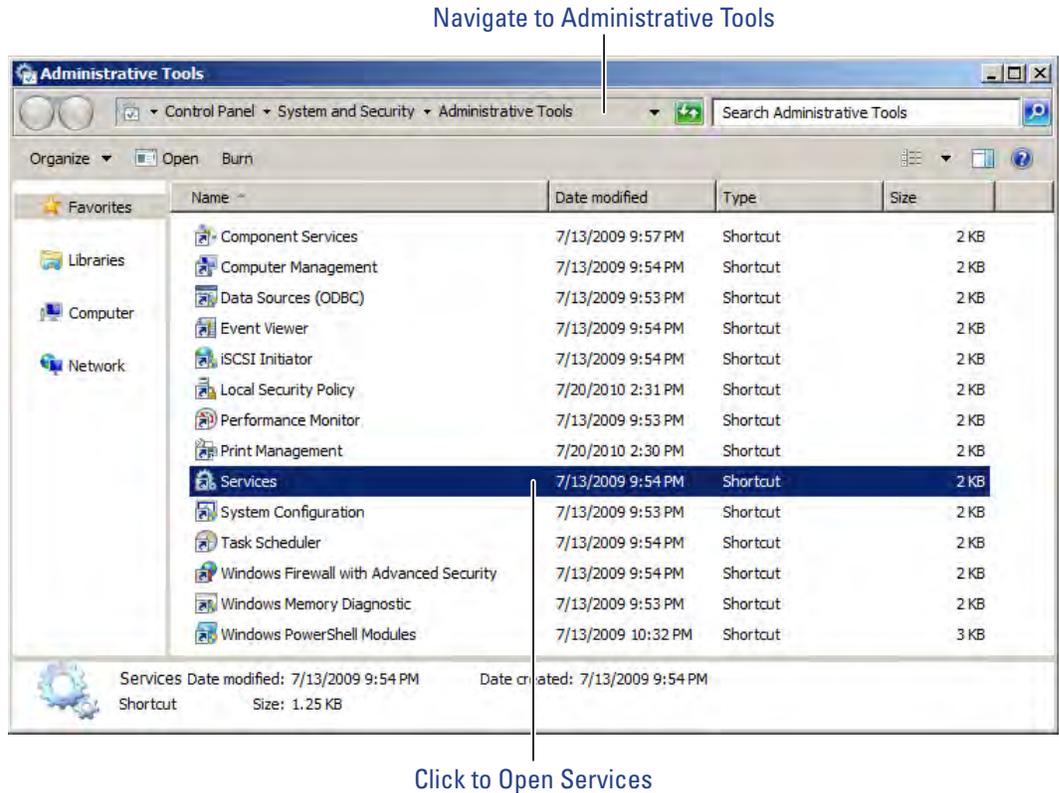
Figure 47 Portal Gateway with Green Circle Icon



## Restarting your Communication Server

If you need to restart your Communication Server, navigate to your system's Services via Administrative Tools. See Figure 48.

Figure 48 Navigate to Services



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

## Importing Portal Gateways in Bulk

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

### ***Generating an XML Bulk Import File***

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

- 1 Click on Scan to generate a list of Portals in your system.
- 2 Select all the Portals you wish to add to your AMS software.
- 3 Click on Export Portal IP Configurations (see Figure 44).
- 4 Choose a location to save your XML file, and click Save. Figure 49 shows a sample XML file.

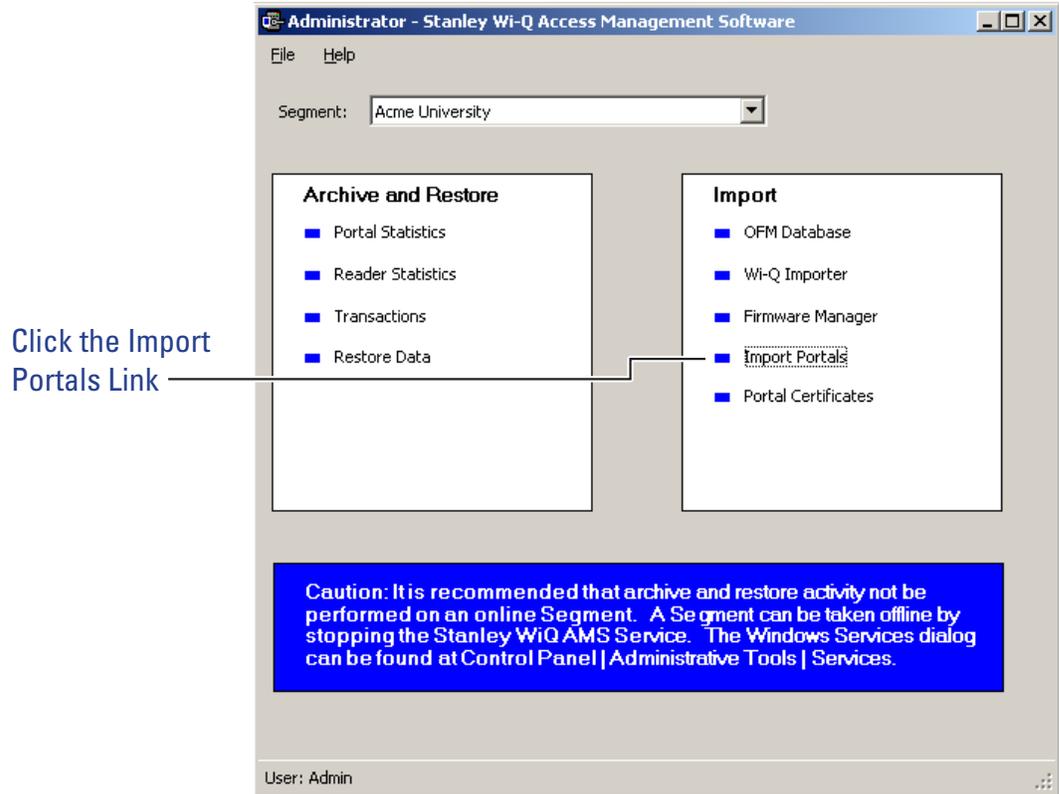
Figure 49 Sample XML file

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

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

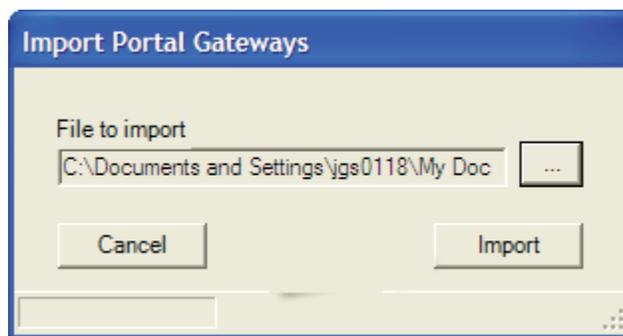
- 1 Start the System Administrator module (Applications dropdown menu inside Configurator).
- 2 Click the Import Portals link from the Import pane. See Figure 50.

Figure 50 System Administrator Portal Gateway Import



- 3 The Import Portal Gateways dialog displays.
- 4 Click the ellipsis button and locate the bulk import XML file.
- 5 Click Open.

Figure 51 Import Portal Gateways



- 6 Click Import.

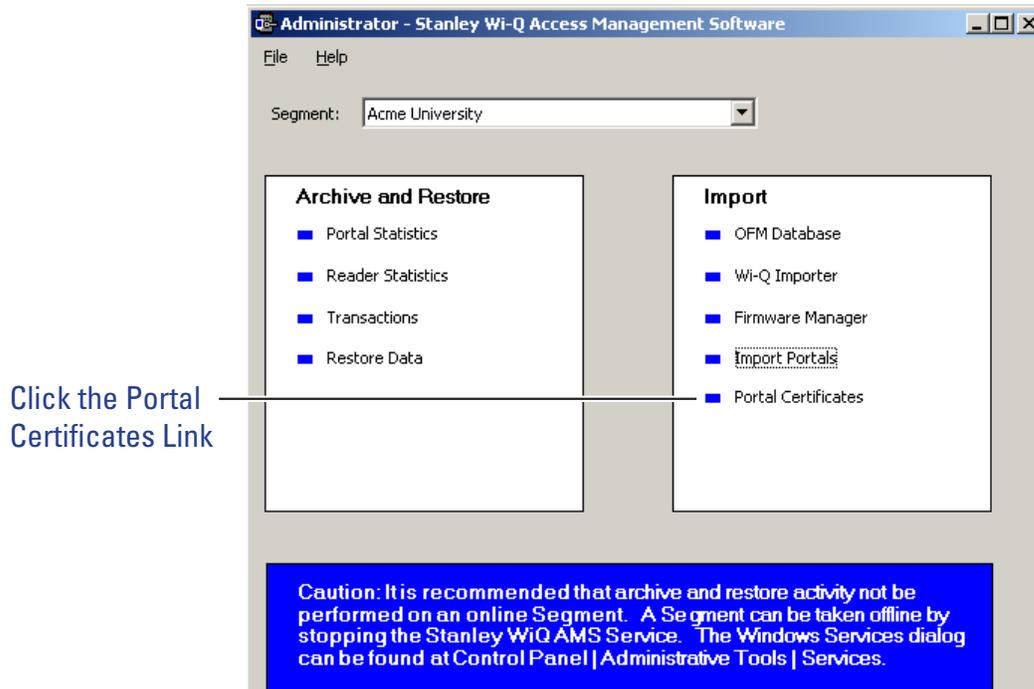
**Note** The Portals are imported (or updated) and a results box details the import. The MAC addresses should automatically show up in Portal Gateways' properties.

## Importing Portal SSL Certificates

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

- 1 From the System Administrator application, click the 'Portal Certificates' link under the Import pane. See Figure 52.

Figure 52 System Administrator Portal Certificates link



- 2 Choose the Portal Gateway that you want to import an SSL certificate to and click the ellipsis button next to it. Then find the certificate file (see Figure 46) and click Open.
- 3 When finished with importing all the Portal Gateway SSL certificates, click Finish.

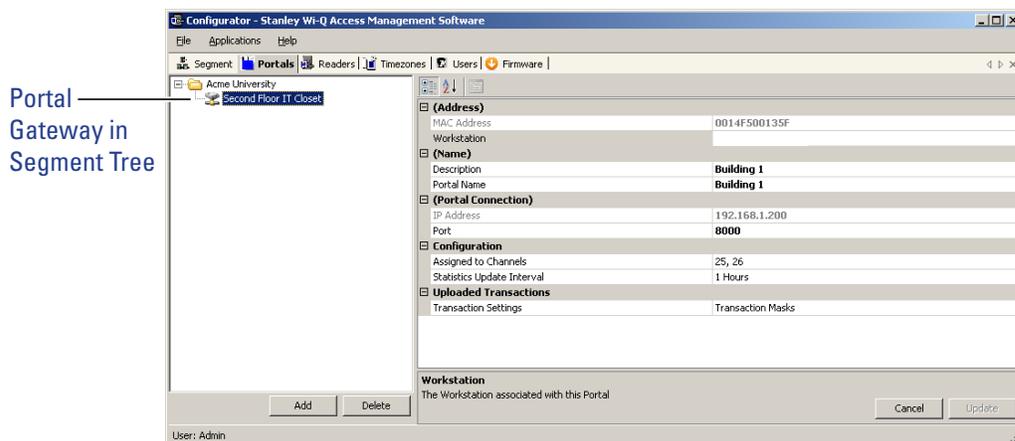
The Portals you have added will now be visible in the Segment Tree. See "Viewing the Segment Tree". You may now check the operational status of your Portal Gateways. See "Portal Gateway Operational Status" on page 74.

## Viewing the Segment Tree

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

Figure 53 shows an example Portal Gateway in the Segment Tree.

Figure 53 Portal Gateway visible in Segment Tree



### To view the Segment Tree

- 1 In the Segment tab, select the segment you wish to work with.
- 2 Click on the Portals tab. The Segment Tree pane displays on the left, and a list of all prepared devices displays on the right. The first item in the Segment Tree is the folder for the selected segment, in this case, Acme University.

The Segment Tree is also viewable from within the Readers tab. See “Adding Controllers to the Segment Tree” on page 89.

### Organizing your Segment Tree

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

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

the system, you can easily locate the Controllers to be assigned. Once you create Segment folders of your own, you can move your Portals to the appropriate folders.

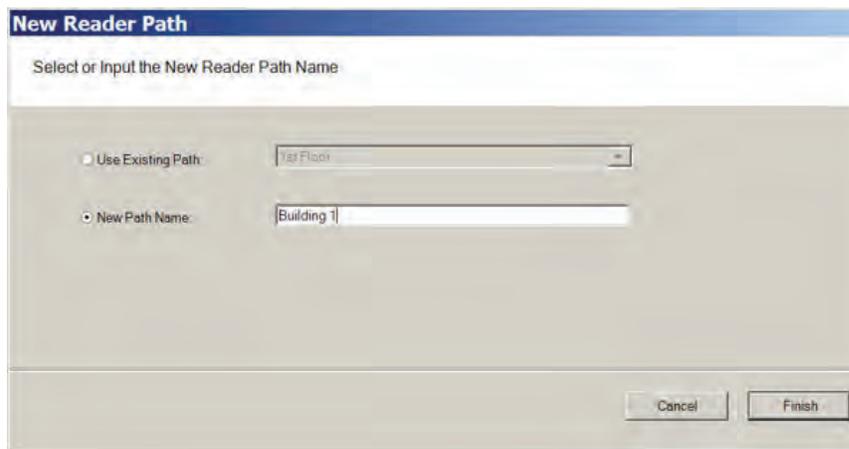
**Note** To delete a folder, you must already have moved any devices in that folder to a different location.

### To create a new segment item folder

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

Figure 54 Defining a New Reader Path

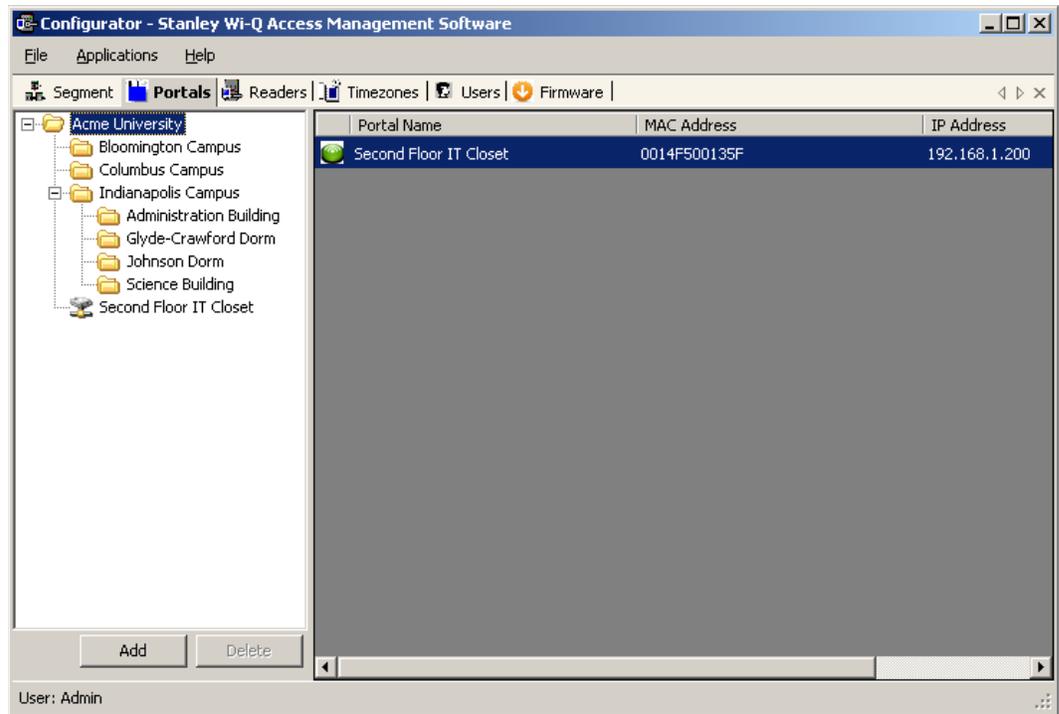
Select New Path Name and enter a name



The screenshot shows a dialog box titled "New Reader Path". Below the title bar, it says "Select or Input the New Reader Path Name". There are two radio button options. The first is "Use Existing Path" which is unselected; next to it is a dropdown menu currently showing "1st Floor". The second option is "New Path Name" which is selected; next to it is a text input field containing "Building 1". At the bottom right of the dialog, there are two buttons: "Cancel" and "Finish".

- 2 Select New Path Name and enter the name.
- 3 Select Finish. The new path folder is added to the Segment Tree. Repeat the process to create the folders needed to define your Segment Tree. Figure 55 shows a Segment Tree with several added folders and sub-folders.

Figure 55 Folders and Sub-Folders in the Segment Tree



### Moving Portal Gateways within the Segment Tree

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

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

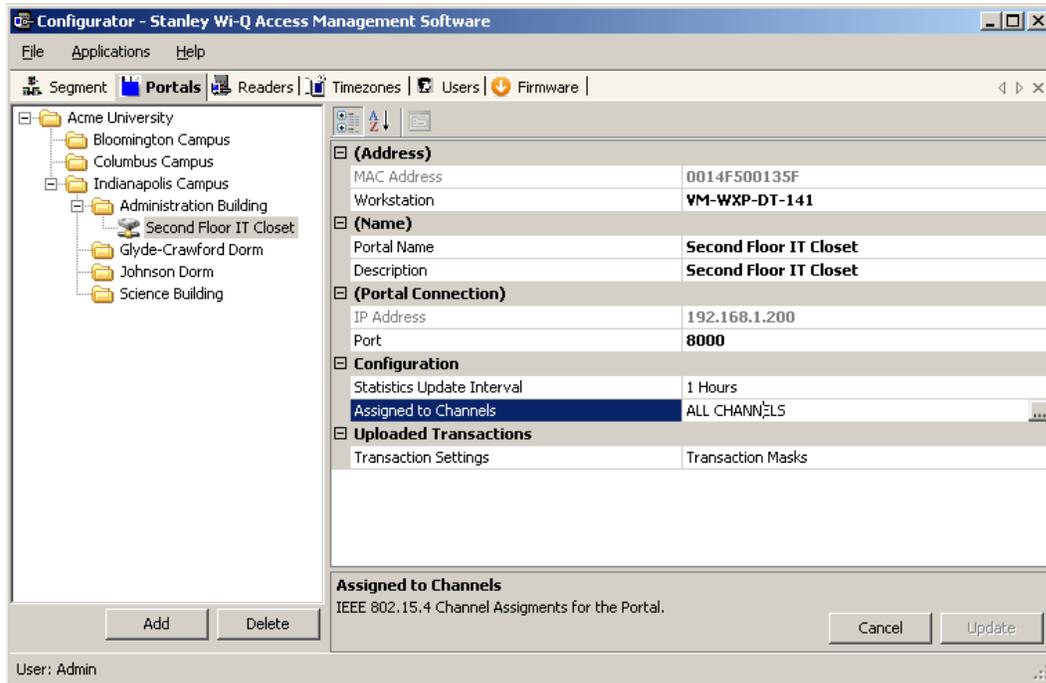
## Assign Portal Channels

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

### To assign Portal channels

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

Figure 56 Portal Properties



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

Figure 57 Portal Channel Selection

The screenshot shows a dialog box titled "IEEE 802.15.4 Channel Selection for Second Floor IT Closet". The main instruction is "Select the channels to be used." Below this, there is a grid of 16 checkboxes arranged in four rows and four columns. The channels are: 11, 12, 13, 14, 15 (Secondary), 16, 17, 18, 19, 20 (Secondary), 21, 22, 23, 24, 25 (Primary), and 26 (Primary). Channels 25 and 26 are checked. Below the grid are two blue links: "Clear All" and "Select All". At the bottom right, there are two buttons: "Cancel" and "Finish".

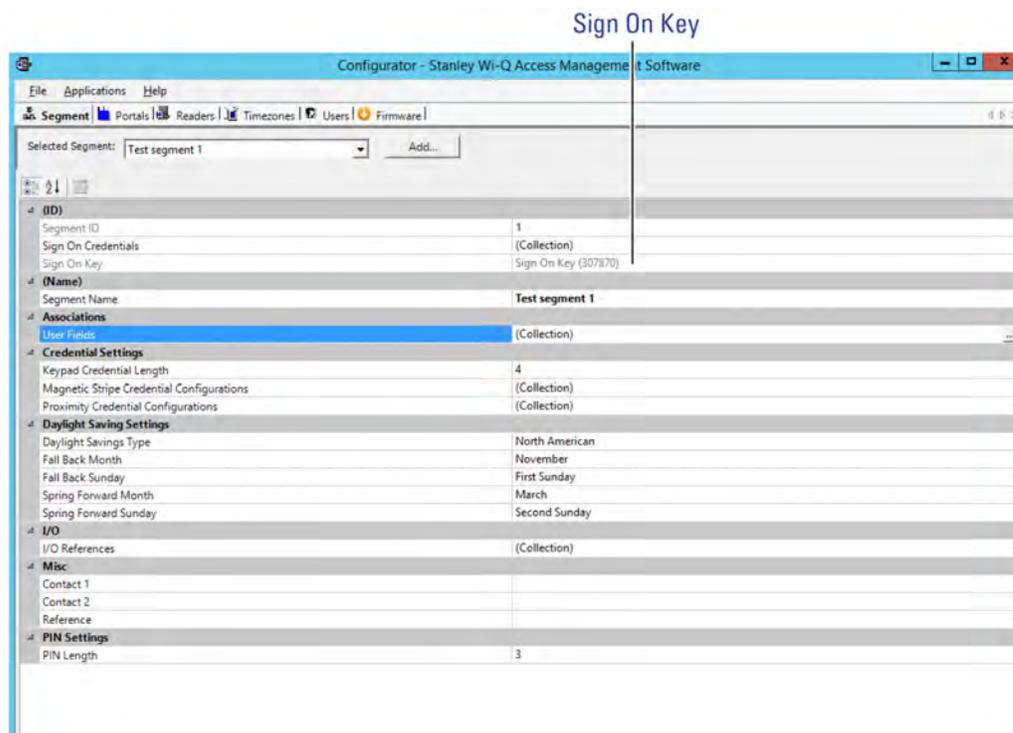
Channel	Selection
11	<input type="checkbox"/>
12	<input type="checkbox"/>
13	<input type="checkbox"/>
14	<input type="checkbox"/>
15 (Secondary)	<input type="checkbox"/>
16	<input type="checkbox"/>
17	<input type="checkbox"/>
18	<input type="checkbox"/>
19	<input type="checkbox"/>
20 (Secondary)	<input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

- 3 Enable or disable channels as needed (at least one channel must be selected).
- 4 Click Finish to save your settings.

## Sign on and Configure Controllers (Task 10)

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

Figure 58 Signing on readers from the Segment tab



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

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

## Signing on Keypad Controllers

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

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

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

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

## Signing on Card Readers

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



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

Figure 61 MAG Card Settings

Segment (Acme University) Magnetic Stripe Card Credential Number Setting

Specify the Credential Number

Credential Number 6262

Select Scan Device

MSR 206

Card Reader

Reader

Scan Cancel Finish

- 5 You can enter the card's 16-digit credential number manually; or, you can scan the card at a local scanning wedge, or select a reader where the card will be scanned.  
  
To Scan a card locally, select Card Reader and Select Scan. You will have about 30 seconds from the time you select Scan to actually scan the card through a reader.  
  
To Scan at a reader, select Reader and select the reader from the drop-down list to scan at from the drop-down list, then select Scan. You will have about 30 seconds from the time you select Scan to actually scan the card through a reader (this option is available only if the reader has been signed on).
- 6 Select Finish to save your settings and return to the Segment Credentials Setup dialog box, or Cancel if you decide not to create the number. The number appears in the Credential Number category and the card is now registered. If you will use a Prox card, see the following additional steps to complete registration.

### **Completing the Credential for a Prox card**

- 1 Under the Proximity Card category, Enforce Expiration Date, select True or False, depending on your preference. If you select true, you will need to register a new card when the expiration date occurs. If False, the card will not expire.
- 2 Under Proximity Card Type, select the type of encryption the card uses from the dropdown menu.
- 3 Select Finish. Once this is done, you can use this card to sign on card readers.

### **To sign on card readers**

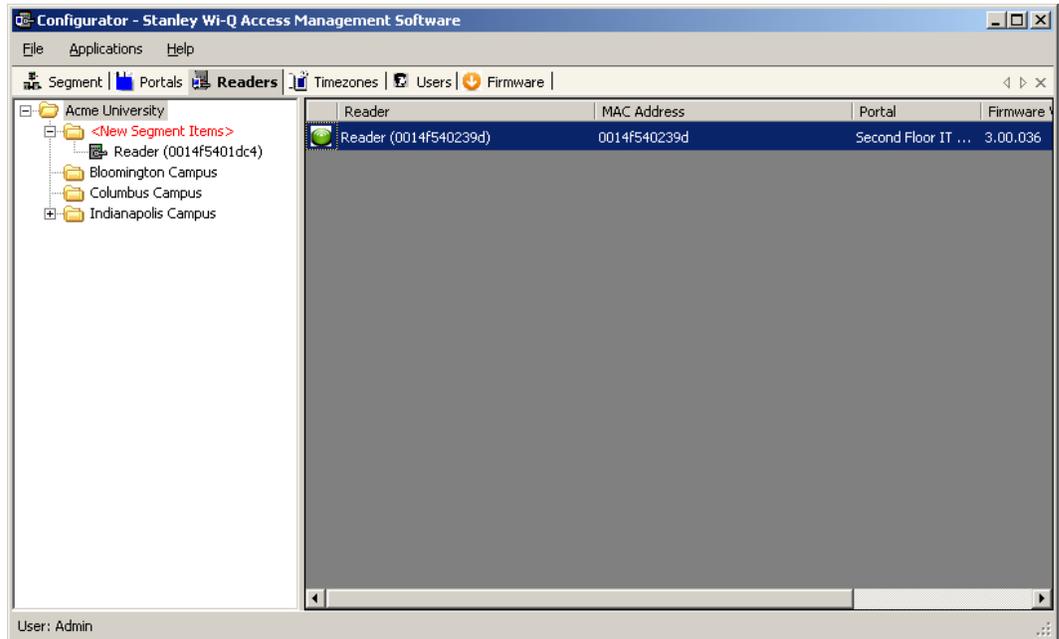
- 1 At each card reader, scan the card you registered with the segment credential.
- 2 Once this is done, the readers will appear in the <New Segment Items> folder, viewable in the Readers tab Segment Tree.

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

## Adding Controllers to the Segment Tree

Within 10 to 15 seconds after you sign on a controller, it will appear in the Configurator <New Segment Items> folder, viewable in the Readers tab. The folder will appear in red to indicate that it has received new Controllers. See Figure 62.

Figure 62 <New Segment Items>



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

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

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

## Copying Reader Parameters

The Copy Reader Parameters feature is useful when you have more than one reader that serves the same users and user groups or will be assigned a special Timezone Group. This feature is available when you first bring a Controller from the <New Segment Items> folder to the Segment Tree, and as a right-mouse-click copy function. It makes sense then that if you are going to use this feature you will want to configure the Users and User Groups before configuring the readers. See “User Groups” on page 103 and “Adding Users to the Segment” on page 121 for steps to create these parameters.

## Configuring New Controllers

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

### To configure a new Controller

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

If you have signed on more than one Controller into your segment, a window will open to ask if you would like to copy a configuration from another reader or create a new configuration. See Figure 63.

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

Figure 63 New Reader Configuration

**New Reader Configuration**

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

Copy Configuration from: Reader (0014f540239d)  Include Users and Groups

New Reader Configuration

OK

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

## Field Category Definitions

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

### Reader Name

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

### Associations

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

### Configuration

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

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

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

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

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

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

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

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

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

**Wiegand Device** — Define if applicable.

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

**Card Formats Assignments** — Assign card formats to the reader.

### ***Assigning Reader Channels***

Perform the following steps to assign reader channels.

- 1 In the Reader tab, select the desired reader within the Segment Tree.
- 2 In the Reader Properties sheet, under the Configuration category, click in the Assigned to Channels field. The ellipsis button appears at the far right of the field.
- 3 Click the ellipsis button to display the Channel Selection for the Reader.

Figure 64 Reader Channel Selection

**IEEE 802.15.4 Channel Selection for Reader (0014f5000121)**

Select the channels to be used.

<input checked="" type="checkbox"/> 11	<input checked="" type="checkbox"/> 15 (Secondary)	<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 (Secondary)	<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)

[Clear All](#) [Select All](#)

Cancel Finish

4 Select your desired channels.

5 Click Finish to save your settings.

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

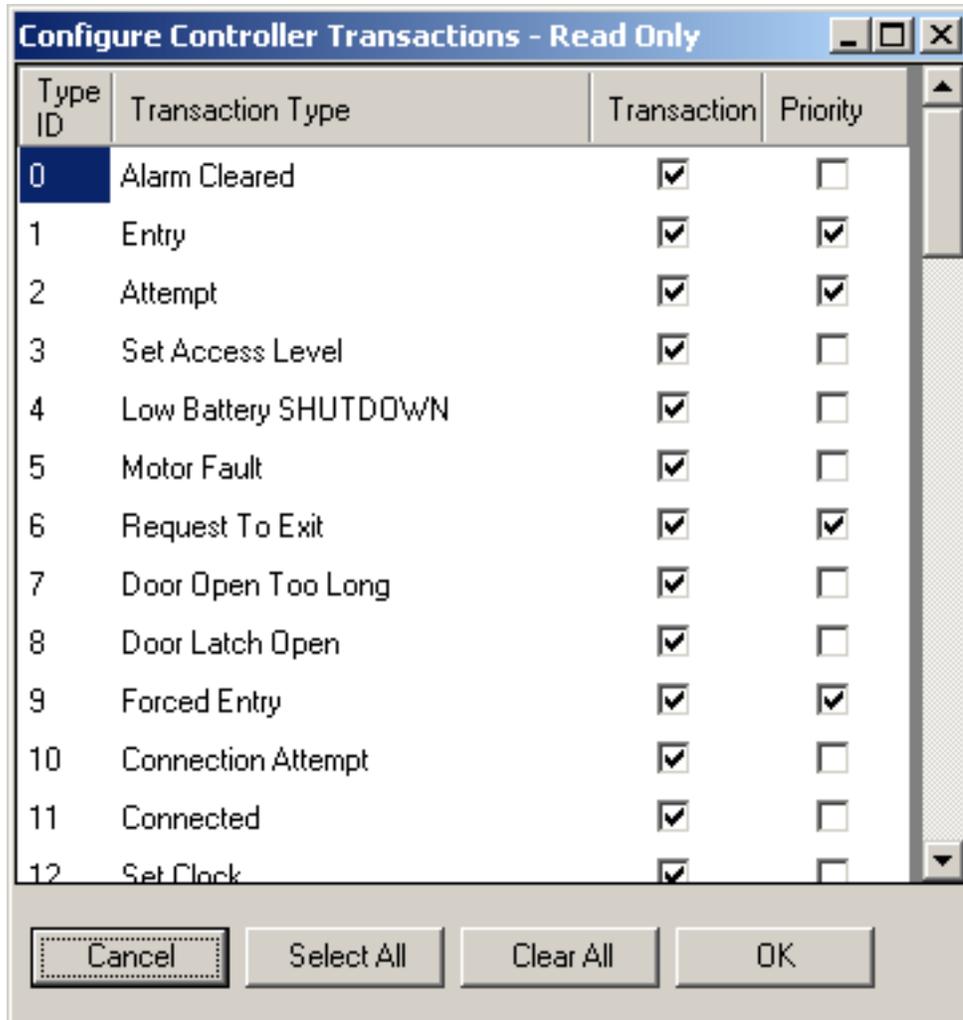
### Reader Control

The Reader Control dropdown list corresponds to settings configured under the Reader Control sub tab in the Timezones tab. See "Configuring Timezones" on page 137 for more information.

## Uploaded Transactions

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

Figure 65 Configure Controller Transactions



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



## 5 Configure AMS Software (Task 11)

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

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

### Associations

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

### User Fields

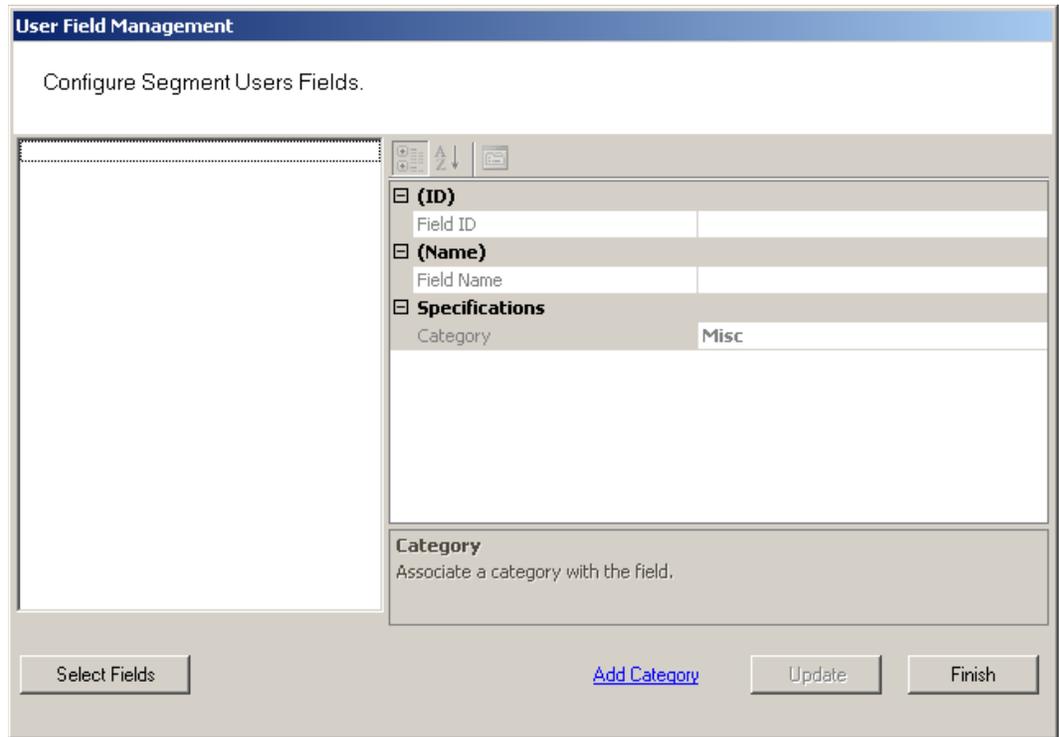
Wi-Q AMS supplies you with a set of common User Fields which are available in the User Tab when you start adding users. You are also supplied with a set of additional User Fields and Categories that you can add to the system if needed. If you do not find the fields and categories you need to fully define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

### Adding Additional User Fields

- 1 In the Segment tab, click on User Fields and select the ellipsis button at the far

right of the field. The User Field Management dialog box opens.

Figure 66 User Field Management



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

Figure 67 Select Segment User Fields

**User Field Management**

Select Segment User Fields.

Field Name
------------

Add <<

Remove >>

Field Name
<input checked="" type="checkbox"/> Telephone Number
<input type="checkbox"/> Company Name
<input type="checkbox"/> Title
<input type="checkbox"/> Address
<input type="checkbox"/> City
<input type="checkbox"/> State
<input type="checkbox"/> Postal Code
<input type="checkbox"/> Country
<input type="checkbox"/> Contact 1
<input type="checkbox"/> Contact 2
<input type="checkbox"/> Reference

Clear All    Select All

Clear All    Select All

Add Field    Finish

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

Figure 68 User Fields in Facility

**User Field Management**

Select Segment User Fields.

Field Name
<input checked="" type="checkbox"/> Telephone Number

Add <<

Remove >>

Field Name
<input checked="" type="checkbox"/> Company Name
<input type="checkbox"/> Title
<input type="checkbox"/> Address
<input type="checkbox"/> City
<input type="checkbox"/> State
<input type="checkbox"/> Postal Code
<input type="checkbox"/> Country
<input type="checkbox"/> Contact 1
<input type="checkbox"/> Contact 2
<input type="checkbox"/> Reference

Clear All    Select All

Clear All    Select All

Add Field    Finish

- 4 Select Finish. Once you add the field to a Segment, it will appear on the Users

Tab in the Configurator module. See the next few sections for steps to complete this process.

## Creating New User Fields

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

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

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

Figure 69 Add, Remove and Configure System User Fields

**User Field Management**

Add, Remove, and Configure System User Fields.

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

**(ID)**  
Field ID: 26

**(Name)**  
Field Name: **Alternate Phone Contact**

**Specifications**  
Category: **Statistics**

**Field Name**  
The Field's Name.

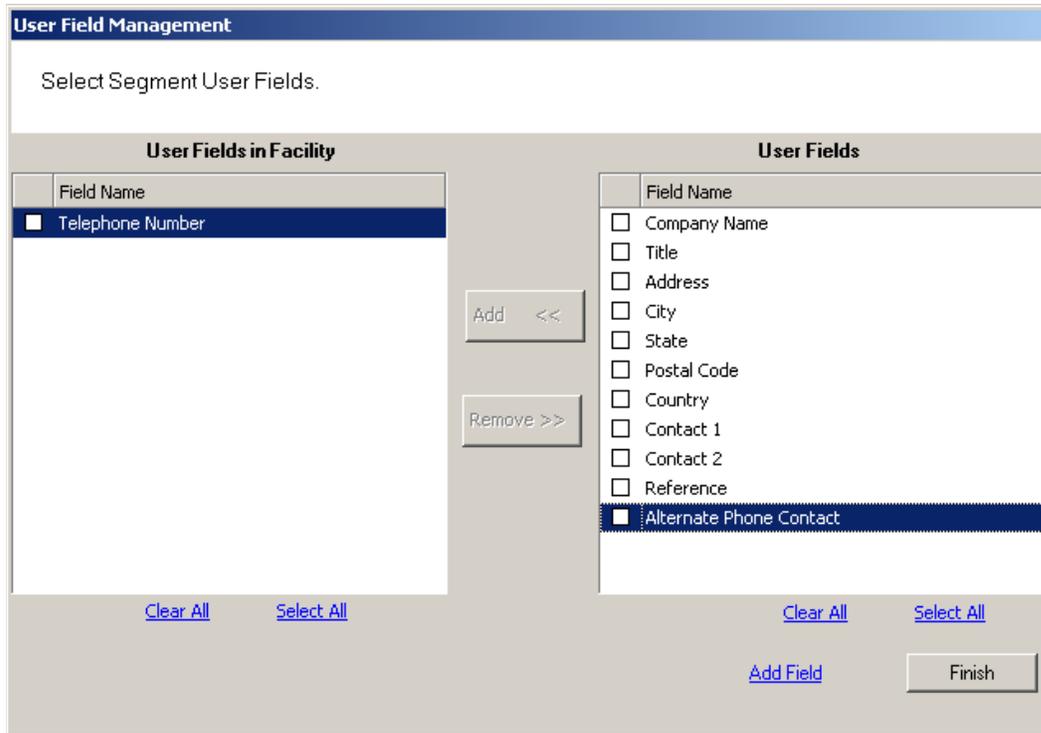
Buttons: Add, Remove, [Add Category](#), Update, Finish

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

**Note** If the category you want is not available, you can also create your own category. See “Adding a New User Fields Category” on page 101.

- 3 In the Field Name category on the right, type in a new name for the new field. In the example, we used Alternate Phone Contact.
- 4 Select Update. When you click Finish, the Select Segment User Fields dialog box shows that your new field is now available for selection.

Figure 70 User Field added to list

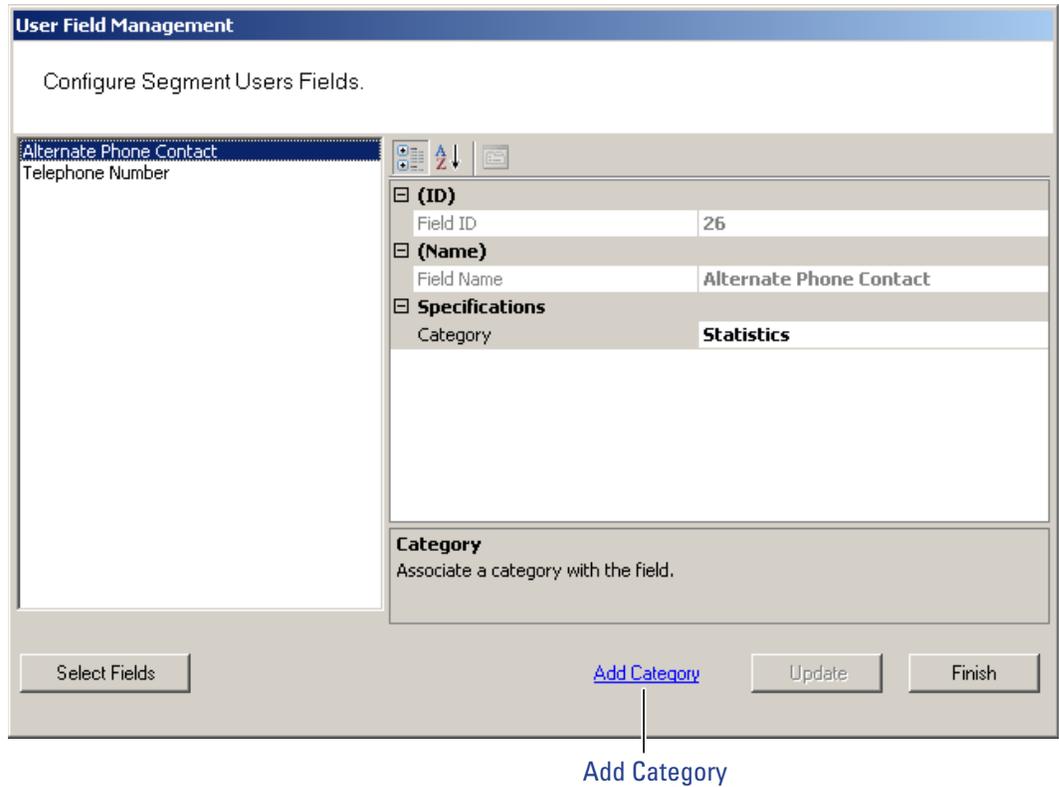


- 5 Select the Checkbox next to the field and click <<Add. The field is transferred to the User Fields in Segment box on the left.
- 6 Select Finish. The new field is now added to the User Field Management dialog box.

## Adding a New User Fields Category

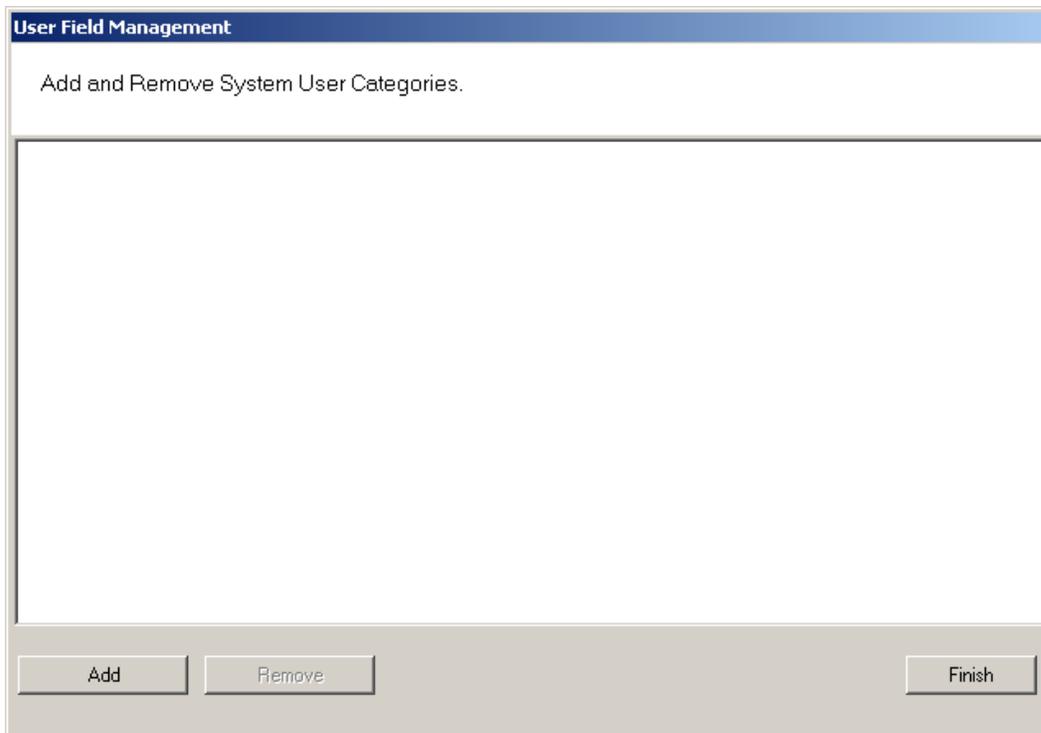
- 1 In the User Field Management of Segment dialog box, click the Add Category Link at the bottom of the dialog box.

Figure 71 Add Category



- 2 The Add and Remove System User Categories window opens.

Figure 72 Adding and Remove System User Categories



- 3 Click the Add button. "Category 1" appears in the text box.
- 4 Double-click on "Category 1" to rename it.
- 5 Click Finish. In the Configure Segment Users Fields dialog box, the new category is now available for selection from the Category drop-down list. Now you can select this category when defining a new User Field.

## Removing User Fields and Categories

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

### *To remove User Fields from the system*

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

### *To remove added Categories from the system*

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

## User Groups

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

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

## Adding User Groups

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

Figure 73 User Groups Setup

**User Groups Setup**  
Add, Delete, and Modify User Groups

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

**Autocode Enabled**  
Enable or Disable User Group Autocoding.

Add Delete Update OK

- 2 The groups you create display on the left. The group's ID, Name, Associations and Timezone appear on the right.
- 3 Select Add. A new Group (Group1) is created and displays on the left.
- 4 In the Group Name box, replace the name Group1 with a name for the new group (for example, Administrative).
- 5 Select OK.

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

### Removing User Groups

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

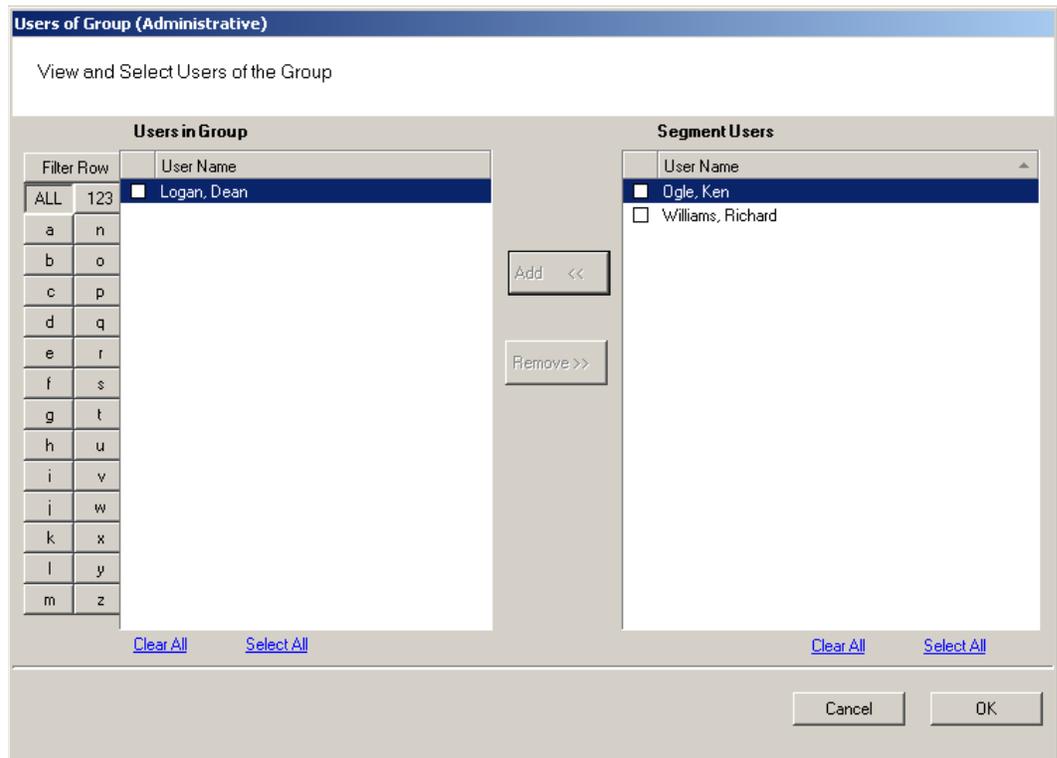
### Associating Users with User Groups

- 1 In the Segment Tab, Associations category, click the User Groups field.
- 2 Select the ellipsis button at the far right of the field.
- 3 In the User Groups Setup dialog box, select the group you wish to associate

with users.

- 4 In the Associations category, click in the Users field and select the ellipsis button. The Users of Group dialog box opens.
- 5 All users in the segment not already assigned to the group are displayed under Segment Users list on the right.

Figure 74 Users of Group



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

- 6 Select the checkbox next to the users you wish to associate with the User Group.
- 7 Select <<Add. The User names will be removed from the Segment Users list on the right and display under Users in Group list on the left.
- 8 Select OK to close the Users of Group dialog box.

### **Removing Users from User Group**

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

### **Timezone User Groups**

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

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

Figure 75 Creating a Timezone User Group

The screenshot shows the 'User Groups Setup' dialog box with the following configuration:

User Groups Setup																															
Add, Delete, and Modify User Groups																															
<ul style="list-style-type: none"><li>Administrative</li><li>Maintenance</li><li><b>Residential</b></li><li>Student</li></ul>	<table border="1"><tr><td colspan="2"><b>(ID)</b></td></tr><tr><td>Group ID</td><td>4</td></tr><tr><td colspan="2"><b>(Name)</b></td></tr><tr><td>Description</td><td><b>Housekeeping Timezone</b></td></tr><tr><td>Group Name</td><td><b>Residential</b></td></tr><tr><td colspan="2"><b>Associations</b></td></tr><tr><td>Interval Collections</td><td>(Collection)</td></tr><tr><td>Readers</td><td>(Collection)</td></tr><tr><td>Users</td><td>(Collection)</td></tr><tr><td colspan="2"><b>Timezone</b></td></tr><tr><td>Autocode Enabled</td><td>False</td></tr><tr><td><b>Is Timezone Group</b></td><td><b>True</b></td></tr><tr><td>PIN Effective Date</td><td>True</td></tr><tr><td>Recode Interval</td><td>False</td></tr><tr><td>Timezone Group ID</td><td>1</td></tr></table>	<b>(ID)</b>		Group ID	4	<b>(Name)</b>		Description	<b>Housekeeping Timezone</b>	Group Name	<b>Residential</b>	<b>Associations</b>		Interval Collections	(Collection)	Readers	(Collection)	Users	(Collection)	<b>Timezone</b>		Autocode Enabled	False	<b>Is Timezone Group</b>	<b>True</b>	PIN Effective Date	True	Recode Interval	False	Timezone Group ID	1
<b>(ID)</b>																															
Group ID	4																														
<b>(Name)</b>																															
Description	<b>Housekeeping Timezone</b>																														
Group Name	<b>Residential</b>																														
<b>Associations</b>																															
Interval Collections	(Collection)																														
Readers	(Collection)																														
Users	(Collection)																														
<b>Timezone</b>																															
Autocode Enabled	False																														
<b>Is Timezone Group</b>	<b>True</b>																														
PIN Effective Date	True																														
Recode Interval	False																														
Timezone Group ID	1																														

**Is Timezone Group**  
Indicates whether this is a timezone group.

Buttons: Add, Delete, Update, OK

- 3 Select Add. Group1 is created.
- 4 In the Name Category, Description, enter a description for the group, for example: Housekeeping Timezone.
- 5 In the Group Name, replace Group1 with the name of your new user group, for example, Residential.
- 6 Under Timezone, change the Is Timezone Group default setting from False to True. Select Update to continue creating groups.
- 7 Select OK to save the new Timezone group.

Once you have created a Timezone group, you will need to set up access times to apply to that group. For more information about Timezones and Timezone User Groups, see "Configuring Timezones" on page 137.

## Credential Settings

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

### Keypad Credential Length

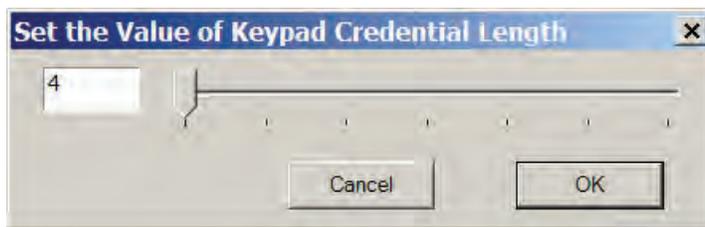
If your access system will have or currently has cards encoded with keypad credentials, you may set the number of digits required here.

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

Perform the following steps to set the Keypad Credential Length.

- 1 In the Segment Tab, under the Credential Settings category, click in the Keypad Credential Length field.
- 2 Click the ellipsis button at the far right of the field. The Set value of Keypad Credential Length dialog box opens.

Figure 76 Setting the Credential Length



- 3 Enter the length or slide the bar to select the position of the Keypad Credential length you will use on segment cards.
- 4 Select OK to save your settings and exit the box.

### Magnetic Stripe Credential Configurations

Before Magnetic cards can be used in the system, you must configure AMS to accept the card types and settings. Figure 77 shows the Magnetic Stripe Credential Configurations Window. Default settings will be sufficient for most systems.

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

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

Figure 77 Magnetic Stripe Credential Configurations

Magnetic Stripe Credential Configurations

Add, Delete, and Modify Magnetic Stripe Credential Configurations

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

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

Add Delete [Card Track Information: Track 2](#) Cancel OK

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

## **Credential Settings**

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

- 1 In the Magnetic Stripe Credential Configurations window, click the Card Track Information link at the bottom of the window.
- 2 The Define Magnetic Stripe Card Track Information window opens. Specify the desired track from the dropdown menu. Then click Finish.
- 3 Click OK to exit the Magnetic Stripe Credential Configurations window.
- 4 In the Segment tab, click Update at the bottom right to update your segment.

### ***Card Track Limits***

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

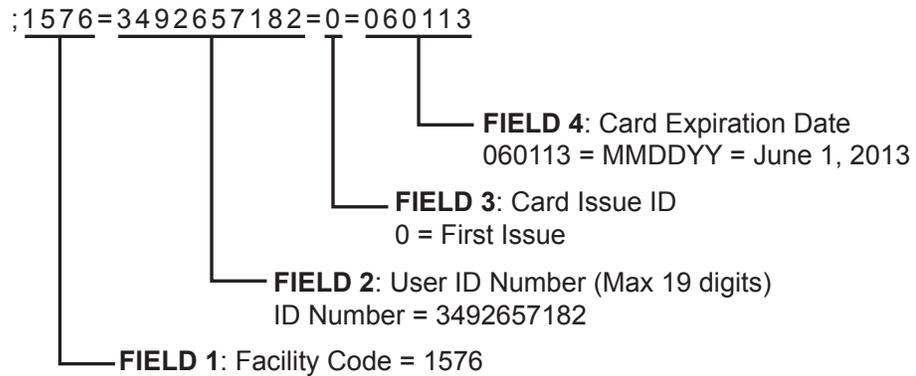
### **Character codes and counts**

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

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

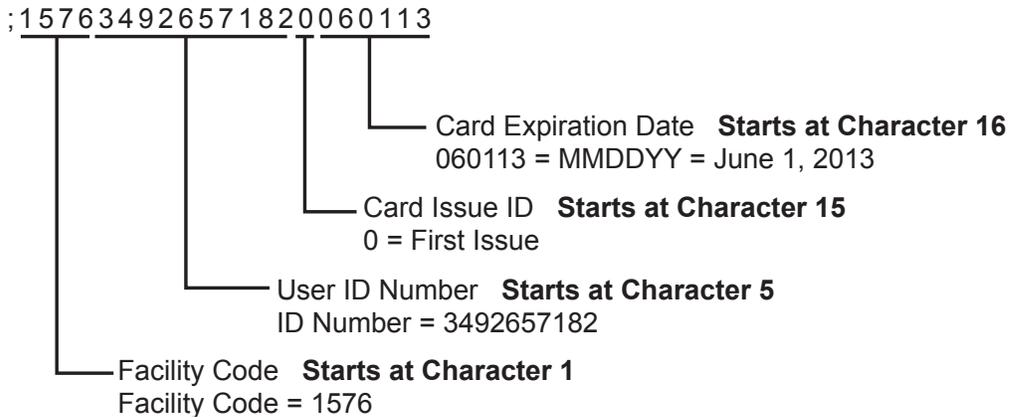
Following is an example of encoded data using field separators on Track 2.

Figure 78 Data Fields



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

Figure 79 Character count fields



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

## Expiration Date Settings

Perform the following steps to define a card expiration date.

- 1 In the Magnetic Stripe Credential Configurations window, under the Expiration Date Settings category, click in the Expiration Date Position Type field.
- 2 Select either Character or Field from the drop-down list. The Expiration Date Format, Position and Valid list boxes activate.
- 3 In the field next to Expiration Date Format, select the date format you need from the drop down list (MMDDYY, etc.).
- 4 In the field next to Expiration Date Position, enter the value to represent either the field position or the character number where the expiration date appears on the card stripe.
- 5 In the field next to Expiration Date Valid, select either To or Thru Expiration date.
- 6 Select OK to save your settings and exit the box.

**Note** If you use the character code format and select the six-digit expiration date format, the value of your next setting (Facility Code Settings) must start with character position 7. If you enter an incorrect value, the system will report an error message. Review the “Character codes and counts” on page 111 if you need clarification.

## Facility Code Settings

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

- 1 Under the Facility Code Settings category, click in the Facility Code Position Type field.
- 2 Select either Character or Field from the drop-down list. The Facility Code fields below activate.
- 3 In the field next to Facility Code, enter your Facility Code number.
- 4 In the field next to the Facility Code Length, enter the length.
- 5 In the field next to Facility Code Position, enter the facility code position.
- 6 Select OK to save your settings and exit the box.

## **Issue Number Settings**

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

Perform the following steps to define an issue number position.

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

## **User ID Settings**

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

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



ID Settings.

- 4 Under the User ID Settings category, change the User ID Length to the number of bits used for User IDs on your card. Set the User ID Position.
- 5 When finished, click OK.

## Daylight Saving Settings

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

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

## I/O

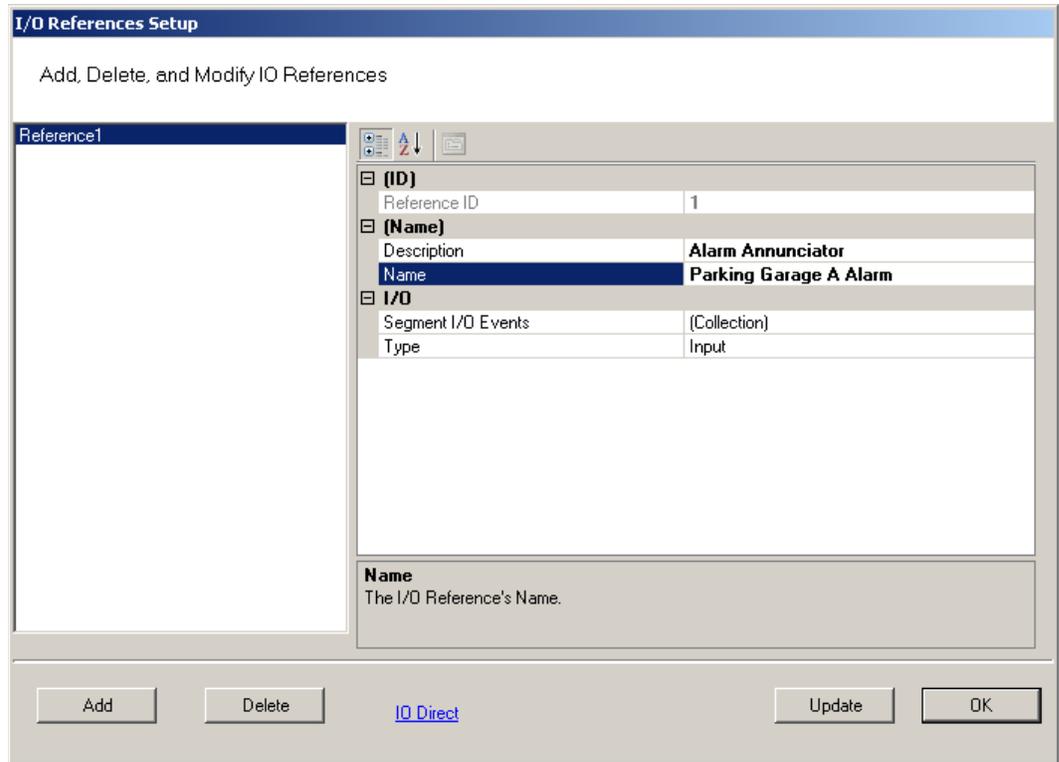
If you are using input/output devices in your system, they are recognized and defined similar to a Controller.

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

### Adding and Modifying I/O References

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

Figure 81 I/O References Setup



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

- 2 Click Add.
- 3 Under Description, replace the default description "Reference1" with a description that will have meaning for your segment, such as Alarm Annunciator.
- 4 Under Name, replace the default name "Reference1" with a name that will have meaning for your segment, such as Parking Garage A Alarm.
- 5 Under the I/O category, click the Segment I/O Events field and select the ellipsis button at the far right. This will open the I/O Events Setup window.

Figure 82 I/O Events Setup

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

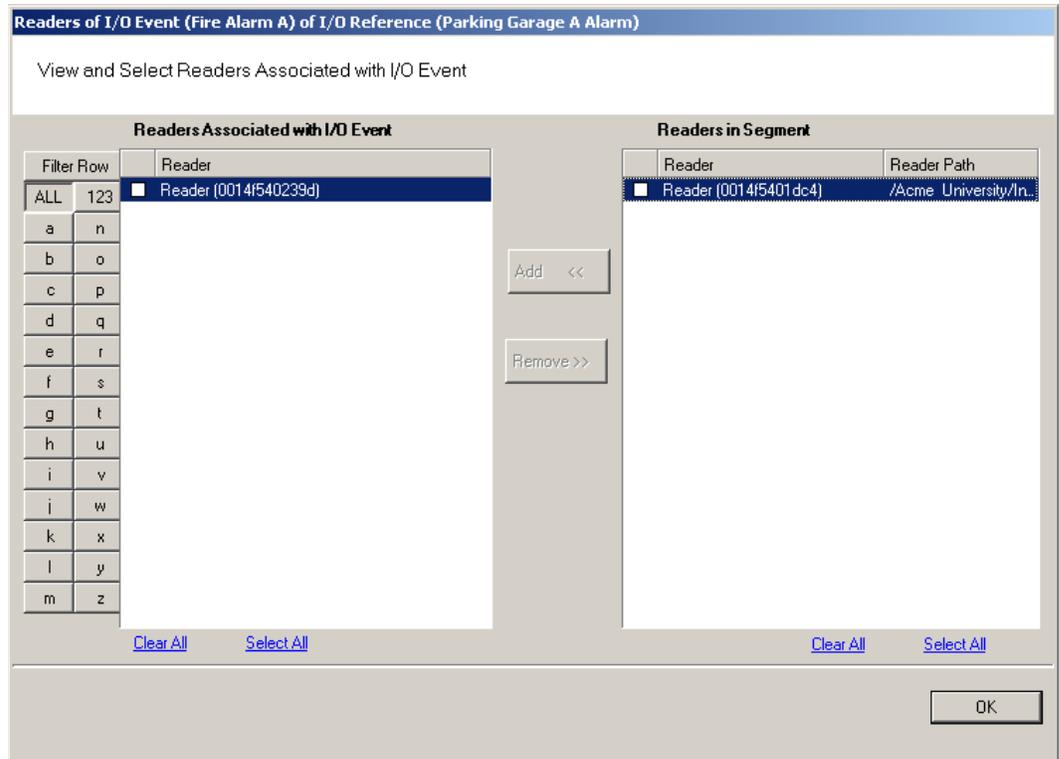
**Name**  
The IO Event's Name.

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

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

- 6 Click the Add button. The system creates an Event ID and adds it to the list in the left hand column.
- 7 Enter a name for the event, such as Fire Alarm A.
- 8 Under the Settings Category, click the Readers field and click the ellipsis button.
- 9 This will open up a new window. See Figure 83. Select a device from the Readers in Segment section that will be associated with the event.
- 10 Click Add << to add it to the list of Readers Associated with I/O Event list.

Figure 83 Associating an I/O event with a Reader



- 11 Click OK to save the association and return to the Setup dialog.
- 12 In the Reader Access level field, select either Unlock or Lockout from the drop-down list.
- 13 In the Reference Trigger State field, select either Active High or Active Low from the drop-down list (this reference will act as a toggle from one state to the other).
- 14 Under Type, select the event type from the drop-down list.
  - Restore Readers To Normal
  - Change Output Reference
  - Override Reader Access Level
  - Override Timezone User Group Access
  - Restore Output Reference To Normal.
- 15 Click Update and continue defining devices then click Finish to save your settings and exit the dialog box.

## Misc

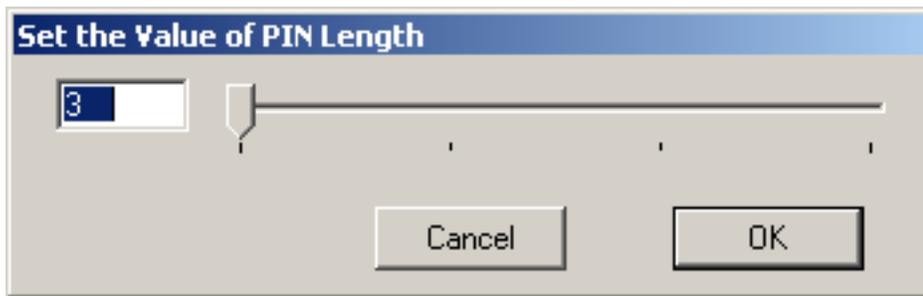
This category contains three fields (Contact 1, Contact 2, and Reference) that you can use to store any miscellaneous information you that will be helpful to you and your system. For example, you may decide to enter the phone number or email address for Stanley Technical Support in case you experience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

## PIN Settings

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

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

Figure 84 Set the Value of PIN Length



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

## Adding Users to the Segment

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

### Before You Begin

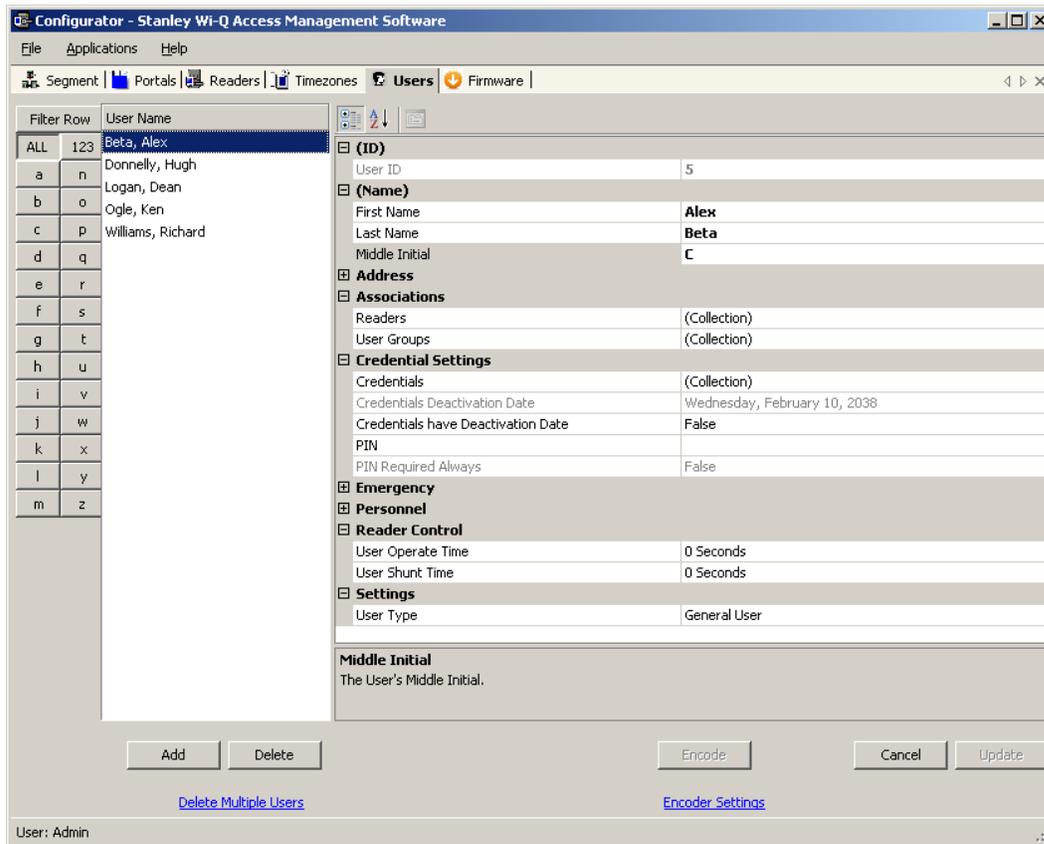
Before you begin adding users to the system for the first time, be prepared to address the following items:

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

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

# Users Tab Overview

Figure 85 Users Tab



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

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

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

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

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

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

### Adding a User Name

- 1 In the Users Tab, select the Add User button. In the ID category, the system will display a new unique User ID.
- 2 In the First Name line, highlight and replace the default text (example: User1) with a first name.
- 3 In the Last Name field, highlight and replace the default text (“\_New”) with a last name. Add a Middle Initial if needed.

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

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

**Associations** — In this category, you associate Users with Readers and User Groups. This task defines which readers will recognize the User's requests for

**Readers of User (Alex Beta)**

View and Select Readers Associated with User

Filter Row		Reader
ALL	123	
a	n	
b	o	
c	p	
d	q	
e	r	
f	s	
g	t	
h	u	
i	v	
j	w	
k	x	
l	y	

Readers in Facility

Reader	Reader Path
<input checked="" type="checkbox"/> Reader (0014f5001534)	/Security, Inc./Building...

Buttons: Add <<, Remove >>, Clear All, Select All, Finish

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

Figure 87 Selecting a reader to associate with a user

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

## User Groups

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

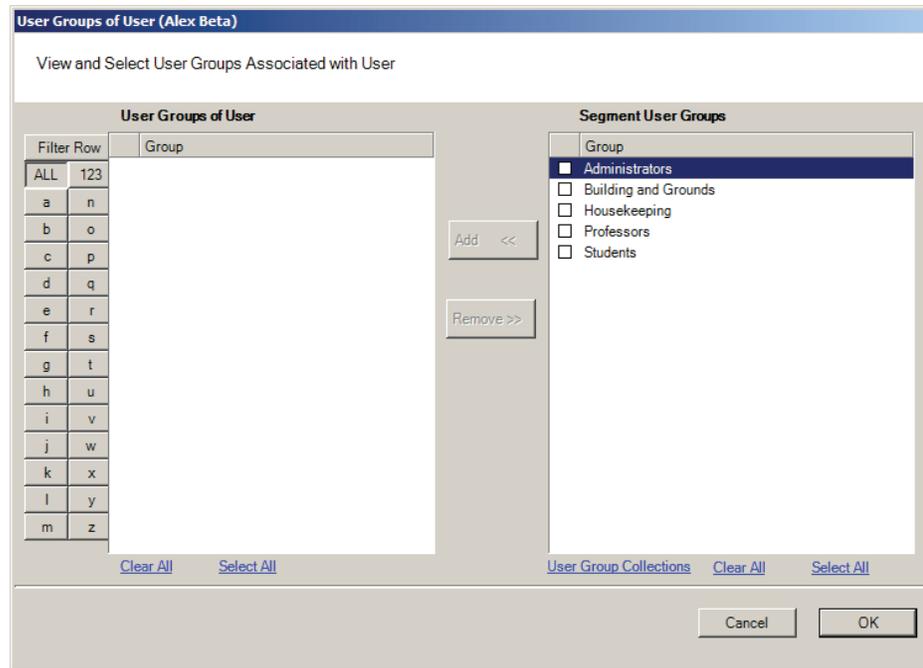
A User Group may also be defined as a Timezone Group. Timezone User Groups further define access levels for the Master Timezone. You can restrict access of certain groups of employees to a specific time period. For example, you may have a housekeeping group designated as a Timezone Group with restricted access to dormitories from 8:00 a.m. to 4:00 p.m., weekdays only. You would then assign Users from the housekeeping department to this group. Steps to add users to User Groups are presented in the following section. For more information about creating Timezone Groups, see “Timezone User Group Collections” on page 142.

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

### To add a user to a User Group

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

Figure 88 User Groups of User



- 2 Select the group(s) to associate with this user and click the Add << button. The groups are added to the User of Groups list.
- 3 Select OK to save your selections and return to the Users Tab. You can add or change User Groups for a user any time by returning to this list.

## Credential Settings

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



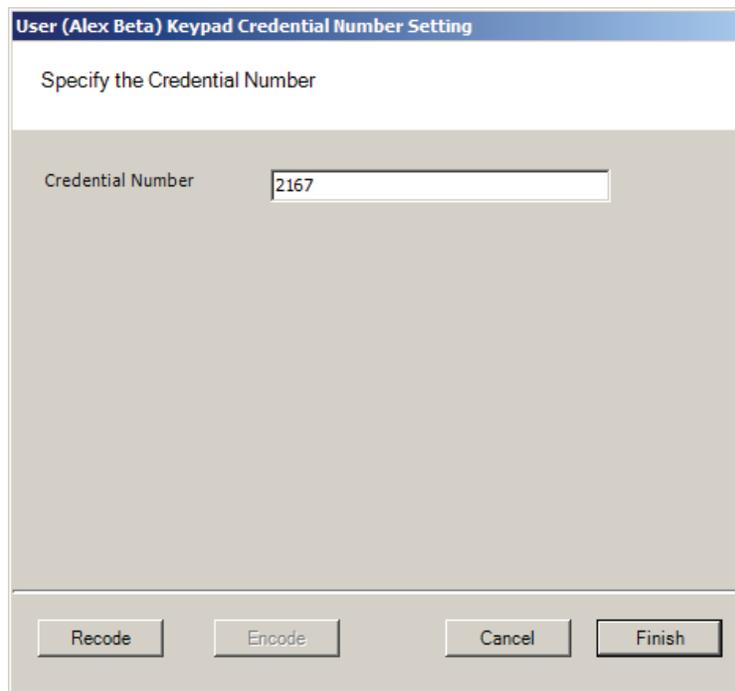
- 2 Select the type of credential the reader will use, for example, Keypad. The credential options in the categories on the right will change, depending on the type selected.

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

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

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

Figure 90 Enter a user credential number



The image shows a dialog box titled "User (Alex Beta) Keypad Credential Number Setting". The main heading inside is "Specify the Credential Number". Below this, there is a label "Credential Number" followed by a text input field containing the number "2167". At the bottom of the dialog, there are four buttons: "Recode", "Encode", "Cancel", and "Finish".

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

**Note** If the credential type you need is not in the list of card types on the left, you can add one. See "Adding a Credential Type" on page 131.

**Credentials Deactivation Date** — You can define whether a user's credentials can be automatically de-activated based on an expiration date. This is useful, for example, when entering credentials for a temporary employee or contractor. If the credential can expire, select True from the drop-down list next to the Credentials have Deactivation Date field, and then enter the de-activation date in the Creden-

tials Deactivation Date field. If the credential cannot be de-activated, select False from the drop-down list. The default deactivation date is 26 years to ensure a user's credential is not inadvertently deactivated.

## Registering the Credential

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

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

### To register a Keypad credential

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

### To register a Magnetic Stripe Card credential

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

Figure 91 Entering a Magnetic Card credential number

The screenshot shows a dialog box titled "User (Alex Beta) Magnetic Stripe Card Credential Number Setting". The main heading inside is "Specify the Credential Number". There is a text input field labeled "Credential Number" containing the value "0000000000006161". Below this is a section titled "Select Scan Device" with three radio button options: "MSR 206", "Card Reader" (which is selected), and "Reader". The "Reader" option has a dropdown menu next to it. At the bottom of the dialog box are four buttons: "Scan", "Encode", "Cancel", and "Finish".

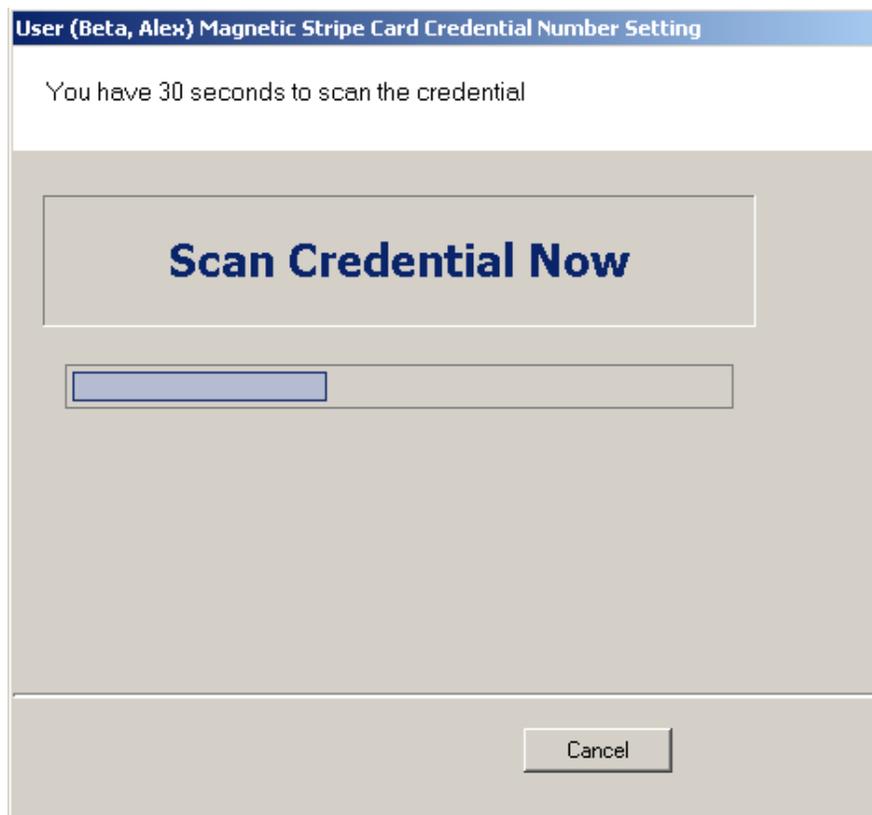
- 3 Enter a Credential Number manually (must be less than 16 characters, zeros will be appended) or select a scan device.

### ***Using a scanning device to register a credential***

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

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

Figure 92 Scan Credentials



- 2 When recognized, the number will display in the Credential Number text box.
- 3 Select Finish and return to the Credential Setup dialog box.

### **Using a local reader**

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

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

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

## Registering a Prox card credential

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

### To register a Prox Card Credential

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

Figure 93 Entering a Proximity Card credential number

The screenshot shows a dialog box titled "User (Alex Beta) Proximity Card Credential Number Setting". The main content area is titled "Specify the Credential Number". Below this title is a text input field labeled "Credential Number" containing the value "4567". Underneath is a section titled "Select Scan Device" which contains three radio button options: "USB Card Reader", "Serial Card Reader", and "Reader". The "Reader" option is selected. To the right of "Serial Card Reader" is a dropdown menu currently displaying "COM1". To the right of "Reader" is a dropdown menu currently displaying "Reader (0014f001534)". At the bottom of the dialog are four buttons: "Scan", "Encode", "Cancel", and "Finish".

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

### USB Card Reader

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

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

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

### Serial Card Reader

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

- 1 When you are ready to scan the card, select the Scan button. You will have 30 seconds to scan the card. When recognized, the number will display in the Credential Number text box.
- 2 Select Finish and return to the Credential Setup dialog box.

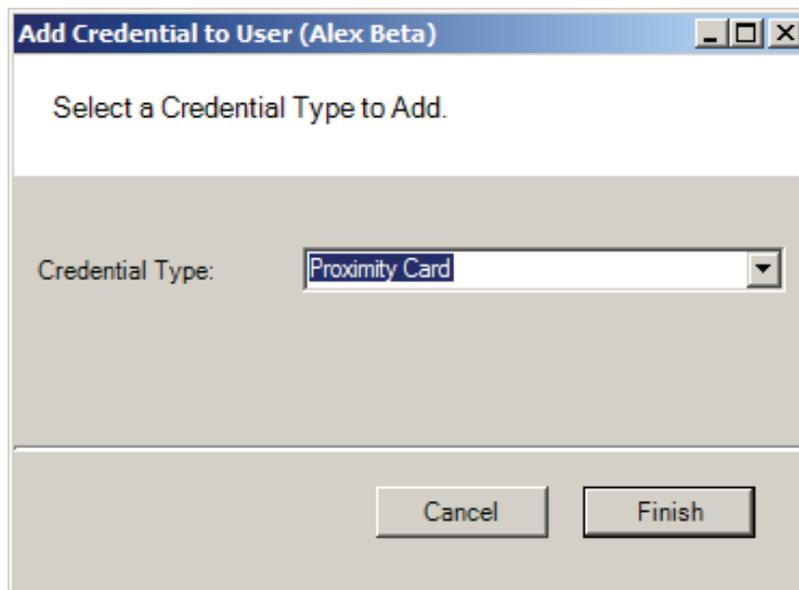
### Adding a Credential Type

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

#### To add a card type to the list

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

Figure 94 Add Credential to User



- 2 Select the Credential Type from the drop-down list, in this case, Proximity Card.
- 3 Select Finish. The User <Proximity Card> Credential Number Setting dialog box opens.
- 4 Now, you may manually enter a credential number or scan the credential with a

scanning device.

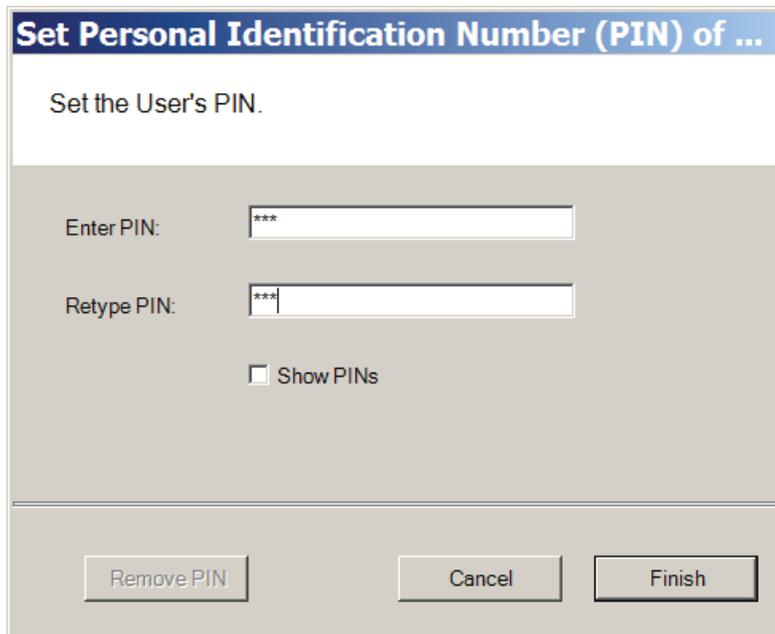
## PIN

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

### To add a PIN Number for a User

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

Figure 95 Set PIN of User



**Set Personal Identification Number (PIN) of ...**

Set the User's PIN.

Enter PIN:

Retype PIN:

Show PINs

- 2 Select the Show PINs check box if you wish to view the numbers instead of asterisks as you type them in.
- 3 Enter a PIN number for the user. Retype the PIN below.
- 4 Click Finish to save the PIN and exit the dialog box.

## Reader Control

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

user.

### To modify User Operate Time

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

### To modify User Shunt Time

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

## Settings

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

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

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

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

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

For a list of Manager and Programmer system override codes, see “System Overrides” on page 160.

### **To assign User Type**

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

## **Portal and Reader Control and Messaging**

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

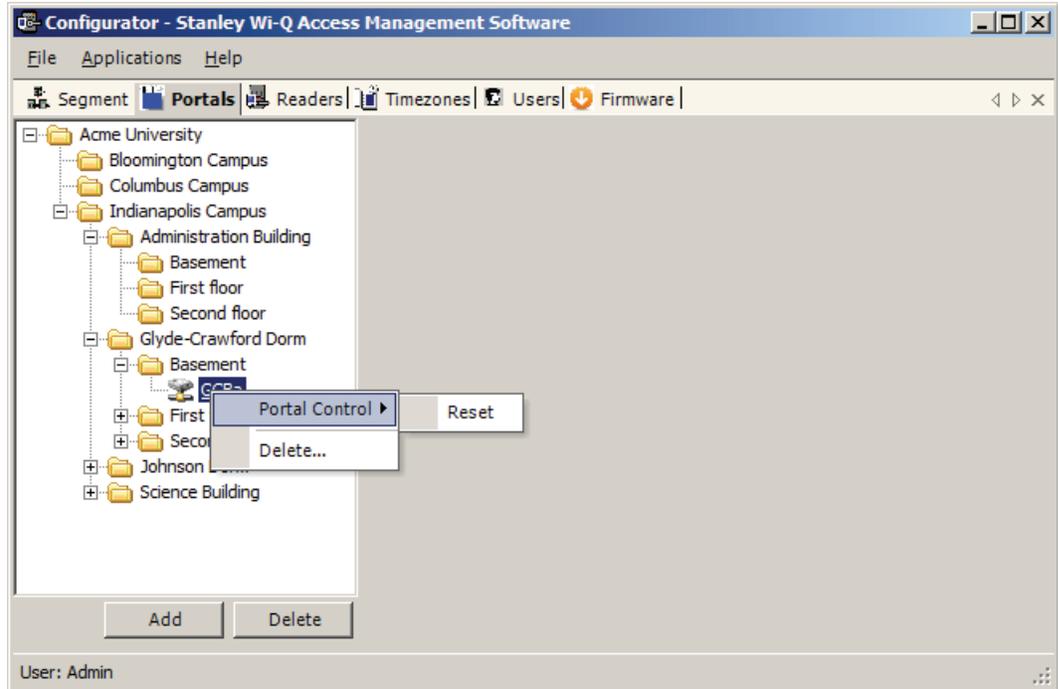
### **Portal Controls**

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

### **To access right-click Portal messaging**

- 1 In the Portals Tab, right-click on the Portal and select the option from the drop-down list. The software will ask you if you wish to proceed with the operation.
- 2 Click Yes. If the Portal is online, the operation is performed. If for any reason the Portal is offline and unable to execute the command, the message will become obsolete after five minutes.

Figure 96 Right-click Portal messaging options



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

## Reader Controls

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

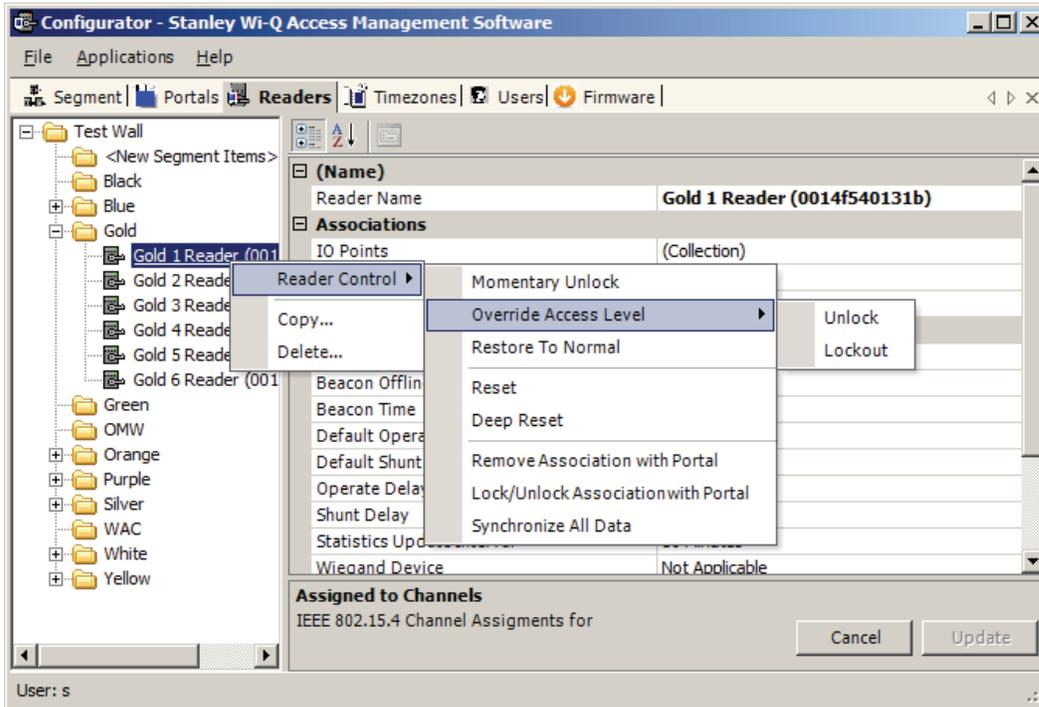
**Note** To delete more than one reader at a time, hold down the control key (CTRL) and select using the left mouse key.

### To Access Right-Click Reader Messaging

- 1 In the Readers tab Segment Tree, right-click on the reader and select the option from the drop-down list. The software will ask you if you wish to proceed with the operation.
- 2 Click Yes. If the reader is online, the operation is performed. If for any reason the reader is offline and unable to execute the command, the message will

become obsolete after five minutes.

Figure 97 Right-click reader messaging options



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

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

**Restore to Normal** — Immediately restores all standard normal operation.

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

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

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

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

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

## Configuring Timezones

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

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

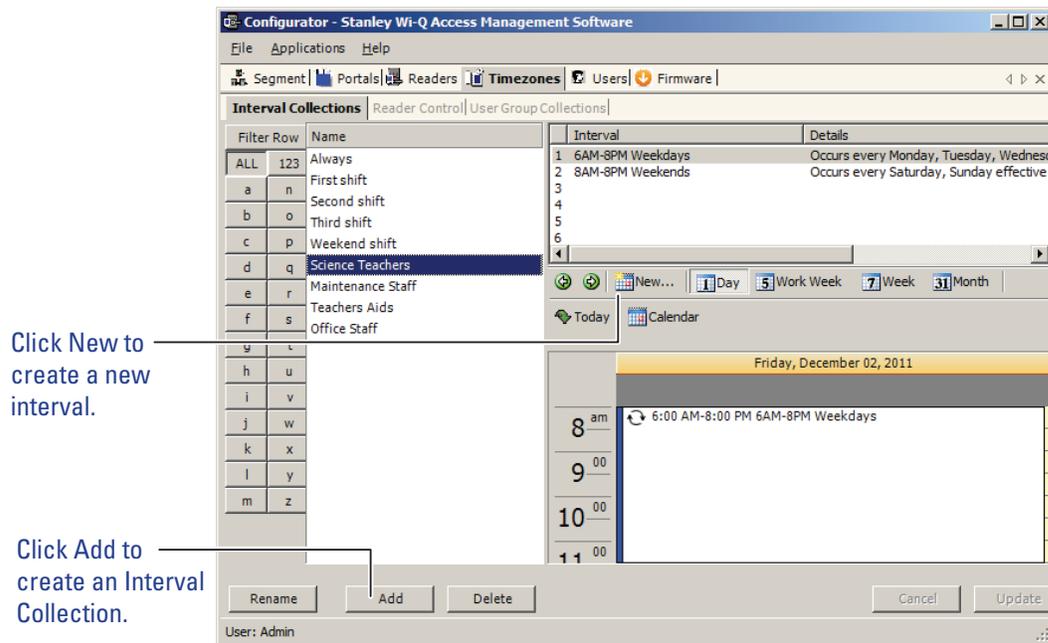
- **Interval Collections** — this is a collection of recurring ranges of time and days of the week, such as 6:00 am to 6:00 pm weekdays AND 8:00 am to 8:00 pm weekends.
- **Reader Control** — this is where you assign access levels to readers and determine how the reader will operate during assigned timezone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

**Note** Readers can be assigned to only one Timezone.

## To create a Timezone Interval Collection

- 1 Select the Interval Collections Tab under the Timezones Tab. The Interval Collection window opens.
- 2 Click the Add button to create a new Timezone Interval Collection.
- 3 Click the New button to create a new interval.

Figure 98 Interval Collection



- 4 The Interval Configuration window opens.

- 5 Enter a brief name for the Interval.
- 6 Select the Start and End Time of the Interval.
- 7 Click the Recurrence checkbox.

Figure 99 Interval Configuration

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

Click Recurrence if the interval repeats.

- 8 Select the Recurrence Pattern of the Interval.
- 9 Select the Range of Recurrence for the Interval.
- 10 Click Finish to save your new Interval. This Interval is now listed as one of the intervals for the Interval Collection.
- 11 Repeat steps 3 to 9 to create other Intervals until the Interval Collection is complete.

### Timezone Interval Template Feature

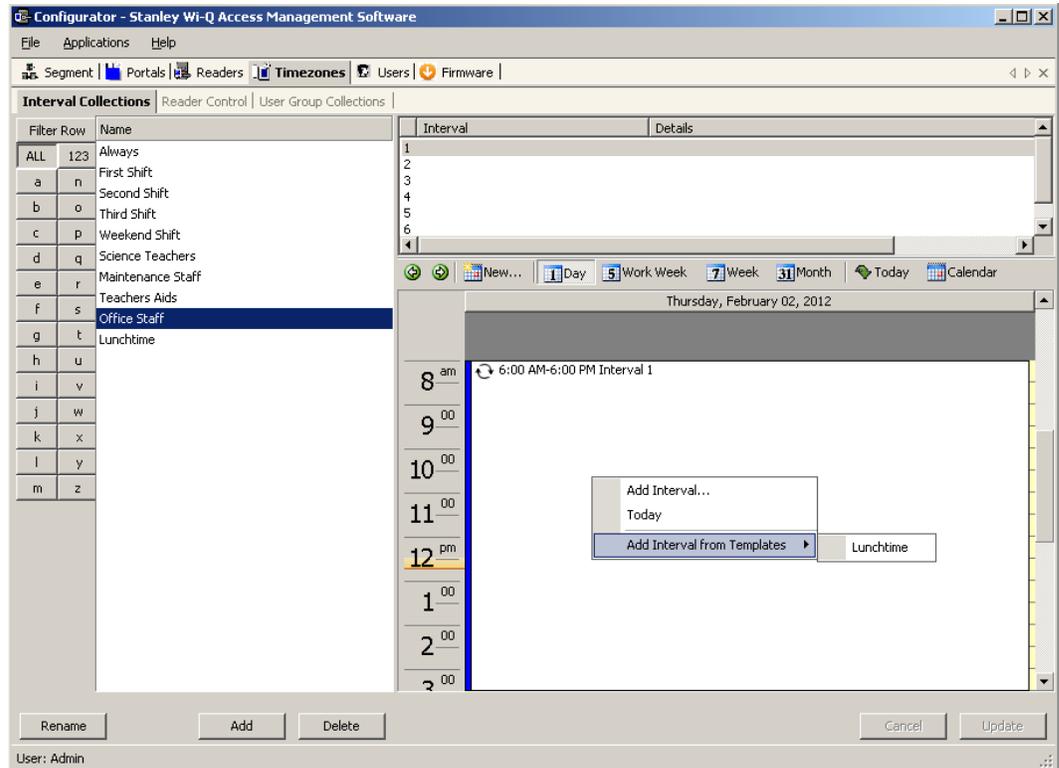
At the top of the Interval Configuration window, there is a “Template” checkbox. Selecting this box will allow the timezone interval you configure to be used as a template for other intervals. For example, if you create a “Lunchtime” interval collection between 12pm and 1pm, and you select the “Template” checkbox (Figure 100), you can add that interval to an existing collection.

Figure 100 Interval Configuration Template

The screenshot shows the "Interval Configuration" dialog box. At the top, the "Subject" field is set to "Lunchtime". Below it, the "Template" checkbox is checked and highlighted with a blue arrow and the label "Template". The "Interval Time" section includes "Start Time" (2/ 2/2012, 12:00 PM) and "End Time" (2/ 2/2012, 01:00 PM), with an "All day interval" checkbox that is unchecked. The "Recurrence" checkbox is checked. Under "Recurrence Pattern", "Daily" is selected, and "Every weekday" is chosen from the sub-options. The "Range of Recurrence" section shows "Start" as 2/ 2/2012, with "No end date" selected. At the bottom, there are "Cancel" and "Finish" buttons.

To add the “Lunchtime” interval to another collection , select the existing interval collection from the list at the left, right-click in the calendar area, and select “Lunchtime” from the Add Interval from Templates options. In our example, we add the Lunchtime interval to the Office Staff Interval Collection. See Figure 101.

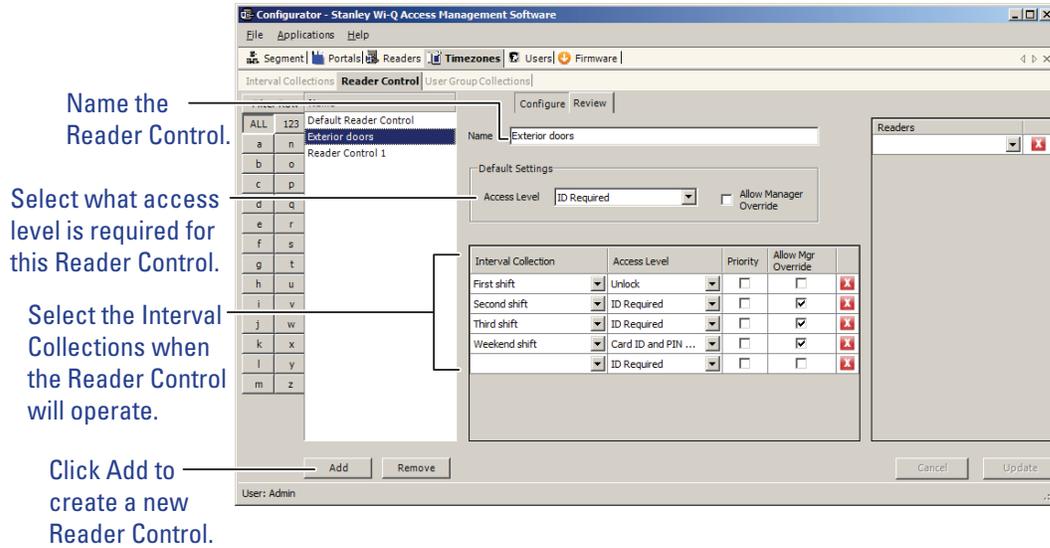
Figure 101 Add Interval from Templates



### To create a Timezone Reader Control

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

Figure 102 Reader Control



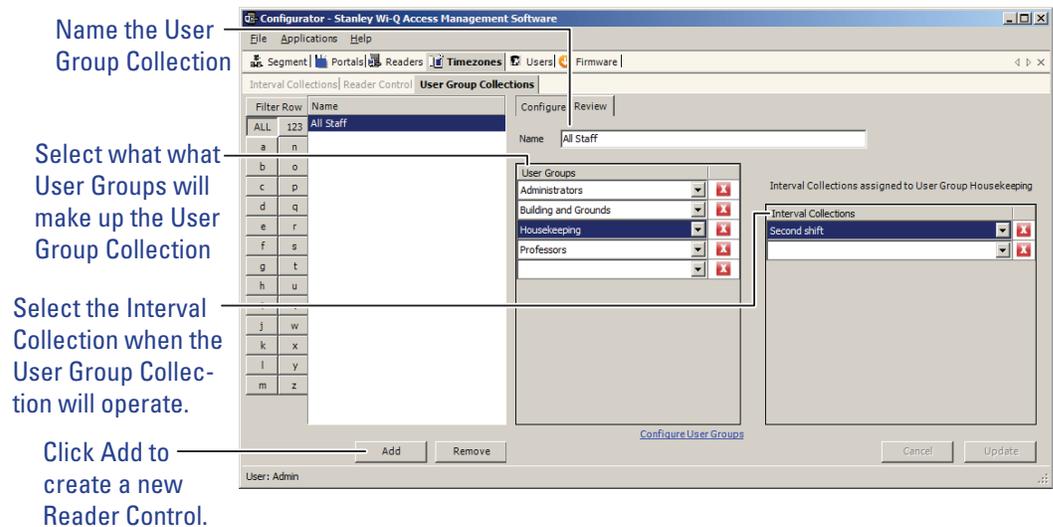
### Timezone User Group Collections

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

## To create the Timezone User Group Collection

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

Figure 103 Creating the timezone user group collection



## 6 Using and Managing the System

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

If you are the Program Administrator responsible for setting up communications between the software and system Portals and Controllers; you will spend most of your time using Configurator. If you are in personnel or security, you may be the person who adds users to the system and gives them access privileges and IDs. You will spend most of your time on the Users tab of Configurator. If you are responsible to oversee security for your organization, you will monitor all access and alarm activity using Transactions. If you are the person responsible to ensure the system is operating at maximum performance, you will use the Statistics Monitor. If your organization is small, you may use all three! You can access all applications from the Configurator main menu. You can also access these applications from the Windows Start Menu under Stanley Security Solutions.

## Wi-Q AMS and Omnilock Configurator

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

### Launching Wi-Q AMS Configurator

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

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

Figure 104 Logging in to Configurator



If you are a AMS User, your System Administrator or IT representative must provide you a Login Name and Password. You will need this to login to the Configurator. If you are a System Administrator, see “Logging in to Configurator” on page 63 for more information about launching the software for the first time.

### **To Login to the Wi-Q AMS Configurator:**

- 1 Enter your case-sensitive Login Name and Password.
- 2 Select Login. Configurator opens at the Segment tab.
- 3 If the System Administrator has created only one segment, you are ready to begin. If more than one segment has been created, select the segment from the drop-down list. Any elements you access in Configurator will be directed to that segment.

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

### **Managing Application Users**

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

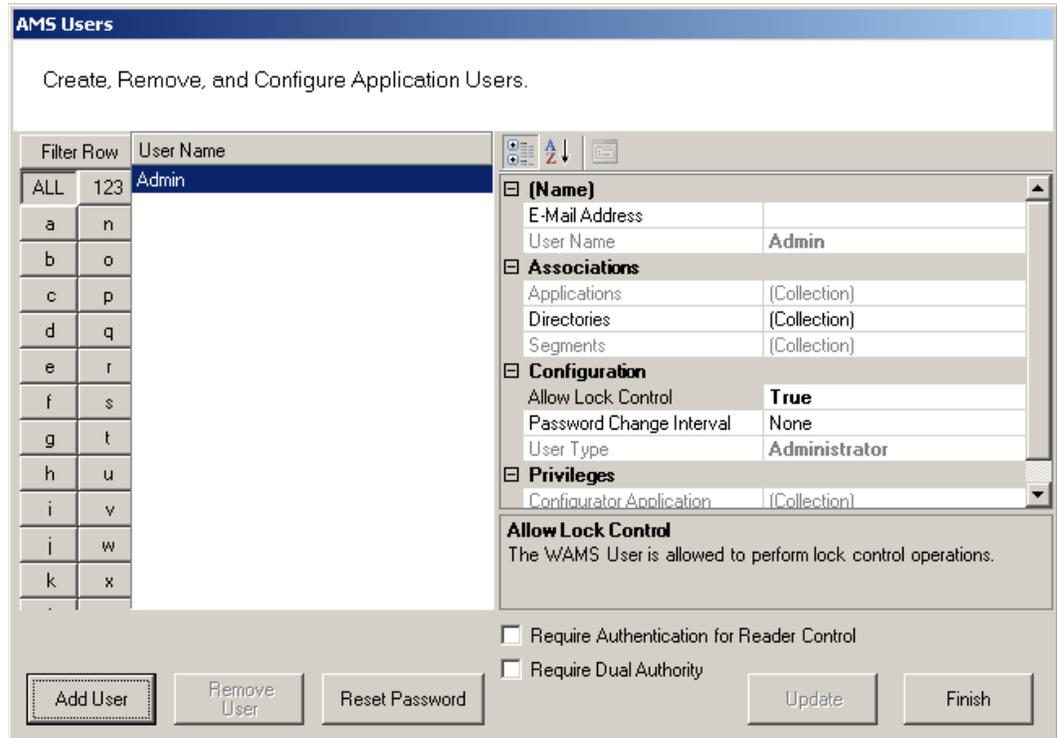
AMS Users must be added to the system as cardholders because they will require some type of physical access to the segment. However, they must also be assigned as AMS Users and be given User names and Passwords if they are to access and operate application software.

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

## To Manage Applications Users:

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

Figure 105 AMS Users



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

## To add an AMS User:

- 1 In the AMS Users dialog box, click Add User. The system creates "User1" in the left column.
- 2 In the Name category on the right, enter an e-mail address (optional), and the user name.
- 3 Under Associations, click the Applications field, then click the ellipsis button at the far right.
- 4 Select which application(s) the User will have access to. Then click Finish.
- 5 In the Directories field, click the ellipsis button. Select the directories linked to the User. Then, click Finish.
- 6 In the Segments field, click the ellipsis button. Select which segments the User

will have access to and supply contact information as needed.

- 7 Under the Configuration category, in the Allow Lock Control field, select either True or False from the drop-down list.
- 8 In the Password Change Interval field, select a change interval from the drop-down list.
- 9 In the User Type field, select a User Type from the drop-down list. (User Types are defined in the following paragraphs.)
- 10 If the user will require Authentication for Reader Control or Dual Authority, select these options at the bottom of the sheet.
- 11 Click Finish to save your settings.

## User Types

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

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

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

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

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

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

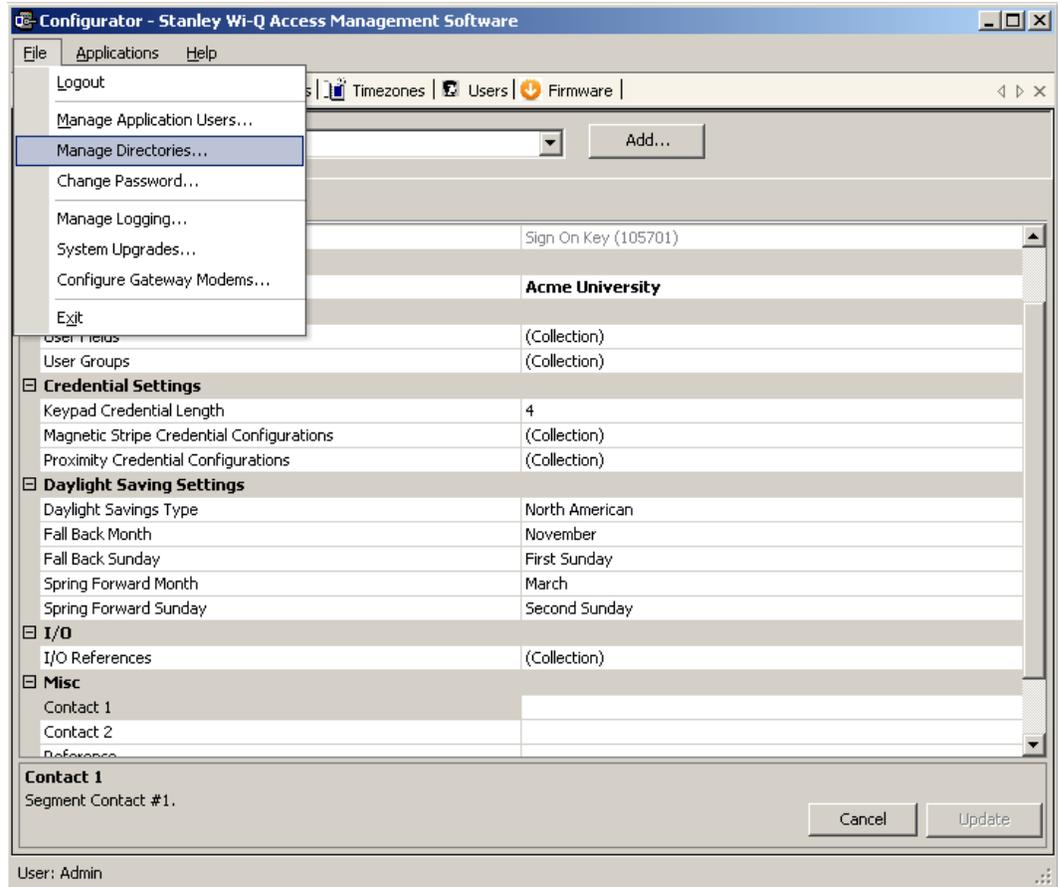
## Linking AMS Users' Windows Accounts to Configurator

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

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

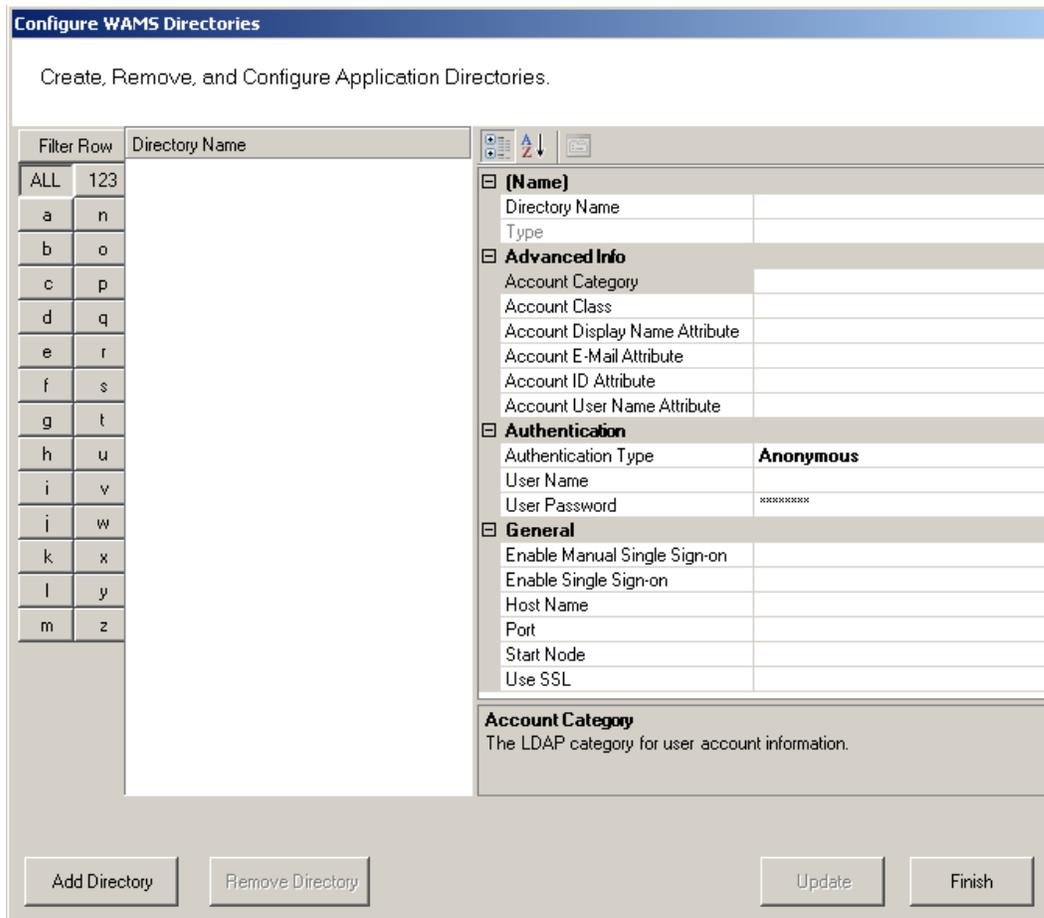
- 1 From the Configurator File menu, select Manage Directories.

Figure 106 Manage Directories



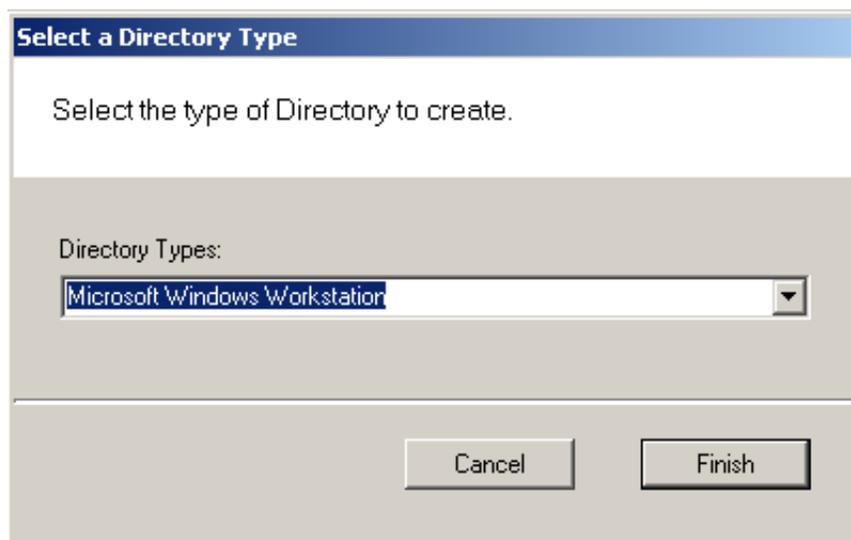
- 2 The Configure Directories dialog box opens. Click on Add Directory.

Figure 107 Configure Directories



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

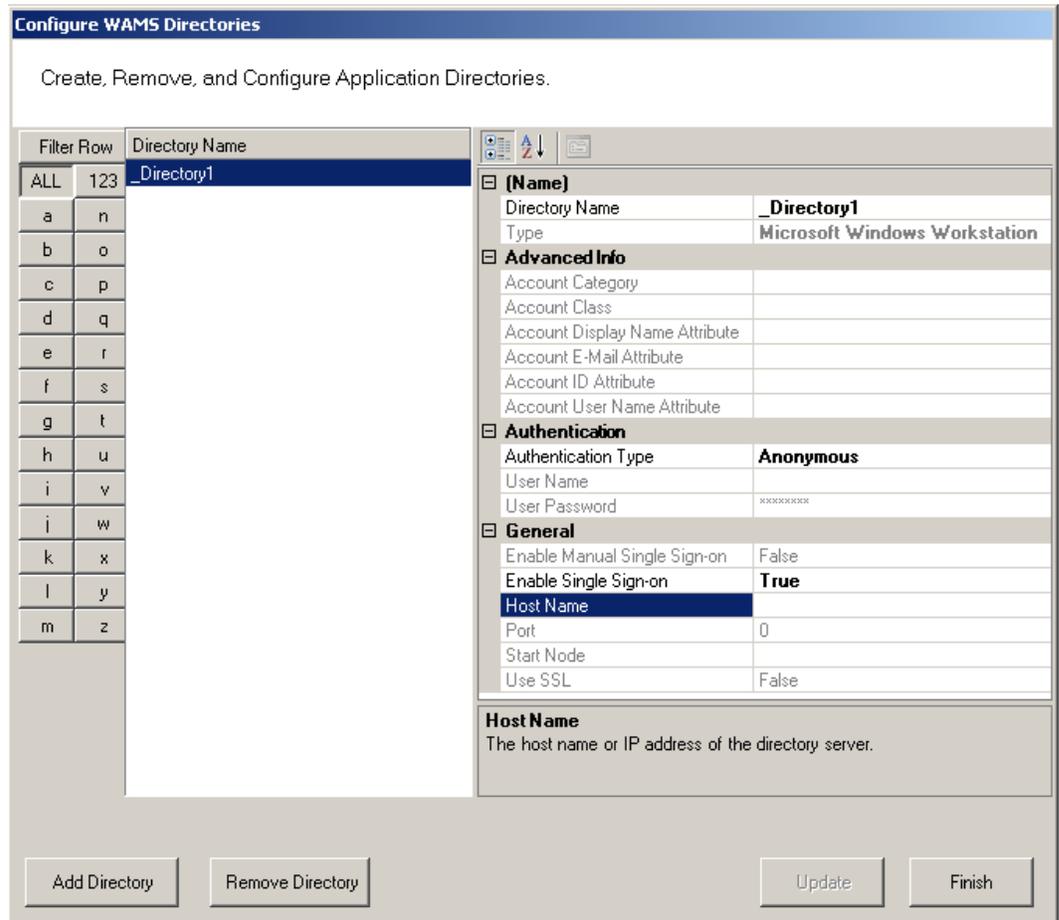
Figure 108 Select a Directory Type



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

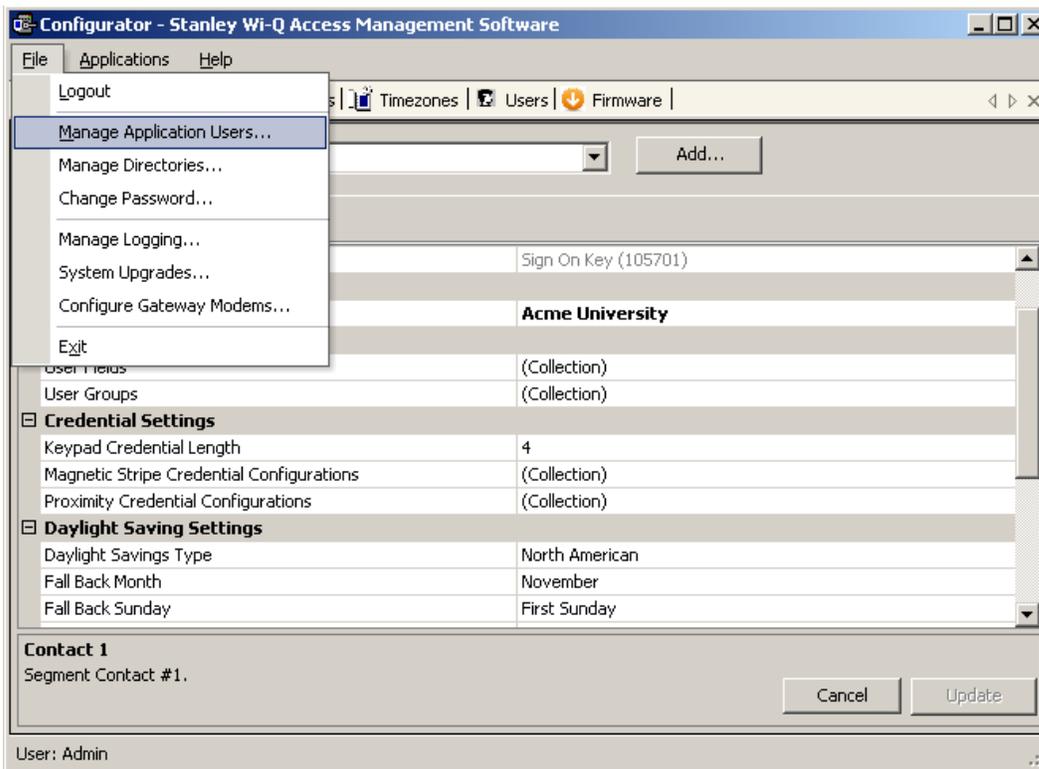
the default name. In the Host Name field, under the General category, type in the computer name of the host. Then, click Finish.

Figure 109 Directory and Host Names



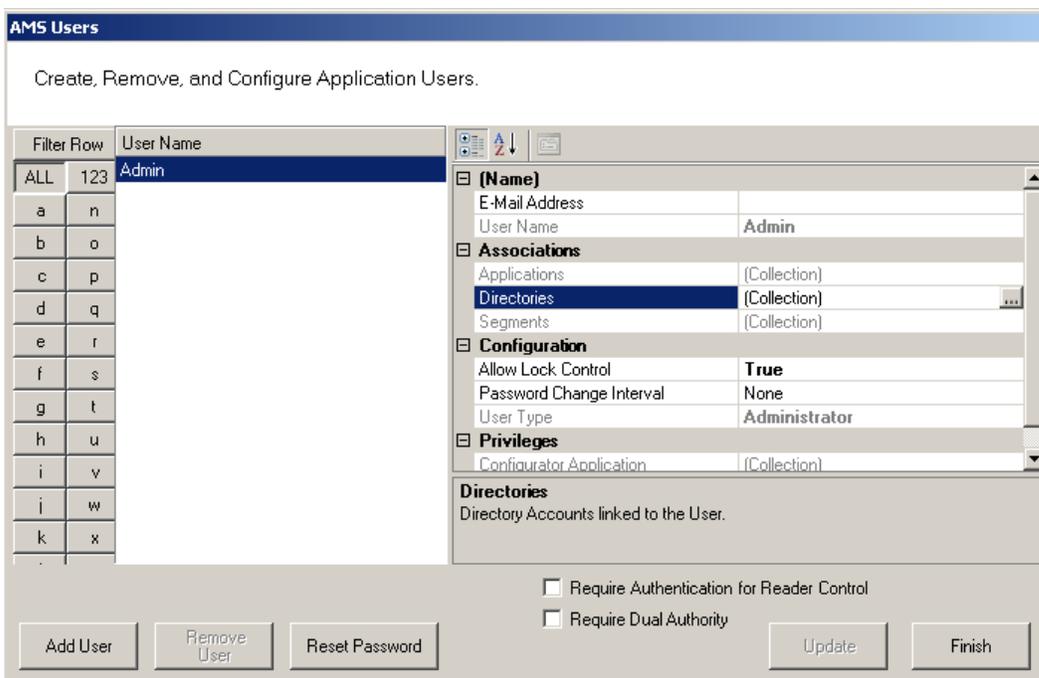
5 From the Configurator File menu, select Manage Application Users.

Figure 110 Manage Application Users



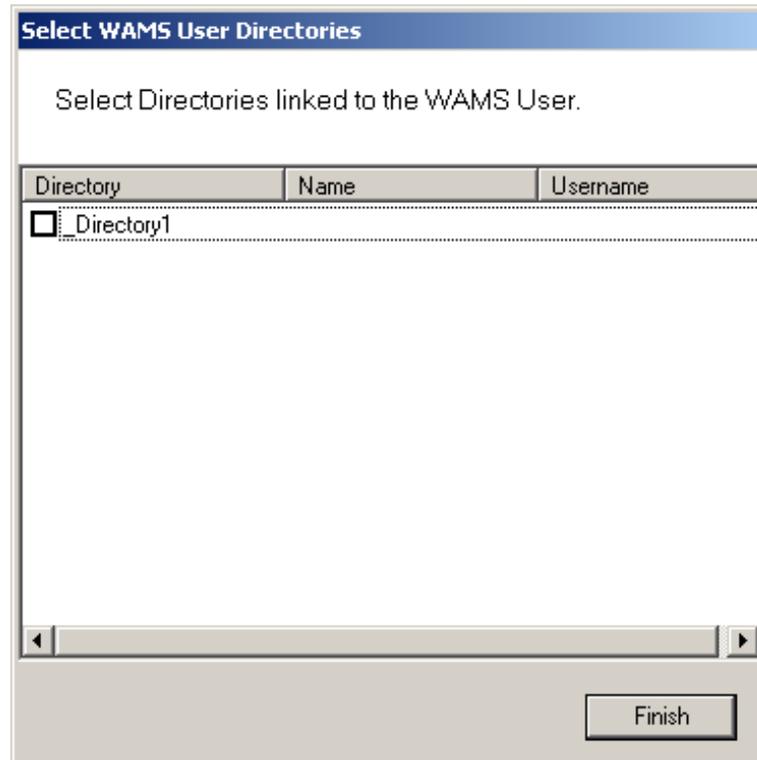
6 The AMS Users dialog box opens. Click in the Directories field, under the Associations column, and select the ellipsis button.

Figure 111 AMS Users



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

Figure 112 Select User Directories



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

Figure 113 Select User Directory Account

Select WAMS User Directory Account

Select Directory Account for the linked to the WAMS User.

Field: Name Condition: contains Value:

Accounts: Search

Names	Username
-------	----------

Cancel Finish

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

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

## Configurator Overview

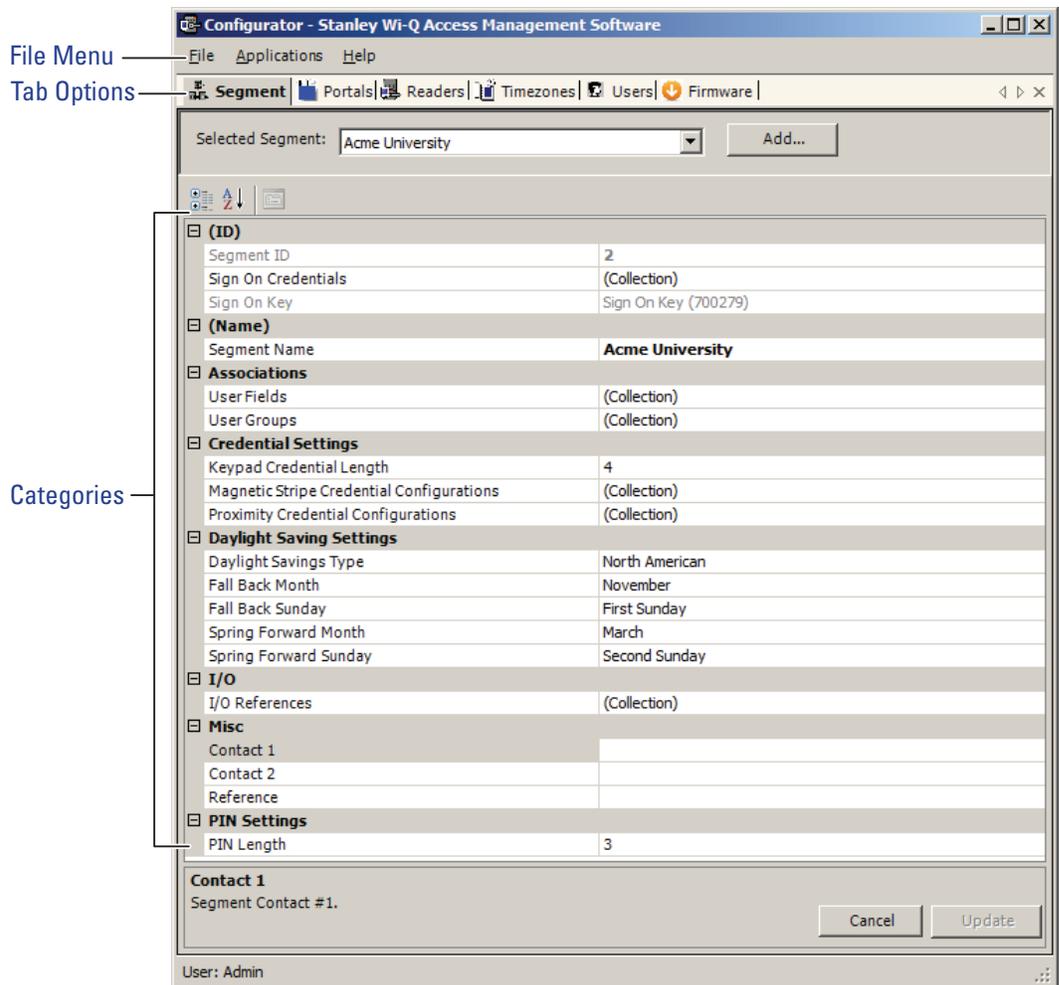
The following sections provide a brief overview of the Configurator module's Display and Tab options.

### Display Options

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

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

Figure 114 Segment Tab



In the Segment and Users Tabs, you can display items by category or sort alpha-

betically. This is useful when displaying the Configurator in full-screen view. A number of global operations are also available from the program File menu.

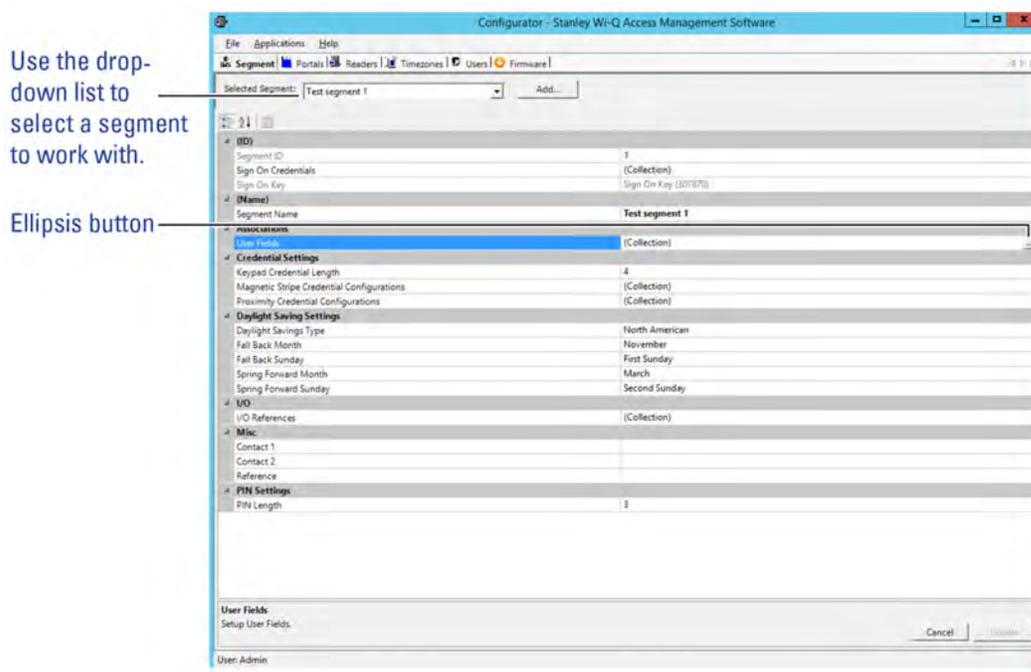
## Segment Tab

Most Segment set up tasks are performed in the Segment Tab, Figure 114. Here, the Program Administrator will create User Groups and configure the software to work with the type of segment access cards or keypad credentials you will use.

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

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

Figure 115 Segment Tab Categories

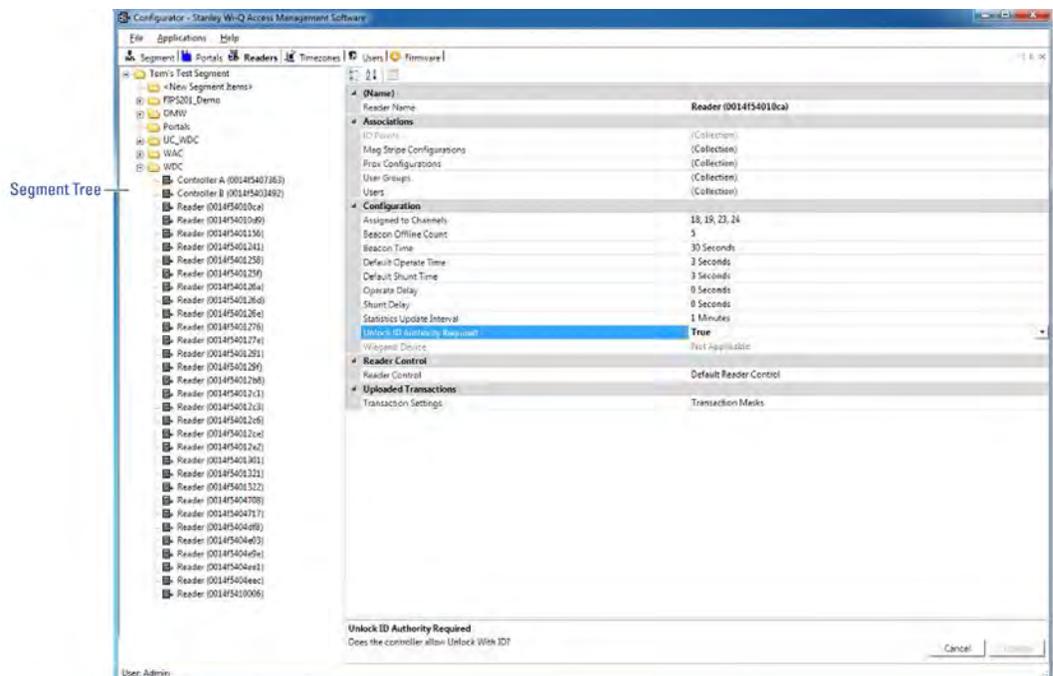


## Portals and Readers Tabs

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

Information about creating the Segment Tree and assigning devices to the various folders in the tree is presented in Chapter 4, “Configuring Segments, Portal Gateways and Controllers” on page 62. Typically, only the Program Administrator will perform tasks using the Readers Tab, Figure 116.

Figure 116 Readers Tab



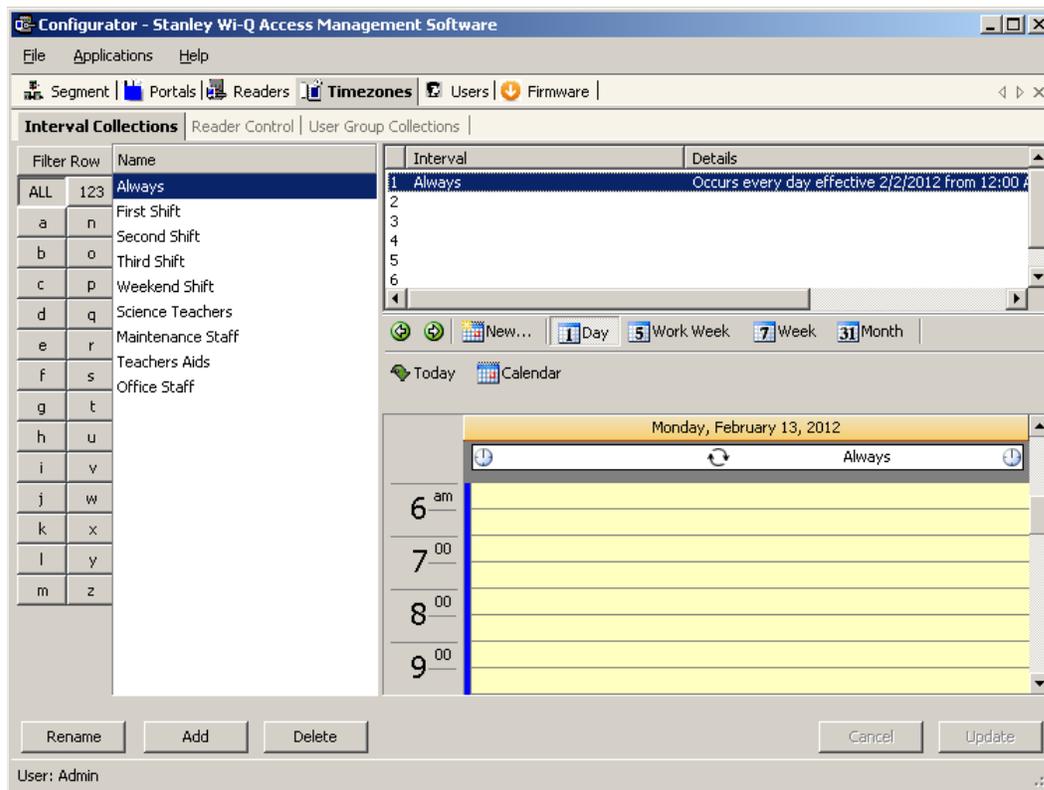
## Timezones Tab

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

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

More information about creating Timezone Intervals and Timezone Groups is presented in later in Chapter 5, “Configure AMS Software (Task 11)” on page 96.

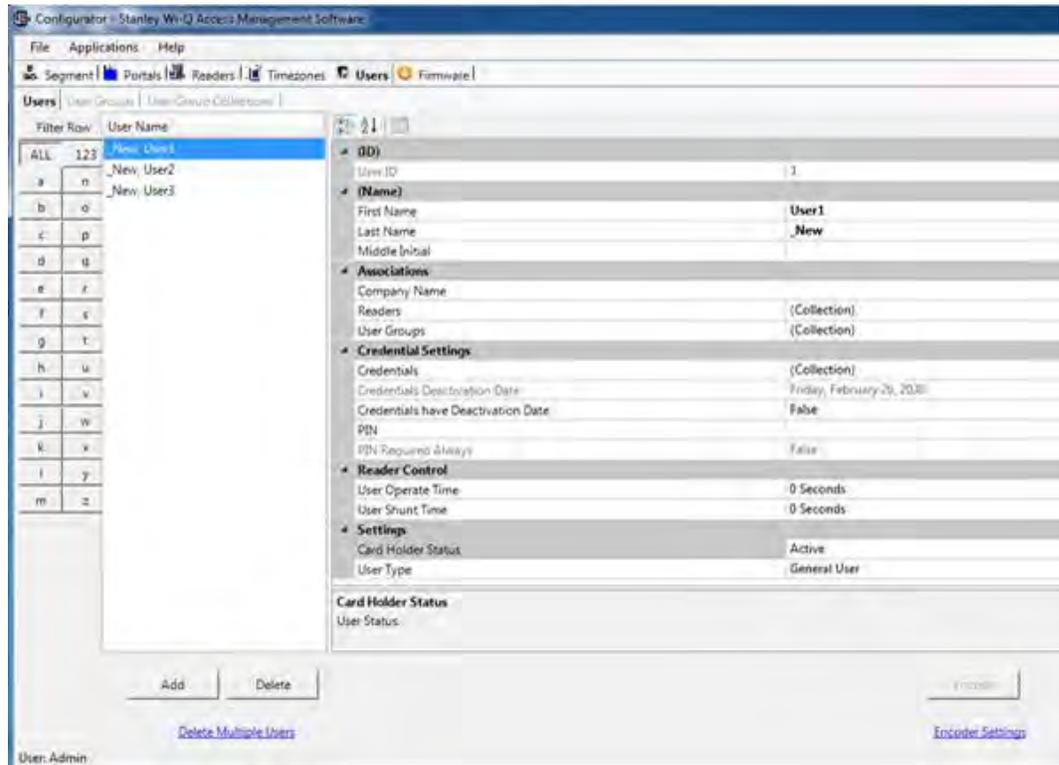
Figure 117 Setting up the Timezones



## Users Tab

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

Figure 118 Users Tab



More information about adding users to the system is presented in Chapter 5, “Configure AMS Software (Task 11)” on page 96.

## Firmware Tab

Firmware updates will be sent to you periodically by Stanley Technical Support. You can upload these firmware files to your database by using the System Administrator Application, and then you can send the updates to your hardware from the Configurator’s Firmware Tab. See “” on page 177.

## System Overrides

### Manager Override at Keypad Controller

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

**Note** MC refers to Manager Credential.

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

## Programmer Override at Keypad Reader

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

**Note** PC refers to Programmer Credential.

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

## Deep Reset

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

### ***To Perform a Deep Reset from within Configurator***

- 1 In the Configurator's Readers Tab, navigate to the desired reader using the Segment Tree.
- 2 In the list on the right, right-click on the reader and select Deep Reset from the drop-down list. Reader data will be cleared.
- 3 To bring the reader back into the software, you must perform a standard sign on procedure.

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

## Segment Item Upgrades

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

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

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

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

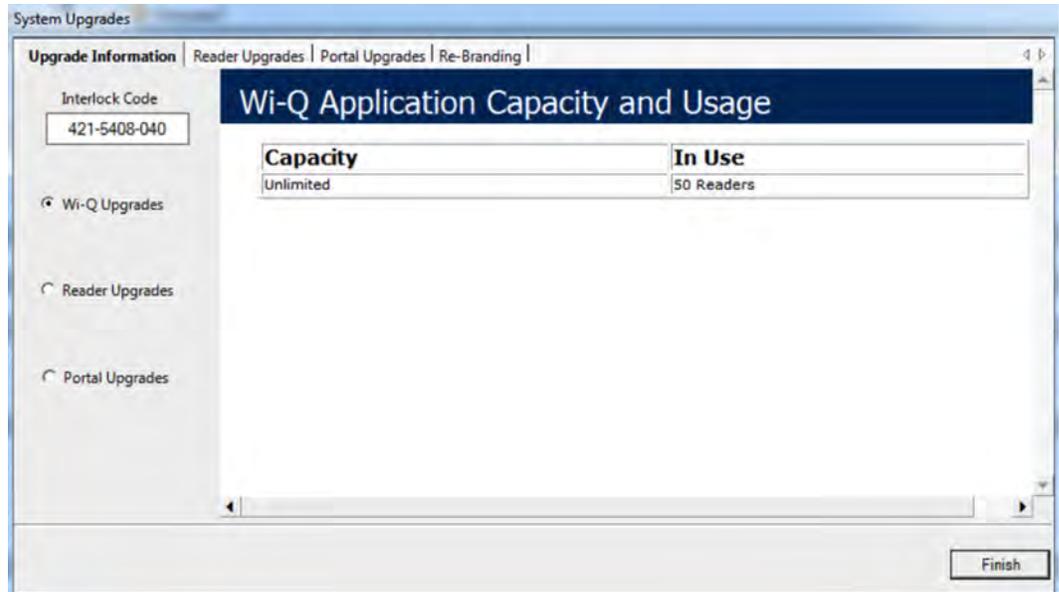
## Determine Segment Reader and Portal Capacity

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

### To view Wi-Q AMS and Omnilock Upgrade use

- 1 In Wi-Q AMS Configurator, Segment Tab, select the Segment you wish to review for upgrade use.
- 2 From the Wi-Q AMS Configurator File menu, select System Upgrades from the dropdown list. The System Upgrades window opens at the Upgrade Information Tab.

Figure 119 Upgrading your system capacity

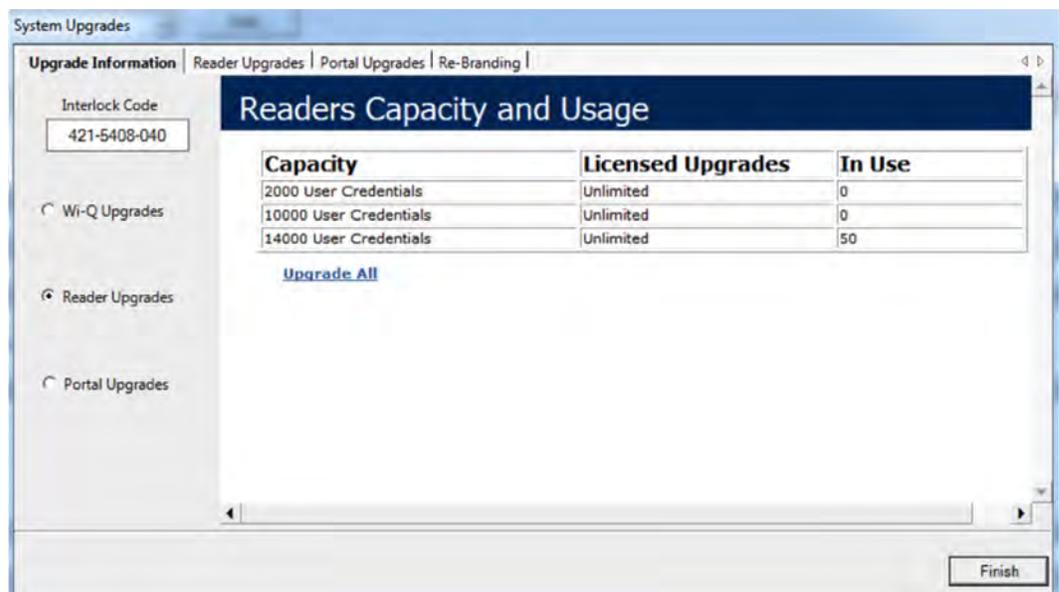


## AMS Upgrades

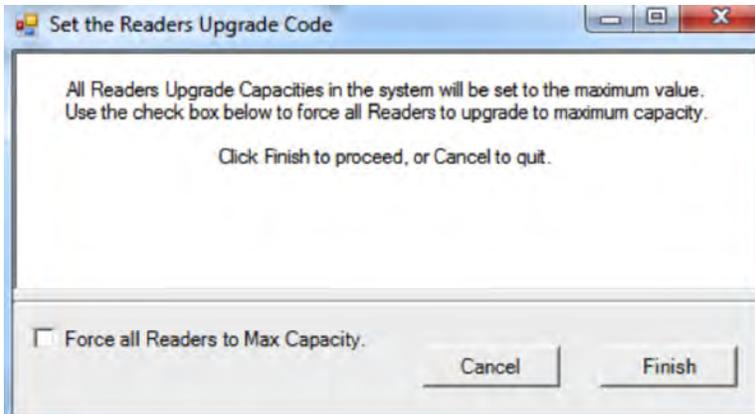
With the Wi-Q AMS Upgrades radio button selected on the left, the property sheet displays the current reader capacity for the segment and how many of those readers are currently in use.

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

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

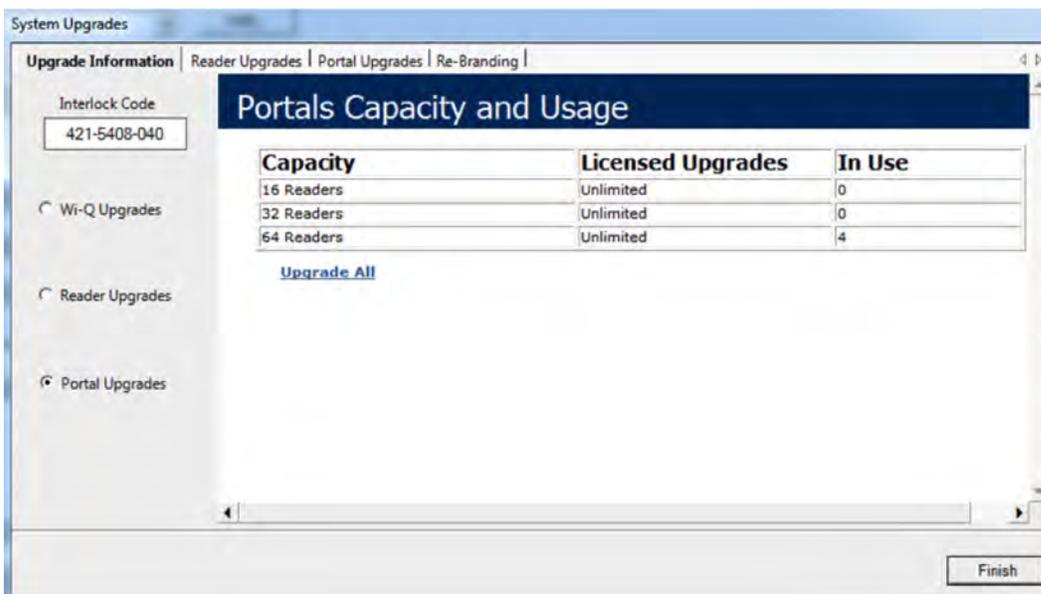


Select the upgrade all link if additional user capacity is needed.

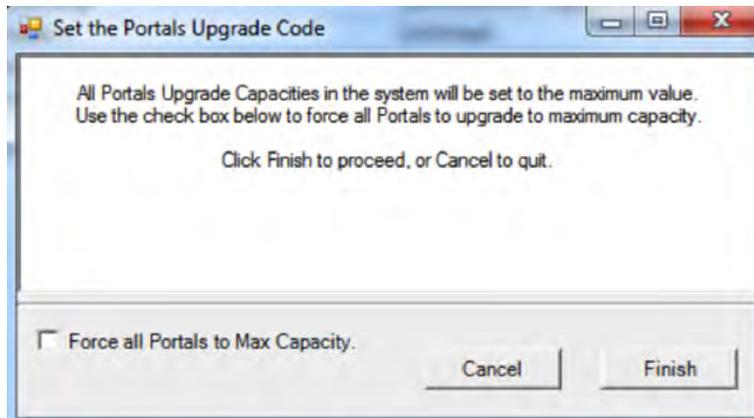


Select force all readers to max capacity and click finish.

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



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



Select force all portals to max capacity and click finish.

## System Administrator

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

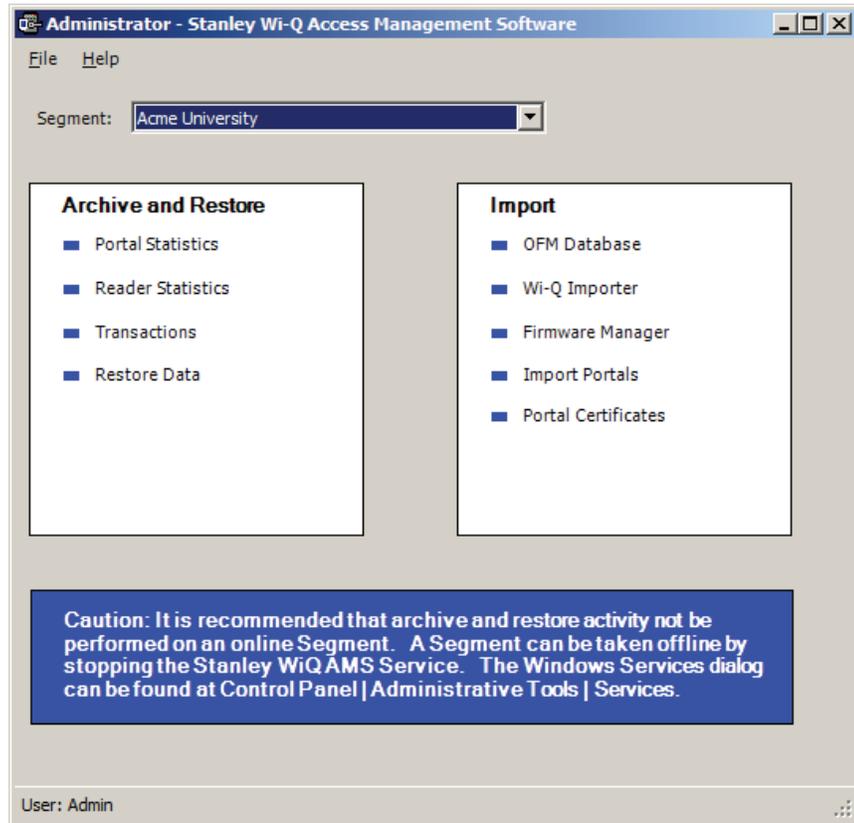
**Note** Archiving and restoring transactions and statistics is not the same as performing a full AMS database back up. Full back up and restore is performed using Microsoft SQL Server Management Studio Express (installed with AMS). Complete steps are described later in this chapter.

### Establish an Archive Protocol

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

# Using System Administrator

Figure 120 System Administrator



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

## Archiving Statistics in the AMS Database

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

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

Once you've selected the Portal or reader to archive, you can also select what

statistics to archive; for example, all statistics, only those statistics greater than a specific ID, or specify a range of statistics older than a specific date.

### **To Archive Statistics**

- 1 In the System Administrator application, select the segment for which you wish to archive statistics.
- 2 In the main window, under Archive and Restore, select a Statistics type, such as Portal Statistics.

Figure 121 Portal Statistics Archival for Segment

**Portal Statistics Archival for Segment (Acme University)**

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

Portal Selection

All Portals

Selected Portal

Statistics Selection

Archive All Statistics

Archive Statistics with IDs less than

Archive Statistics older than

- 3 In the Portal Selection box, select one of the following:
  - All Portals — All Portals' data will be archived.
  - Selected Portal — Choose a Portal ID from the drop-down list. Data from only that Portal will be archived.

- 4 In the Statistics Selection box, select one of the following:
  - Archive All Statistics — All statistics in the database will be archived.
  - Archive Statistics with IDs less than — Define an ID number. Only statistics with IDs less than the defined number will be affected.
  - Archive Statistics older than — Select a date. Only data older than the date selected will be archived.
- 5 When you have selected the appropriate options, click the Archive button and click Yes if you wish to continue with the archive.
- 6 In the Windows browser, navigate to a folder or create a new one in which to archive the file. You should create a filename that will be meaningful to your segment (for example, all\_Portals, or siteA\_Portals). These files will be accessible under this location should you wish to restore them at a later date.
- 7 Click OK. The system will display the status of the archive activity as it proceeds.
- 8 Click Finish to exit Portal Statistics Archive.

### **Restoring Data to the Database**

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

#### ***To Restore Data to AMS***

- 1 From the Configurator Segment Tab, select the segment for which you wish to archive statistics.
- 2 From the Applications menu on the Configurator menu bar, select System Administrator. The Systems Administrator window opens.
- 3 Select the Segment you wish to work with. From the left window pane, select Restore Data. The Windows browser window opens.
- 4 Select the file you wish to restore to AMS, then click Open.
- 5 The system reports that the records will be restored to the Segment. Click Yes to continue. The system will display the status of the archive activity as it proceeds.

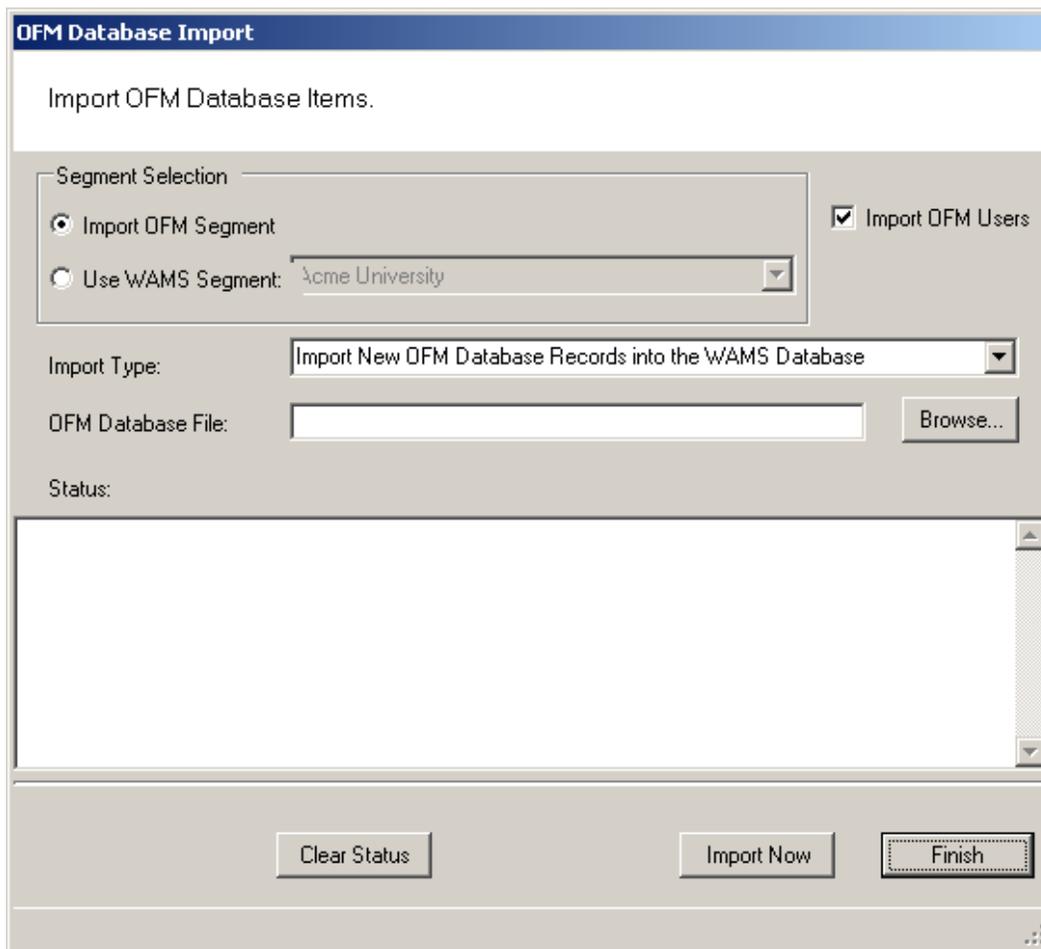
## Importing Data from a Legacy OFM Database

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

### To Import Data to AMS

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

Figure 122 OFM Database Import



The screenshot shows the "OFM Database Import" dialog box. The title bar reads "OFM Database Import". Below the title bar, the text "Import OFM Database Items." is displayed. The dialog is divided into several sections:

- Segment Selection:** This section contains two radio buttons. The first is "Import OFM Segment" (selected). The second is "Use WAMS Segment:" followed by a dropdown menu showing "Acme University". To the right of this section is a checked checkbox labeled "Import OFM Users".
- Import Type:** A dropdown menu is set to "Import New OFM Database Records into the WAMS Database".
- OFM Database File:** A text input field is empty, with a "Browse..." button to its right.
- Status:** A large, empty text area with a vertical scrollbar on the right side.

At the bottom of the dialog, there are three buttons: "Clear Status", "Import Now", and "Finish". The "Finish" button is highlighted with a dashed border. A small icon of three dots is visible in the bottom right corner of the dialog box.

- 3 In the Segment Selection box, select one of the two options:
  - Import OFM Segment — This option imports a new segment in its entirety and automatically gives it the name of the existing Segment in the OFM Database.
  - Use Segment — This option activates the drop-down list. Select the Segment into which you wish to import data. It will import any new data and update any existing records with the same ID based on the import type.
- 4 Select the Import OFM Users option if you want to include OFM Database existing Users and User Groups.
- 5 From the Import Type dropdown menu, select the type of import you wish to perform:
  - Import New OFM Records into the Database — This will import only new records.
  - Merge New and Changed OFM Data into the Database — This will import all data and add or update any records that are new since the last import.
- 6 Select Browse to find the OFM Database File.
- 7 Select Import Now. The data will begin to transfer and you will see the records scroll through the Status window. This should take only a few minutes, depending on the size of the data being imported.

### **Import Data from a Standard Comma-Delimited File**

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

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

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

### **AMS Importer imports files in a few easy steps:**

- Create the data file in the appropriate program, such as Microsoft Word, Excel,

or other text-based program and save it as a .txt or .csv format.

- Prepare the Wi-Q AMS Import Utility to accept the file.
- Import the data.
- Send the Data to the database.

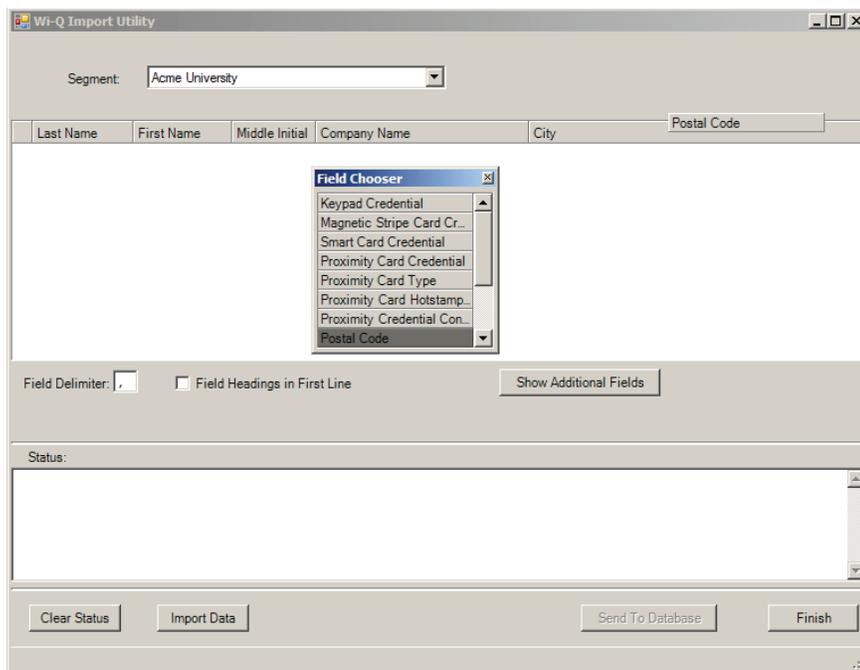
In the Import Utility, you can view the data as it imports into the window and make any corrections to the file or column headers until you are satisfied with the import before you actually send it to the database.

Detailed instructions are presented in the next few sections.

### To prepare Wi-Q AMS Import Utility

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

Figure 123 Import Utility



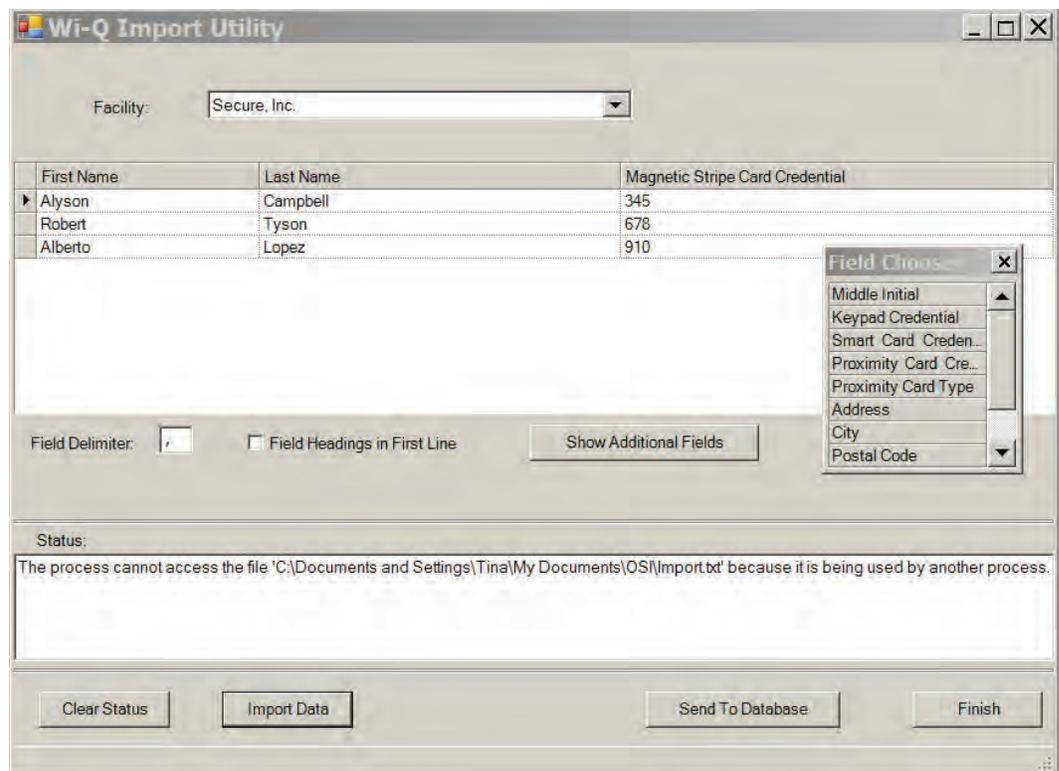
- 3 Use the cursor to drag the column headers into any order you wish.

- 4 If you wish to import additional data into user fields associated with the segment, click Show Additional Fields to display the Field Chooser and double-click or drag to add them to the header.
- 5 Enter the appropriate Field Delimiter for the import file, the default is a comma.
- 6 If you have field headings in the first line of your data file, click the Field Heading in First Line check box.

### To import the data

- 1 Once all column headers are in the order you wish, click Import Data.
- 2 Navigate to the location of the data file you created and click Open.
- 3 The Data appears under the appropriate column headers in the upper window. If the file is large, you can watch the progress in the Status box on the bottom of the window.

Figure 124 Using the Import Utility



- 4 Review the data import. Scroll the window to ensure the data has imported in the appropriate column headers. If not, you can rearrange the column headers and import the file again. You can do this as many times as you need to ensure you will get a good import.
- 5 Once you are satisfied that the data has imported as intended, click Send to Database. The data will now appear in the appropriate fields throughout AMS.

## Backing Up and Restoring Your AMS Database

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

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

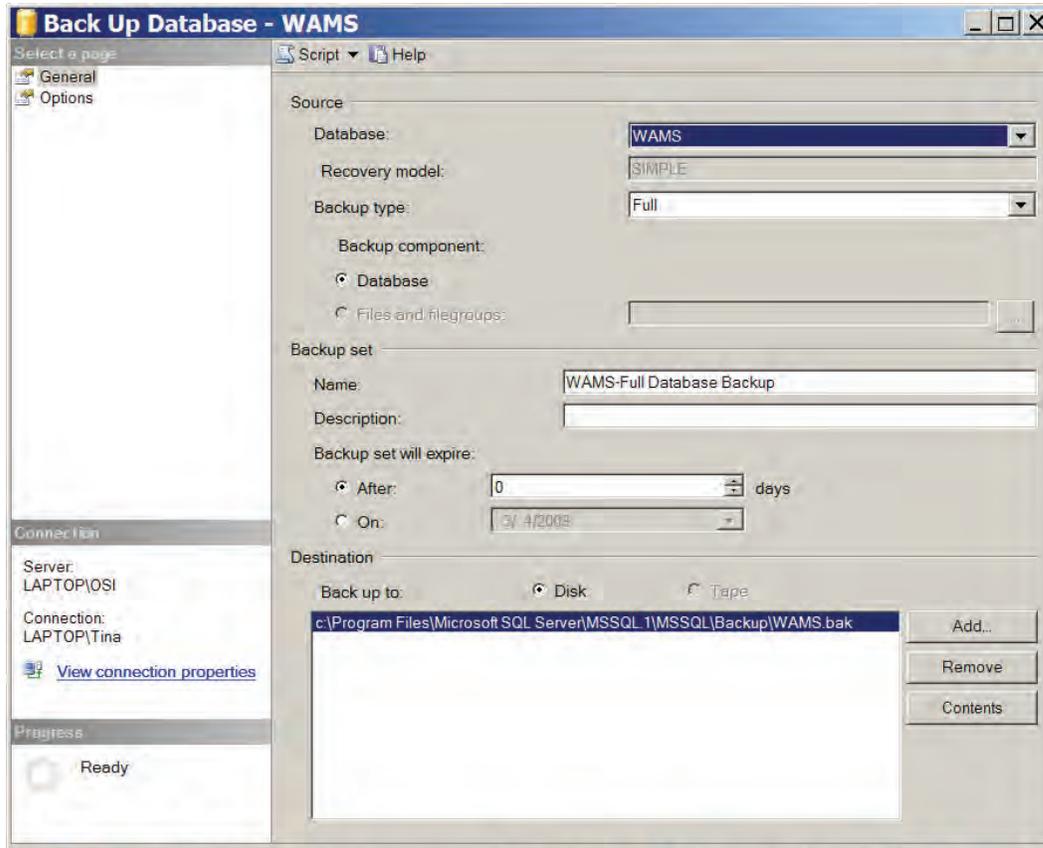
### Backing Up the Database

Perform the following steps to back up the database.

- 1 Exit AMS.
- 2 From the Windows Start menu, select Programs>Microsoft SQL Server Management Studio Express. The connect to Server dialog box opens.
- 3 Enter the Server type, Server name, and choose your Authentication type. Then, click Connect.



Figure 126 Backup Database



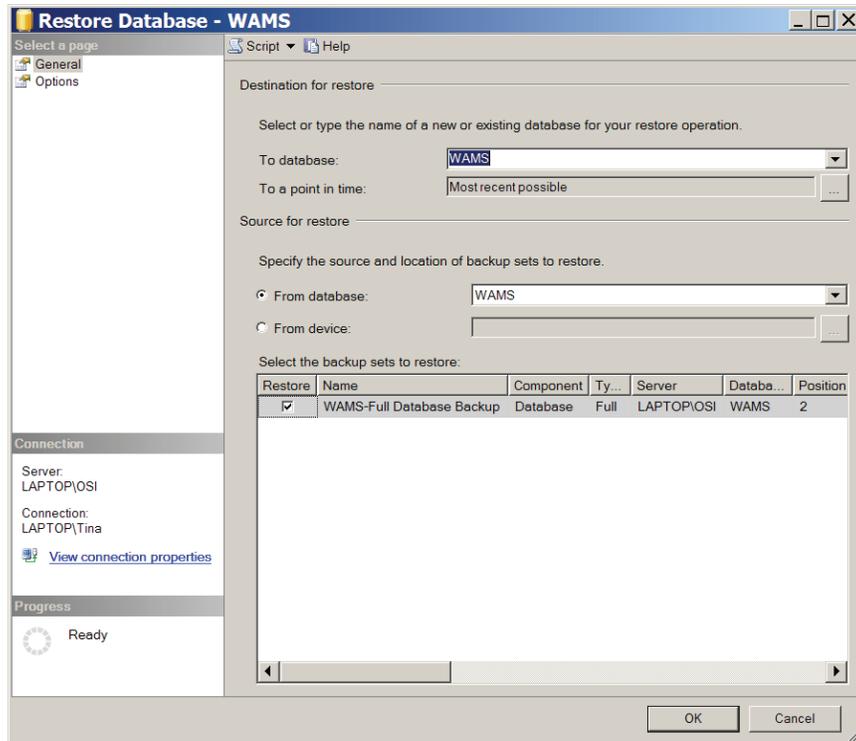
- 6 Define a Backup Type (full or differential) and add a description of the backup (optional).
- 7 The default destination displays. You can change the destination, if needed, for example if you wish to move the database to a new location on a different computer.
- 8 Click OK. The backup progresses and the system reports when the backup is complete.

### To Restore the database

- 1 Exit AMS.
- 2 From the Windows Start menu, select Programs>Microsoft SQL Server Management Studio Express. The connect to Server dialog box opens.
- 3 Enter the Server type, Server name, and choose your Authentication type. Then, click Connect.

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

Figure 127 Restore Database



- 6 The location defaults to the original location. You can specify a different location, for example, if you wish to move the database to a different computer.
- 7 Specify the source from which to restore and select a backup set to restore.
- 8 Select the backup set you wish to restore from the available list.
- 9 Click OK. The restore progresses and the system reports when the restore is complete.

## Firmware Updates

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

### Firmware File Types

Every Controller has two firmware files:

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

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

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

### Uploading Firmware Files

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

Figure 128 Manage Firmware Files

File Name	Description	Version	Uploaded
-----------	-------------	---------	----------

- 2 Click on the ellipsis button next to the File to upload field. Browse to your Portal gateway or Controller file(s). Once you've located your file, click Open.
- 3 Provide a unique name and description of the firmware file. If you are uploading a Controller firmware file, it is recommended that you build either "Boot" or "Application" into your description name, depending on the file type.
- 4 Click Upload. The firmware file will be added to the list at the bottom of the screen and added to your database.

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

- 5 Click Finish once all of your files are uploaded.

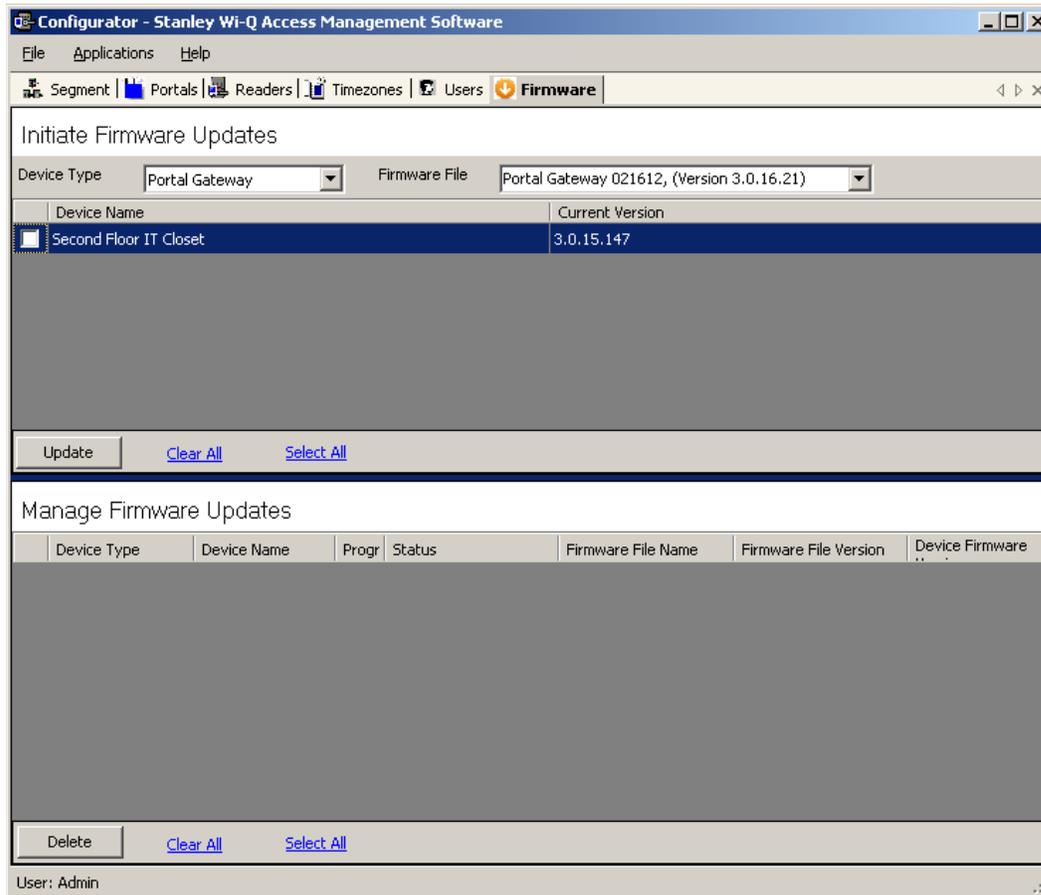
You are now ready to send the updates to your hardware.

## Firmware Reprogram

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

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

Figure 129 Configurator Firmware Tab



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

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

- 3 Check the boxes next to the devices that need updating. You can click Select All or Clear All as needed.
- 4 Once you've made your selections, press Update.
- 5 The devices will be added to the Manage Firmware Updates queue below, where you can view the download progress and status.

## Transactions Monitor

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

### To Launch Transactions

- 1 Select Start>All Programs> Stanley Security Solutions >Stanley Wi-Q AMS> Transactions.
- 2 Enter your Login and Password. Transactions opens at the Transactions Tab.
- 3 From here you can view all transaction and alarm activity for the segment you select.

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

### Transactions Overview

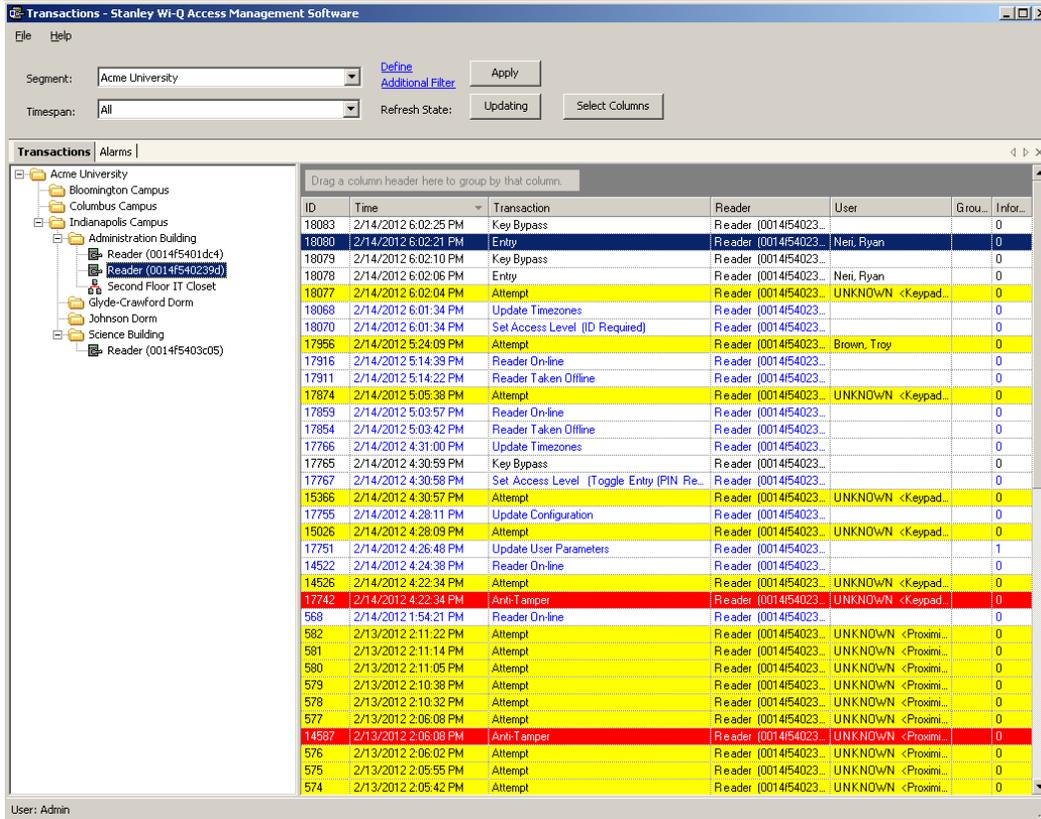
As activity takes place throughout the segment, AMS tracks each event as a transaction. The most obvious use of Transactions is to recognize and investigate when security has been compromised. You can immediately locate the source of an alarm and take the action necessary to respond according to your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

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

## Transactions Tab

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

Figure 130 Transactions



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

## Reader and Portal Controls

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

Figure 131 Accessing Portals and Readers in the Transactions tab

The screenshot shows the 'Transactions' tab in the Stanley Wi-Q Access Management Software. The interface includes a menu bar (File, Help), a Segment dropdown set to 'Acme University', and a Timespan dropdown set to 'All'. The main area is divided into a tree view on the left and a data table on the right. The tree view shows a hierarchy starting with 'Acme University', followed by 'Administration Building', 'Reader (0014f5401dc4)', and the selected 'Reader (0014f540239d1)'. A context menu is open over the selected reader, with 'Reader Control' highlighted. The data table below shows a list of transactions with the following columns: ID, Time, Transaction, Reader, User, Gr., and Inf.. The table contains 20 rows of transaction data, including events like 'Key Bypass', 'Entry', 'Attempt', 'Reader On-line', and 'Anti-Tamper'.

ID	Time	Transaction	Reader	User	Gr.	Inf.
18...	2/14/2012 6:02...	Key Bypass	Reader (001...		0	
18...	2/14/2012 6:02...	Entry	Reader (001...	Neri, Ryan	0	
18...	2/14/2012 6:02...	Key Bypass	Reader (001...		0	
18...	2/14/2012 6:02...	Entry	Reader (001...	Neri, Ryan	0	
17...	2/14/2012 9:24...	Attempt	Reader (001...	UNKNOWN...	0	
17...	2/14/2012 5:14...	Reader On-line	Reader (001...		0	
17...	2/14/2012 5:14...	Reader Taken Offline	Reader (001...		0	
17...	2/14/2012 5:05...	Attempt	Reader (001...	UNKNOWN...	0	
17...	2/14/2012 5:03...	Reader On-line	Reader (001...		0	
17...	2/14/2012 5:03...	Reader Taken Offline	Reader (001...		0	
17...	2/14/2012 4:31...	Update Timezones	Reader (001...		0	
17...	2/14/2012 4:30...	Key Bypass	Reader (001...		0	
17...	2/14/2012 4:30...	Set Access Level (Toggle...	Reader (001...		0	
15...	2/14/2012 4:30...	Attempt	Reader (001...	UNKNOWN...	0	
17...	2/14/2012 4:28...	Update Configuration	Reader (001...		0	
15...	2/14/2012 4:28...	Attempt	Reader (001...	UNKNOWN...	0	
17...	2/14/2012 4:26...	Update User Parameters	Reader (001...		1	
14...	2/14/2012 4:24...	Reader On-line	Reader (001...		0	
14...	2/14/2012 4:22...	Attempt	Reader (001...	UNKNOWN...	0	
17...	2/14/2012 4:22...	Anti-Tamper	Reader (001...	UNKNOWN...	0	
568	2/14/2012 1:54...	Reader On-line	Reader (001...		0	
582	2/13/2012 2:11...	Attempt	Reader (001...	UNKNOWN...	0	

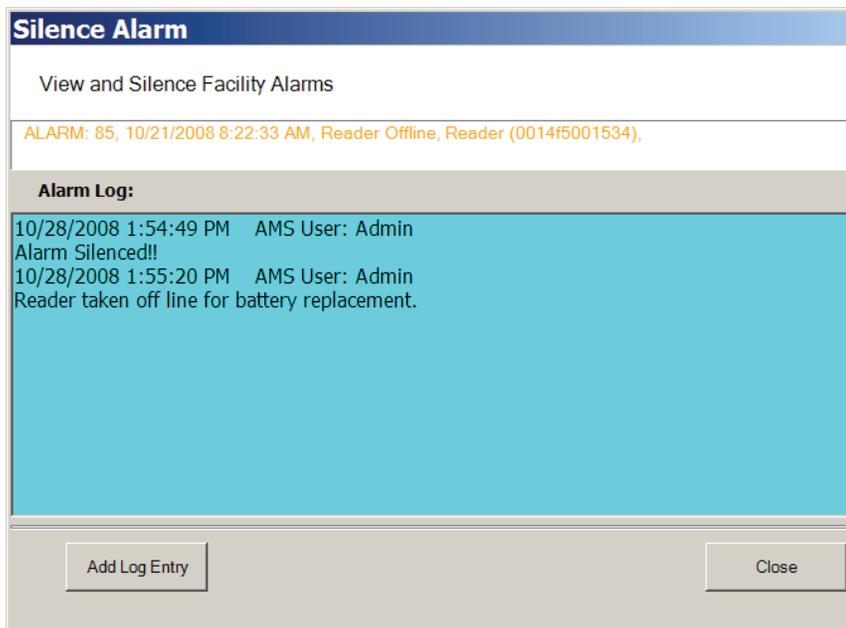
User: Admin

## Alarms Tab

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

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

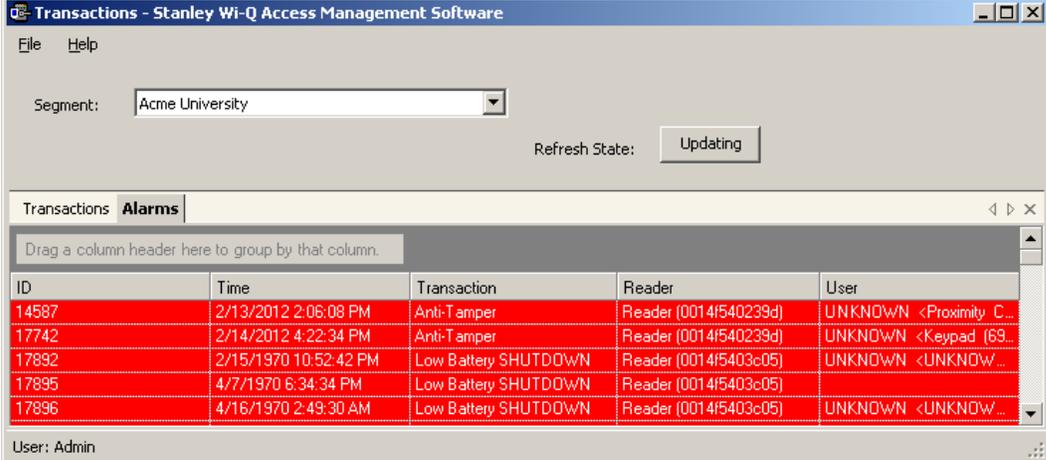
Figure 132 Silencing an alarm in the Alarms tab



## Create an Alarm Response Protocol

Remember, when you “Silence” an alarm in Wi-Q AMS Transactions, you are only silencing a .wav file; you are not resolving the problem. It is important to establish Alarm Response protocols within your segment and follow up with action. See “Responding to Alarms” on page 188.

Figure 133 Alarms Tab



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

## Transaction Types

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

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

## Organizing and Sorting Transactions

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

## Display by Timespan

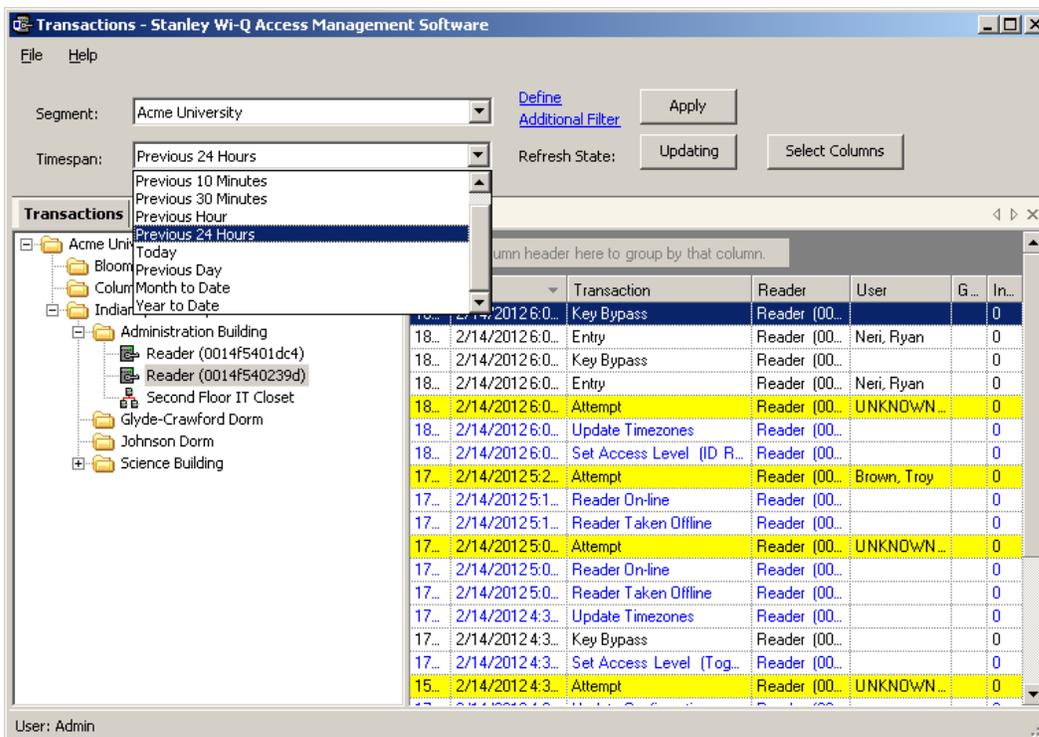
By default, Transactions displays all transactions in the order they occur. If you are monitoring all transactions, you may want to simply watch them as they occur. However, in large systems, your effort may best be served by limiting transactions to only those that have occurred in the previous ten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

### To set the display timespan

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

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

Figure 134 Transactions Timespan



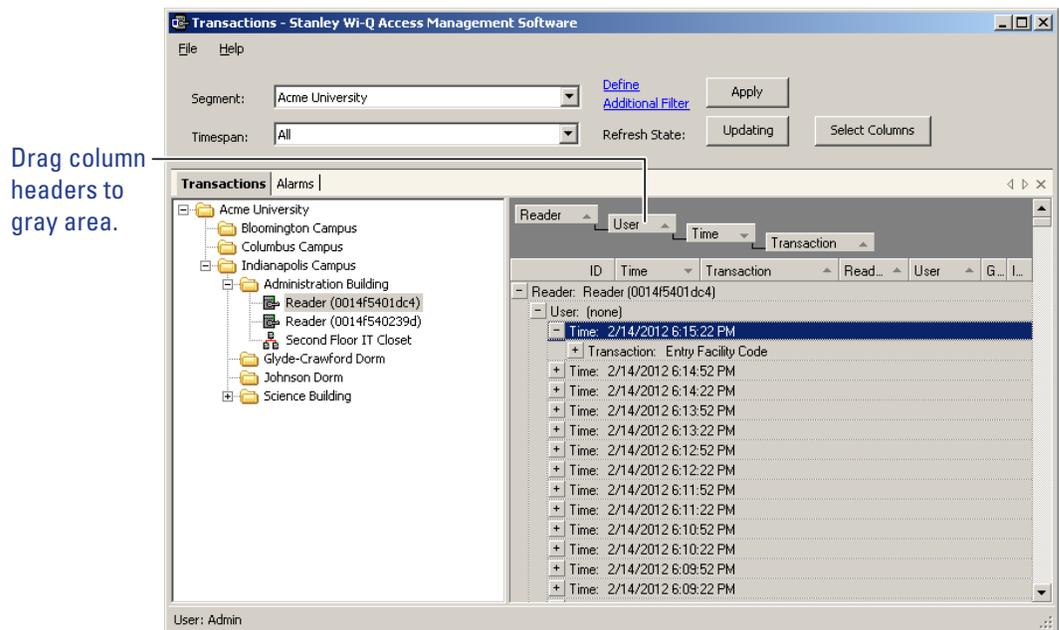
## Sort by Column Header

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

## View Transactions in Tree Levels

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

Figure 135 Transactions in Tree Levels



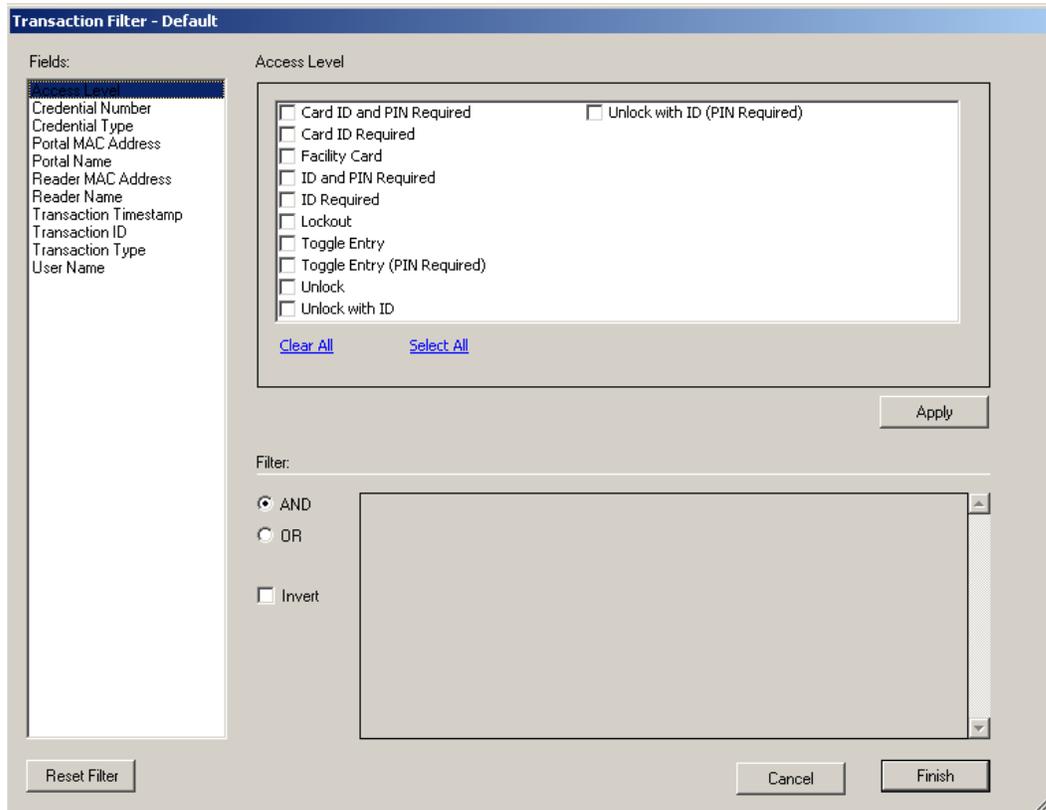
In this example, we placed Readers at the top of the tree; however, you can place them in any hierarchy you wish. When you select the plus sign next to the top level, the second and third level items expand to display. It's easy to create a Transactions Tree: simply drag and drop the column headers into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

## Transaction Filters

If you want to search for a specific transaction by certain criteria (user name,

reader name, etc.), click on Define Additional Filter at the top of the Transactions module. The Transaction Filter dialog box will open.

Figure 136 Transaction Filters



A list of fields is located on the left side of the dialog box. Clicking on a field will bring up checkbox or dropdown options specific to the selected field. In Figure 141, the Access Level field is selected. Here, you can check multiple options. Once you've selected your options, click Apply. The Filter section at the bottom of the dialog box will reflect what filter you've applied.

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

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

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

## Responding to Alarms

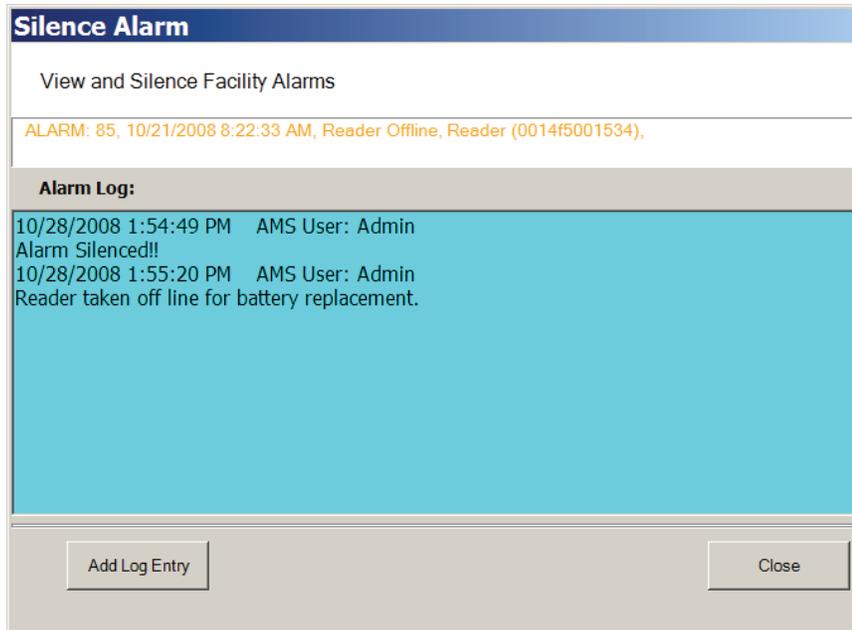
When an alarm occurs, the system immediately displays it in red in the Transactions Tab. The alarm will be categorized as either an Anti-Tamper or a Forced Entry type. At this point, you will take action according to your segment's security plan. In a small segment, you may simply dispatch a person to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

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

### **To respond to and silence an alarm**

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

Figure 137 Log Entry Recorded



- 8 Select Close. In the Alarms Tab, the alarm line changes from red to yellow and the alarm sound stops.
- 9 You can continue to add comments in the alarm's log until the condition is resolved.

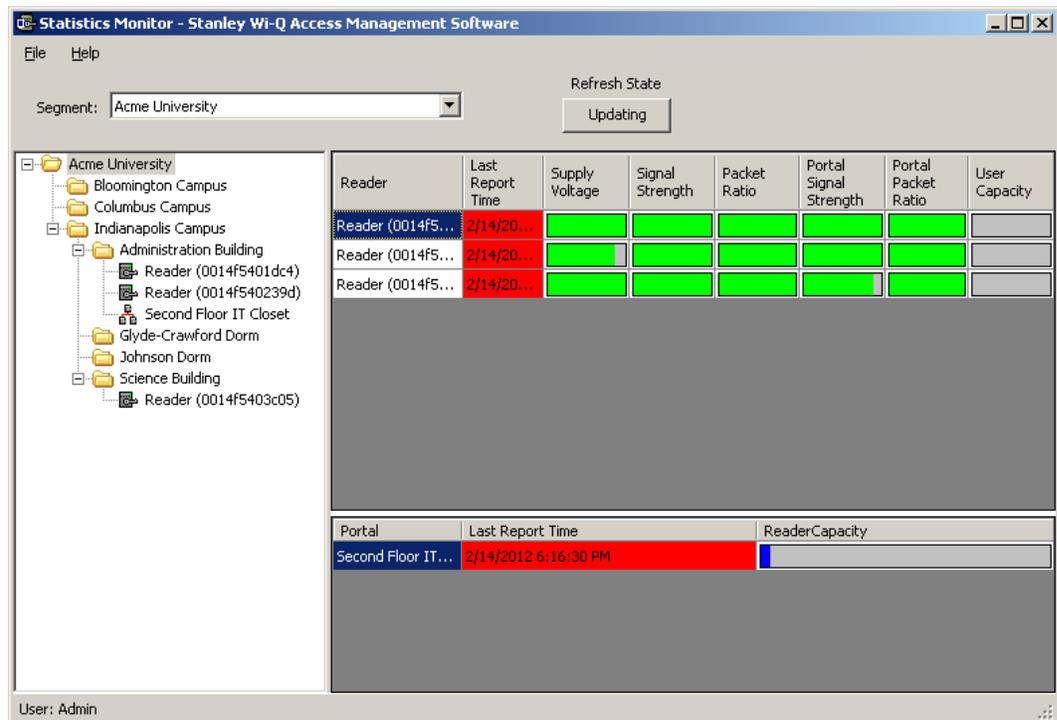
## Statistics Monitor

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

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

## Reader Statistics

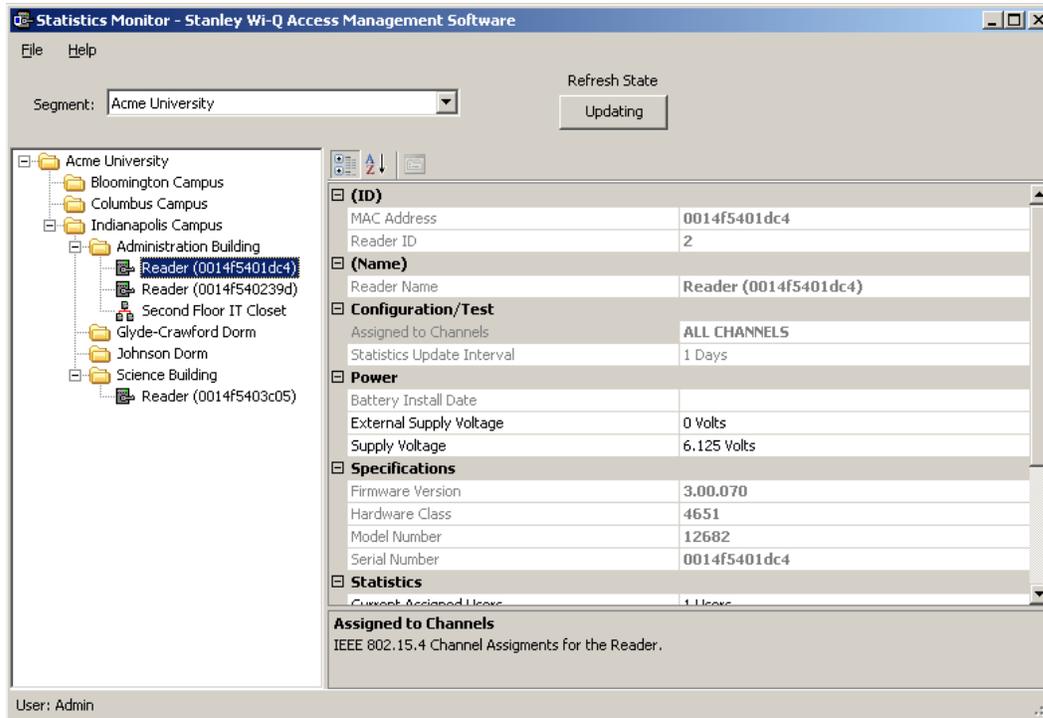
Figure 138 Viewing Reader Statistics



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

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

Figure 139 Display reader detail



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

## Automatic Updates

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

## Configuration/Test

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

## Power

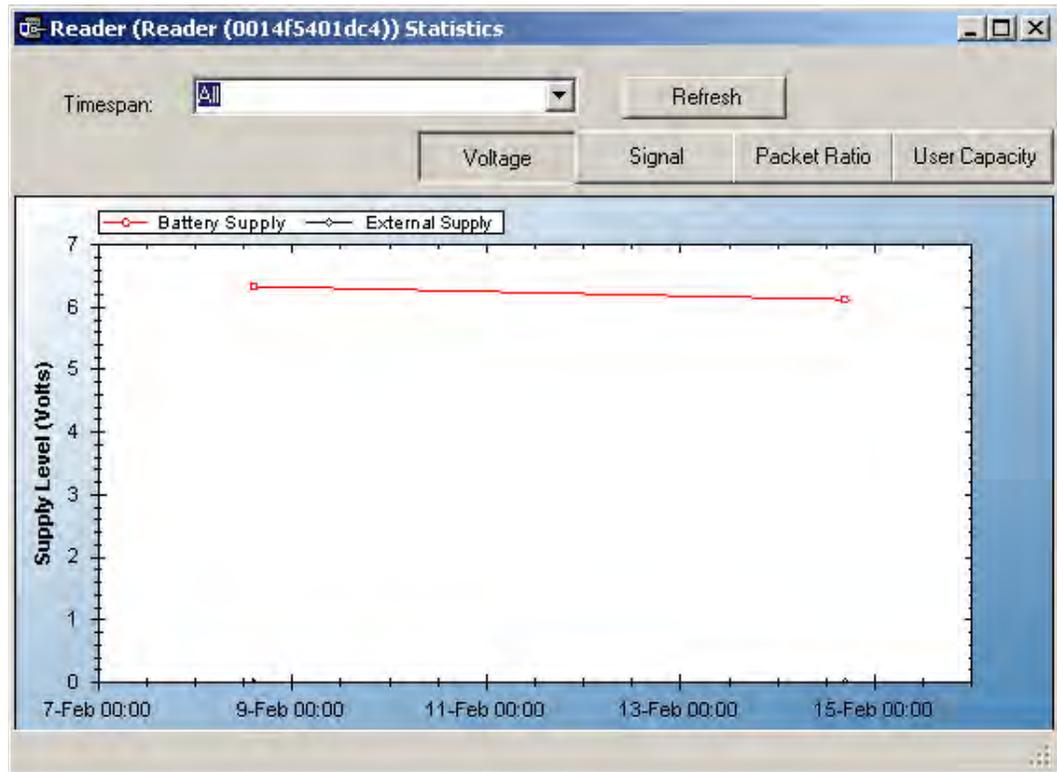
To view individual reader performance:

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

## Voltage Tab

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

Figure 140 Reader Statistics Voltage Tab



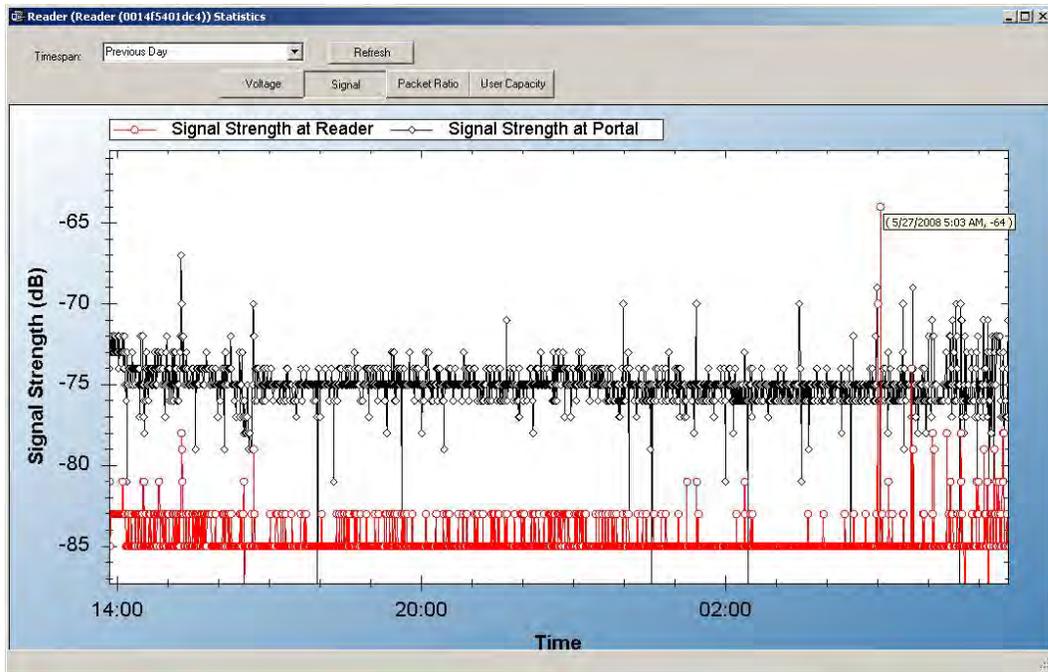
Every minute, the reader sends a beacon to the Portal Gateway with signal strength, battery voltage, external supply voltage and packet transfer ratio information. These statistics are stored at the rate defined by the Statistics Update Interval.

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

## Signal Tab

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

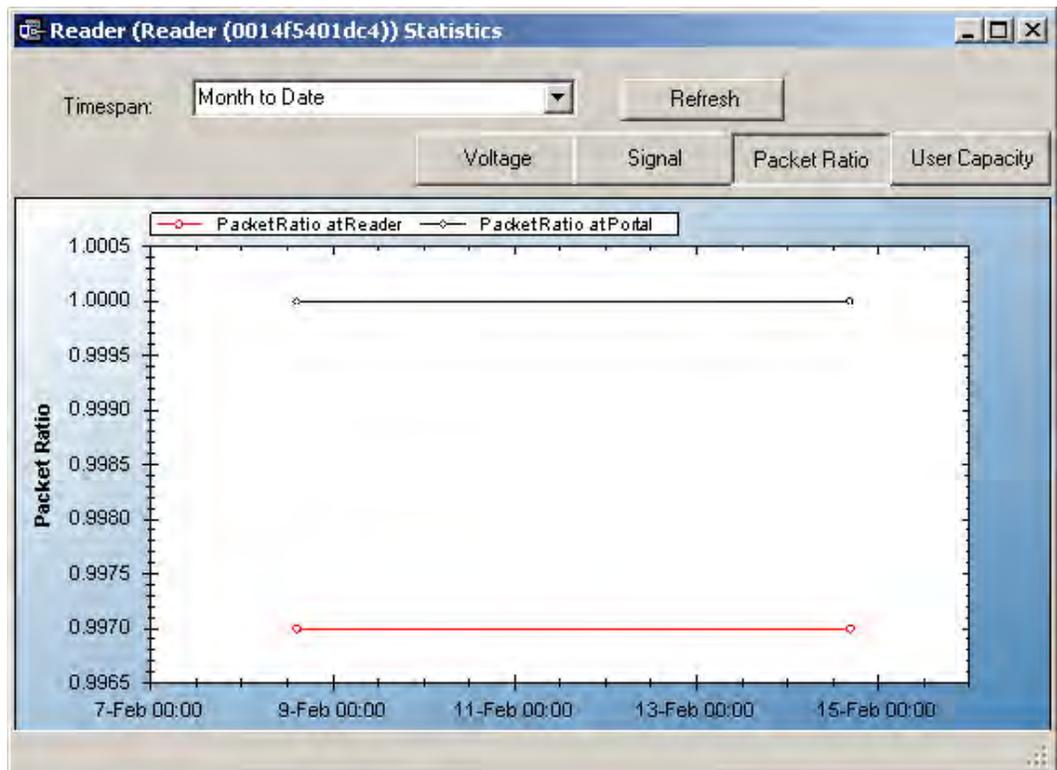
Figure 141 Reader Statistics Signal Tab



## Packet Ratio Tab

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

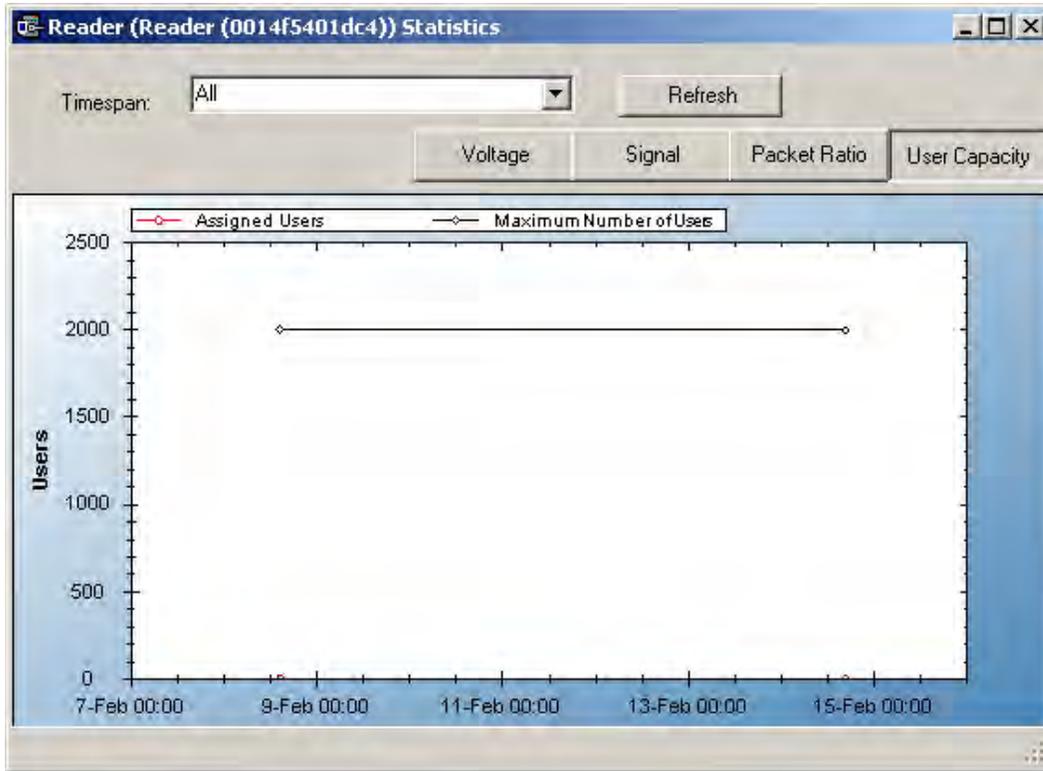
Figure 142 Reader Statistics Packet Ratio Tab



## User Capacity

This chart shows the Max allowable users for this reader and the current use. If you find that the use is nearing capacity, you may want to consider upgrading the reader capacity. See "Segment Item Upgrades" on page 162.

Figure 143 Reader Statistics User Capacity Tab



## Portal Statistics

Portal Statistics display at the bottom of the Statistics Monitor. Select the top level in the Segment Tree to display all Portals in the system. See Figure 143.

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

Figure 144 Statistics Monitor Portal Properties

The screenshot shows the 'Statistics Monitor - Stanley Wi-Q Access Management Software' interface. The 'Segment' dropdown is set to 'Acme University'. The left pane shows a tree view with 'Acme University' expanded to 'Second Floor IT Close'. The right pane displays the following properties:

ID	
Installation Date	7/4/1776 12:00:00 AM
IP Address	192.168.1.200
MAC Address	0014F500135F
Portal Location	/Acme University/Indianapolis Campus/Administrati

Name	
Description	Second Floor IT Closet
Portal Name	Second Floor IT Closet

Configuration/Test	
Assigned to Channels	25, 26
Statistics Update Interval	1 Hours

Specifications	
Firmware Version	3.0.15.147
Model Number	12811
PAN ID	256
Serial Number	0014F500135F

Statistics	
Associated Readers	3 Readers
Last Report Time	2/16/2012 1:55:10 PM
Maximum Readers	64 Readers

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

User: Admin

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

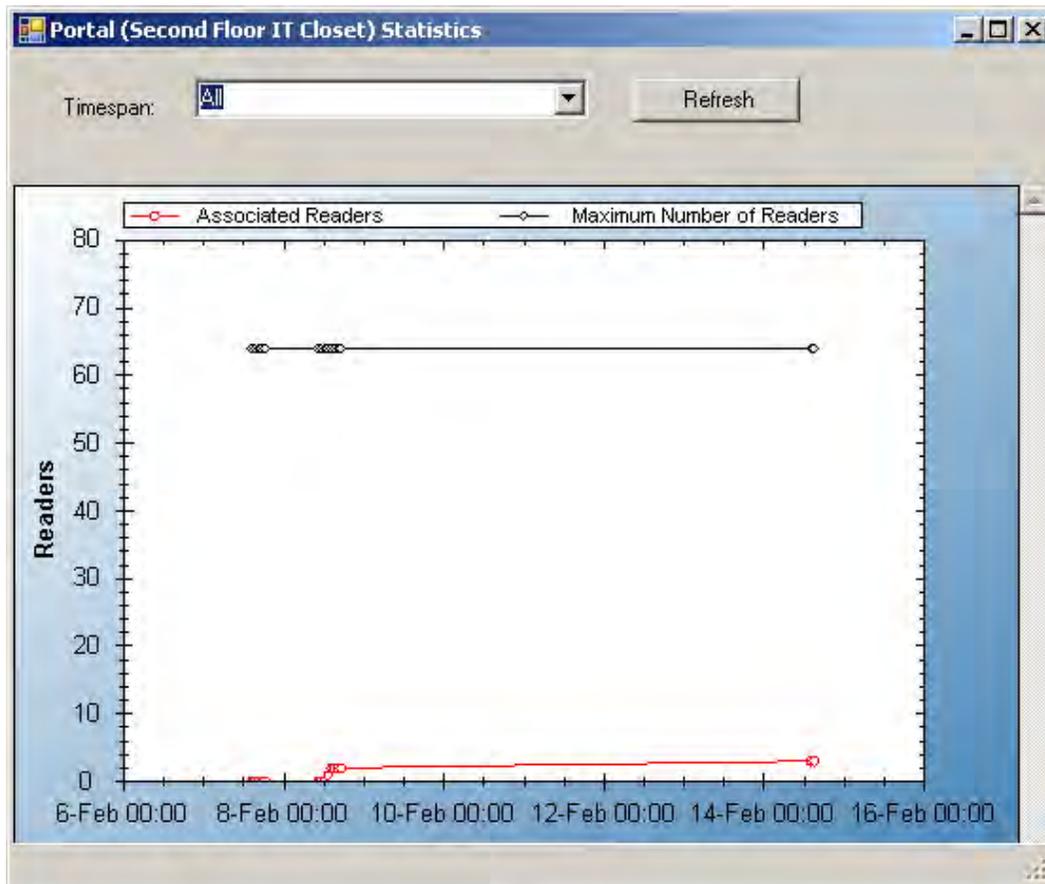
## Portal Diagnostics

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

### To review associated readers at Portals

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

Figure 145 Portal Statistics



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

## Configuration/Test

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

## Reports

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

### To Launch Wi-Q AMS Reports

- 1 Select Start>All Programs> Stanley Security Solutions >Stanley Wi-Q AMS> Wi-Q Reports.
- 2 Enter your Login and Password. Reports opens.

### Reports Overview

The software provides seven reports that you can modify:

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

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

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

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

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

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

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

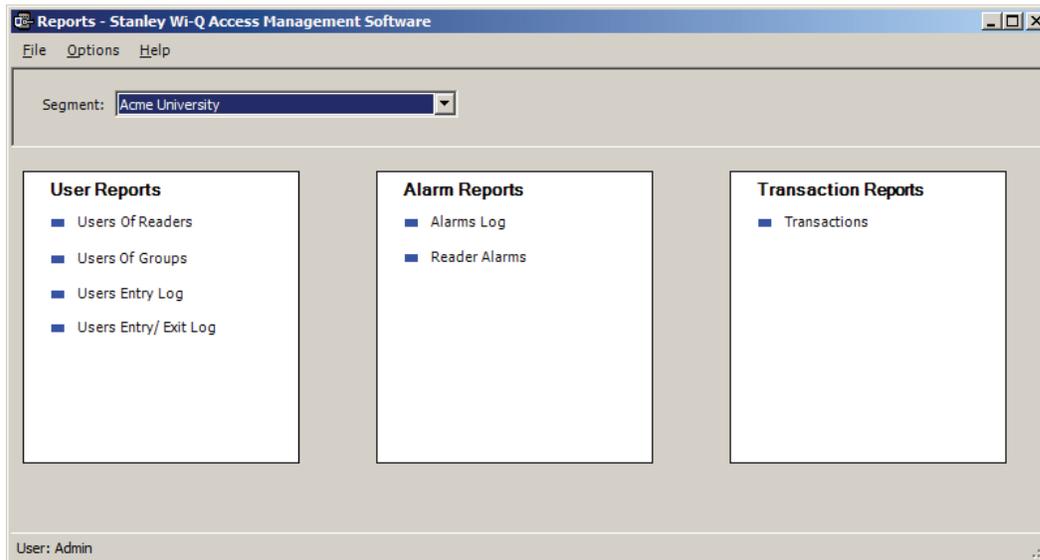
## Creating Reports

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

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

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

Figure 146 Reports

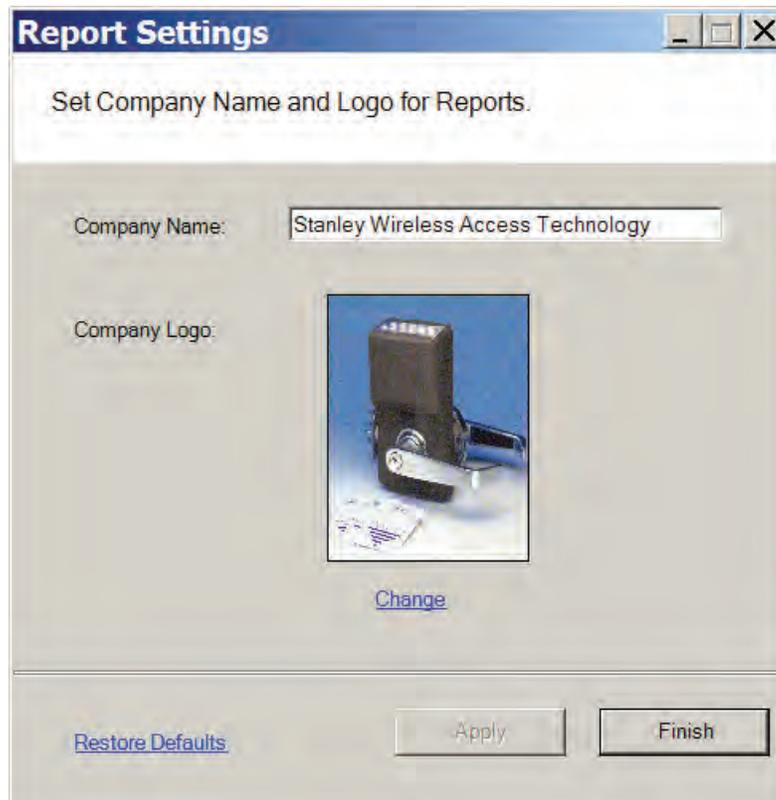


## Configure Report Settings

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

- 1 In the Segment box, select the Segment for which you wish to create the setting.
- 2 Select Options>Report Settings. The Set Company Name and Logo for Reports dialog box opens.

Figure 147 Setting up a company name for a report



- 3 In the Company Name field, type in the company name you wish to appear on your reports.
- 4 Under Company logo, click the Change link. Use the Select Logo browser to navigate to the file you wish to include.
- 5 Click Open. The file is now uploaded to the Reports settings.
- 6 Click Finish to save your settings and begin working with Reports.

## Generating a Report

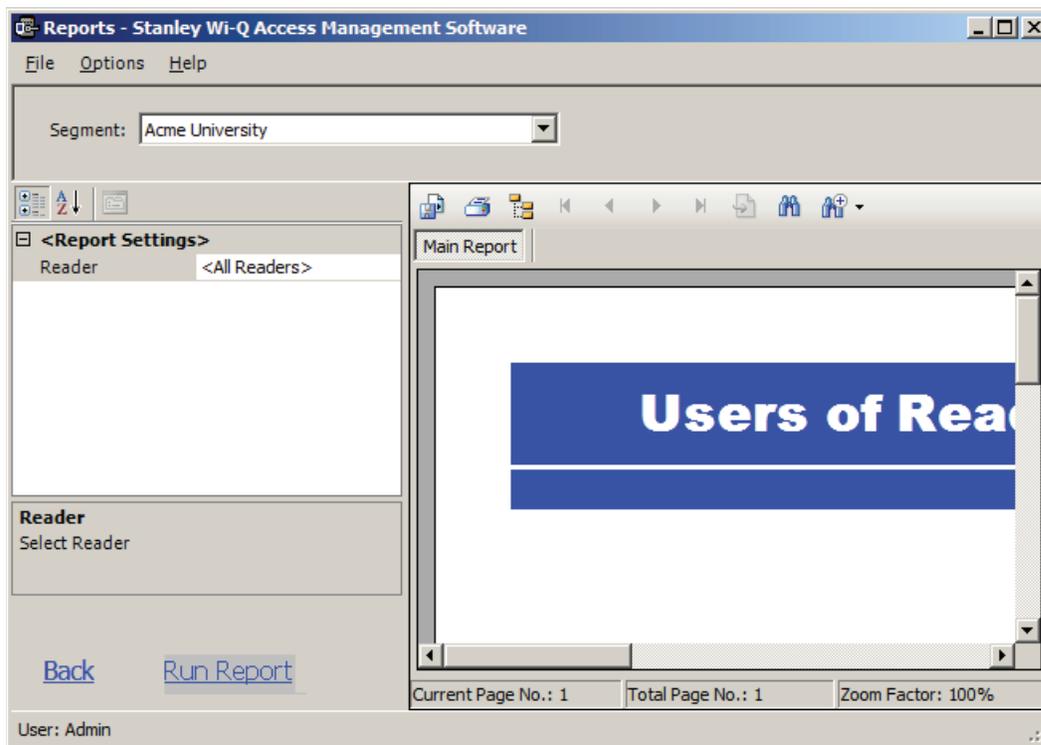
This section presents steps to create some example reports. Once you are familiar with the basic operations, you will be able to create your own reports using the selections available in Reports. First we'll look at a Users of Readers report with All Users selected. Then we'll look at a filtered report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

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

## To Generate a Report

- 1 In the Reports main screen, under the User Reports box, click on Users of Readers. Reports opens at the basic users of Readers Reports generator.
- 2 In the Segment box, select the Segment you wish to report on.
- 3 Available report settings are listed on the left, and the results are shown on the right. For this particular report, the default will be <All Readers>.

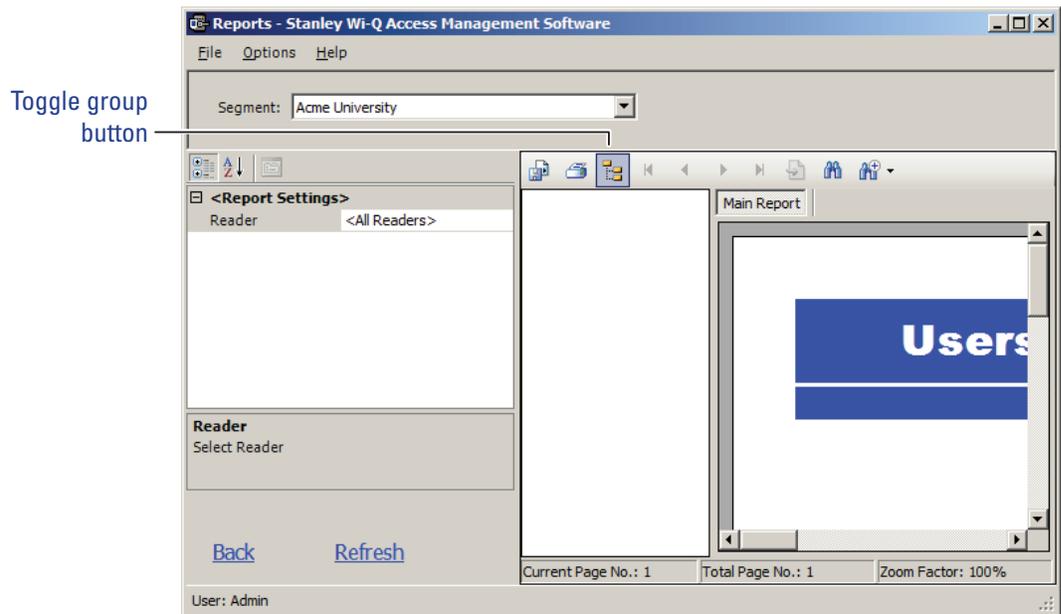
Figure 148 Viewing System Reports



- 4 Use the scroll bars to view the data, use menu icons to export, print, scroll through multi-paged reports, or use the Zoom tools to get a closer look.
- 5 If you have a large number of readers, Click the Toggle Group Tree icon and

highlight a specific reader to jump to its section in the report.

Figure 149 Toggle Group



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

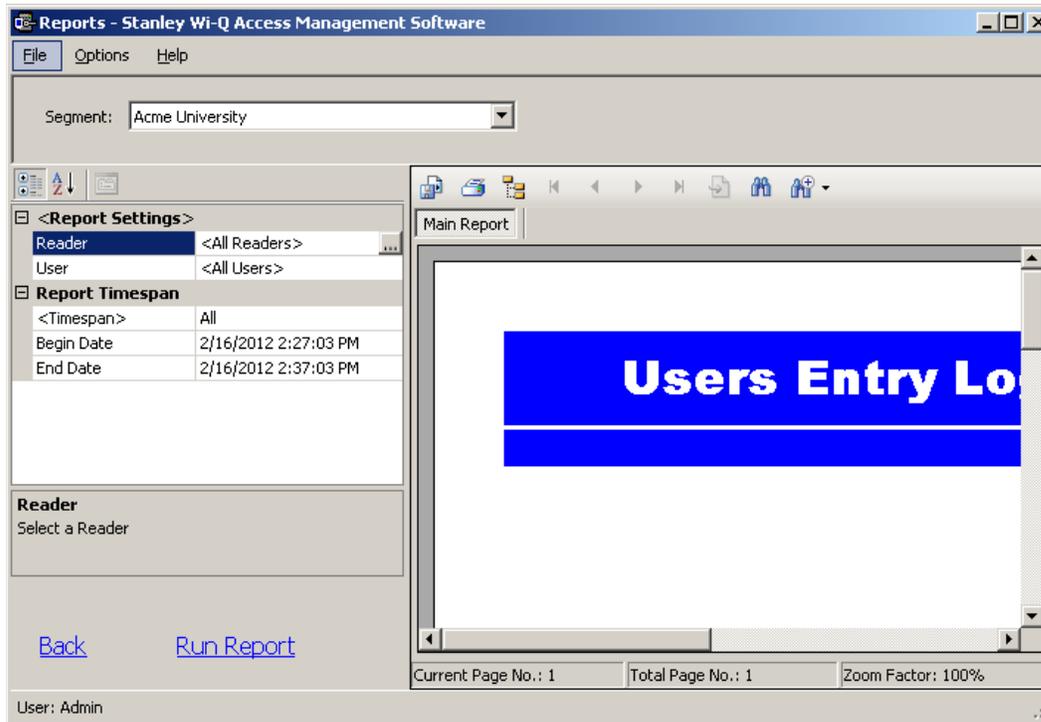
## Generating Filtered Reports

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

## To create filtered report

- 1 In the Reports main screen, select the Segment you wish to report on.
- 2 Under the User Reports box, click on Users Entry Log. The report opens (Figure 155). In this report set up, more selections are available for this report than for the Users of Readers report, including Reader, User, and Report Timespans. You can use any or all of these selections to filter your report. Each report type will have different selections available depending on the data available for the report. The defaults are always All.

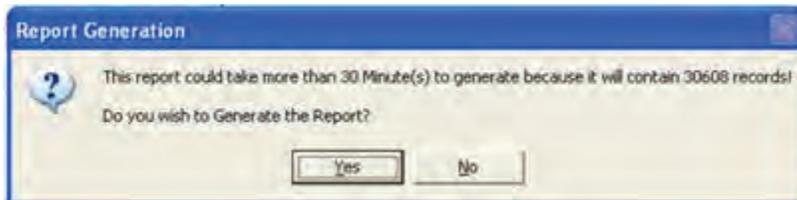
Figure 150 Users of Readers Report



- 3 To select a specific reader for this report, click on the Reader field's ellipsis button. The Select Reader dialog box opens.
- 4 Clear the All Readers box just below the drop-down list box.
- 5 Select the reader to filter from the drop-down list.
- 6 Click Finish. The report results will display data for only the reader you selected.

## Generating Larger Reports

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

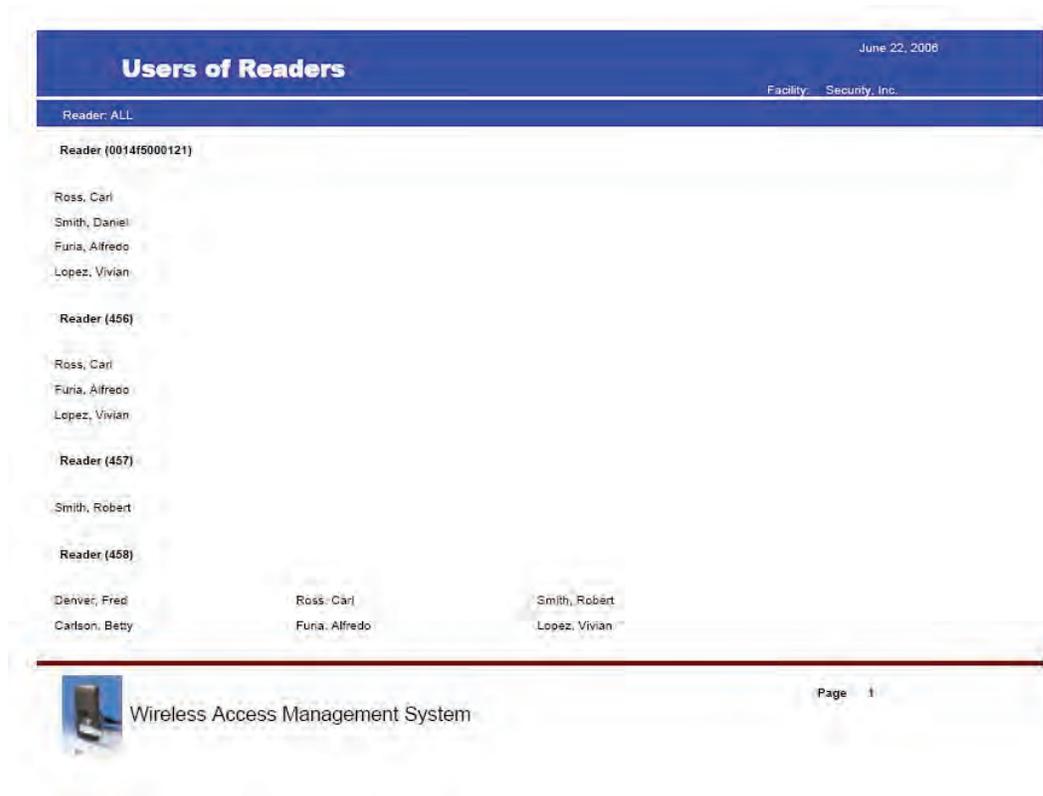


In the example, AMS detected that the defined report contains over 30,000 records and will take more than 30 minutes to generate. If this is acceptable, simply select Yes and the report will be generated. Select No if this is an inconvenient time to generate the report, or review your report definitions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

## Printing and Exporting Reports

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

Figure 151 Sample report file



### To print a report

- 1 Create the report using the features described in the previous sections.
- 2 Click the Printer icon in the menu bar.
- 3 Navigate to the printer you wish to use.
- 4 Print using the appropriate actions for the chosen printer.

### **To export a report**

- 1 Create the report using the features described in the previous sections.
- 2 In the menu bar, click the Export Report option.
- 3 In the Export Report dialog box, select a format type from the drop-down list.  
The available types are:
  - Crystal Reports (\*.rpt)
  - Adobe Acrobat (\*.pdf)
  - Microsoft Excel (\*.xls)
  - Microsoft Excel Data Only (\*.xls)
  - Microsoft Word (\*.doc)
  - Rich Text Format (\*.rtf)
- 4 Navigate to the location you wish to export to.
- 5 Enter a filename for the file.
- 6 Click Save.

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

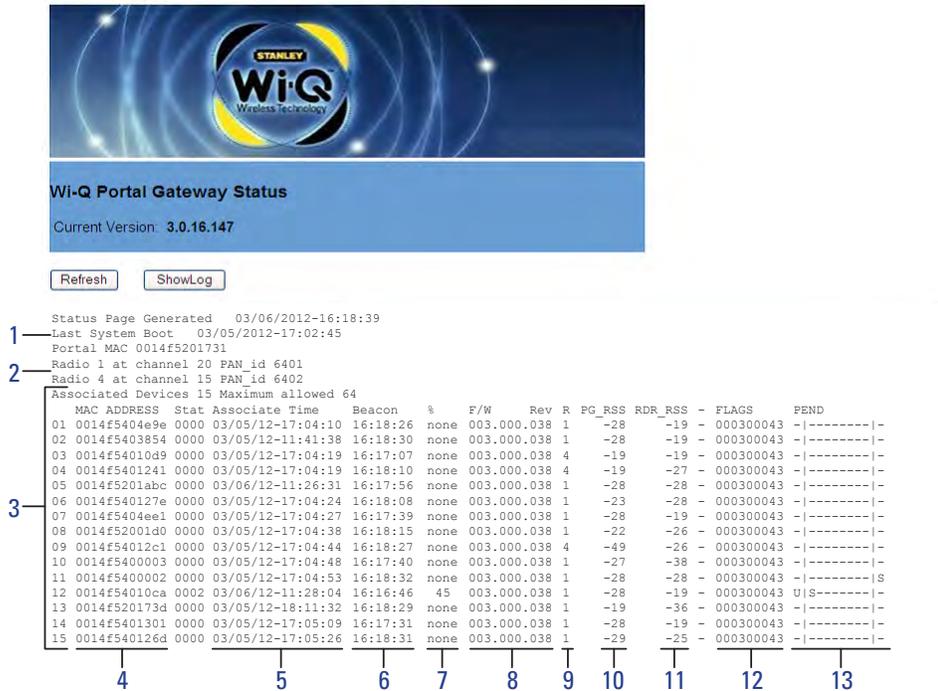
## 7 Advanced Troubleshooting

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 two ways:

- Inside the Portal Configuration Module, select Scan. Locate the desired Portal in the list and click on its hyperlink. See Figure 43 on page 68.
- Type your desired Portal's IP address directly into your internet browser.

Your browser will display the status of your Portal Gateway and associated devices. See Figure 157.

Figure 157 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 157, item 12).

**Note** The typical Wi-Q and Omnilock device status code is 00030043. This is the example used in the chart below.

Bit		Portal Gateway Status Flag	Definition	
Right END	<b>3</b> 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.	
	<b>4</b> 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	<i>NOT USED</i>		
<b>0</b>	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	<i>NOT USED</i>		
	Bit 10	<i>NOT USED</i>		
	Bit 11	<i>NOT USED</i>		
	<b>0</b> Bit 12	<i>NOT USED</i>		
	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.	
	<b>3</b>	<b>Bit 16</b>	CONTROLLER_REPORT_TIME_UPDATED	Set during association and when report time is updated
		<b>Bit 17</b>	CONTROLLER_LIF_IS_VALID	Set when a LIF beacon is received
Left END	Bit 18-31	<i>NOT USED</i>		

## Update Flags in the PEND Column

Figure 158 is a section of the Associated Devices listed in Figure 157. 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 158 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 -|-----|

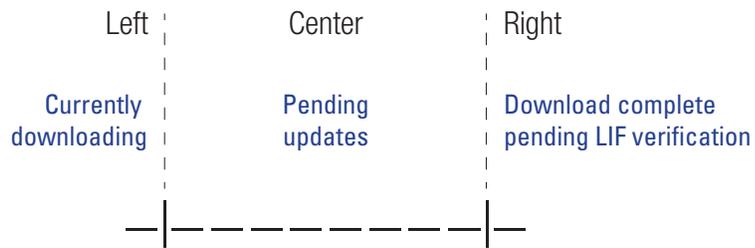
11 0014f5400002 0000 03/05/12-17:04:53 16:18:32 none 003.000.038 1 -28 -28 - 000300043 -|-----|S
12 0014f54010ca 0002 03/06/12-11:28:04 16:16:46 45 003.000.038 1 -28 -19 - 000300043 U|S-----|
13 0014f520173d 0000 03/05/12-18:11:32 16:18:29 none 003.000.038 1 -19 -36 - 000300043 -|-----|
14 0014f5401301 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.

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

Figure 159 shows the significance of update flag placement between the dividing lines in each entry of the PEND column.

Figure 159 Update Flag Placement in PEND Column



Item 11 in Figure 158 shows that the Controller's Segment download is complete pending LIF verification.

Item 12 in Figure 158 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.

# A Glossary

<b>10Base-T</b>	The most common Ethernet wiring standard.
<b>access level</b>	An access control relationship made between a controller or controllers and a time zone or time zones. An access level is assigned to a badge ID for the purpose of granting access through a controller or controllers during a specified time.
<b>access panel</b>	A circuit board with on-board memory that is responsible for making most of the decisions in an access control system.
<b>activation/deactivation date</b>	The date that a credential becomes active or expires.
<b>antipassback</b>	A configuration limiting the ability of consecutive uses for a credential at a reader. Usually, configured with readers installed on both the secure and non-secure side of an opening. Once a credential has been used in a reader to gain access on one side of the opening, the credential cannot be used in the same reader until the credential is used to gain access to a reader from

	the opposite side of the opening.
<b>APB exempt</b>	Antipassback exempt. The cardholder with this privilege is exempt from antipassback rules.
<b>badge</b>	The credential or token that carries a cardholder's data.
<b>badge ID</b>	Part of the access control information that is encoded to a token. This information, usually numerical, is unique to a particular credential holder.
<b>card format</b>	The way that data is arranged and ordered on the card.
<b>cardholder</b>	An individual who is issued a particular credential.
<b>chassis type</b>	The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.
<b>common door</b>	A configuration setting that allows for the allocation of duplicate badge ID ranges in separate offline locks.
<b>communication port</b>	The connector on the bottom of a Lock that allows the lock to be connected to a reader.
<b>communication server</b>	The server application designed to provide network services to access panels, controllers, PCs and PDAs.
<b>credential</b>	A physical token, usually a card or fob, encoded with access control information.
<b>cylindrical</b>	Lock chassis that installs into a circular bore in the door.
<b>deadbolt override</b>	The ability for an authorized credential to retract both the spring latch and the deadbolt when the deadbolt is engaged
<b>directional antenna</b>	An antenna type optimized to focus signal from point-to-point over longer distances and through obstacles.

<b>dual access</b>	The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening.
<b>ethernet</b>	The most common networking standard in the world, formally known as IEEE 802.3.
<b>exit hardware</b>	Lock chassis type that supports exit hardware trim lock.
<b>extended unlock</b>	The extra period of time the lock will unlock when an authorized credential with extended unlock privileges is presented.
<b>guest</b>	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.
<b>Host</b>	The computer on which Wi-Q AMS software is installed and set up to manage Portal Gateways and readers on the network.
<b>IP address</b>	The numeric address (like 192.168.1.1) that identifies each device in a TCP/IP network.
<b>input</b>	A hardware connection point used for status reporting of a particular sensor.
<b>intelligent system controller (ISC)</b>	See access panel.
<b>I/O device</b>	A device, such as an alarm or parking gate that can be configured to operate on the network using a Wireless Access Controller.
<b>issue code</b>	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.
<b>MAC address</b>	The Media Access Control number (MAC). A unique, 12-digit number assigned by the

	manufacturer of a network device.
<b>mortise</b>	A lock chassis that installs into a mortised cavity in the edge of a door.
<b>omni-directional antenna</b>	An antenna type optimized to provide signal coverage in all directions.
<b>packet</b>	A discrete chunk of data, being transferred on a TCP/IP or other addressable network.
<b>passage mode</b>	The ability to double present an authorized credential within the strike time to unlock an opening. The lock is returned to its original status by a second, double presentation of an authorized credential.
<b>portal gateway</b>	The Portal Gateway is a wireless device connected to the Host computer through a secure connection to transfer data signals from Wireless Controller locks to and from the Host computer.
<b>request to exit</b>	A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation.
<b>segment code</b>	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.
<b>sign-on key</b>	Number generated within AMS to establish the connection between the readers and the Portals, and ultimately to a segment in the software.
<b>site survey kit</b>	The Wi-Q Technology Site Survey Kit tool used to determine optimum Portal Gateway location to verify signal strength before permanently installing the hardware.
<b>time interval</b>	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.

<b>time zone</b>	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.
<b>unlock duration</b>	The time that the lock momentarily unlocks.
<b>use limit</b>	A configuration limiting a credential to a defined number of uses.
<b>Web Interface</b>	The software program that allows setup and communication between the Portal Gateway and the Host Computer.
<b>Wi-Q Technology</b>	Provides efficient, online access control decisions at the door.
<b>Wireless Access Controller</b>	Wireless Access Controller provides additional capability to connect stand-alone controllers and locks.

**wireless reader lock**

The wireless reader lock controls user access at the door and grants user requests according to how they are configured in the software.

# **B Lock installation**



# Installation Instructions for Wi-Q™ Technology 9KQ Cylindrical Locks

## Planning the installation

### Contents

These installation instructions describe how to install your 93KQ Cylindrical Lock. Topics covered include:

<i>Planning the installation</i> .....	1
<i>Preparing the door and door jamb</i> .....	2
<i>Installing the lock</i> .....	7
<i>Completing the installation</i> .....	13

Patents

Products covered by one or more of the following patents:  
5,590,555 5,794,472 5,083,122 6,720,861

### Site survey

Use the following survey to record information about the installation site. You need this information to determine how to prepare the door for the lock.

### Door information

Door handing and bevel:

- Left hand (LH)
- Left hand, reverse bevel (LHRB)
- Right hand (RH)
- Right hand, reverse bevel (RHRB)

Door thickness: \_\_\_\_\_ inches (1 3/4" to 2 1/4")

### Environment information

Ambient temperature:

- Is within specifications. See the tables below.

This product meets the following Locked Door Outdoor test requirements for ANSI/BHMA 156.25:

Side of door	Range
Outside	-31°F to +151°F (-35°C to +66°C)

This product meets the following Full Indoor test requirements for ANSI/BHMA 156.25:

Side of door	Range
Inside and outside	+32°F to +120°F (0°C to +49°C)

### Components checklist

Use the following checklist to make sure that you have the items necessary to install your Electronic Wireless Cylindrical Lock.

#### Components provided in the box:

- Chassis with outside lever and outside rose liner assembly
- Top and bottom inside covers
- Fire plate
- Battery holder with batteries
- Inside rose liner
- Outside escutcheon assembly
- Inside lever
- Throw member package
- Latch
- Hub washers
- Trim hole insert package
- Plastic bushing package
- Escutcheon screw package
- Door status switch assembly
- Strike package
- Bar code ID sticker (for your records)
- Installation template and instructions

#### Other components:

- Core and control key
- Temporary operator card

### Special tools checklist

Use the following checklist to make sure that you have the special tools necessary to install your Electronic Wireless Cylindrical Lock.

- KD303 Drill jig
- T20 TORX® bit driver
- KD325 Strike plate locating pin
- KD315 Faceplate marking chisel

## Preparing the door and door jamb

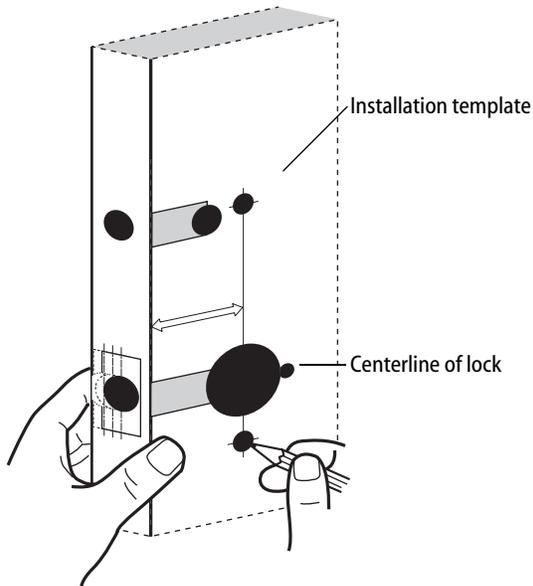


Figure 1 Positioning the template

### 1 Position template and mark drill points

*Note: If the door is a fabricated hollow metal door, determine whether it is properly reinforced to support the lock. If door reinforcement is not adequate, consult the door manufacturer for information on proper reinforcement. For dimensions for preparing metal doors, see the Q01 and G02 Templates—Installation Specifications for 93KQ Cylindrical Locks.*

*Note: If the door is a LH or RH door, mark the inside of the door. If the door is a LHRB or RHRB door, mark the outside of the door.*

#### For uncut doors and frames

- 1 Measure and mark the horizontal centerline of the lever (the centerline for the chassis hole) on the door and door jamb. Mark the vertical centerline of the door edge.

*Note: The recommended height from the floor to the centerline of the crossbore or chassis hole is 38".*

- 2 Fold the *Q05 Template—Installation Template for 93KQ Cylindrical Locks* on the dashed line and carefully place it in position on the high side of the door bevel.

*Note: For steel frame applications, align the template's horizontal centerline for the latch with the horizontal centerline of the frame's strike preparation.*

- 3 Tape the template to the door.
- 4 Center punch the necessary drill points. Refer to the instructions on the template.

#### For doors with standard cylindrical preparation

- 1 Fold the *Q05 Template—Installation Template for 93KQ Cylindrical Locks* on the dashed line. Looking through the hole from the opposite side of the door, align the template so that you see the template outline of the 2 1/8" diameter chassis hole.
- 2 Tape the template to the door.
- 3 Center punch the necessary drill points. Refer to the instructions on the template.

## Preparing the door and door jamb

### 2 Drill holes and mortise for latch face

- 1 Drill the holes listed below:
  - upper and lower trim holes
    - ◆ 5/8" diameter
    - ◆ through door
  - harness hole
    - ◆ 3/4" diameter
    - ◆ through door
  - motor wire hole
    - ◆ 7/16" diameter
    - ◆ through door
    - ◆ before drilling chassis hole
  - chassis hole
    - ◆ 2 1/8" diameter
    - ◆ through door
    - ◆ after drilling motor wire hole
  - latch hole
    - ◆ 1" diameter
    - ◆ meets chassis hole
  - door status switch hole
    - ◆ 1" diameter
    - ◆ meets harness hole
  - anti-rotational hole, see "Use drill jig to drill through-bolt holes" on page 5.
    - ◆ 5/16" diameter
    - ◆ through door

**Note 1:** To locate the center of a hole on the opposite side of the door, drill a pilot hole completely through the door.

**Note 2:** For holes through the door, it is best to drill halfway from each side of the door to prevent the door from splintering.

- 2 Mortise the edge of the door to fit the latch face.
- 3 Drill the holes for the screws used to install the latch.

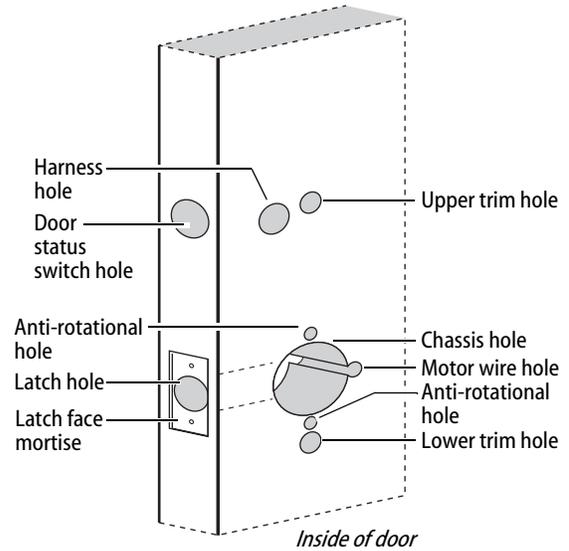


Figure 2 Drilling holes and mortising for the latch face

## Preparing the door and door jamb

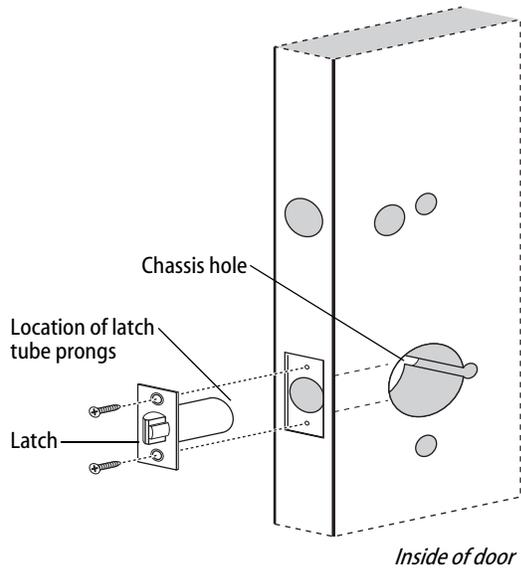


Figure 3 Installing the latch in the door

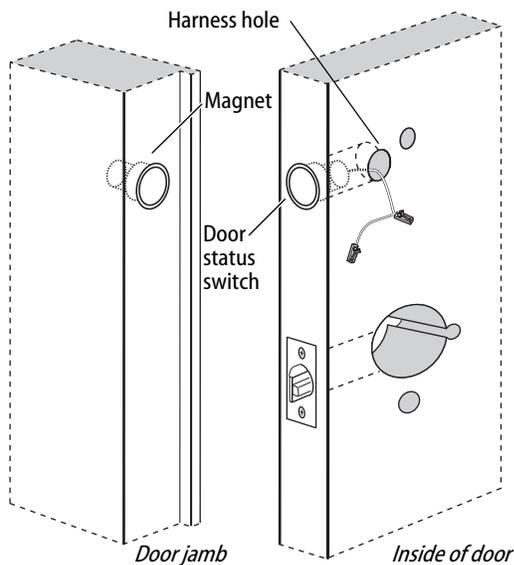


Figure 4 Installing the door status switch and magnet

### 3 Install latch

- 1 Install the latch in the door.  
*Note: The latch tube prongs should be centered and should project into the chassis hole.*
- 2 Check that the door swings freely.

### 4 Install door status switch and magnet

- 1 On the door jamb, mark the drill point for the 1" diameter magnet hole. This hole should be directly opposite the door status switch reader harness hole when the door is closed.
- 2 Drill a 1" diameter hole for the magnet, at least 1 3/4" deep.
- 3 Insert the magnet in the hole.
- 4 Insert the door status switch assembly into the door status switch hole in the edge of the door, feeding the connectors out the harness hole to the inside of the door, as shown in Figure 4.

## Preparing the door and door jamb

### 5 Use drill jig to drill through-bolt holes

- 1 Press the drill jig (KD303) onto the door, engaging it with the latch tube prongs (see the close-up in Figure 5). Make sure the front edge of the jig is parallel with the door edge.
- 2 Drill the through-bolt holes (5/16" diameter) halfway into the door.
- 3 Turn over the drill jig and repeat steps 1 and 2 from the opposite side of the door.

*Note: Replace the drill jig after 10 door preparations.*

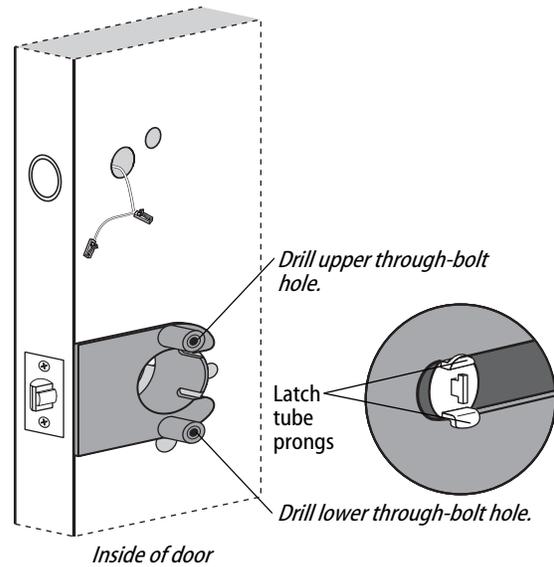


Figure 5 Installing the drill jig and drilling the through-bolt holes

## Preparing the door and door jamb

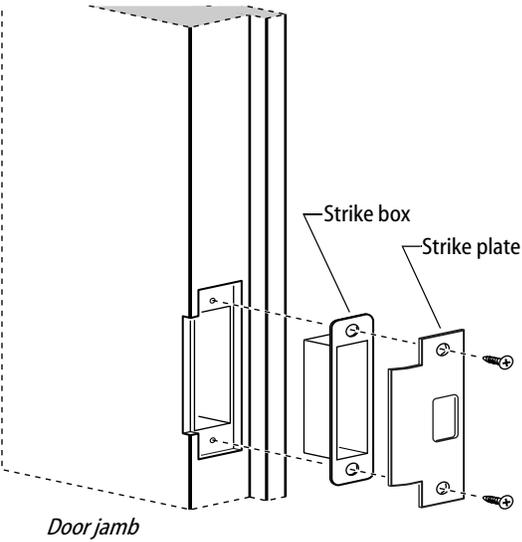


Figure 6a Installing the strike box and strike plate

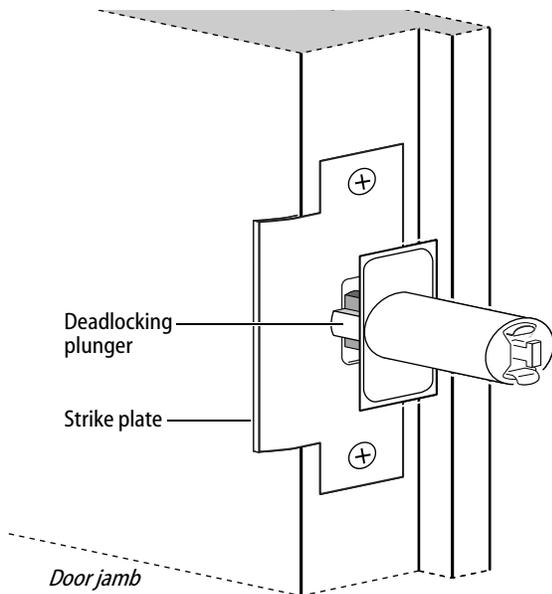


Figure 6b Aligning the deadlocking plunger with the strike plate

### 6 Install strike box and strike plate

- 1 In alignment with the center of the latchbolt, mortise the door jamb to fit the strike box and strike plate.
- 2 Drill the holes for the screws used to install the strike box and strike plate.
- 3 Insert the strike box and secure the strike with the two screws provided.
- 4 Check the position of the deadlocking plunger against the strike plate.

**Caution:** The deadlocking plunger of the latchbolt must make contact with the strike plate, as shown in Figure 6b. The plunger deadlocks the latchbolt and helps prevent someone from forcing the latch open when the door is closed.

## Installing the lock

### 7 Remove outside lever or knob

- 1 Insert the control key into the core and rotate the key 15 degrees to the right.
- 2 Insert a flat blade screwdriver into the figure-8 core hole and into the lever.
- 3 Press the screwdriver blade in the direction of the arrow in Figure 7.

*Note: You cannot remove the lever if the screwdriver blade is inserted too far past the keeper.*

- 4 Slide the lever or knob off of the sleeve.

**Caution: Be careful that you do not disconnect the lever keeper spring.**

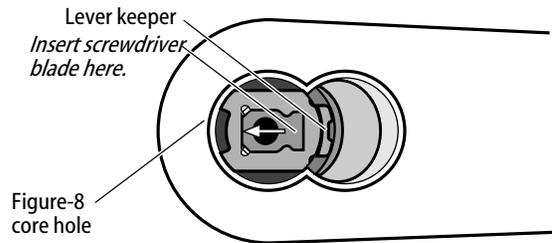


Figure 7 Removing the outside lever

### 8 Adjust for door thickness

- 1 Determine the door's thickness.
- 2 Pull the rose locking pin and rotate the outside rose liner until the proper groove on the through-bolt stud lines up with the hub face.

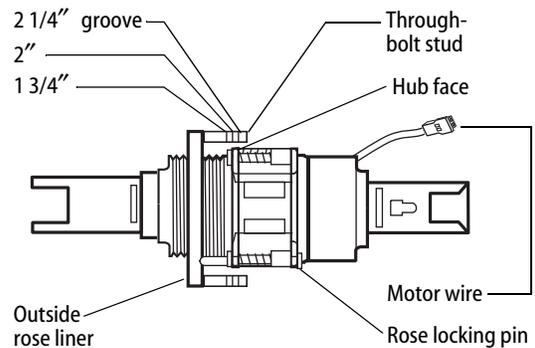


Figure 8 Adjusting the rose liner for the door thickness

## Installing the lock

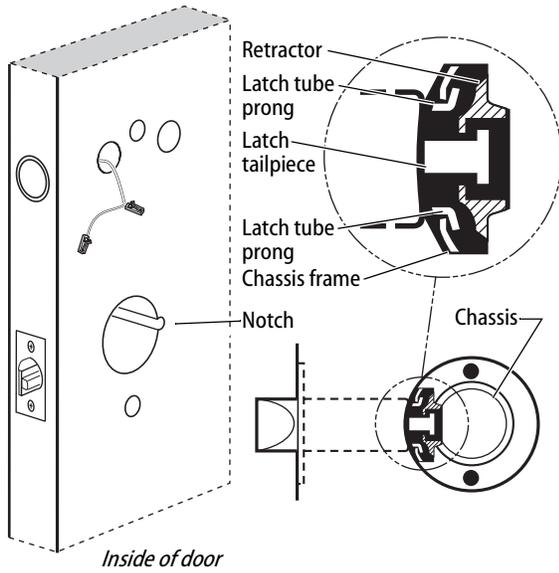


Figure 9 Installing the lock chassis and engaging the retractor in the latch

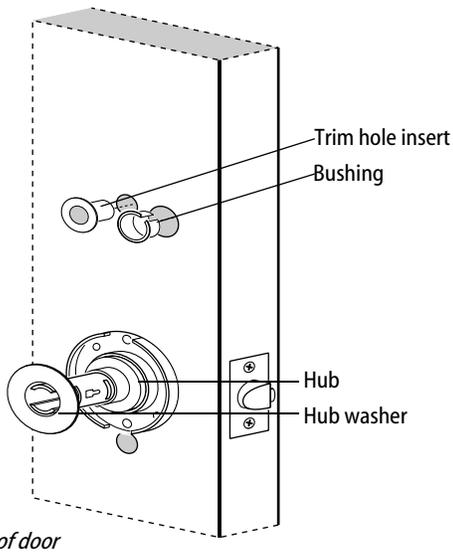


Figure 10 Installing the outside trim hole insert, bushing, and hub washer

### 9 Install lock chassis and engage retractor in latch

From the outside of the door, insert the lock chassis into the 2 1/8" chassis hole, routing the motor wire through the notch.

**Caution:** Make sure that the latch tube prongs engage the chassis frame and that the latch tailpiece engages the retractor.

### 10 Install the trim hole insert, bushing, and hub washer on outside of door

- 1 On the outside of the door, insert the trim hole insert into the upper trim hole, as shown in Figure 10.
- 2 Insert the bushing into the harness hole.
- 3 Slide a hub washer over the chassis sleeve so it rests on the hub.

## Installing the lock

### 11 Install fire plate

Position the fire plate on the inside of the door so that the chassis fits through the square opening in the fire plate, as shown in Figure 11.

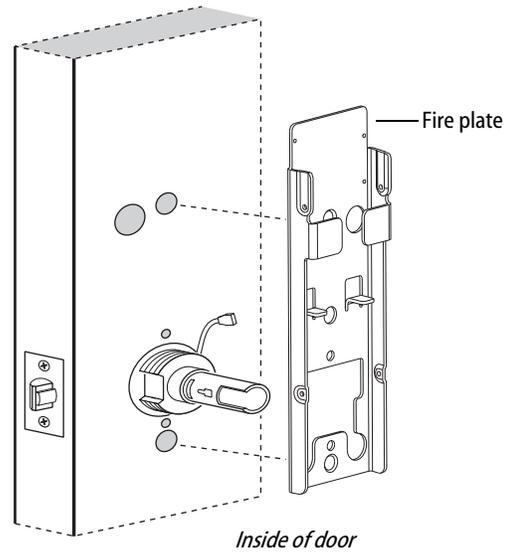


Figure 11 Installing the fire plate

### 12 Install through-bolts and inside rose liner

- 1 Place the inside rose liner on the chassis, aligning the holes in the rose liner with the holes prepared in the door, as shown in Figure 12.

**Caution: Make sure that the motor wire is pulled toward the top of the fire plate and avoid routing it over any surface that could damage the sleeving or wire insulation.**

- 2 Install the through-bolts through the rose liner and door in the top and bottom holes.

**Caution: Make sure that there is clearance for the motor wire between the rose liner and the door.**

- 3 Tighten the rose liner to the door and fire plate with the through-bolts.
- 4 Install the hub washer over the rose liner.

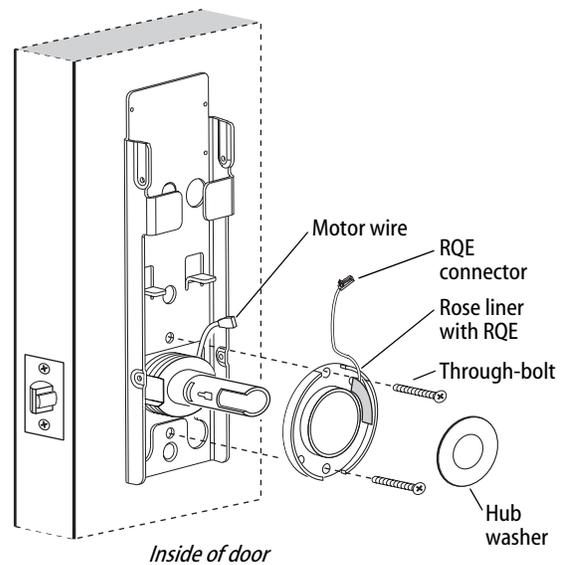


Figure 12 Installing the through-bolts and rose liner (9K shown)

## Installing the lock

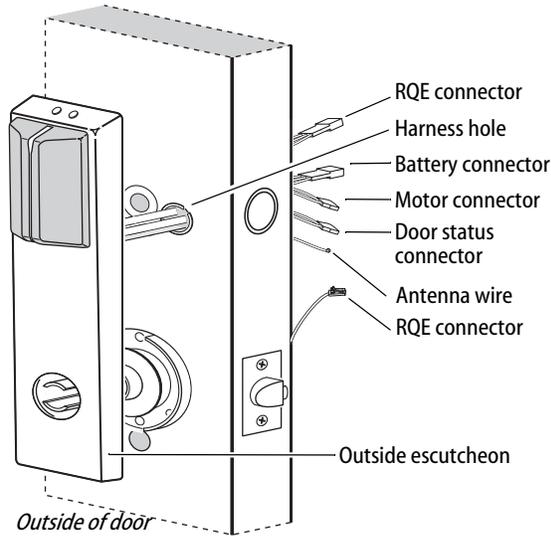


Figure 13 Feeding the wire harness connectors through the harness hole

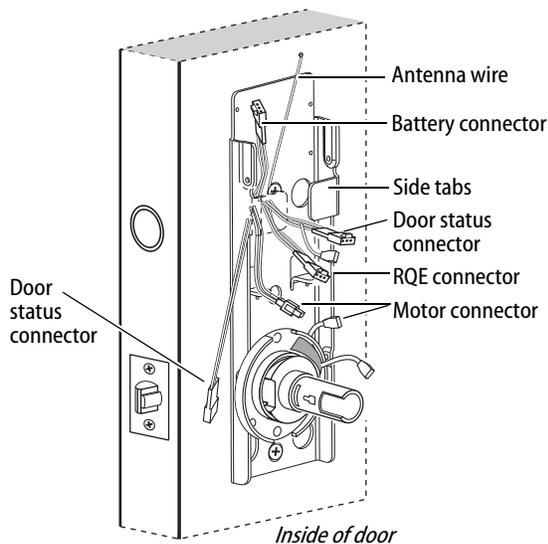


Figure 14 Routing the wires on the fire plate

### 13 Route wire harness and position outside escutcheon

- 1 From the outside of the door, feed the motor connector, battery connector, door status switch, and antenna wire, through the harness hole.

**Caution:** When routing the connectors, make sure the wire harness is not routed across any sharp edges or over any surface that could damage its sleeving or wire insulation.

- 2 On the inside of the door, insert the two countersunk mounting screws into the holes at the top and bottom of the fire plate.
- 3 Tighten the mounting screws until the fire plate is securely mounted to the door.

### 14 Route wires on fire plate

- 1 Route the motor connector wire, RQE connector, and door status connector underneath the side tabs as shown in Figure 14.
- 2 Route the battery connector and antenna wire above the side tabs. See Figure 15 for additional detail.

## Installing the lock

### 15 Connect motor wires, RQE, and door status switch

1 From the inside of the door, make the following connections:

- ◆ Motor
- ◆ RQE
- ◆ Door status switch

Wire connection	Color	No. of wires	No. of pins
Motor	Yellow-Gray	2	2
RQE	Orange-Brown	2	3
Door status	White	2	2

2 Insert the plastic wire tie through the mounting clip and secure the wires as shown in Figure 15. See Figure 15 for additional detail.

**Caution: When making the motor connection, make sure:**

- ◆ there are no loose wire connections where the wires are inserted into the connectors
- ◆ the connectors are firmly mated.

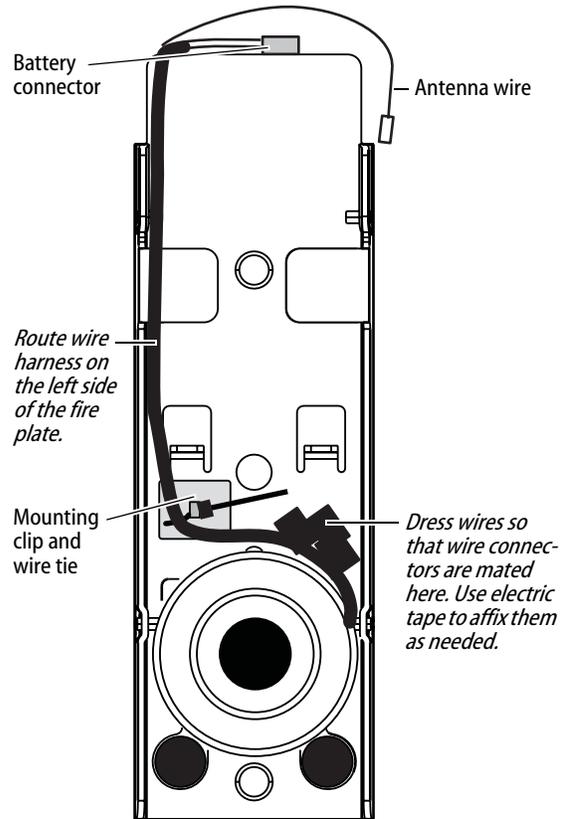


Figure 15 Routing the wires (view of the inside escutcheon)

## Installing the lock

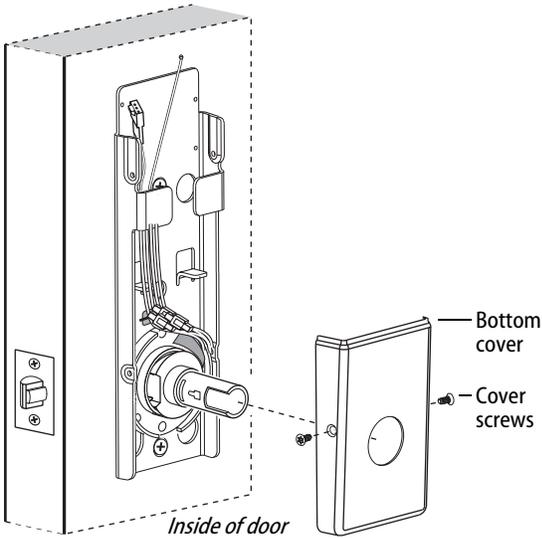


Figure 16 Installing the bottom cover

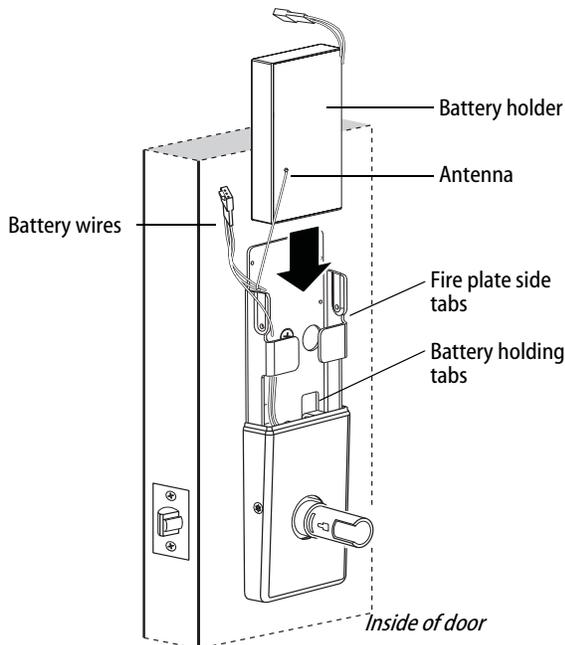


Figure 17 Installing the battery holder, eight-cell

### 16 Install bottom cover (inside escutcheon)

- 1 **Making sure that the cover does not pinch the wires**, guide the bottom cover over the chassis onto the fire plate.
- 2 Use two cover screws to secure the cover to the side of the fire plate, as shown in Figure 16.

*Note: Phillips Type 2 and T20 Torx options are available for the cover mounting screws.*

**Caution: Dress all wires away from possible pinch points before putting the bottom cover in place.**

### 17 Install battery holder

- 1 Position the battery wires against the fire plate side wall, as shown in Figure 17.
- 2 Slide the battery holder behind the fire plate side tabs until it rests on the bent battery holding tabs.

**Caution: When routing the battery wires, make sure the wires are not routed across any sharp edges or over any surface that could damage their sleeving or wire insulation.**

- 3 Connect the battery holder to the battery connector on the wire harness.

**Caution: When connecting the battery holder, make sure:**

- ◆ there are no loose wire connections where the wires are inserted into the connectors.
- ◆ the connectors are firmly mated.

## Completing the installation

### 18 Install inside and outside levers

*Note: To use a core and throw member from a manufacturer other than BEST with a Electronic Stand-alone Lock, see the Installation Instructions for 9K Non-interchangeable Cores & Throw Members (T56093) and skip task 19.*

- With the handle pointing toward the door hinges, position a lever on the outside sleeve and push firmly on the lever until it is seated. Repeat, placing the other lever on the inside sleeve.

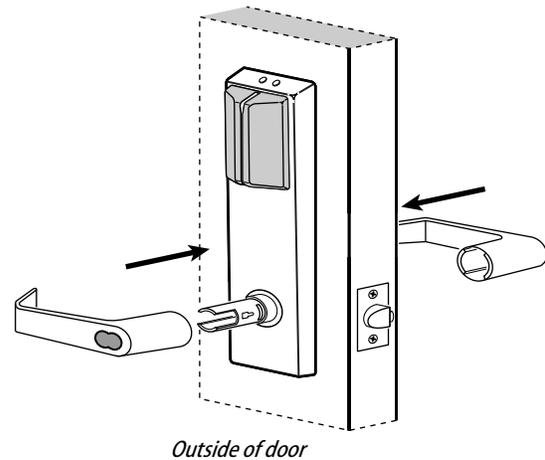


Figure 18 Installing the levers

### 19 Install core and throw member

- 1 Install the blocking plate onto the throw member.

**Caution: You must use the blocking plate to prevent unauthorized access.**

**For 6-pin core users only:** Install the plastic spacer (not shown, supplied with permanent cores) instead of the blocking plate, on the throw member.

- 2 Insert the control key into the core and rotate the key 15 degrees to the right.
- 3 Insert the throw member into the core.
- 4 Insert the core and throw member into the lever with the control key.
- 5 Rotate the control key 15 degrees to the left and withdraw the key.

**Caution: The control key can be used to remove cores and to access doors. Provide adequate security for the control key.**

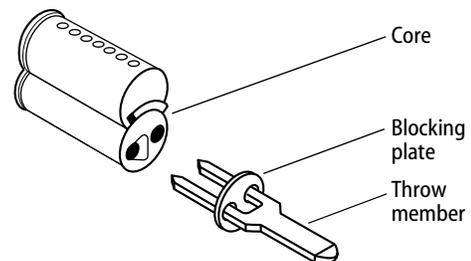


Figure 19a Installing the blocking plate and throw member

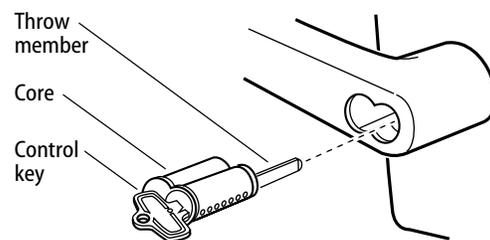


Figure 19b Installing the core

## Completing the installation

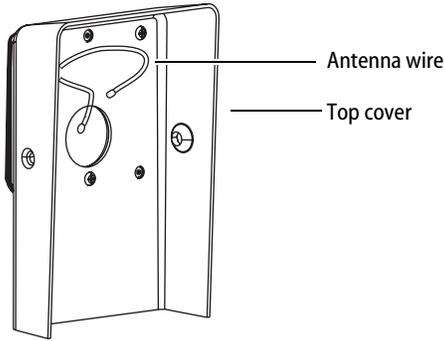


Figure 20a Inside view of top cover

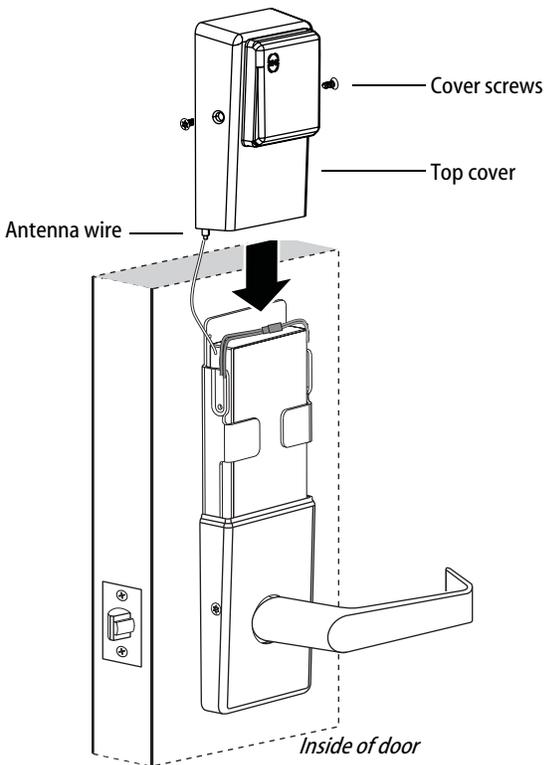


Figure 20b Installing the top cover

### 20 Install top cover (inside escutcheon)

- 1 Connect the antenna to its mating connector.
- 2 Place the top cover against the door and above the fire plate. Slide the top cover down toward the bottom cover as shown in Figure 20b.

**Caution:** As you slide the top cover onto the fire plate, feed the antenna wire down into the bottom cover. Be sure not to pinch the antenna wire on the bottom cover as you slide the top cover into place.

- 3 Use two cover screws to secure the cover to the side of the fire plate, as shown in Figure 20b.

*Note:* Phillips Type 2 and T20 Torx options are available for the cover mounting screws.

## Completing the installation

### 21 Test lock

#### For 9KQ Locks with keypad:

To test the lock for proper operation before the lock is programmed, follow these instructions:

- 1 Press **1234**.
- 2 Press #.  
The green light flashes and the locking mechanism unlocks.
- 3 Turn the lever and open the door.

#### For all other locks:

To test the lock for proper operation before the lock is programmed, use the temporary operator card that came with the lock. This card is for temporary use only. After permanent cards have been programmed for the lock, the temporary card should be deleted.

- 1 Use the temporary operator card to activate the lock.  
*Note: If the lock has a proximity card reader, it may have already been activated by the presence of an object near the card reader.*
- 2 Use the temporary operator card to access the lock.
- 3 The green light flashes and the locking mechanism unlocks.
- 4 Turn the lever or knob and open the door.
- 5 With the door closed, insert and turn the key to unlatch the door.

**If the mechanism doesn't unlock, refer to the following table.** For additional troubleshooting instructions, see the Service Manual.

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

© 2008–09 Stanley Security Solutions, Inc  
T82619/Rev B 3109013 ER-7991-12 Oct 2009

**BEST ACCESS SYSTEMS**  
a Product Group of Stanley Security Solutions, Inc.



# Installation Instructions for Wi-Q™ Technology 45HQ Mortise Locks

## Contents

These installation instructions describe how to install your 45HQ Mortise Lock. Topics covered include:

*Preparing the door* ..... 1  
*Configuring and installing the mortise case*..... 3  
*Installing the trim* ..... 4  
*Completing the installation*..... 9

Patents

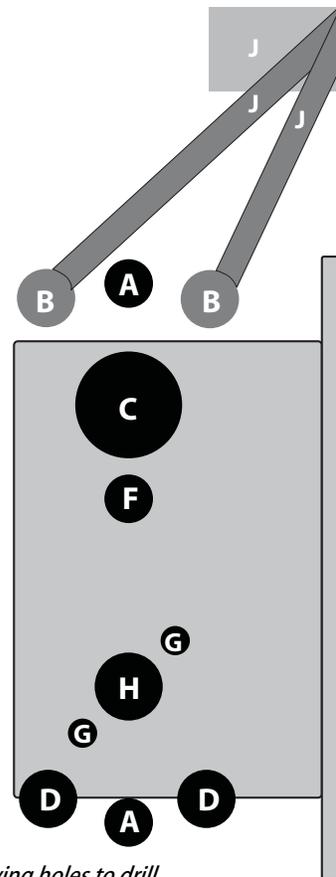
Products covered by one or more of the following patents:  
 6,720,861

### 1 Identify holes to drill

- Determine the lock function to be installed.  
 Caution: Determine the inside and outside, hand, and bevel of the door.
- See the *Holes by Function* table and Figure 1 to determine the holes to be drilled for the lock function.

<i>Holes by Function</i>	Functions			
	DV		TV	
Holes to drill	I/S	O/S	I/S	O/S
<b>A</b> Forged trim (2 holes) <sup>†</sup>	Through door		Through door	
<b>B</b> Harness <sup>†</sup>	Through door		Through door	
<b>C</b> Standard cylinder		■		■
<b>D</b> Sensor & motor wire (2 holes)	■		■	
<b>F</b> Thumb turn			■	
<b>G</b> Trim mounting (2 holes) <sup>‡</sup>	Through door		Through door	
<b>H</b> Lever <sup>††</sup>	Through door		Through door	
<b>J</b> Door sensing channel (2 holes)	DO NOT DRILL		See Figure 1	

<sup>†</sup> Determine trim holes based on trim type.  
<sup>‡</sup> Because these holes pass through the mortise pocket, it is recommended that each hole be drilled separately rather than straight through.



For hole sizes, see the Q06 Template (T82606).

Figure 1 Identifying holes to drill

## Preparing the door

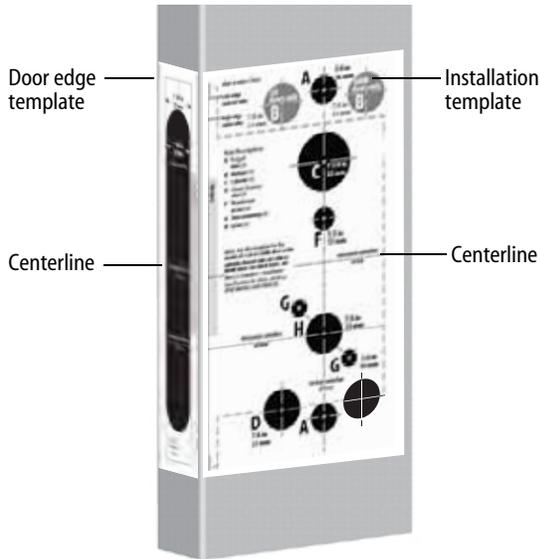


Figure 2 Aligning the templates



Figure 3 Installing the door status switch

### 2 Align templates

Note: If the door is a fabricated hollow metal door, determine whether it is properly reinforced to support the lock. If door reinforcement is not adequate, consult the door manufacturer for information on proper reinforcement. For dimensions for preparing metal doors, see the Q03 Template—Installation Specifications for 45HQ Mortise Locks (T82603).

- 1 Separate the four templates provided on the Q06 Template—Installation Template for 45HQ Mortise Locks (T82606).
- 2 Position one of the door edge templates on the door, making sure that the lock case mortise shown on the template aligns with the mortise pocket prepared in the door.
- 3 Using the centerlines on the door edge template as a guide, position the appropriate door template on each side of the door. You need to take the bevel into account. Tape the templates to the door.

### 3 Center punch and drill holes

- 1 Center punch the necessary drill points. See the instructions on the template.
- 2 Drill the holes.

Note 1: To locate the center of a hole on the opposite side of the door, drill a pilot hole completely through the door.

Note 2: For holes through the door, it is best to drill halfway from each side of the door to prevent the door from splintering.

### 4 Install door status switch

*(optional for deadbolt TV function locks only)*

- 1 Position the shield on the door status switch with the notch facing downwards (towards the mortise pocket).

Caution: Make sure the wires are not routed across any sharp edges or over any surface that could damage its sleeving.

## Configuring & installing the mortise case

- 2 Feed the wires for the door status switch into the door status switch hole and through the channel into the mortise cavity and out through one of the sensor and motor wire holes.
- 3 Press fit the door status switch assembly into the door status switch hole.

### 5 Rotate latchbolt (if necessary)

Note: If a function specific mortise case was ordered, some steps for configuring the case have already been performed at the factory.

- 1 Determine whether you need to rotate the latchbolt to match the handing of the door.

Note: The angled surface of the latchbolt must contact the strike when the door closes.

- 2 If you need to rotate the latchbolt, insert a flat blade screwdriver into the latch access point approximately 1/2" into the case and press to extend the latch out of the case. See Figure 4.
- 3 Rotate the latchbolt 190 degrees (slightly past 180 degrees) and allow it to retract into the case.

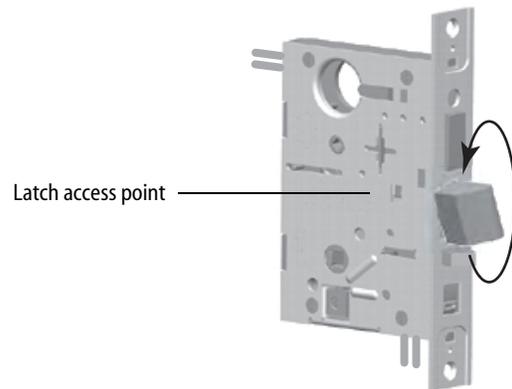


Figure 4 Rotating the latchbolt

### 6 Position hub toggles (if necessary)

- 1 Check whether the hub toggles are in the proper position for the lock. See the table below and Figure 5.

#### Hub toggle positions

Function	Hub toggle positions
DV, TV	Inside down (always unlocked) & outside up (lockable)

Note: For LH & LHRB doors, the inside is the back side of the case and the outside is the cover side of the case.

For RH & RHRB doors, the inside is the cover side of the case and the outside is the back side of the case. The cover is mounted to the case with four screws.

- 2 To change the position of a hub toggle, remove the toggle screw, move the toggle into the desired position, and re-tighten the screw.

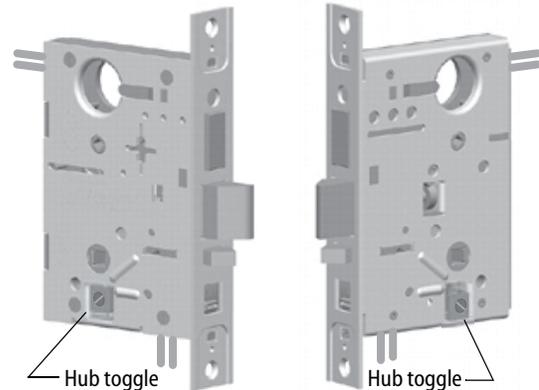


Figure 5 Positioning hub toggles

## Installing the trim

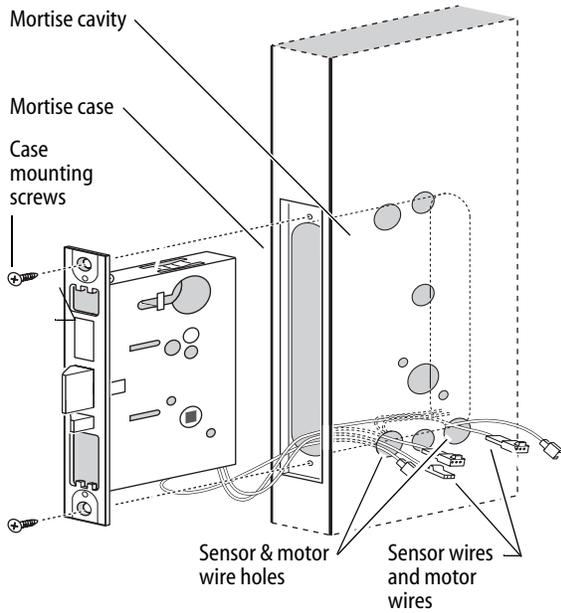


Figure 6 Installing the mortise case (inside of door)

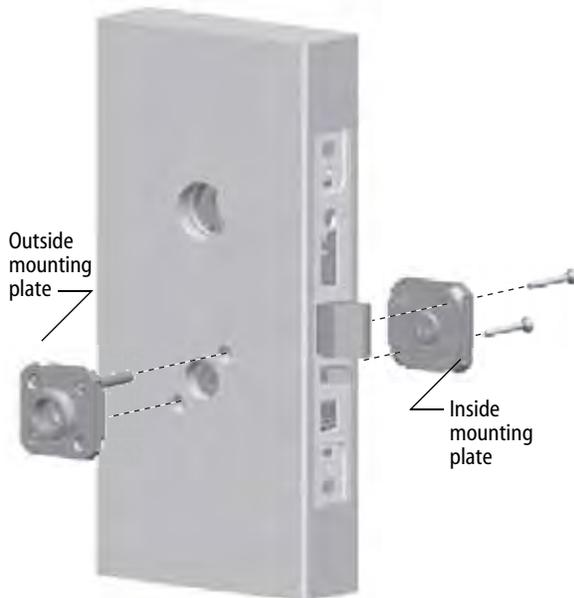


Figure 7 Installing the trim mounting plates

### 7 Install mortise case

- 1 Drill the holes for the case mounting screws.
- 2 Insert the mortise case into the mortise cavity, while feeding the sensor and motor wires into the mortise cavity and out the two sensor & motor wire holes to the inside of the door as shown in Figure 6.

Note: The armored front of the mortise case self-adjusts to the door level.

- 3 Secure the mortise case with the case mounting screws.

### 8 Install trim mounting plates

- 1 Insert the outside trim mounting plate through the door and mortise case.
- 2 Position the inside trim mounting plate opposite the outside trim mounting plate and screw them securely in place.

Caution: Do not overtighten the trim mounting plate screws. Overtightening may damage the locking mechanism.

- 3 By temporarily installing a lever, test the lock to make sure that it doesn't bind.

## Installing the trim

### 9 Install concealed cylinder & core

- 1 Use a cylinder wrench to thread the cylinder into the mortise case so that the groove around the cylinder is even with the door surface as shown in Figure 8.  
Caution: A malfunction can occur if the cylinder is threaded in too far.
- 2 Secure the cylinder in the mortise case with the cylinder retainer screw.
- 3 Insert the control key into the core and rotate the key 15 degrees to the right.
- 4 With the control key in the core, insert the core into the cylinder.
- 5 Rotate the control key 15 degrees to the left and withdraw the key.  
Caution: The control key can be used to remove cores and to access doors. Provide adequate security for the control key.

### 10 Install trim hole insert and bushing

- 1 Insert the trim hole insert into the upper trim hole on the outside of the door, as shown in Figure 9.
- 2 Insert the bushing into the harness hole on the outside of the door, as shown in Figure 9.

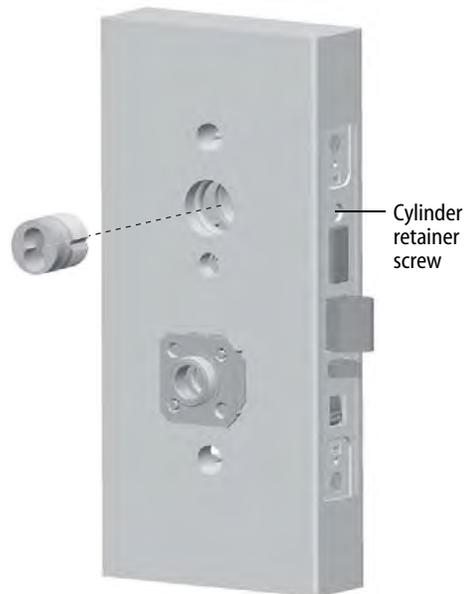


Figure 8 Installing the concealed cylinder

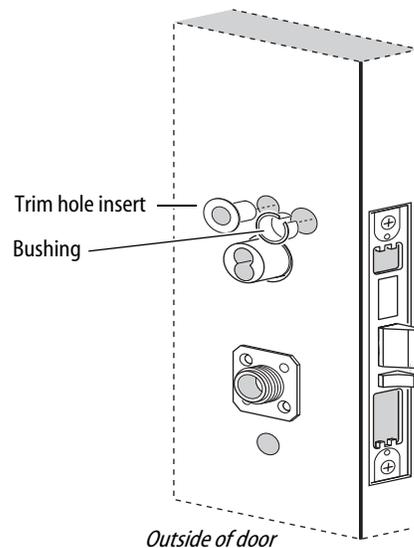


Figure 9 Installing the trim hole insert and bushing

## Installing the trim

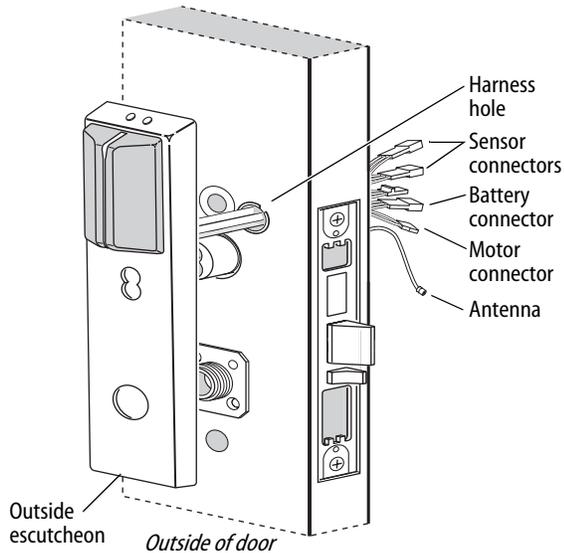


Figure 10 Feeding the wire harness connectors through the harness hole

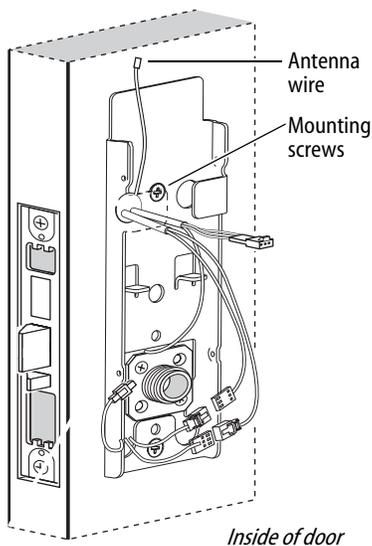


Figure 11 Installing the fire plate

### 11 Route wire harnesses and position outside escutcheon

- 1 From the outside of the door, feed the motor connector, battery connector, and sensor connectors through the harness hole.

Caution: When routing the connectors, make sure the harnesses are not routed across any sharp edges or over any surface that could damage their sleeving or wire insulation.

- 2 Perform these steps:
  - a Firmly press the outside escutcheon in position on the door. The core should be flush with the outer surface of the escutcheon.
  - b If necessary, adjust the cylinder depth plus or minus one turn so that the core is flush with the outer surface of the escutcheon.
  - c Secure the cylinder in the mortise case with the cylinder clamp screw.
- 3 Rest the outside escutcheon on the door by inserting the trim studs into the trim holes.

### 12 Install fire plate

- 1 From the inside of the door, feed the wiring through the fire plate harness hole.
- 2 Position the fire plate on the door so that the inside mounting plate fits through the square opening in the fire plate.
- 3 Insert the two counter sunk mounting screws into the holes at the top and bottom of the fire plate.
- 4 Tighten the mounting screws until the fire plate is securely mounted to the door.

## Installing the trim

### 13 Connect wire harnesses

- From the inside of the door, make the following connections:

Wire connection	Colors	No. of wires	No. of pins
Motor	Yellow-gray	2	2
Key override sensor	Gray	2	3
Deadbolt sensor	Blue	2	3
RQE	Orange-brown	2	3
Door sensing	White	2	2
Latchbolt sensing	Purple	2	2

- Insert the plastic wire tie through the mounting clip and secure the wires as shown in Figure 12.

Note: It is physically possible to connect the key override sensor connector from the mortise case to the battery connector from the wire harness. To avoid this mistake, connect only the connectors with matching wire colors.

Caution: When making the motor connection and sensor connections, make sure:

- ◆ there are no loose wire connections where the wires are inserted into the connectors
- ◆ the connectors are firmly mated

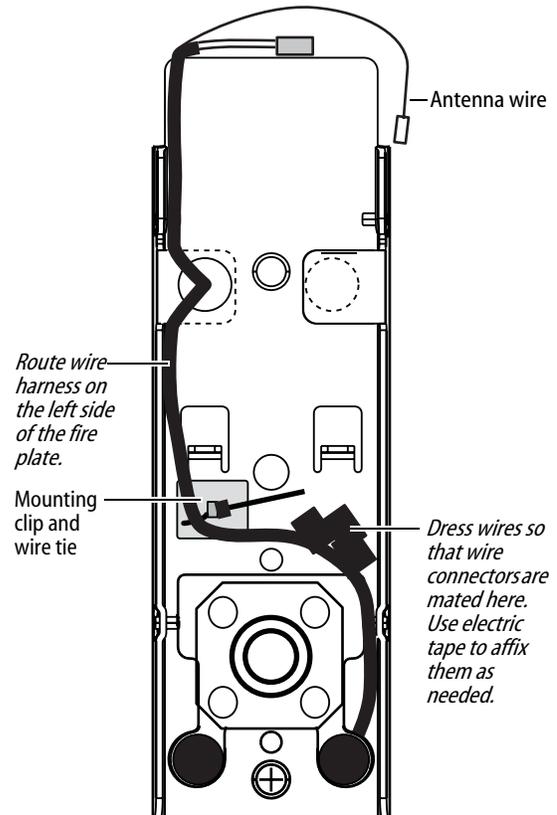


Figure 12 Routing the wires

## Installing the trim

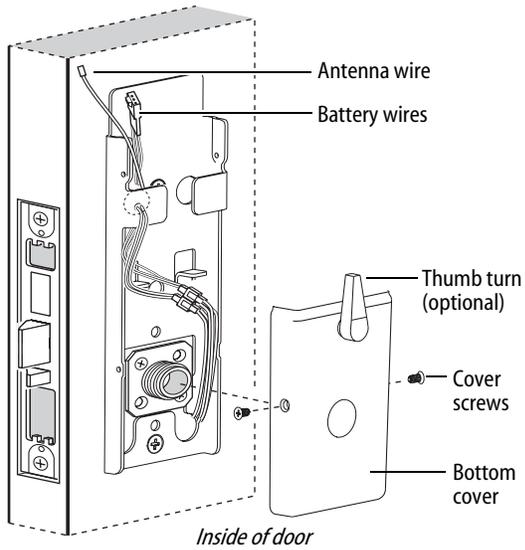


Figure 13 Installing the bottom cover

### 14 Install bottom cover (inside escutcheon)

- 1 Position the battery wires above the side tabs and against the side of the fire plate, as shown in Figure 13.
- 2 **Optional for Thumb Turn option only:** Make sure that the Thumb Turn is in the upright position, as shown in Figure 13.
- 3 **Making sure that the cover does not pinch the wires,** guide the bottom cover over the chassis onto the fire plate.

Note: Phillips Type 2 and T20 Torx options are available for the cover mounting screws.

## Completing the installation

### 15 Install battery holder

- 1 Position the battery wires against the fire plate side wall, as shown in Figure 14.
- 2 Slide the battery holder behind the fire plate side tabs until it rests on the bent battery holding tabs.

Caution: When routing the battery wires, make sure the wires are not routed across any sharp edges or over any surface that could damage their sleeving or wire insulation.

- 3 Connect the battery pack to the battery connector on the wire harness.

Caution: When connecting the battery pack, make sure:

- ◆ there are no loose wire connections where the wires are inserted into the connectors.
- ◆ the connectors are firmly mated.

### 16 Install inside and outside levers

- 1 Unscrew the inside spindle one full turn to allow the spindles to turn freely.
- 2 With the handle pointing toward the door hinges, insert the outside lever and spindles assembly into the lock from the outside of the door.
- 3 Slide the inside lever onto the inside spindle and secure it with the set screw.

- 4 Making sure that the core is positioned properly in the outside escutcheon (DV and TV function Locks only) and the escutcheons are aligned properly on the door, tighten the escutcheon mounting screws.

Note: If a core is not available, you can use the cylinder wrench to help you align the core opening in the escutcheon.

- 5 Turn the levers to check that they operate smoothly.

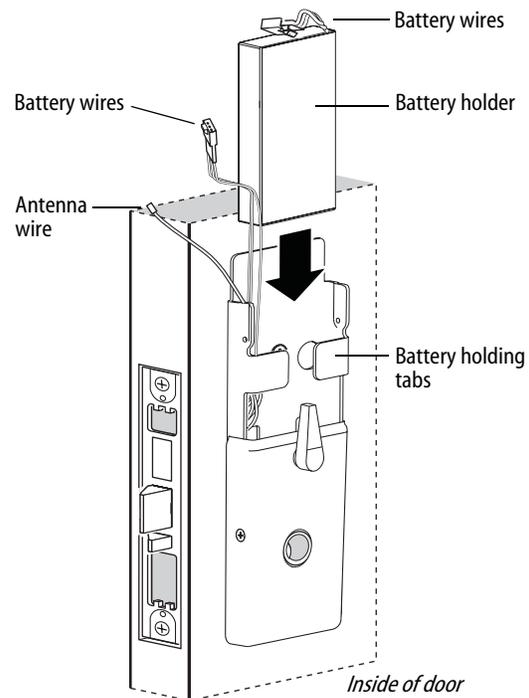


Figure 14 Installing the battery holder

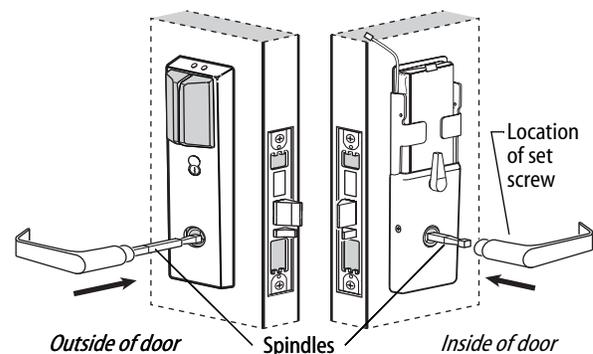


Figure 15 Installing the levers

## Completing the installation

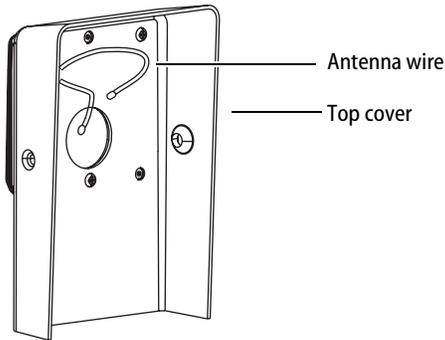


Figure 16 Inside view of top cover

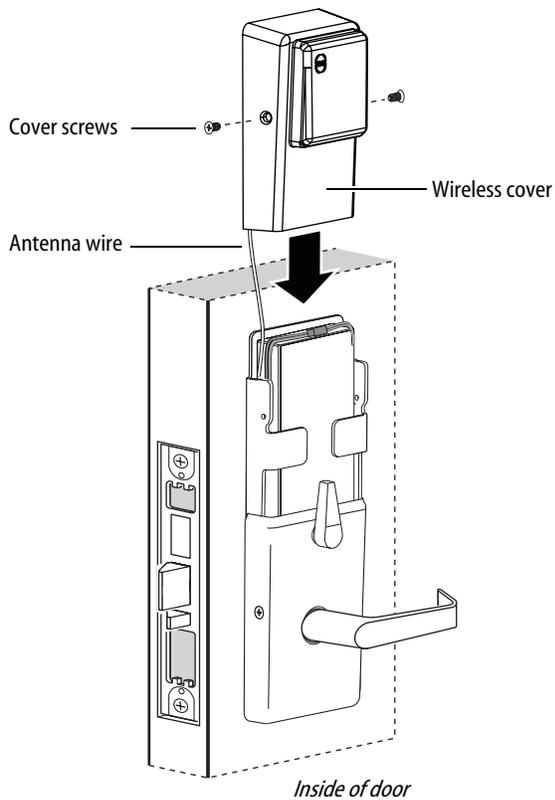


Figure 17 Installing the top cover

### 17 Install top cover (inside escutcheon)

- 1 Connect the antenna to its mating connector.
- 2 Place the top cover against the door and above the fire plate. Slide the top cover down toward the bottom cover as shown in Figure 17.

Caution: As you slide the top cover onto the fire plate, feed the antenna wire down into the bottom cover. Be sure not to pinch the antenna wire on the bottom cover as you slide the top cover into place.

- 3 Use two cover screws to secure the cover to the side of the fire plate, as shown in Figure 17.

Note: Phillips Type 2 and T20 Torx options are available for the cover mounting screws.

### 18 Install mortise case faceplate

- 1 Secure the mortise case faceplate to the mortise case with the faceplate mounting screws.
- 2 Check the lock for proper operation.

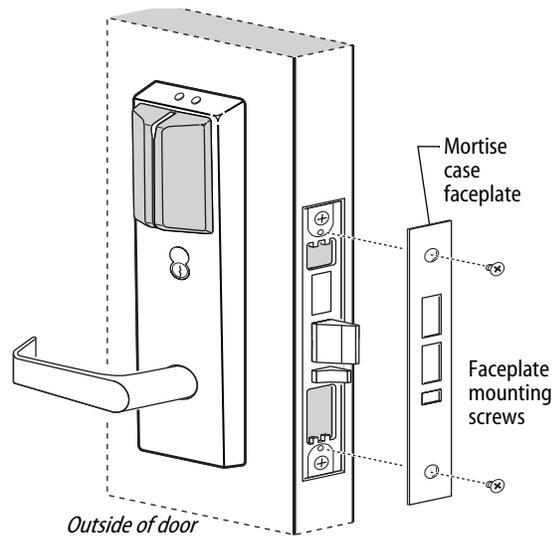


Figure 18 Installing the mortise case faceplate

## Completing the installation

### 19 Install strike box and strike plate

- 1 Insert the strike box into the mortise in the door jamb. Place the strike plate over the strike box and secure the strike with the screws provided.

- 2 Check the position of the auxiliary bolt against the strike plate.

Caution: The auxiliary bolt must make contact with the strike plate. The auxiliary bolt deadlocks the latchbolt and prevents someone from forcing the latch open when the door is closed. If the incorrect strike is installed, a lock-in can occur.

Note: The recommended gap between the door and jamb is 1/8" .

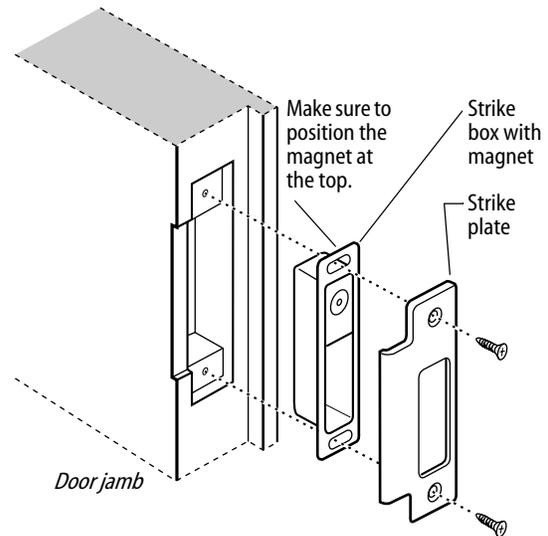


Figure 19a Installing the strike box and strike plate

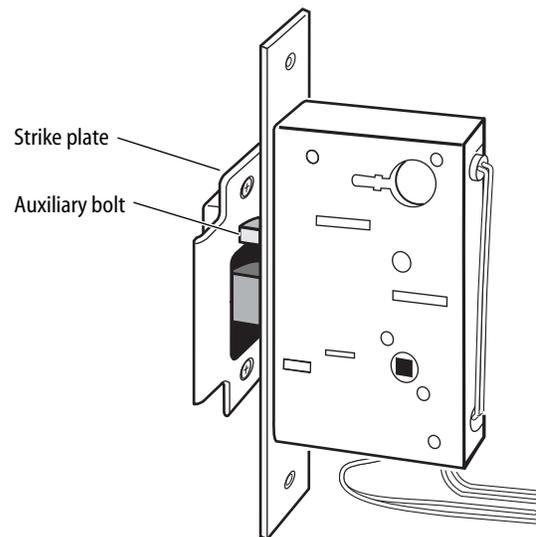


Figure 19b Positioning the strike

## Testing the lock

### 20 Test lock

#### For 45HQ Locks with keypad

To test the lock for proper operation before the lock is programmed, follow these instructions:

- 1 Press **1234**.
- 2 Press #.

*The green light flashes and the locking mechanism unlocks.*

- 3 Turn the lever and open the door.

#### For all other locks:

To test the lock for proper operation before the lock is programmed, use the temporary operator card that came with the lock. This card is for temporary use only. After permanent cards have been programmed for the lock, the temporary card should be deleted.

- 1 Use the temporary operator card to activate the lock.  
Note: If the lock has a proximity card reader, it may have already been activated by the presence of an object near the card reader.
- 2 Use the temporary operator card to access the lock.  
The green light flashes and the locking mechanism unlocks.
- 3 Turn the lever and open the door.

If the mechanism doesn't unlock, refer to the following table. For additional troubleshooting instructions, see the Service Manual.

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

#### For all locks

- 1 Insert and turn the key to unlatch the door.

#### For all TV function locks

- 2 From the inside of the door, turn the turn knob and make sure that the deadbolt operates properly.



# Installation Instructions for Wi-Q Technology™ EXQ Exit Hardware Trim



## Introduction

These installation instructions describe how to install your BEST® Wi-Q Technology™ EXQ Series Exit Hardware Trim. Electronic Stand-Alone Exit Hardware Trim is available for use with the following types of wide stile exit devices: Precision® brand manufactured by Stanley (2000 Series), Von Duprin® (98/99 Series), and Sargent® (8800 Series).

Not all features are available for all exit device configurations. The table below details what sensors are available for which exit device configurations:

Device	DS <sup>a</sup>	TS <sup>b</sup>	LS <sup>c</sup>
<b>Precision</b>			
Rim (2100)	■	■	■
Surface Vertical (2200)	■	■	■
Mortise (2300)	■		
Wood Door Concealed (2700)	■	■	■
Concealed Vertical (2800)	■	■	■
<b>Von Duprin<sup>d</sup></b>			
Rim	■	■	
Surface Vertical	■		
Concealed Vertical	■		
<b>Sargent<sup>e</sup></b>			
Rim <sup>f</sup>	■		

- a. Door position sensing
- b. Request-to-exit (PHI touchbar monitoring)
- c. Latch sensing
- d. Von Duprin is a registered trademark of Von Duprin, Inc.
- e. Sargent is a registered trademark of Sargent Mfg. Co.
- f. Latch must have lift-type trim input (8863)

## Contents

These instructions cover the following topics:

<i>Planning the installation</i> .....	1
<i>Preparing the door</i> .....	3
<i>Installing the exit hardware and trim</i> .....	7
<i>Completing the installation</i> .....	16

## Site survey

Use the following survey to record information about the installation site and hardware application.

Exit hardware type:

- rim
- mortise
- surface vertical rod
- concealed vertical rod

Door handing and bevel:

- Left-hand reverse bevel (LHRB)
- Right-hand reverse bevel (RHRB)

Door type:

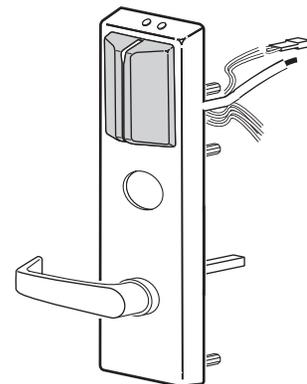
- Wood
- Metal

Door thickness: \_\_\_\_\_ inches (1-3/4" to 2-1/4")

## Components checklist

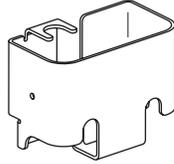
Use the following checklist to make sure that you have the items necessary to install your EXQ Exit Hardware Trim.

- Escutcheon and lever assembly

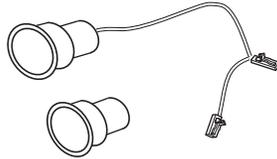


**Installation Instructions for Wi-Q Technology™ EXQ Exit Hardware Trim**

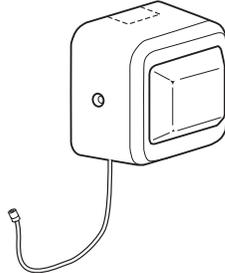
- Battery bracket



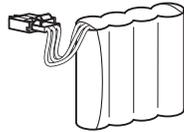
- Door position switch with magnet



- Battery cover with antenna



- Battery pack



- Battery cover screw package

- Bar code ID sticker (for your records)

- Cable ties, butt-splices, and tape

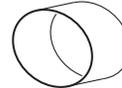
- Installation templates and instructions



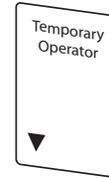
- 7-pin core (only included if ordered with trim)



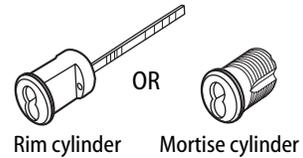
- Cylinder mounting sleeve (for Von Duprin functions only)



- Temporary operator card



- Key cylinder and keys (only included if ordered with trim).



**Tools required**

Use the following checklist to make sure that you have the tools necessary to install your EXQ Exit Hardware Trim.

- Electric drill (preferably corded)
- Jigsaw
- Wire strippers
- Phillips screwdriver
- Measuring tape
- Straight edge
- Square
- Pencil/marker
- 7/16" dia drill bit
- 7/8" dia drill bit
- 1" dia hole saw

**For Precision® Hardware and Sargent installations**

- 1-3/8" dia hole saw (EV function only)
- 1-1/8" dia hole saw

**For Von Duprin® installations**

- 2" dia hole saw
- 3/4" dia hole saw

**For BEST® cylinders**

- BEST ED211 cylinder wrench

**For surface vertical exit devices**

- Razor blade

## Preparing the door

### 1 Mark centerlines

**Note 1:** If retrofitting to an existing exit hardware installation, skip this task. Instead, remove the exit hardware from the door.

**Note 2:** If the door is a fabricated hollow metal door, determine whether it is properly reinforced to support the lock. If door reinforcement is not adequate, consult the door manufacturer for information on proper reinforcement.

- 1 Prepare the push side of the door according to the exit device manufacturer's installation instructions.

**Note:** The tape-on template supplied with the EXQ trim will supersede the exit device template in the trim area.

- 2 Transfer horizontal and vertical centerlines to the outside of the door face.

**Note:** When measuring from the edge of the door, take into account the door bevel (if any).

### 2 Determine required door prep

- 1 Determine which template is applicable (Q08 for Precision and Sargent, Q07 for Von Duprin) and discard the other one.
- 2 Based on the kind of exit device you have, use the table below to locate the appropriate door preparation.
- 3 On the template, circle the holes needed for your installation and cross out those that are not applicable.

	Device	Figure
Precision	Rim (2100)	Figure 2
	Surface Vertical (2200)	Figure 3
	Mortise (2300)	Figure 4
	Wood Door Concealed (2700)	Figure 3
	Concealed Vertical (2800)	Figure 3
Von Duprin	Rim (with RQE)	Figure 5
	Rim (without RQE)	Figure 7
	Surface Vertical	Figure 7
	Concealed Vertical	Figure 7
	<b>Sargent Rim</b>	Figure 6

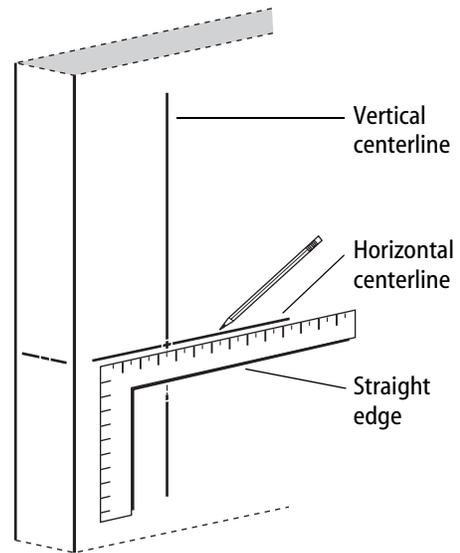


Figure 1 Marking centerlines on outside door face

**Note:** Follow the Precision 2300 door preparation for Sargent, ignoring any steps directly pertaining to the mortise lock or key cylinder.

## Preparing the door

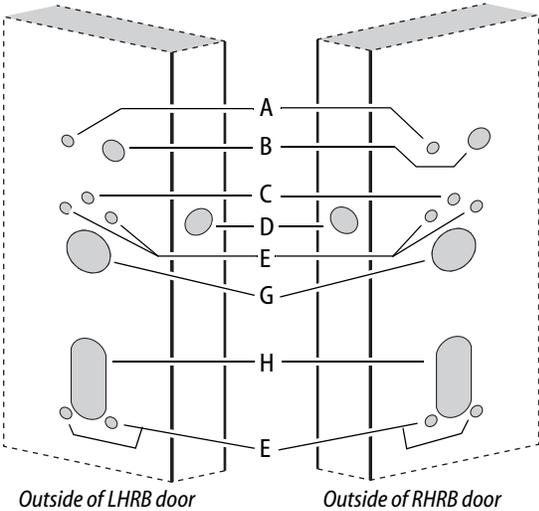


Figure 2 Outside door prep for use with Precision exit hardware, 2100 Series

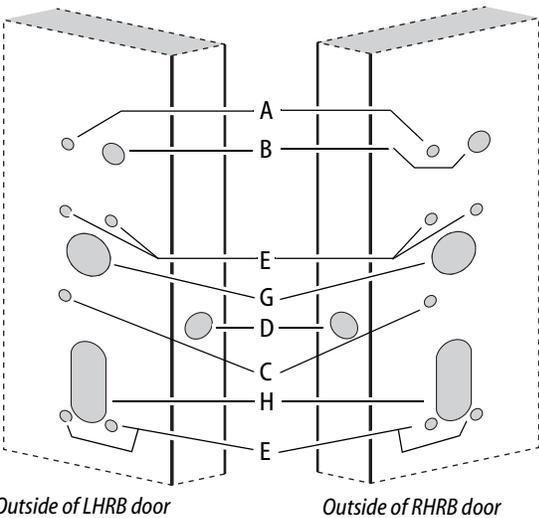


Figure 3 Outside door prep for use with Precision exit hardware, 2200, 2700, and 2800 Series

Hole	Description	Instructions
A	Battery bracket hole	7/16" diameter, thru door
B	Battery bracket/harness hole	7/8" diameter, thru door
C	Sensor harness routing hole	7/16" diameter, thru door
D	Door sensing switch mounting hole and channel	1" diameter hole, drilled 1-3/4" deep, then 7/16" channel to intersect door sensing wire routing hole.
E	Escutcheon mounting holes	7/16" diameter, thru door
F	Door sensing switch magnet hole (in door frame or opposing door leaf)	1" diameter hole, drilled 1-3/4" deep (NOT SHOWN).
G	Cylinder hole	<b>Precision:</b> 1-3/8" diameter, thru door (for 2300, only into mortise cavity) <b>Von Duprin:</b> 2" diameter thru door
H	Lift finger slot	<b>Precision/Sargent:</b> 1-1/8" diameter slot, thru door <b>Von Duprin:</b> 3/4" diameter slot, thru door

## Preparing the door

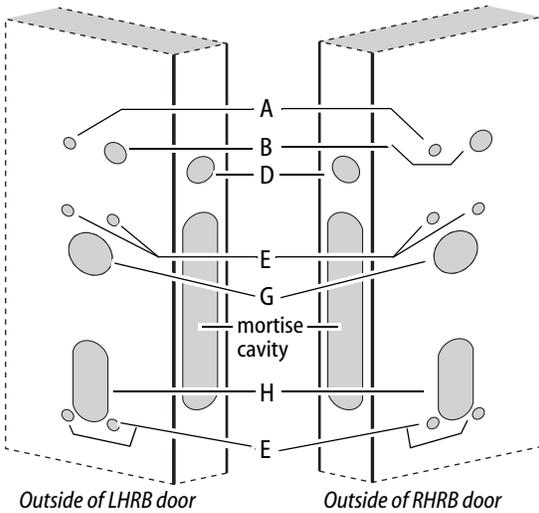


Figure 4 Outside door prep for use with Precision exit hardware, 2300 Series

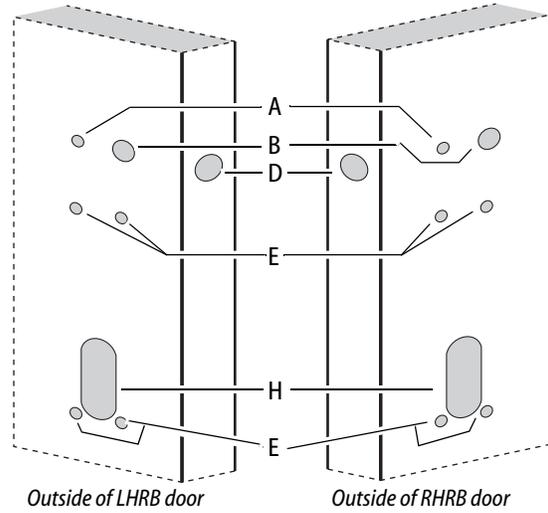


Figure 6 Outside door prep for use with Sargent 8863 exit hardware

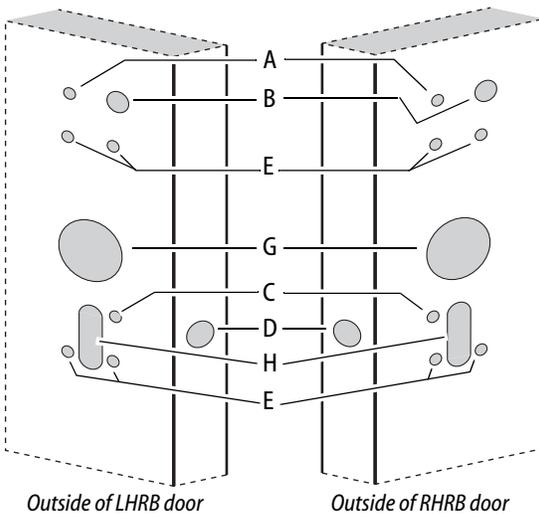


Figure 5 Outside door prep for use with Von Duprin exit hardware, Rim **with** RQE only

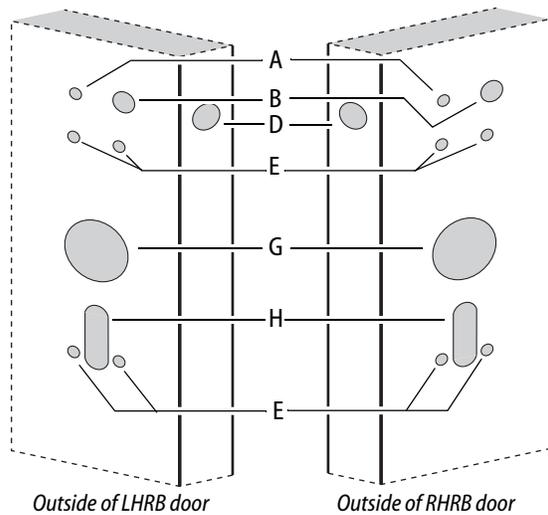


Figure 7 Outside door prep for use with Von Duprin exit hardware. Use for all Von Duprin vertical rods and rim **without** RQE

## Preparing the door

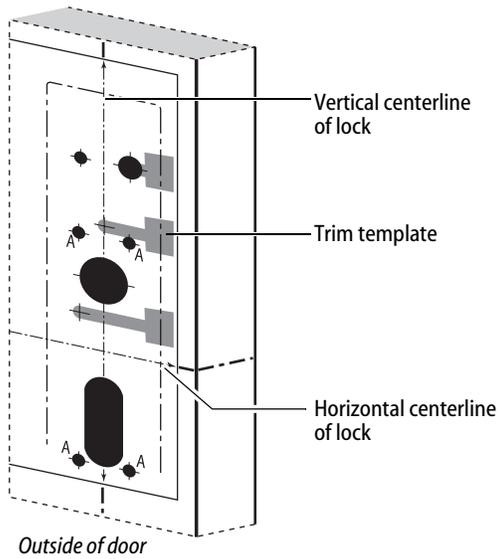


Figure 8 Positioning the trim template, Q08 LHRB shown

### 3 Position trim template and mark drill points

#### 1 For new installations

- Cut the applicable template along the dashed lines.
- Align the horizontal and vertical centerlines marked on the template with the centerlines marked on the **OUTSIDE** of the door (from step 1). See Figure 8.

#### For retrofit installations

Align the mounting holes for the escutcheon and lock stile case shown on the template with the mounting holes already present in the door.

**Note:** The outside escutcheon is mounted using the four lock stile case mounting holes ('A' holes); these holes must be 7/16" in diameter and drilled completely through the door.

- Tape the template to the **OUTSIDE** of the door in the properly aligned position.
- Center punch the necessary drill points. Refer to the instructions on the template and the figures of the previous step.

### 4 Mortise for mortise case and faceplate (mortise exit devices only)

**Note:** If retrofitting the EXQ Exit Hardware Trim to an existing exit hardware installation, skip this task.

Mortise the edge of the door for the mortise case and faceplate; follow the instructions provided by the exit hardware manufacturer.

## Installing the exit hardware and trim

### 5 Drill holes

**Caution:** Double-check for the correct lock function, hand, and bevel before drilling.

- 1 Drill the trim holes that are required for your application; follow the instructions on the trim template and refer to the figures in step 2.

**Note 1:** To locate the center of a hole on the opposite side of the door, drill a small pilot hole through the door.

**Note 2:** For holes through a wood door, drill halfway from each side of the door to keep the door from splintering.

### 6 Install mortise case (mortise exit devices only)

Install the mortise case in the door; follow the instructions provided by the exit hardware manufacturer.

### 7 Install door sensing switch

- 1 Clip off the purple wires and connector and remove.
- 2 Clip off the connector from the white door sensing harness (with black sleeving) and leave as much wire as possible. See Figure 9. These wires will be butt-spliced to the sensing harness from the trim. See "Route sensor wires" on page 14.
- 3 Route the door sensing switch wires through the channel and out through the wire routing hole to the exit device side. See Figure 9.
- 4 Press-fit the door sensing switch into the 1" diameter hole in the door.
- 5 Mark and drill 1" diameter hole in the frame, aligned with the door position switch (for the magnet).  
**Note:** For double-door applications, this hole will be into the edge of the opposing door leaf (not the frame).
- 6 Press-fit the door sensing magnet into the 1" diameter hole in the frame.

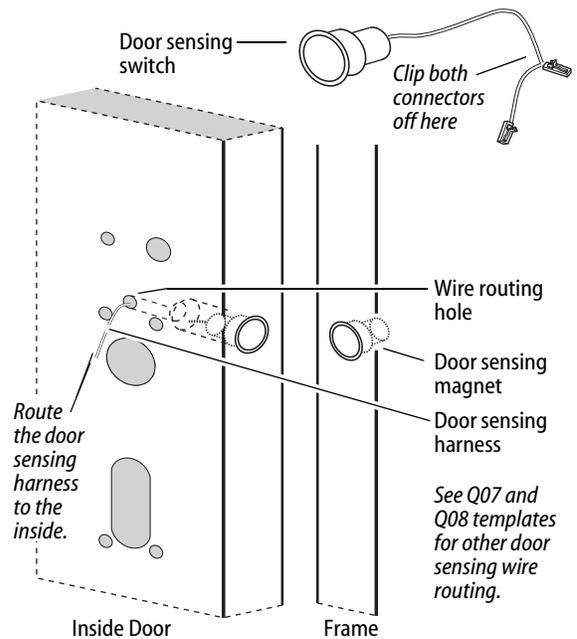


Figure 9 Installing the door sensing switch and magnet, Precision 2100 shown

## Installing the exit hardware and trim

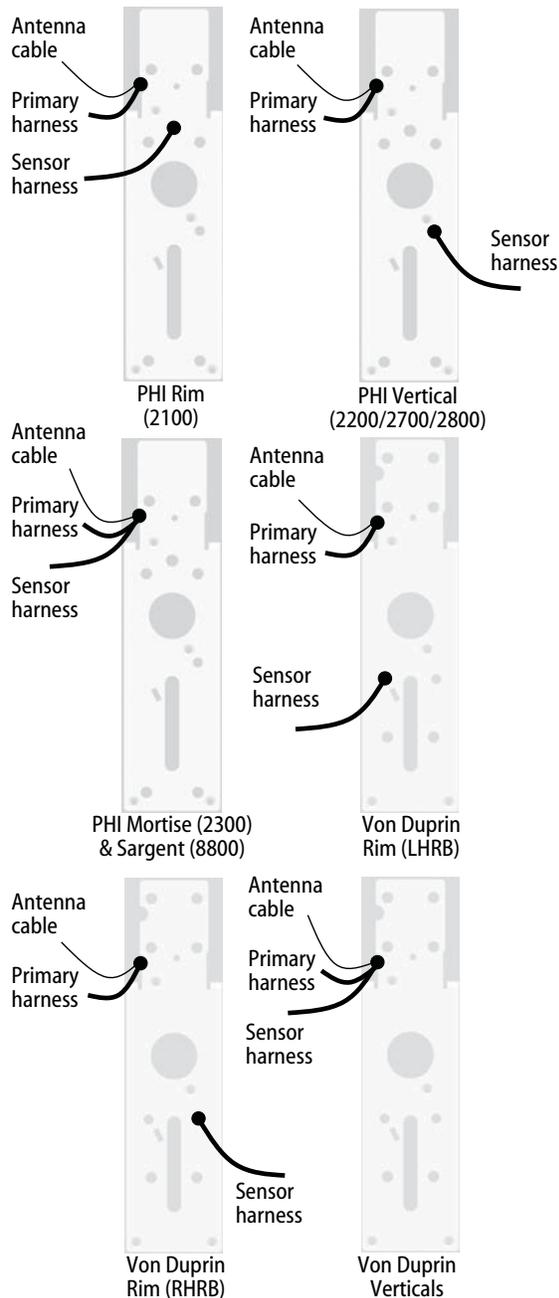


Figure 10 Variations of EXQ Trim rear view

### 8 Re-route sensor harness (if applicable)

Looking at the back of the trim, compare it to the pictures in Figure 10. If your trim does not match the proper picture, then follow the applicable steps below to re-route the sensor harness.

## Installing the exit hardware and trim

- 1 Carefully peel the black gasket off of the back of the trim. Set it aside to be re-applied later.
- 2 Remove the backplate from the trim by removing the four screws that attach it.
- 3 While the gasket and backplate are removed, change the handing of the trim if necessary.  
Do so by removing the four threaded guide pins and retaining ring as shown in Figure 11, pulling out and flipping the lever 180 degrees, and then reassembling.

### For Precision 2100 devices

- 4 Re-route the sensor harness out through the alternate wire-routing hole as shown in Figure 12.
- 5 Reattach the backplate ensuring that the springs are properly seated and wires are not pinched.
- 6 Reapply the gasket.

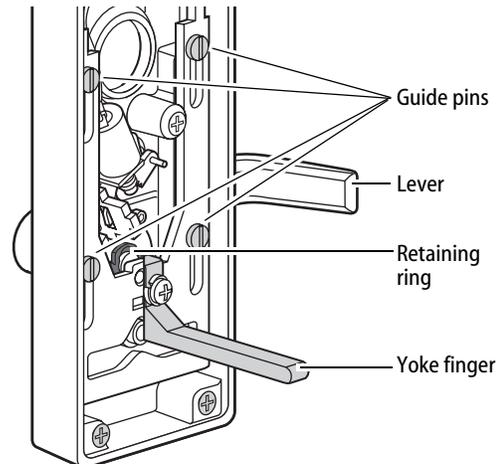


Figure 11 Changing the hand of the trim (if needed)

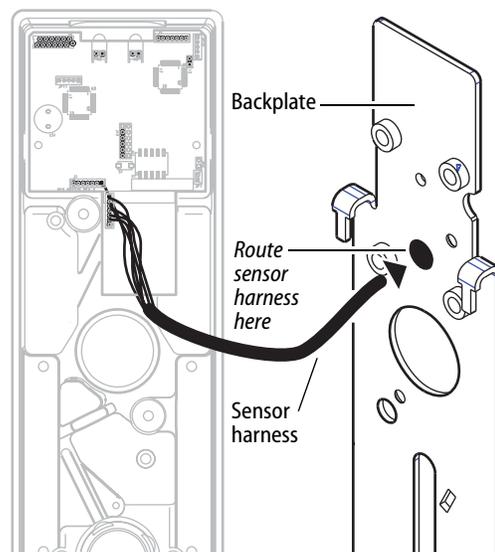


Figure 12 Re-routing the sensor harness for Precision 2100 exit devices

## Installing the exit hardware and trim

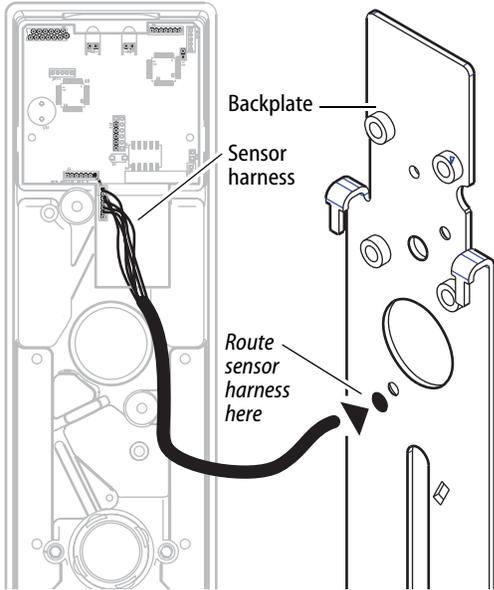


Figure 13 Re-routing the sensor harness for Precision 2200, 2700 and 2800 exit devices

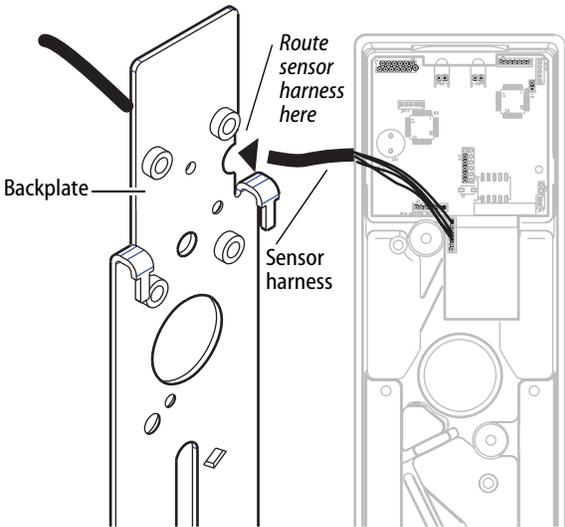


Figure 14 Re-routing the sensor harness for Precision 2300 and Sargent 8800 exit devices

### For Precision 2200, 2700 and 2800 devices

- 4 Re-route the sensor harness around the cylinder hole and around the escutcheon boss, then out through the alternate wire-routing hole as shown in Figure 13.
- 5 Reattach the backplate ensuring that the springs are properly seated and wires are not pinched.
- 6 Reapply the gasket.

### For Precision 2300 and Sargent 8800 devices

- 4 Re-route the sensor harness toward the top of the escutcheon to the same area as the battery cable, antenna cable and relay shunts. See Figure 14.
- 5 Reattach the backplate ensuring that the springs are properly seated and wires are not pinched.
- 6 Reapply the gasket.

### For Von Duprin Rim devices with RQE

- 4 Re-route the sensor harness around the cylinder hole and around the escutcheon boss, then out through one of the alternate wire-routing holes (based on handing) as shown in Figure 15.
- 5 Reattach the backplate ensuring that the springs are properly seated and wires are not pinched.
- 6 Reapply the gasket.

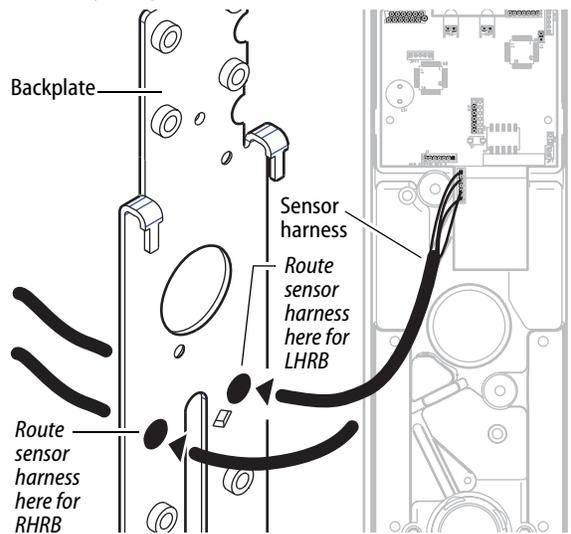


Figure 15 Re-routing the sensor harness for Von Duprin with RQE

## Installing the exit hardware and trim

### For Von Duprin vertical rod devices and rim without RQE

- 4 Re-route the sensor harness as shown in Figure 16.
- 5 Reattach the backplate ensuring that the springs are properly seated and wires are not pinched.
- 6 Reapply the gasket.

## 9 Install cylinder (Von Duprin only)

- 1 To determine the correct spindle length, try the cylinder in the door while holding the escutcheon and lock stile case in place.  
Then break off the spindle at the groove where it will engage correctly with the latching mechanism.  
If necessary break off the mounting screws as shown in Figure 17.
- 2 From the front of the escutcheon, insert the cylinder into the cylinder opening.
- 3 Holding the cylinder in position in the escutcheon, insert the cylinder mounting sleeve through the back of the escutcheon, over the cylinder.
- 4 Orient the cylinder and clamp plate as shown in Figure 17. From the back of the escutcheon, secure the cylinder and mounting sleeve using the clamp plate and mounting screws.

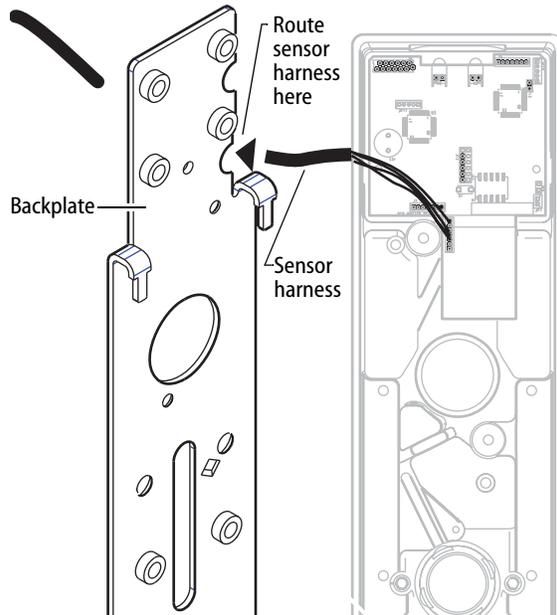


Figure 16 Re-routing the sensor harness for Von Duprin vertical rod and rim without RQE exit devices

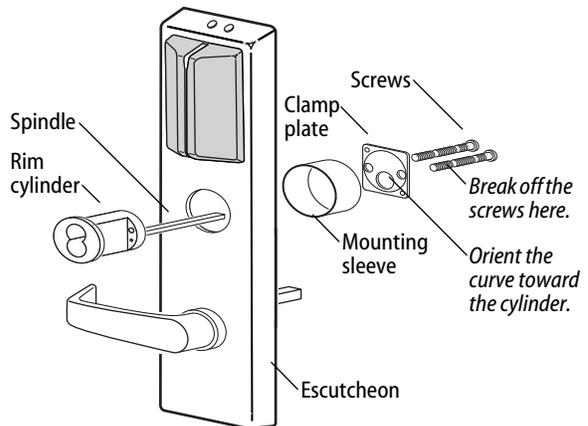


Figure 17 Installing the cylinder for Von Duprin rim and rod exit devices

## Installing the exit hardware and trim

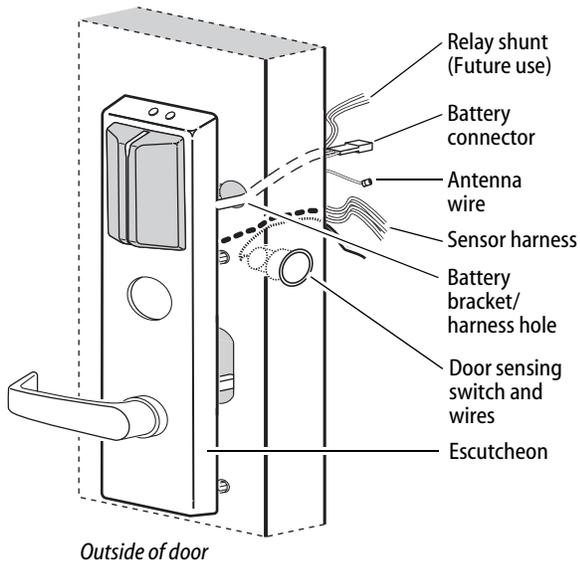


Figure 18 Feeding the wires through the door

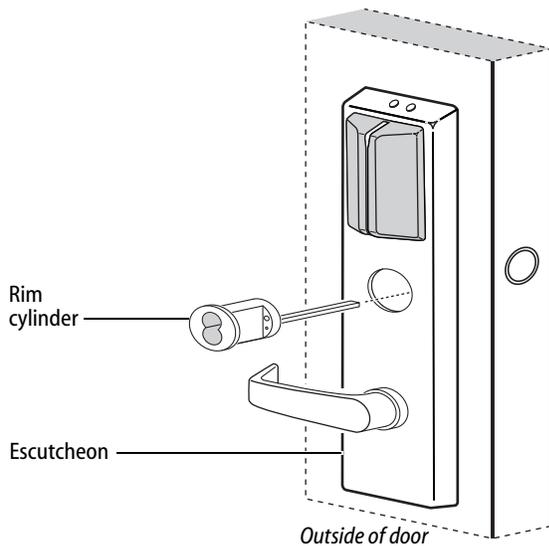


Figure 19 Installing the cylinder

### 10 Route wire harnesses and position escutcheon

- 1 From the outside of the door, feed the antenna wire and battery connector (with relay shunt) through the battery bracket/harness hole as shown in Figure 18.

**Caution 1:** When routing the connectors, make sure the harnesses are not routed across any sharp edges or over any surface that could damage their sleeving or wire insulation.

**Caution 2:** Do not strain the wire harness either by pulling too hard on it or by dangling the escutcheon from it.

- 2 Route the sensor harness through the door (same hole as the door sensing wires).
- 3 Rest the escutcheon on the door by inserting the trim studs into the mounting holes.

### 11 Install cylinder (Precision devices)

**For rim and vertical rod exit device installations (rim cylinder)**

- 1 To determine the correct spindle length, try the cylinder in the door while holding the escutcheon and lock stile case in place.

Then break off the spindle at the groove where it will engage correctly with the latching mechanism.

Break off the mounting screws at the groove where they will secure the clamp plate to the cylinder.

- 2 Insert the cylinder through the cylinder opening in the escutcheon and into the door as shown in Figure 19.
- 3 Orient the cylinder and clamp plate as shown in Figure 20. From the inside of the door, secure the cylinder using the clamp plate and mounting screws.

## Installing the exit hardware and trim

### For mortise exit device installations (mortise cylinder)

- 1 For doors less than 2" in thickness, place the cylinder ring provided on the cylinder.
- 2 Rotate the cylinder cam to the 12 o'clock position, as shown in Figure 21.
- 3 Using a cylinder wrench (ED211), insert the cylinder through the cylinder opening in the escutcheon and screw the cylinder into the mortise case. Make sure that the figure-8 hole is in the 12 o'clock position.

**Caution:** Do not screw the cylinder in too tightly. Doing so may cause users to be locked out.

## 12 Install exit hardware and secure escutcheon

### For Precision 2200, 2700 and 2800 exit devices only

- Drill a 5/16" hole through the front part of the chassis as shown in Figure 22. (This hole is used to pass the sensor harness and door position switch wires into the chassis area.)

### For all exit devices

- 1 Make any adjustments to the exit hardware necessary for compatibility with lever function outside trim.
- 2 Install the exit hardware (lock stile case, touch bar assembly, latches and rods [if applicable], and related hardware); follow the instructions provided by the exit hardware manufacturer.

**Note:** The escutcheon is secured on the outside of the door by the screws used to mount the lock stile case on the inside of the door.

**Caution:** When securing the escutcheon, make sure that it does not pinch any wires.

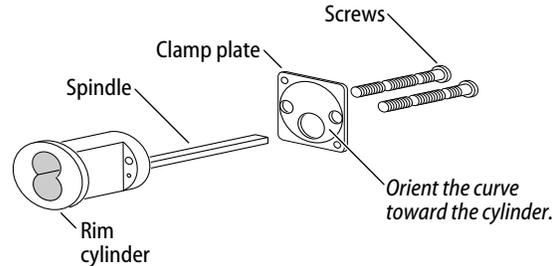


Figure 20 Rim cylinder components

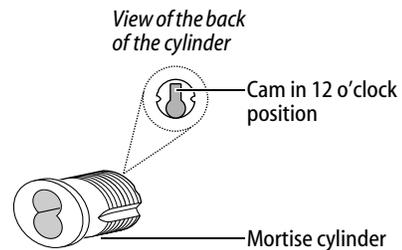


Figure 21 Mortise cylinder components

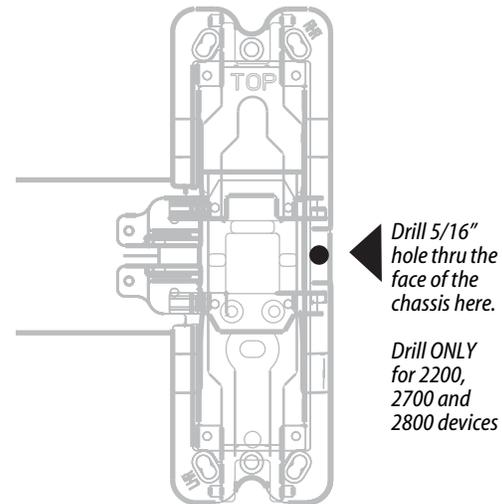


Figure 22 Drilling 5/16" hole for Precision 2200, 2700, and 2800 exit devices only

## Installing the exit hardware and trim

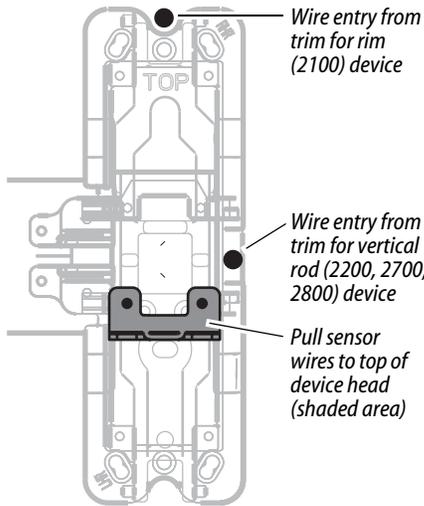


Figure 23 Pulling sensor harnesses to the top of the device head

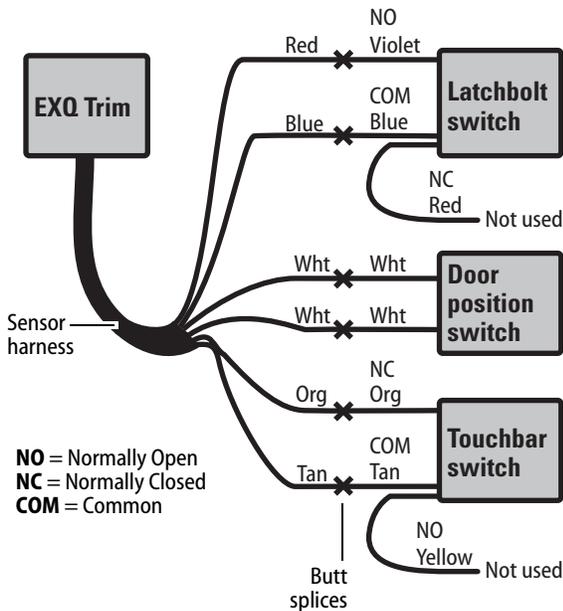


Figure 24 Schematic diagram for connecting Precision sensor harness wires

### 13 Route sensor wires

Use the following table to determine sensing wire functions:

Wire function	Colors	No. of wires
Touchbar monitoring (RQE)	Orange and tan	2
Door sensing	White	2
Latchbolt sensing	Red and blue	2

- 1 Pull wires from the sensor harness, door position switch, latchbolt switch, and touchbar switch to the top of the device head as shown in Figure 23.

**Note:** For Precision 2300, Sargent 8800, or any Von Duprin application without RQE, pull the door position switch and sensor harness wires into the battery bracket area rather than the device head.

**Note:** For Von Duprin applications with RQE, touchbar switch wires must be re-routed into the device head in such a way as to avoid any pinching or contact with moving parts. The sensor harness can be routed into the head area through any suitable hole in the chassis.

- 2 Cut the wires to the appropriate length (that is, remove the excess to leave minimal slack after the spliced connections).
- 3 Strip the wire ends for connection using the butt-splices.
- 4 Make wire connections as detailed in Figure 24 or Figure 25 using the butt-splices (provided).

**Note:** For Sargent devices, connect the door position switch to the two white sensor harness wires.

**Note:** In the case of unused wires, be sure to cover the ends with electrical tape.

## Installing the exit hardware and trim

- 5 Make sure to route and dress the wires so that they do not interfere with any moving parts.
- 6 Tape the wires to the device head (some tape is provided).

**Note:** For Precision 2200, 2700, and 2800 exit devices, use cable ties in addition to the tape, to hold wires as shown in Figure 26.

- 7 Install the case cover.

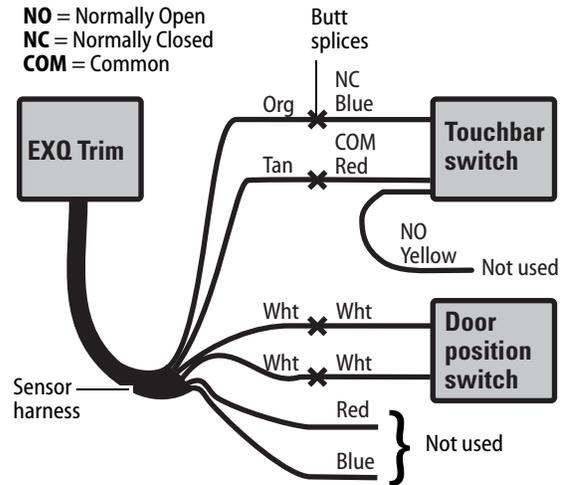


Figure 25 Schematic diagram for connecting Von Duprin sensor harness wires

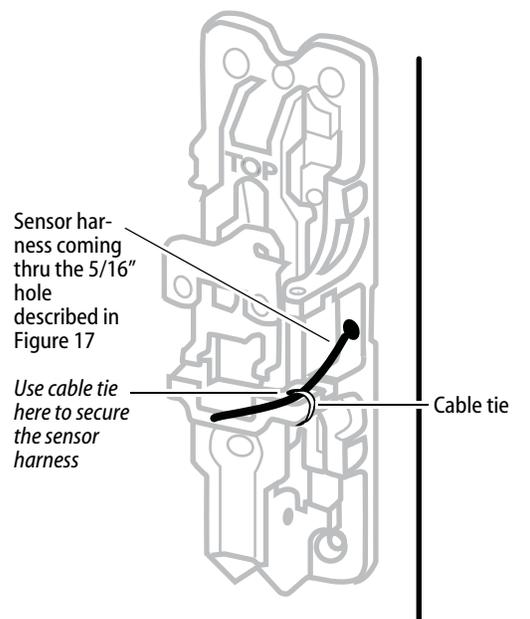


Figure 26 Using cable ties to hold wires for Precision 2200, 2700, and 2800 exit devices

## Installing the exit hardware and trim

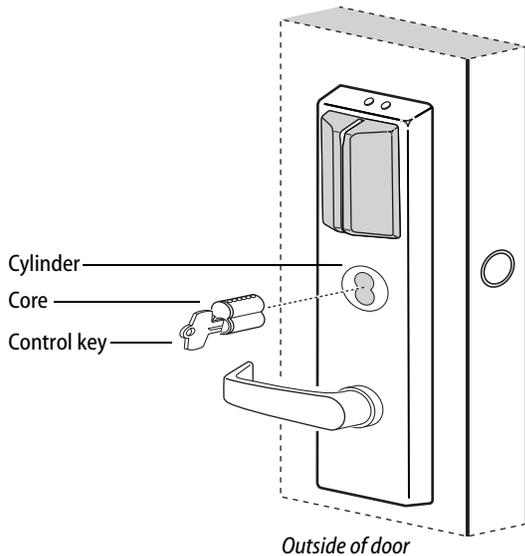


Figure 27 Installing the core

### 14 Install core

- 1 Insert the control key into the core and rotate the key 15 degrees to the right.
- 2 With the control key in the core, insert the core into the cylinder as shown in Figure 27.
- 3 Rotate the control key 15 degrees to the left and withdraw the key.

**Caution:** The control key can be used to remove cores and to access doors. Provide adequate security for the control key.

### 15 Install mortise case faceplate (mortise exit devices only)

- 1 Secure the mortise case faceplate to the mortise case; follow the instructions provided by the exit hardware manufacturer.
- 2 Check the lock for proper operation.

### 16 Install strike(s)

**Note:** If retrofitting the trim to an existing exit hardware installation, skip this task.

- 1 Install the strike(s) in the door frame or door stop; follow the instructions provided by the exit hardware manufacturer.
- 2 Check the lock for proper alignment between the strike(s) and latch(es).

## Completing the installation

### 17 Install battery bracket on door

- 1 Position the battery bracket on the inside of the door as shown in Figure 28.

**Note:** If installing with a surface rod exit device, the battery bracket is mounted over the upper rod.

- 2 Secure the battery bracket to the door using two of the mounting screws provided.

**Note:** For doors less than 2" in thickness, use the 1 1/4" screws. For doors 2" or greater, use the 1 3/4" screws.

**Caution:** When routing the wire harness, make sure the wires are not routed across any sharp edges or over any surface that could damage their sleeving or wire insulation. Keep away from any moving parts.

- 3 Tape all wires to the bracket using the tape provided.

**Note:** For Precision 2300, Sargent 8800, or any Von Duprin exit device without RQE, sensor harness and door position switch wires will also be run into this area of the battery bracket.

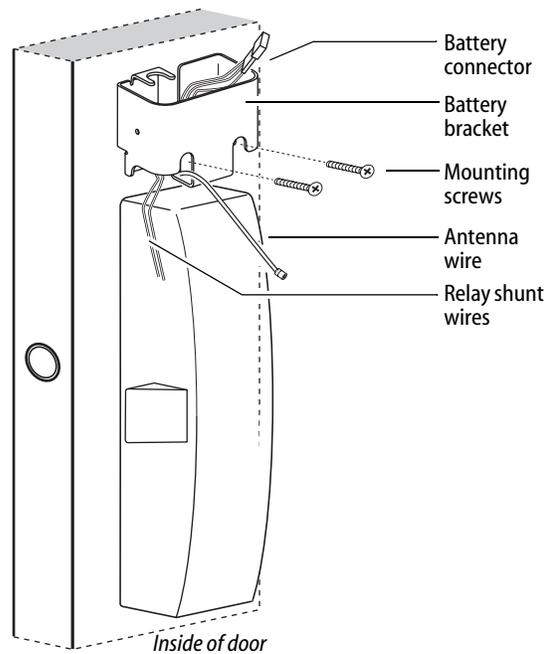


Figure 28 Installing the battery bracket on the door

## Completing the installation

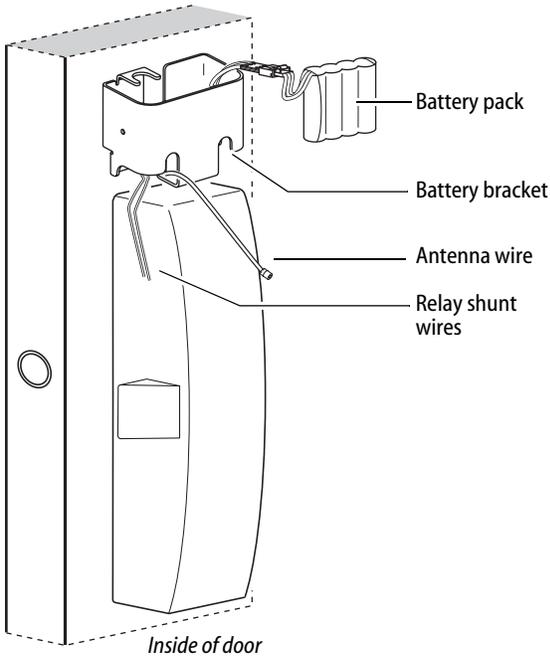


Figure 29 Connecting the battery pack

### 18 Install battery pack in bracket

- 1 Connect the battery pack to the battery connector on the wire harness as shown in Figure 29.

**Caution:** When connecting the battery pack, make sure:

- there are no loose wire connections where the wires are inserted into the connectors
- the connectors are firmly mated.

- 2 Place the battery pack in the holder inside the battery bracket and dress the wire harness inside the bracket.

**Caution:** The battery pack fit will be snug. Make sure you do not damage the sleeving on the battery pack. Doing so may cause the batteries to drain.

- 3 If installing with a surface vertical rod device, dress the wire harness inside the bracket to the left of the rod so that the harness will not interfere with the movement of the rods.

We recommend that you loosely coil the harness and use a cable tie to secure the coil. To avoid damaging the harness, do not put any sharp bends in it or flex it close to the connectors.

**Caution:** Failure to dress the wire harness away from the rod could damage the wire harness, causing the lock's electronics to not work properly.

## Completing the installation

### 19 Install battery/antenna cover

- 1 **If installing with a surface vertical rod exit device,** carefully use a razor blade to remove the knockouts for the rod from the battery cover. See Figure 30.
- 2 Connect the antenna to its mating connector.
- 3 Coil the antenna wire carefully inside the battery cover.

**Caution:** Carefully bend, but do not twist or kink the antenna wire. Doing so may significantly reduce or completely interrupt signal transmission.

- 4 **Making sure that the battery/antenna cover does not pinch any wires,** place the battery/antenna cover over the bracket and battery.
- 5 Secure the battery cover with the provided self-tapping screws.

**Caution:** Tighten screws firmly but do not over-tighten. Over-tightening may strip screw holes or crack the cover.

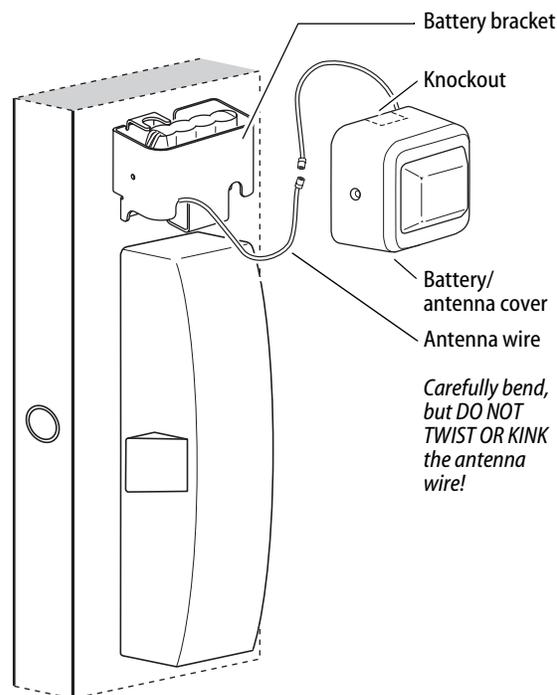


Figure 30 Installing the battery cover over the battery bracket and connecting the antenna

## Completing the installation

### 20 Test lock

#### For EXQ Locks with keypad only:

To test the lock for proper operation before the lock is programmed, follow these instructions:

- 1 Press **1234**.
- 2 Press **#**.  
The green light flashes and the locking mechanism unlocks.
- 3 Turn the lever and open the door.

#### For all other locks:

To test the lock for proper operation before the lock is programmed, use the temporary operator card that came with the lock. This card is for temporary use only. After permanent cards have been programmed for the lock, the temporary card should be deleted.

- 1 Use the temporary operator card to activate the lock.
- 2 Use the temporary operator card to access the lock.  
The green light flashes and the locking mechanism unlocks.
- 3 Turn the lever or knob and open the door.
- 4 With the door closed, insert and turn the key to unlatch the door.

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

LEDs	Sounder	You should
Single red flash	1 short tone	Use the card at a moderate speed.
Single red flash	3 short tones	Use the temporary operator card provided with the lock. <b>or</b> Perform a door reset to restore to the factory default settings (the lock may already be associated/programmed)
Alternating red and green flashes	none	Check the motor connection.
none	none	Check the battery connection.

**Important: When the trim and exit hardware installation is complete, perform all testing specified by the exit hardware manufacturer.**



# Installation Instructions for Stanley Wi-Q™ Technology WQX-WAC Wireless Access Controllers

## Introduction

The WQX Wireless Access Controller (WAC) controls access to one door or access point. It runs on four AA batteries, or can be externally powered with a DC power supply. The WAC can be purchased integrated in a box with power supply or can be purchased stand-alone. If purchased as a stand-alone unit the power supply powering the WAC (WQX alone with no other devices connected) must be able to deliver at least 500mA.<sup>a</sup>

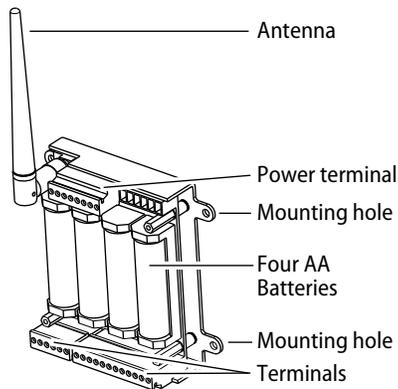


Figure 1 Wireless Access Controller, shown without cover

## Site survey

If a site survey has not been completed, contact your Stanley Representative.

## Components checklist

Use the following checklist to make sure that you have the items necessary to install your Wireless Access Controller.

- a. Power for WAC device only. Calculate power requirements for attached readers separately.

## Components provided in the box

- Wireless Access Controller with antenna
- Batteries
- Documentation

## Optional components

- Indoor ceiling mount omni-directional antenna
- Indoor wall mount directional antenna
- Outdoor mount directional antenna
- Outdoor mount omni-directional antenna
- Enclosure

## 1 Mount Wireless Access Controller

The standard WAC comes with a small antenna, but you may need a supplemental antenna for your application. See the *Site Survey Tool Quick Reference Guide* for more antenna information.

- 1 Determine the appropriate location for the wireless single door controller, making sure that the antenna will have maximum exposure for signal transmission.
- 2 Mount the Wireless Access Controller box.
- 3 Screw on antenna as shown in Figure 1 so that it's vertical and upright.
- 4 Install batteries if needed.

## 2 Install other hardware as necessary

Make sure all other system components are mounted and installed. System components may include:

- Electronic or electric lock or strike
- Request-to-exit switch
- Power supply for lock or strike
- Reader: either magstripe, proximity, keypad or combination readers. The default reader is a Weigand, 26-bit, 8-bit word type.

## Planning the installation

Manufacturer	Part number
Stanley	909028065
Indala	FP2511A
XceedID	XF-1050-B
HID	5355AGK00
Essex	KTP-163-SN

- Sensors: door, latch, deadbolt, key, and/or other.  
**Note:** Some sensors may be included inside the lock. The BEST 45HW may include door, latch, deadbolt, and key sensors.

### 3 Pull wire and make connections to wireless access controller

- 1 Determine what connections you need to make based on your application.
- 2 Using Figure 2 and Table 1 make the connections.

Table 1 WAC Connections and descriptions

Terminal	Description
<b>Strike NC</b>	Normally-closed terminal where the locking mechanism connects
<b>Strike COM</b>	Common return path for current through the locking mechanism
<b>Strike NO</b>	Normally-open terminal where the locking mechanism connects
<b>SHUNT NC</b>	Normally-closed relay terminal that shunts door force alarm if access is granted or RQE is activated
<b>SHUNT COM</b>	Return path for the shunt relay
<b>SHUNT NO</b>	Normally-open terminal for the shunt relay
<b>KEY</b>	Detects and reports a key-over-ride event

Table 1 WAC Connections and descriptions

Terminal	Description
<b>GND</b>	Return path for the key-over-ride switch and RQE
<b>RQE</b>	Request-to-exit input
<b>DS</b>	Door status input
<b>GND</b>	Return path for door status and latch status
<b>LS</b>	Latch status input
<b>WIEGAND 0</b>	Wiegand D0 terminal
<b>GND</b>	Ground (the wiegand reader must be grounded at this point)
<b>WIEGAND1</b>	Wiegand D1 terminal
<b>RED</b>	Red LED control input
<b>GND</b>	LED ground point
<b>GRN</b>	Green LED control input
<b>ANT</b>	Antenna connection
<b>Negative DC terminal</b>	Power connection
<b>Negative DC terminal</b>	Power connection. Use the extra negative DC terminal to 'daisy-chain' power to another wireless access controller or reader. <sup>a</sup>
<b>Positive DC 9–24V terminal</b>	Power connection
<b>Positive DC 9–24V terminal</b>	Power connection. Use the extra positive DC terminal to 'daisy-chain' power to another wireless access controller or reader. <sup>a</sup>

- a. Make sure the power supply is of appropriate wattage to supply enough power.

**Important note:** When using the WAC to daisy-chain other devices, be sure that the other devices will accept the voltage supplied to the WAC.

## Planning the installation

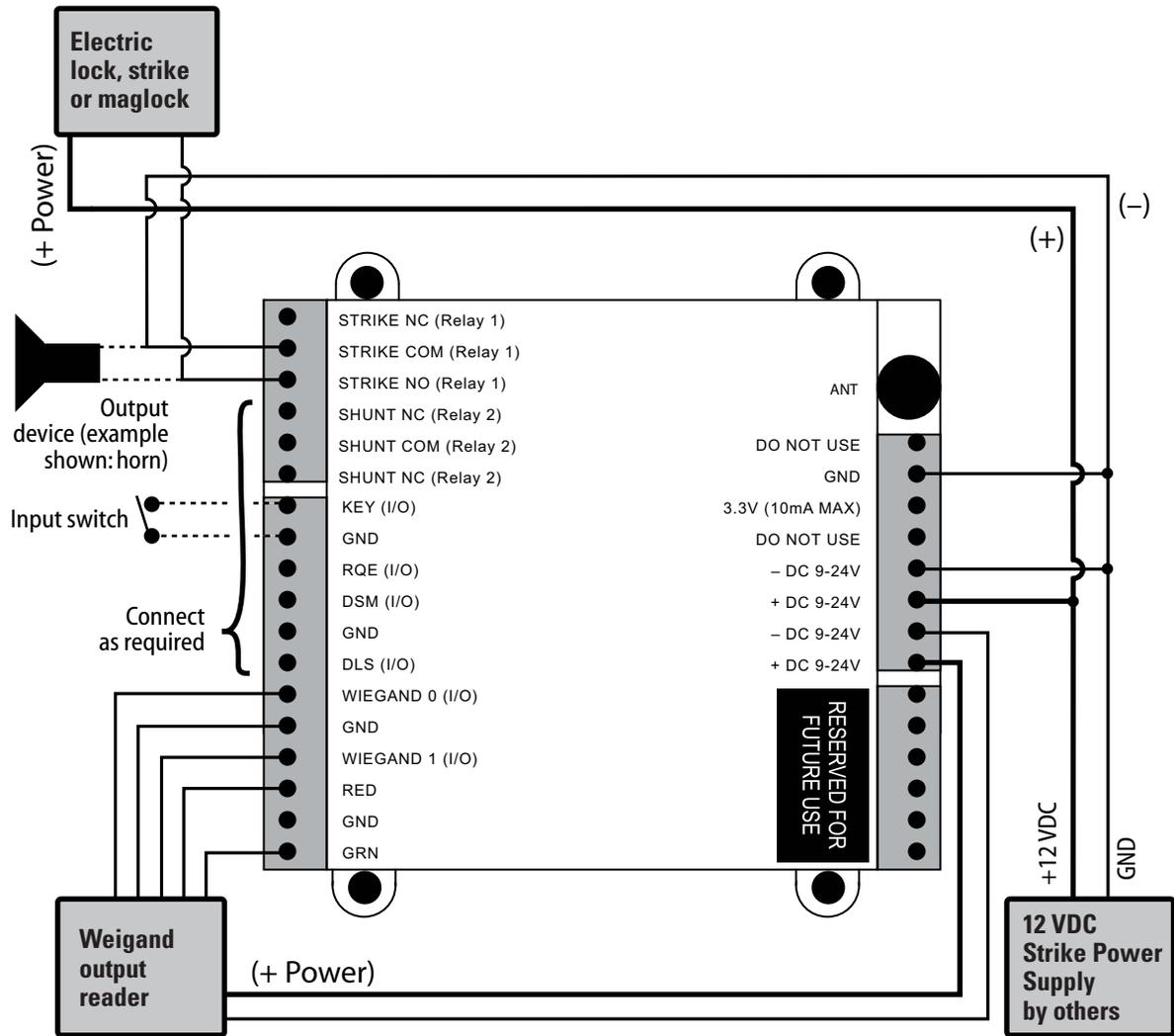


Figure 2 Wireless Access Controller, typical installation.  
See Table 1 for a description of connections.

## Planning the installation

### 4 Sign on WAC

The process of bringing a WAC into the Stanley Wi-Q™ Access Management System (AMS) is known as signing on.

If the connected reader doesn't have a keypad, a sign-on keypad is required. If no wired keypad is installed, a sign-on keypad is available as accessory WQD-WAC-PAD.

#### Connect the sign-on keypad to the WAC Wireless Access Controller

- 1 Once the WAC is wired, connect the sign-on keypad to the WAC reader terminal.

#### Signing on a WAC Wireless Access Controller

- 2 Enter **5678** on the keypad.

*This will cause the green LED to blink the on the WAC three times.*

- 3 Enter the sign-on key for the facility in the AMS database.

**Note:** *The sign-on key can be found under the facility sign-on credential field in the Wi-Q Technology™ Access Management System (AMS). Refer to the Stanley Wi-Q AMS User Guide.*

*You should see the red and green LEDs blinking and the blue light turns ON to indicate that the radio on the board is active. Once the reader signs on to one of the portal gateways in your facility, the green LED on the WAC blinks three times. At this point the WAC should appear under the New Facility Item folder in AMS (it may take up to 2 minutes for this to occur).*

### 5 Test WAC

#### For Wireless Access Controller with keypad only:

To test the WAC for proper operation before it's programmed, follow these instructions:

- 1 Press **1234**.
- 2 Press **#**.

*The green light flashes and the locking mechanism unlocks or you should hear a relay click.*

- 3 Operate the lock and open the door.

#### For Wireless Access Controllers wired to card readers:

To test the lock for proper operation before the lock is programmed, use the temporary operator card that came with the device. This card is for temporary use only. After permanent cards have been programmed into the device, the temporary card will no longer unlock the lock (once users are programmed into the WAC).

- 1 Using the installed reader to access the lock, present the temporary operator card to gain access.

*The green light flashes and the locking mechanism unlocks.*

#### If the mechanism doesn't unlock, use the on-board LEDs and refer to the following table.

WAC on-board LEDs	You should
Single red flash	Use the card at a moderate speed.
Three red flashes	Use the temporary operator card provided with the lock. or Perform a deep reset to restore to the factory default settings (the lock may already be associated/programmed)

## Planning the installation

WAC on-board LEDs	You should
none	Check the battery connection.
no blue light	Reset. Sign-on the WAC using the sign-on procedure.

LEDs	You should
Single red flash	Use the card at a moderate speed.
Three red flashes	Use the temporary operator card provided with the lock.

### Resetting the WAC

The WAC has two reset functions:

- **Soft reset** – restores previous functionality. Use this under normal operation. It will reset the WAC, but DOES NOT ERASE USERS.
- **Hard reset** – restores factory settings. Use this reset only when moving the WAC or after exhausting all other troubleshooting options.

### Using the soft reset function

- Hold the reset button until the green LED flashes five times and then release. See Figure 3.  
*Lights will alternate red/green rapidly.*  
*The WAC is restored to its previous functionality*

### Using the hard reset function

**Caution: Use this procedure only to restore the factory default settings. Performing these steps will erase all user data that may have been programmed into the WAC.**

- Hold the reset button for up to 30 seconds — until the green LED flashes and then the red LED flashes three times. Then release. See Figure 3.  
*All users are erased and the WAC is restored to its factory default settings.*

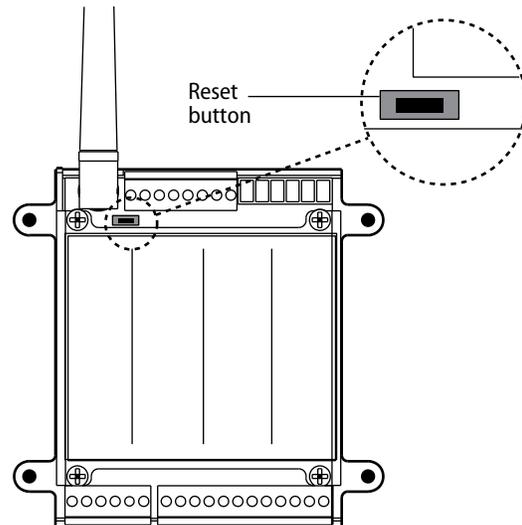


Figure 3 Using the reset button

*Installation Instructions for Stanley Wi-Q™ Technology WQX-WAC Wireless Access Controllers*

**STANLEY**

# OMNILOCK® Installation Instructions for Stanley Omnilock 9KOM Cylindrical Locks

## Planning the installation

### Contents

These installation instructions describe how to install your 9KOM Cylindrical Lock. Topics covered include:

<i>Planning the installation</i> .....	1
<i>Preparing the door and door jamb</i> .....	2
<i>Installing the lock</i> .....	7
<i>Completing the installation</i> .....	9

### Site survey

Use the following survey to record information about the installation site. You need this information to determine how to prepare the door for the lock.

### Door information

Door handing and bevel:

- Left hand (LH)
- Left hand, reverse bevel (LHRB)
- Right hand (RH)
- Right hand, reverse bevel (RHRB)

Door thickness: 1-3/4 to 2 inches (44 to 50 mm). If other than 1 3/4" (44 mm), see "Optional: Adjust for door thickness" on page 6.

### Environment information

Model	Side of door	Temperature Range	Exposure
Standard	Outside	+32°F to +129°F 0°C to +54°C	Drip proof. Inadvertent water splash accepted.
Weatherized	Outside	-4°F to +129°F -20°C to +54°C	Direct exposure to rain and snow
Extreme Weatherized <sup>a</sup>	Outside	-40°F to +129°F -40°C to +54°C	Direct exposure to rain and snow
	Inside	+32°F to +129°F 0°C to +54°C	N/A

a. See Stanley installation instruction *Addendum (T83317) Extreme Weatherized Installation* for the extreme weatherized model.

### Components checklist

Use the following checklist to make sure that you have the items necessary to install your Electronic Stand-alone Cylindrical Lock.

#### Components provided in the box:

- Outside lever
- Inside lever
- Throw member package
- Latch
- Strike package
- Through-bolt screws
- Installation template and instructions
- Four AA size batteries (or 2 weatherized packs)

#### Other components:

- Programming Default ID Card (provided with software)

### Special tools checklist

Use the following checklist to make sure that you have the special tools necessary to install your Electronic Stand-alone Cylindrical Lock.

- KD303 Drill jig
- KD325 Strike plate locating pin
- KD315 Faceplate marking chisel

## Preparing the door and door jamb

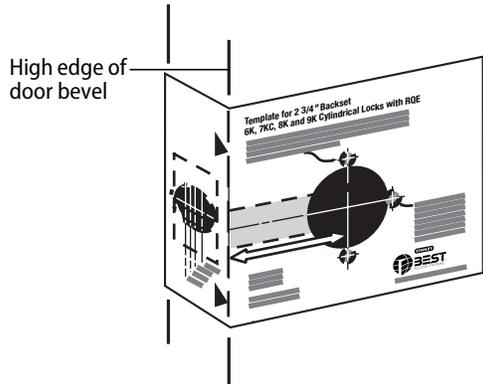


Figure 1 Positioning the template

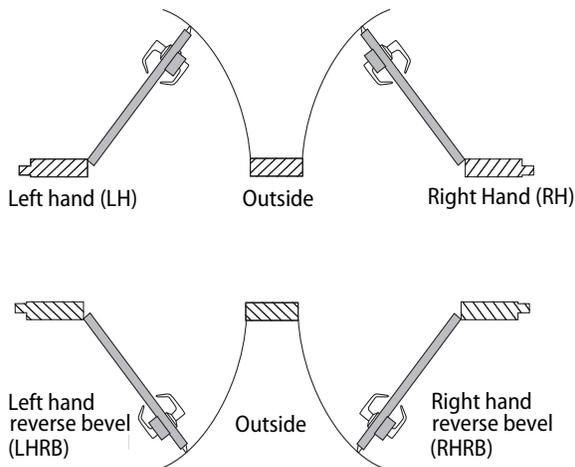


Figure 2 Door handing chart

### 1 Position template and mark drill points

**Note:** If the door is a fabricated hollow metal door, determine whether it is properly reinforced to support the lock. If door reinforcement is not adequate, consult the door manufacturer for information on proper reinforcement. For dimensions for preparing metal doors for locks with 2 3/4" (70 mm) backset, see Template T56052 or T56053 Door and Frame Preparation for 63K, 73KC, 83K, and 93K Cylindrical Locks.

**Note 1:** If the door is a LH or RH door, mark the inside of the door. If the door is a LHRB or RHRB door, mark the outside of the door. See Figure 2.

**Note 2:** For Extreme Weatherized model template, see Installation Addendum for Stanley Omnilock 9KOM Extreme Weatherized Locks (T83319).

#### For uncut doors and frames

- 1 Measure and mark the horizontal centerline of the lever (the centerline for the chassis hole) on the door and door jamb. Mark the vertical centerline of the door edge.

**Note:** The recommended height from the floor to the centerline of the lock (centerline of 2 1/8" (54 mm) hole) is 40 5/16" (1024 mm).

- 2 Fold the template on the dashed line and carefully place it in position on the high side of the door bevel as shown in Figure 1.

**Note:** For steel frame applications, align the template's horizontal centerline for the latch with the horizontal centerline of the frame's strike preparation.

- 3 Tape the template to the door.
- 4 Center punch the necessary drill points. Refer to the instructions on the template.

## Preparing the door and door jamb

### For doors with standard cylindrical preparation

- 1 Fold the template on the dashed line. Looking through the hole from the opposite side of the door, align the template so that you see the template outline of the 2 1/8" (54 mm) diameter chassis hole.
- 2 Tape the template to the door and enter punch the necessary drill points.

## 2 Drill holes and mortise for latch face

**Note:** To locate the center of a hole on the opposite side of the door, drill a pilot hole completely through the door.

- 1 Drill the holes in order listed below:
  - **motor wire hole**
    - ◆ 7/16" (11 mm) diameter through door
    - ◆ always drill before drilling chassis hole
  - **chassis hole**
    - ◆ 2 1/8" (54 mm) diameter through door
    - ◆ drill after drilling motor wire hole
  - **latch hole**
    - ◆ 1" (25 mm) diameter
    - ◆ meets chassis hole
  - (OPTIONAL) **Door Status Switch**
    - ◆ 1" (25 mm) diameter on door
    - ◆ 1" (25 mm) diameter on jamb
    - ◆ 1-3/4" (44mm) deep on door
    - ◆ 1" (25 mm) deep on jamb

**Note:** The latch tube prongs should be centered and should project into the chassis hole.

- 2 Mortise the edge of the door to fit the latch face.
- 3 Drill the holes for the latch screws.
- 4 Install the latch in the door as shown in Figure 4.
- 5 For optional door status switch: Position the bit inside the hole. Then drill a 3/8" (10mm) channel at an angle that will connect the door status switch hole to the chassis hole as shown in Figure 4.
- 6 Press fit both switch pieces as shown in Figure 4.
- 7 Check that the door swings freely.

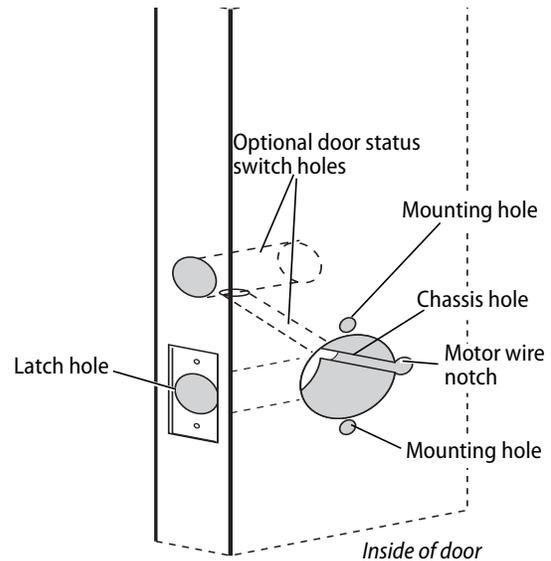


Figure 3 Drilling holes and mortising for the latch face

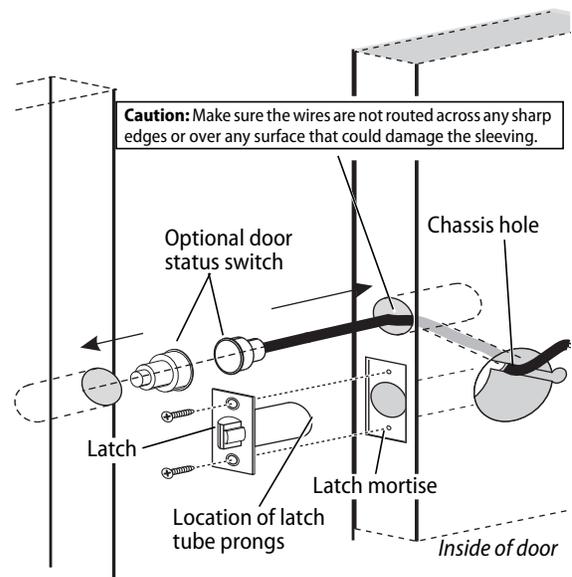


Figure 4 Installing the latch in the door

## Preparing the door and door jamb

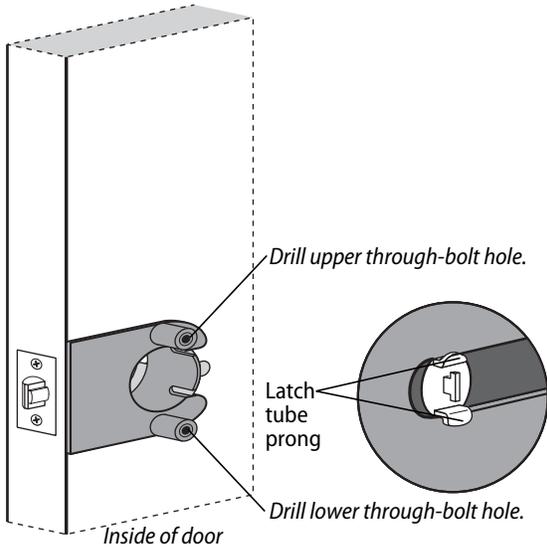


Figure 5 Installing the drill jig and drilling the through-bolt holes

### Use drill jig to drill through-bolt holes

- 1 Press the drill jig (KD303) onto the door, engaging it with the latch tube prongs (see the close-up in Figure 5). Make sure the front edge of the jig is parallel with the door edge.
- 2 Drill the through-bolt holes ( $5/16''$  (8 mm) diameter) halfway into the door.
- 3 Turn over the drill jig and repeat steps 1 and 2 from the opposite side of the door.

**Note 2:** Replace the drill jig after 10 door preparations.

## Preparing the door and door jamb

### 3 Install strike box and strike plate

- 1 Align with the center of the latchbolt, then mortise the door jamb to fit the strike box and strike plate. See Figure 6.
- 2 Drill the holes for the screws used to install the strike box and strike plate.
- 3 Insert the strike box and secure the strike with the two screws provided.
- 4 Check the position of the deadlocking plunger against the strike plate.

**Caution:** The deadlocking plunger of the latchbolt must make contact with the strike plate, as shown in Figure 7. The plunger deadlocks the latchbolt and helps prevent someone from forcing the latch open when the door is closed.

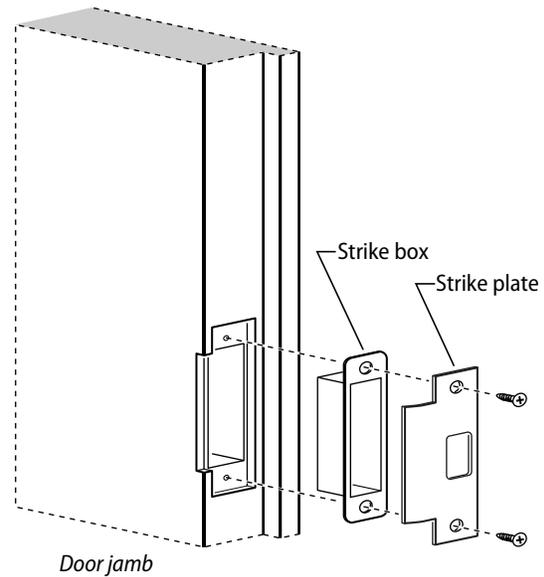


Figure 6 Installing the strike box and strike plate

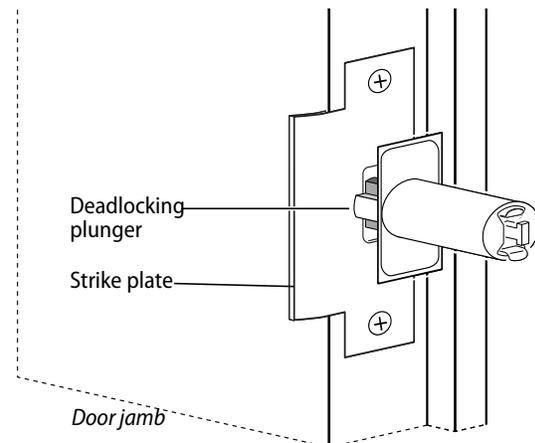


Figure 7 Aligning the deadlocking plunger with the strike plate

## Installation Instructions for Stanley Omnilock 9KOM Cylindrical Locks

### Preparing the door and door jamb

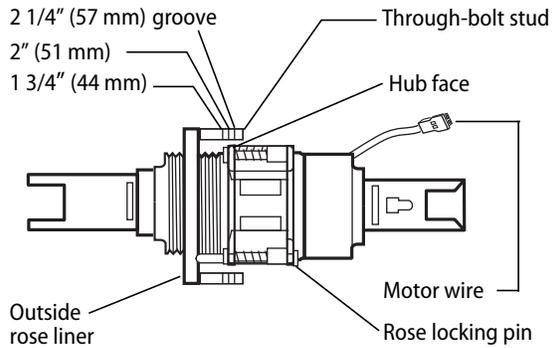


Figure 8 Adjusting the rose liner for the door

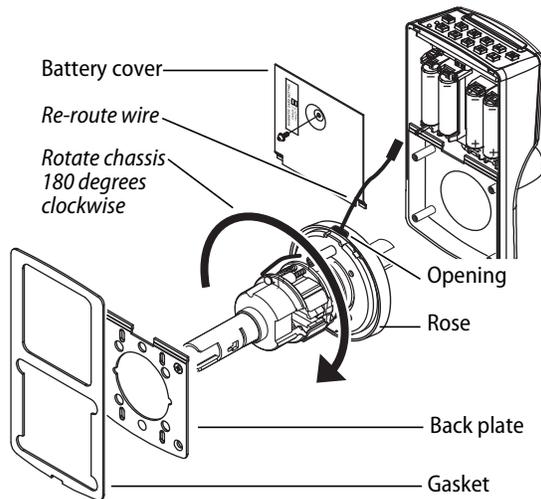


Figure 9 Adjusting the rose liner for the door

#### 4 Optional: Adjust for door thickness

**Note:** The default door thickness is 1 3/4" (44 mm). If your door is thicker than 1 3/4" (44 mm), use the following instructions.

- 1 Determine the door's thickness.
- 2 Pull the rose locking pin and rotate the outside rose liner until the proper groove on the through-bolt stud lines up with the hub face. See Figure 8.

#### 5 Optional: Adjust handing

**Note:** This is required only if the lock hand does not meet your application. The lockset is normally preset for a right-hand door. Verify the handing of the lock per Figure 2 and, if required, change the handing of the lock.

- 1 In order: remove the gasket, battery cover, and back plate. See Figure 9.
- 2 Remove the chassis.
- 3 Rotate the chassis 180 degrees clockwise (looking at the back or opposite the latch).

**Note:** Do not pull the wire.

- 4 Pry off the rose that holds the wire in place.
- 5 Re-route the wire back through the opening in the rose.
- 6 Press the rose back on.
- 7 Reinstall the chassis.

## Installation Instructions for Stanley Omnilock 9KOM Cylindrical Locks

### Installing the lock

#### 6 Install batteries

Four alkaline AA batteries (or two weatherized packs, if installing a weatherized unit) are furnished with your Omnilock system and must be installed before proceeding.

**Note:** For the Extreme Weatherized model, see *Installation Addendum for Stanley Omnilock 9KOM Extreme Weatherized Locks (T83319) for battery and escutcheon installation.*

- 1 Remove the gasket from the rear of the housing assembly as shown in Figure 10.
- 2 Remove the screw from the battery cover and remove the cover.
- 3 Install batteries with proper polarity as shown in Figure 11. (For weatherized battery packs, simply connect the wires from the battery pack to the circuit board as shown in Figure 12.)

**Note:** Be sure red and black motor wires are connected before attempting step 4. Align the wires together so that the wire colors match.

- 4 Press and hold the reset button on the PC board (as shown in Figure 11) until the green light on the keypad flashes (about three seconds), then release the button. If the green light does not flash see "Troubleshooting" on page 10.
- 5 Replace the battery cover. See Figure 10. Make sure that the tabs on the lower edge of the battery cover are hooked over the edge of the back plate and secure the cover with the screw.
- 6 Replace the gasket. See Figure 10. Make sure that it is inside the edge of the housing.
- 7 A label on the housing assembly battery cover indicates the magnetic card track (track 2 or track 3) that the system is set to read. See Figure 10.

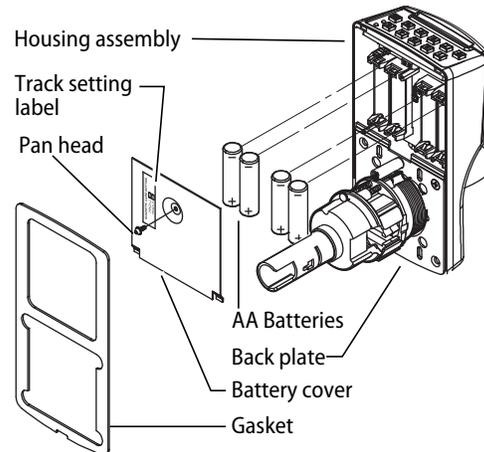


Figure 10 Installing batteries

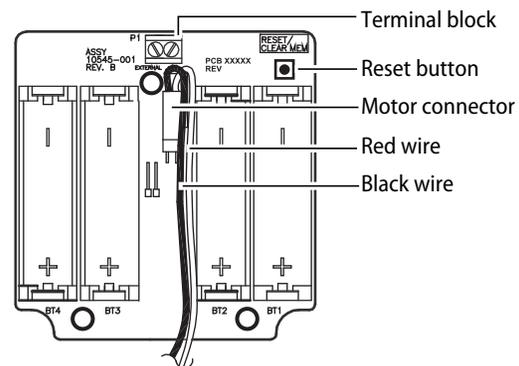


Figure 11 Using the reset button

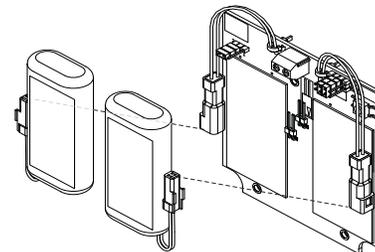


Figure 12 Weatherized battery packs

**Stanley Omnilock**

a Product Group of Stanley Security Solutions, Inc.

## Installing the lock

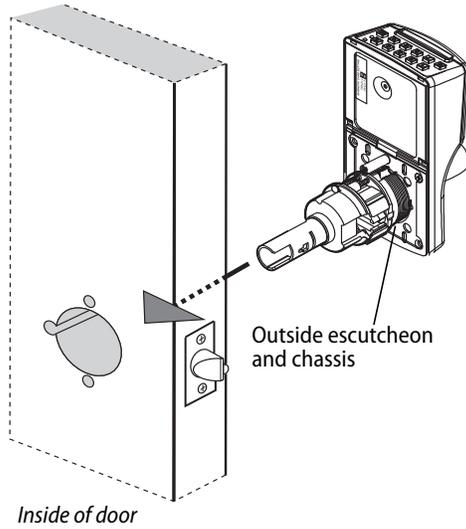


Figure 13 Installing the outside escutcheon and lock chassis

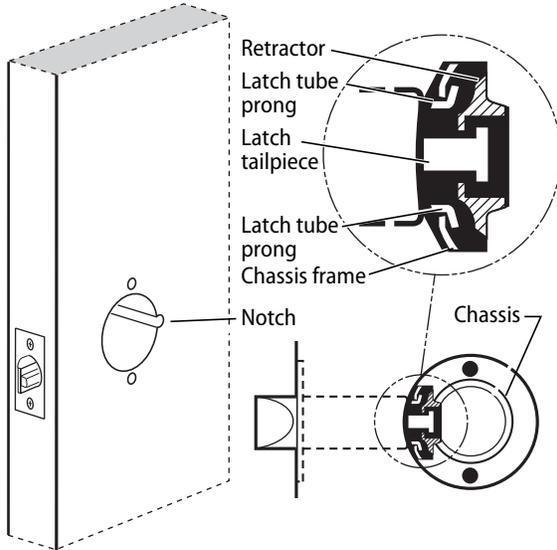


Figure 14 Installing the lock chassis and engaging the retractor in the latch

### 7 Install outside escutcheon and lock chassis and engage retractor in latch

- 1 From the outside of the door, insert the lock chassis and outside escutcheon into the 2 1/8" (54 mm) chassis hole. See Figure 13.
- 2 Make sure that the latch tube prongs engage the chassis frame and that the latch tailpiece engages the retractor. See Figure 14.

## Installation Instructions for Stanley Omnilock 9KOM Cylindrical Locks

### Installing the lock

#### 8 Install through-bolts, inside rose and lever

- 1 Place the inside rose liner on the chassis, aligning the holes in the rose liner with the holes prepared in the door as shown in Figure 15.
- 2 Install the through-bolts through the rose liner and door in the top and bottom holes.
- 3 Tighten the rose liner on the door with the through-bolts.
- 4 Press the inside rose onto the rose liner.
- 5 Push the inside lever onto the chassis shaft until it clicks in place.

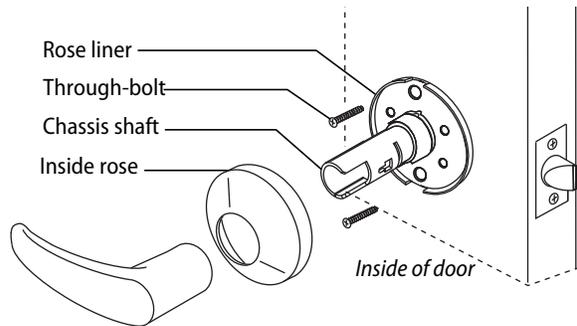


Figure 15 Installing the through-bolts and rose liner

#### 9 Install outside lever, core and throw member

##### For a non-IC lever handle

- 1 Place the cylinder inside the outside lever. See Figure 16.
- 2 Install the retainer into the outside lever.
- 3 Insert the key into the cylinder and rotate the key 90 degrees clockwise. Slide the lever assembly onto the chassis shaft until the lever clicks as it engages against the lever catch.
- 4 Pull on the lever to test that the lever catch is engaged. Turn the key back to the original position and remove it from the cylinder.

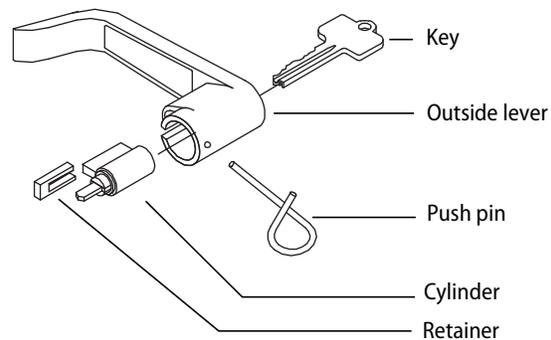


Figure 16 Installing outside lever (applies to both IC and non-IC levers)

##### For interchangeable core handles

- 1 Push the outside lever onto the chassis shaft until the lever clicks as it engages against the lever catch.
- 2 Install the blocking plate onto the throw member, then install the throw member in the core. See Figure 17.

**Caution: You must use the blocking plate to prevent unauthorized access.**

**For 6-pin core only:** Install the plastic spacer (not shown, supplied with permanent cores), instead of the blocking plate, on the throw member.

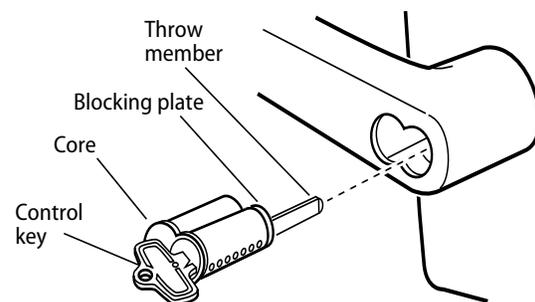


Figure 17 Installing the core

**Stanley Omnilock**

a Product Group of Stanley Security Solutions, Inc.

## Installing the lock

- 3 Insert the control key into the core and rotate the key 15 degrees to the right.
- 4 Insert the throw member into the core.
- 5 Insert the core and throw member into the lever with the control key
- 6 Return the control key to the original position and withdraw the key.

**Caution:** The control key can be used to remove cores and to access doors. Provide adequate security for the control key.

### 10 Test lock

To test the lock for proper operation before the lock is programmed:

#### For keypad locks

- 1 Press **1234 for the 2000 series, or 5011234 for the 500 series.**

*The green light flashes and the latch unlocks.*

- 2 Turn the lever and open the door.

*During the unlock time, the green light flashes. Then the red light flashes and the latch relocks.*

#### For magnetic stripe or proximity card only locks

**Note:** If the lock has a proximity card reader, it may have already been activated by the presence of an object near the card reader.

- 1 Align the magnetic stripe card with the V mark by the card slot.

- 2 Insert and then remove the card.

*The green light flashes and the latch unlocks.*

- 3 Turn the lever and open the door.

*During the unlock time, if using the Programming Default ID Card, the green light flashes. Then the red light flashes and the latch relocks.*

### Troubleshooting

If the mechanism does not unlock, remove the battery cover and check for proper orientation and seating of the batteries and motor connector. Ensure that wires are not pinched. Reset the electronics by pressing and holding the reset button on the circuit board until the light flashes green (approx three seconds), then release. See Figure 12.

*The system will go through a self-test and the green light will flash five times. You will hear the lock unlock, then relock three times. A red flash indicates a PC board or drive system problem. If a red flash or no flash is observed, check for proper orientation and seating of the batteries and motor connector, ensure that wires are not pinched, then repeat the reset process.*

## Installation Instructions for Stanley Omnilock 9KOM Cylindrical Locks

### Installing the lock

#### Removing the levers (when needed)

##### Removing the IC outside lever

- 1 Insert the control key into the core and rotate the key 15 degrees to the right.
- 2 Remove the core and throw member from the lever.
- 3 Insert a flat blade screwdriver into the figure-8 core hole and against the trapezoid-shaped lever keeper.
- 4 Push the screwdriver blade in the direction of the arrow in Figure 18.

**Caution:** Use the flat of the screwdriver to push the lever keeper sideways. Using the screwdriver tip to pry the keeper at an angle may result in unseating the retaining spring. For assistance, contact your local Stanley Omnilock dealer.

**Note:** You will not be able to remove the lever if the screwdriver blade is inserted past the keeper into the center hole.

- 5 Slide the lever from the sleeve.

##### Removing the non-IC outside lever

- 1 Insert the key into the cylinder and turn it 45 degrees clockwise.
- 2 Depress the lever catch through the hole in the outside lever by using the push pin or other suitable tool. See Figure 19.
- 3 Slide the outside lever off.

##### Removing the inside lever

- 1 Depress the lever catch through the hole in the inside lever by using the push pin or other suitable tool as shown in Figure 20.
- 2 Slide the inside lever off.

**Note:** Reinstall lever(s) according to "Install through-bolts, inside rose and lever" on page 9, or "Install outside lever, core and throw member" on page 9

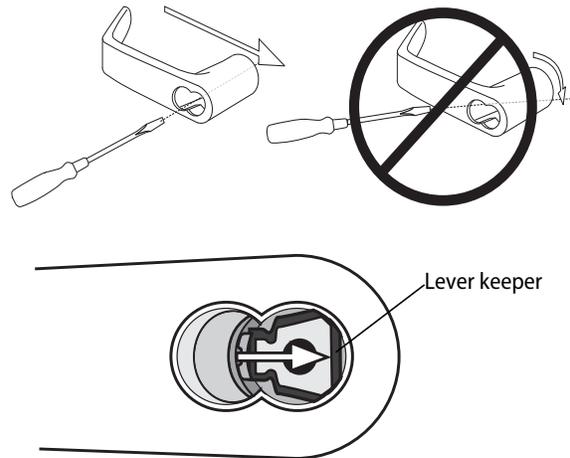


Figure 18 Push the lever keeper to remove the lever

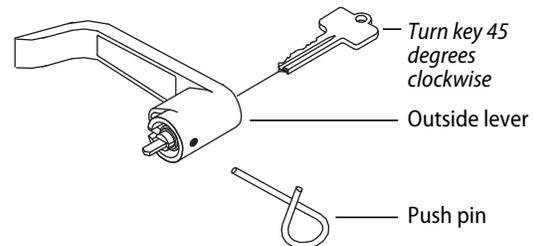


Figure 19 Removing the outside non-IC lever

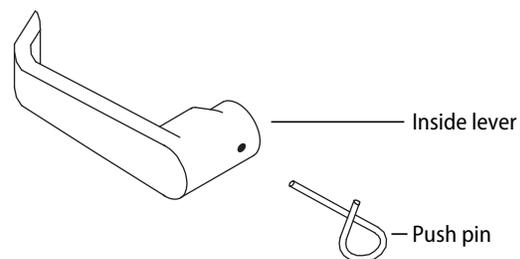


Figure 20 Removing the inside lever





# OMNILOCK®

## Installation Instructions for Stanley Omnilock 45HOM Mortise Locks

### Planning the installation

#### Contents

These installation instructions describe how to install your 45HOM Mortise Lock. Topics covered include:

*Planning the installation*.....1  
*Preparing the door and door jamb*.....4  
*Installing the lock*.....7  
*Completing the installation*.....9

#### Site survey

Use the following survey to record information about the installation site. You need this information to determine how to prepare the door for the lock.

#### Door information

Door handing and bevel:

If a handing change is required, see “Rotate latchbolt (if necessary)” on page 4.

- Left hand (LH)
- Left hand, reverse bevel (LHRB)
- Right hand (RH)
- Right hand, reverse bevel (RHRB)

Door thickness: 1-3/4 to 2 inches (44 to 50 mm).

#### Environment information

Model	Side of door	Temperature Range	Exposure
Standard	Outside	+32°F to +129°F 0°C to +54°C	Drip proof. Inadvertent splashing of water spray acceptable.
Weatherized	Outside	-4°F to +129°F -20°C to +54°C	Direct exposure to rain and snow
Extreme Weatherized <sup>a</sup>	Outside	-40°F to +129°F -40°C to +54°C	Direct exposure to rain and snow
	Inside	+32°F to +129°F 0°C to +54°C	N/A

a. See Stanley installation instruction *Addendum (T83317) Extreme Weatherized Installation* for the extreme weatherized model installation.

#### Components checklist

Use the following checklist to make sure that you have the items necessary to install your Omnilock Mortise Lock.

#### Components provided in the box:

- Inside and outside trim cassettes
- Inside and outside rose and rose ring
- Outside escutcheon assembly
- Mortise case assembly
- Mortise cylinder and collar
- Outside lever and spindle assembly
- Inside lever
- Strike package
- Installation template and instructions
- Screw package
- Mortise case faceplate
- Batteries
- Torx T15 driver
- 1/8" hex wrench

#### Other components:

- Programming Default ID Card (provided with software)

## Planning the installation

For hole sizes, see the OM1 Template T83316

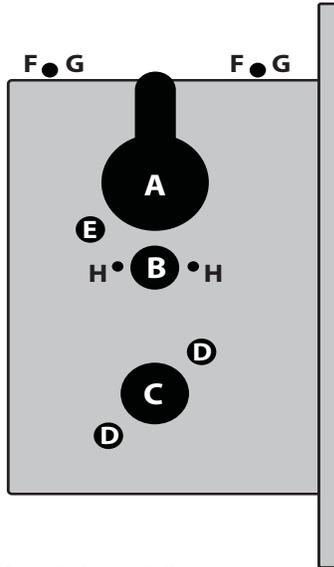


Figure 1 Identifying holes to drill

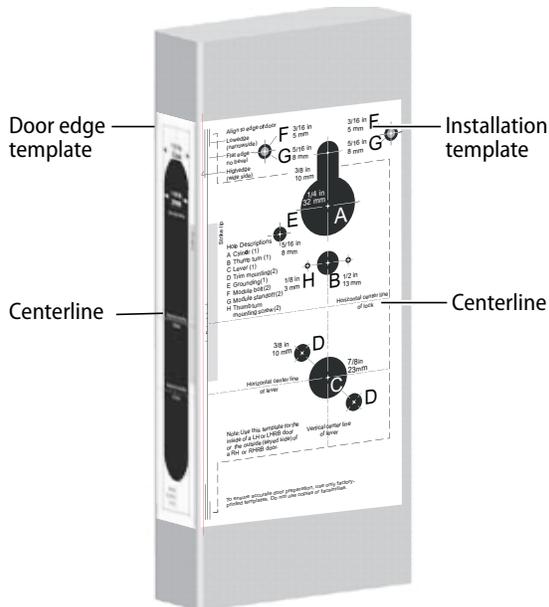


Figure 2 Aligning the templates

### 1 Identify holes to drill

- 1 Determine the lock function to be installed.
- 2 Determine the inside and outside, hand, and bevel of the door.
- 3 See the *Holes by Function* table and Figure 3 to determine the holes to be drilled for the lock function.

Holes by Function	Functions			
	DV		TV	
	In	Out	In	Out
A Cylinder		■		■
B Thumb turn			■	
C Lever <sup>a</sup>	Through door		Through door	
D Trim mounting (2 holes) <sup>a</sup>	Through door		Through door	
E Grounding hole		■		■
F Through bolt hole	Through door		Through door	
G Standoff hole		■		■
H Thumb turn mounting screw (2 holes)			■	
J Door Status Switch (Optional)			Door Edge	

- a. Because these holes pass through the mortise pocket, it is recommended that each hole be drilled separately rather than straight through.

### 2 Position template and mark drill points

**Note:** If the door is a fabricated hollow metal door, determine whether it is properly reinforced to support the lock. If door reinforcement is not adequate, consult the door manufacturer for information on proper reinforcement. For dimensions for preparing metal doors, see the OM2 Template — Installation Specifications for 45HOM Mortise Locks (T83318).

## Installation Instructions for Stanley Omnilock 45HOM Mortise Locks

### Planning the installation

- 1 Separate the templates provided on the *OM1 Template — Installation Template for 45H Mortise Locks (T83316)*.

**Note:** If installing an Extreme Weatherized model, see *Installation Addendum for Stanley Omnilock 45HOM Extreme Weatherized Locks (T83317)*. This includes the template for locating the extreme weatherized module mounting holes.

- 2 Position one of the door edge templates on the door, making sure that the lock case mortise shown on the template aligns with the mortise pocket prepared in the door.
- 3 Using the centerlines on the door edge templates as guides, position the appropriate door template on each side of the door. You need to take the bevel into account. Tape the templates to the door.

### 3 Center punch and drill holes

- 1 Center punch the necessary drill points. See the instructions on the template.
- 2 Drill the holes.

**Note 1:** To locate the center of a hole on the opposite side of the door, drill a pilot hole completely through the door.

**Note 2:** For holes through the door, it is best to drill halfway from each side of the door to prevent the door from splintering.

### 4 Optional: Install door status switch (Optional for TV function wireless locks only)

- 1 Locate the centerpoint for the door status switch 2 1/2" (64mm) above the top of the faceplate mortise on the edge of the door as shown in Figure 4.
- 2 Drill a 1" (25 mm) diameter hole 1 3/4" (44 mm) deep for the door status switch.
- 3 Position the drill so the tip of the bit is approximately 1" (25 mm) into the hole and the

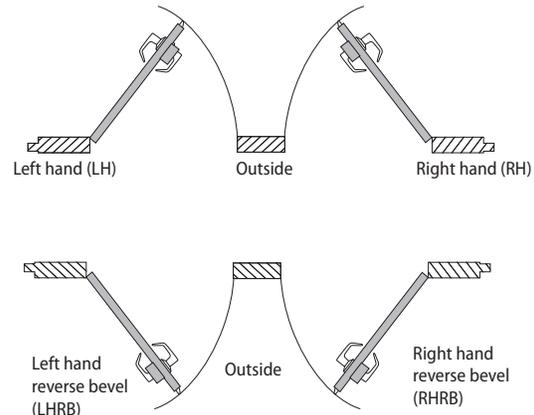


Figure 3 Door Handing Chart

### Optional for Wireless TV Models

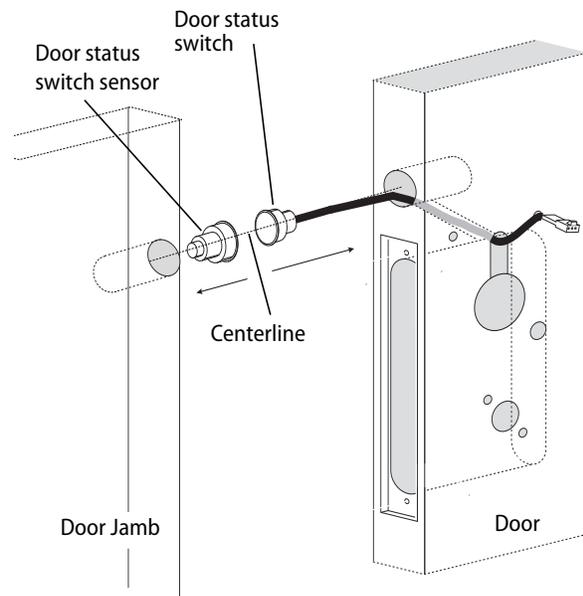


Figure 4 Installing the door status switch

## Configuring & installing the mortise

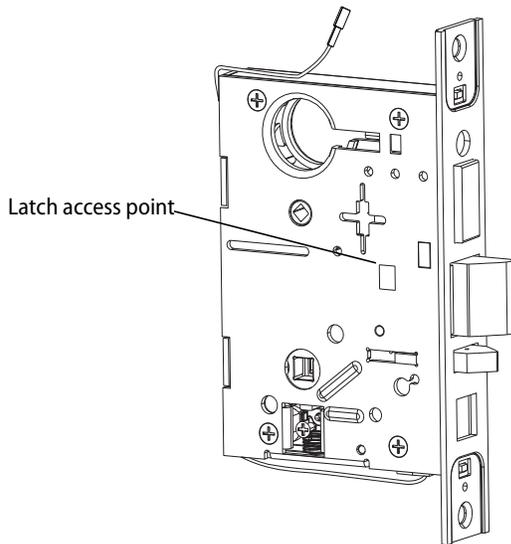


Figure 5 Rotating the latchbolt

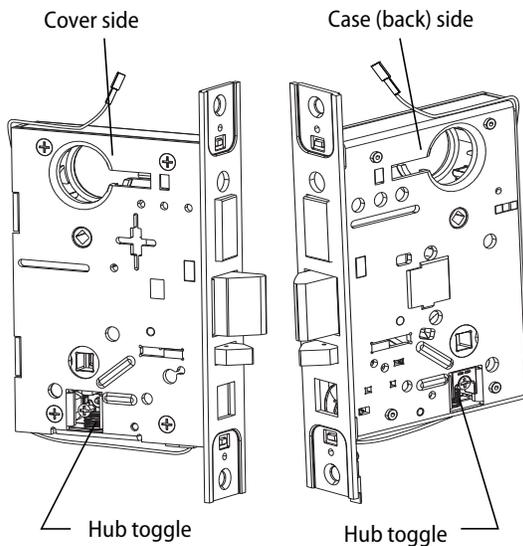


Figure 6 Positioning hub toggles

bit is close to the top edge of the hole. Then drill a 3/8" (10mm) channel at approximately a 35° angle from the door status switch hole into the mortise cavity as shown in Figure 4.

**Caution:** Make sure the wires are not routed across any sharp edges or over any surface that could damage the sleeving.

- 4 Press fit the door status switch assembly into the door status switch hole.
- 5 On the door jamb, drill a corresponding hole for the door status switch sensor. Use the door switch centerline as a guide. Press fit the sensor into the jamb.

### 5 Rotate latchbolt (if necessary)

**Note:** If a function specific mortise case was ordered, some steps for configuring the case have already been performed at the factory.

- 1 Determine whether you need to rotate the latchbolt to match the handing of the door.

**Note:** The angled surface of the latchbolt must contact the strike when the door closes.

- 2 If you need to rotate the latchbolt, insert a flat blade screwdriver into the latch access point approximately 1/2" (13 mm) into the case and press to extend the latch out of the case. See Figure 5.
- 3 Rotate the latchbolt past 180 degrees, keeping constant pressure on the latch access point. Then allow the latch to rotate back slightly and retract into the case.

### 6 Position hub toggles (if necessary)

- 1 Check whether the hub toggles are in the proper position for the lock. See the table below.

#### Hub toggle positions

Inside **down** (always unlocked)

Outside **up** (lockable)

## Installation Instructions for Stanley Omnilock 45HOM Mortise Locks

### Installing the trim

- For LH & LHRB doors, the inside is the case (back) side of the case and the outside is the cover side of the case. For RH and RHRB doors, the inside is the cover side of the case and the outside is the case (back) side of the case. The cover is mounted to the case with four screws.
- To change the position of a hub toggle, loosen the toggle screw, move the toggle into the desired position, and re-tighten the screw.

### 7 Install mortise case

- Drill the holes for the case mounting screws.
- Insert the mortise case into the mortise cavity, while feeding the motor wires and any optional sensor wires into the mortise cavity and keyhole to the inside of the door as shown in Figure 7.

**Note:** The armored front of the mortise case self-adjusts to the door bevel.

Option	DV	TV	Stand Alone	Wireless
Key Override Sensor (KOS)	■	■	■☒	■
Request-to-Exit (RQE)	■	■☒		■
Door Status Switch (DS) <sup>a</sup>	■	■☒		■
Latch Status Switch (LS)	■			■

a. Door status switch is located differently for DV and TV functions.

- Secure the mortise case with the case mounting screws.

### 8 Install trim mounting plates

- Insert the outside trim mounting plate through the door and mortise case.

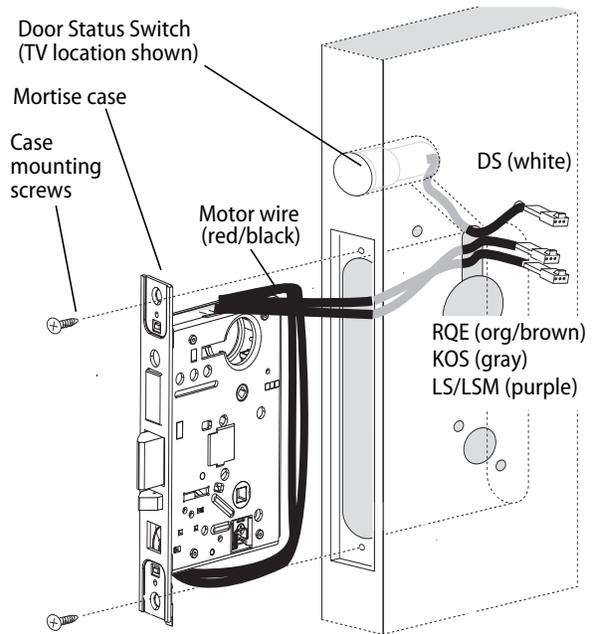


Figure 7 Installing the mortise case

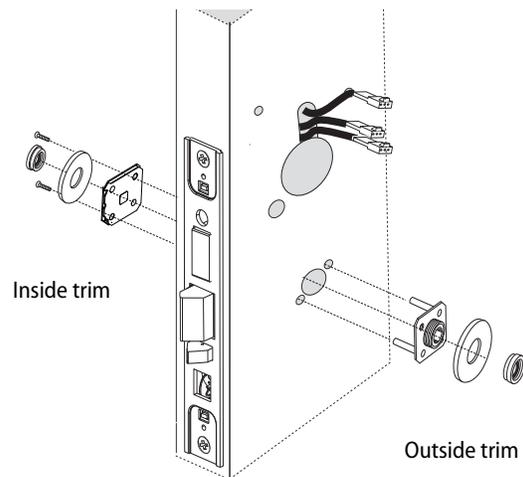


Figure 8 Installing the trim mounting plates

## Installing the lock

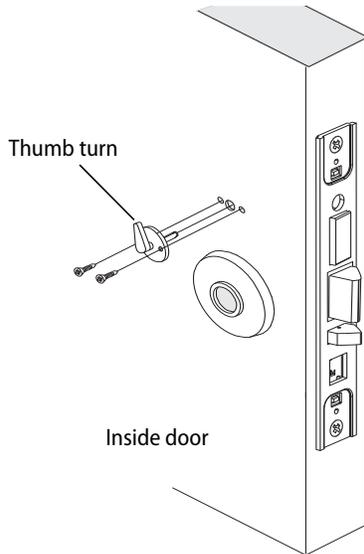


Figure 9 Installing the thumb turn

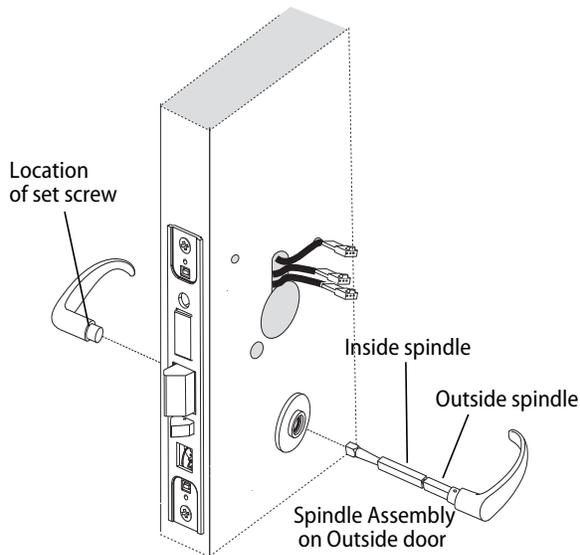


Figure 10 Installing the levers

- 2 Position the inside trim mounting plate opposite the outside trim mounting plate and screw them securely in place.

**Caution: Do not overtighten the trim mounting plate screws. Overtightening may damage the locking mechanism.**

- 3 Temporarily install a lever and test the lock to make sure that it doesn't bind.

### 9 Install thumb turn (TV function only)

- 1 Orient the thumb turn so it points up when the deadbolt is retracted, and toward the hinge edge of the door when the deadbolt is extended.
- 2 Install the thumb turn using the two screws provided. See Figure 9.

### 10 Install inside and outside levers

- 1 Unscrew the inside spindle one full turn to allow the spindles to turn freely. See Figure 10.
- 2 Remove the label from the inside spindle.
- 3 With the handle pointing toward the door hinges, insert the outside lever and spindle assembly into the lock from the outside of the door.
- 4 Slide the inside lever onto the inside spindle and secure it with the set screw.
- 5 Turn the levers to check that they operate smoothly.

## Installation Instructions for Stanley Omnilock 45HOM Mortise Locks

### Installing the lock

#### 11 Install batteries

Four alkaline AA batteries (or two weatherized packs if installing a weatherized unit) are furnished with your Omnilock system and must be installed before proceeding with operation verification and system installation.

**Note:** For the Extreme Weatherized model, see Addendum (T83317) Extreme Weatherized Installation for battery and escutcheon installation.

- 1 Remove the gasket from the rear of the housing assembly as shown in Figure 11.
- 2 Remove the screw from the battery cover and remove the cover.
- 3 Install batteries with proper polarity as shown in Figure 12. (For weatherized battery packs, simply connect the wires from the battery pack to the circuit board as shown in Figure 13.)

**Note:** Be sure red and black motor wires are connected before attempting step 4. Align the wires together so that the wire colors match.

- 4 Press and hold the reset button on the PC board (as shown in Figure 12) until the green light on the keypad flashes (about three seconds) then release the button. If green light does not flash, see "Troubleshooting" on page 12.
- 5 Replace the battery cover. See Figure 11. Make sure that the tabs on the lower edge of the battery cover are hooked over the edge of the back plate and secure the cover with the screw.
- 6 Replace the gasket. See Figure 11. Make sure that it is inside the edge of the housing.

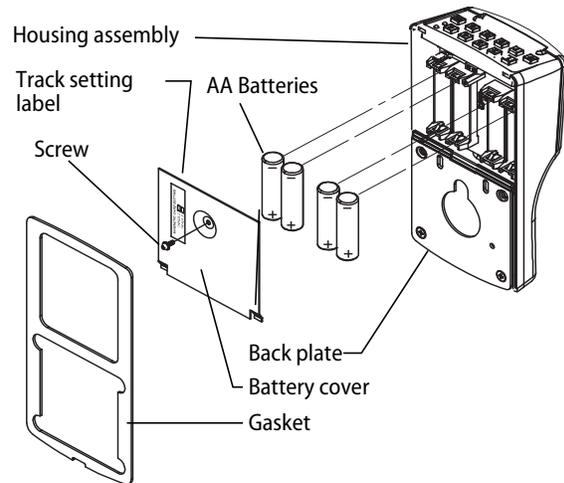


Figure 11 Installing batteries

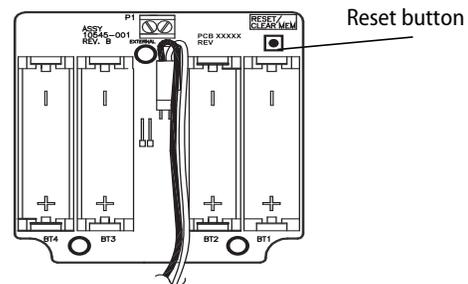


Figure 12 Using the reset button

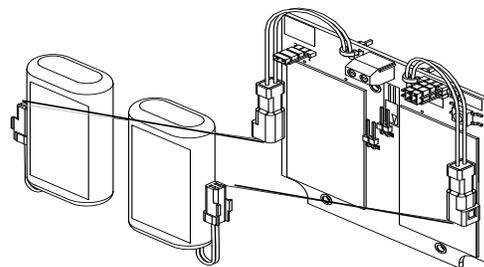


Figure 13 Installing weatherized batteries

## Installing the lock

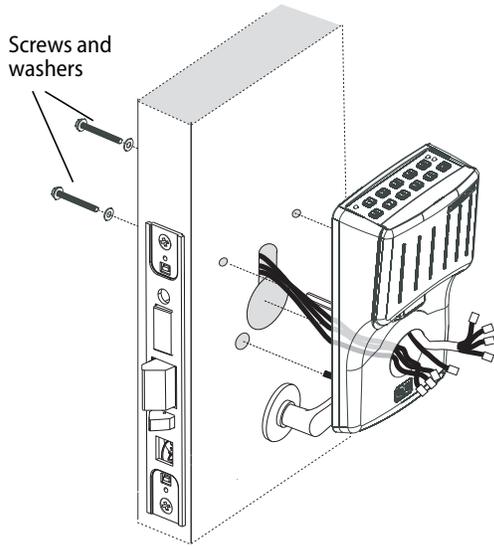


Figure 14 Installing the outside escutcheon

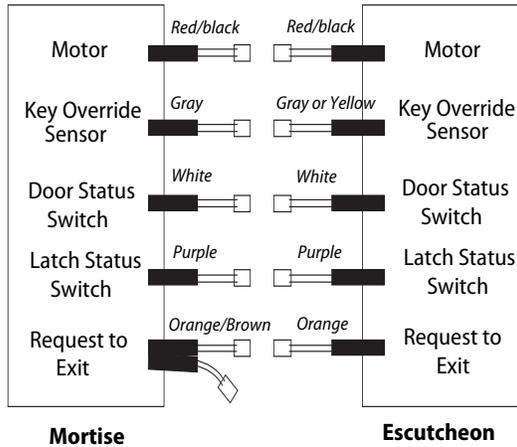


Figure 15 Simplified wiring diagram

### 12 Install outside escutcheon

- 1 Ensure that no wires are pinched when attaching the escutcheon to the door.
- 2 Insert the standoffs and grounding spring into the predrilled holes. Use screws and washers to attach the escutcheon from the inside of the door.

### 13 Connecting escutcheon wires

- 1 Connect the red and black motor wire from the mortise case to the red and black escutcheon motor wire. Align the wires together so that the wire colors match.
- 2 Connect the color-coded wires of the escutcheon wiring harness to the corresponding wire options on your mortise case. **Some wires may not be used.**

**Note:** Two RQE status switches are installed in the mortise case. However, only the switch for the inside of the lock needs to be connected. You will need to connect the 'Case Side' pair of RQE wires for LH and LHRB doors or the 'Cover Side' pair of RQE wires for RH and RHRB doors. See Figure 16. Wires are labeled.

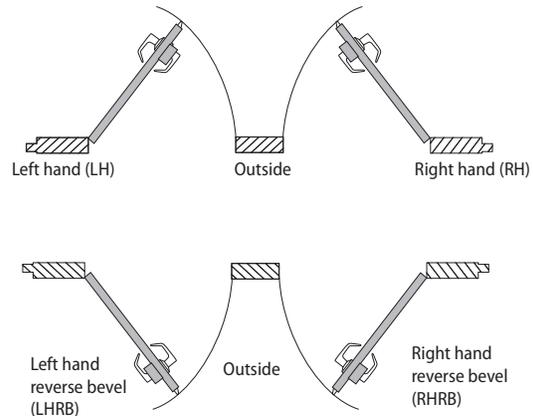


Figure 16 Door Handing Chart

## Finishing the installation

### 14 Install cylinder

- 1 Push any excess wires into the escutcheon housing. Make sure no wires are pinched.
- 1 Make sure cylinder collar is positioned on the cylinder.
- 2 Thread the cylinder into the mortise case. Rotate the cylinder until the cylinder is flush against the collar and the cylinder cam is in the 12 o'clock position. See Figure 17.

**Caution: A malfunction can occur if the cylinder is threaded in too far.**

- 3 Secure the cylinder in the mortise case with the cylinder retainer screw.

### 15 Install mortise case faceplate

- 1 Secure the mortise case faceplate to the mortise case with the faceplate mounting screws. See Figure 18.
- 2 Check the lock for proper operation.

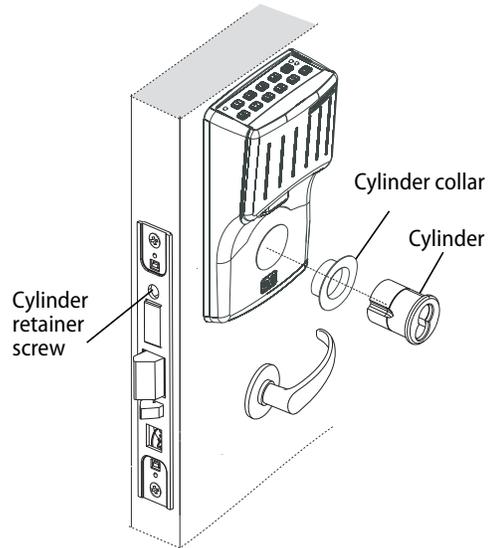


Figure 17 Installing the standard cylinder

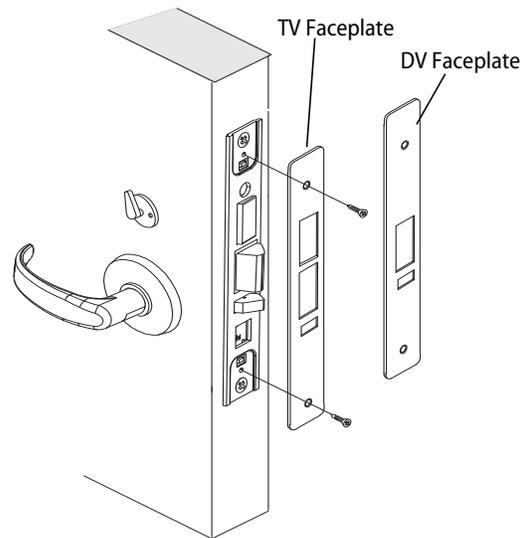


Figure 18 Installing the mortise case faceplate

## Finishing the installation

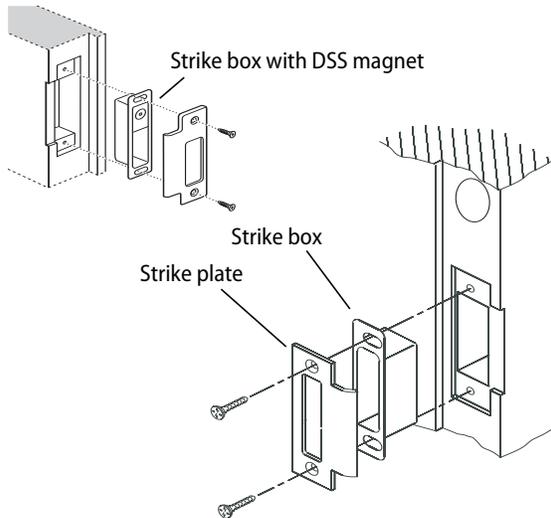


Figure 19 Installing the strike box and strike plate

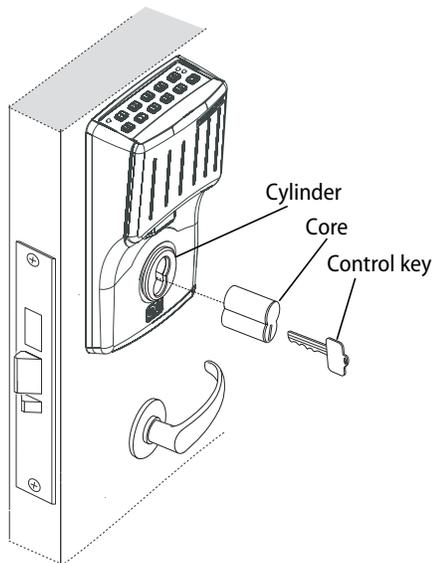


Figure 20 Installing the core

### 16 Install strike box and strike plate

- 1 If the door jamb has not been mortised for the strike box and strike plate, perform these steps:
  - a On the door jamb, locate the horizontal centerline of the strike (3/8" (10mm) above the centerline of the lock), as well as the vertical centerline of the strike.
  - b Mortise the door jamb to fit the strike box and strike plate.
  - c Drill the holes for the screws used to install the strike box and strike plate.

- 2 Insert the strike box into the mortise in the door jamb. Place the strike plate over the strike box and secure the strike with the screws provided.

**Note:** If installing a DV wireless model with a Door Status Switch, ensure that the magnet is located at the top of the strike box. See Figure 19.

- 3 Check the position of the auxiliary bolt against the strike plate (or the filled area of the strike box).

**Note:** The recommended gap between the door and jamb is 1/8" (3 mm).

### 17 Install core

- 1 Insert the control key into the core and rotate the key 15 degrees (midway between the 12 o'clock and 1 o'clock positions) to the right.
- 2 With the control key in the core, insert the core into the cylinder.
- 3 Return the control key to the 12 o'clock position and withdraw the key.

**Caution:** The control key can be used to remove cores and to access doors. Provide adequate security for the control key.

## **Finishing the installation**

---

### **18 Check operation**

Check the operation of the lock. For example, check that:

- door latches and opens properly
- deadbolt operates properly
- key access works
- door gap is 1/8" (3 mm)
- auxiliary bolt is held inside the case when the door is closed.

For assistance, contact your local Stanley Omnilock dealer.

### **19 Test lock**

To test the lock for proper operation before the lock is programmed, follow these instructions:

#### **For keypad locks**

- 1 Press **1234 for the 2000 series, or 5011234 for the 500 series.**

*The green light flashes and the latch unlock.*

- 2 Turn the lever and open the door.

*During the unlock time, the green light flashes. Then the red light flashes and the latch relocks.*

#### **For magnetic stripe or proximity card locks only**

**Note:** *If the lock has a proximity card reader, it may have already been activated by the presence of an object near the card reader.*

- 1 Align the magnetic stripe card with the V mark by the card slot.

- 2 Insert and then remove the card.

*The green light flashes and the latch unlocks.*

- 3 Turn the lever and open the door.

*During the unlock time, if using the Programming Default ID Card, the green light flashes. Then the red light flashes and the latch relocks.*

## Finishing the installation

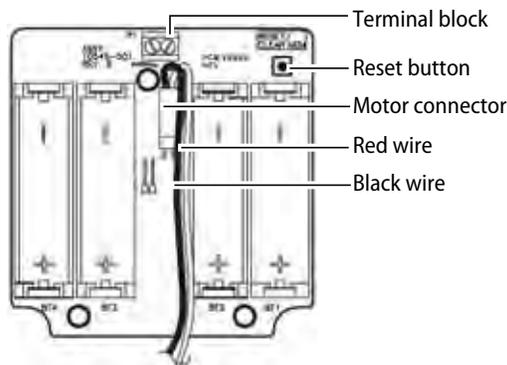


Figure 21 Using the reset button

### 20 Troubleshooting

If the mechanism doesn't unlock, remove the battery cover and check for proper orientation and seating of the batteries and motor connector. Ensure that wires are not pinched. Reset the electronics by pressing and holding the reset button on the circuit board until the light flashes green (approximately three seconds), then releasing the button. See Figure 21.

**Note:** *The system will go through a self-test and the green light will flash five times. You will hear the lock unlock, then relock three times. A red flash indicates a PC board or drive system problem. If a red flash or no flash is observed, check for proper orientation and seating of the batteries and motor connector, ensure that wires are not pinched, then repeat the reset process.*

### Check operation

- 1 Press **1234 for the 2000 series, or 5011234 for the 500 series.**

*During the unlock time, the green light flashes; then the red light flashes and the latch relocks.*

- 2 Turn the lever and open the door.
- 3 If your system has a magnetic card reader, verify proper operation of the system using the magnetic card reader; otherwise, see "Test lock" on page 11.

A label on the housing assembly battery cover indicates the magnetic card track (track 2 or track 3) that the system is set to read. See Figure 11.



**STANLEY**  
Security Solutions

**STANLEY**  
**OMNILOCK**

6161 East 75th Street | Indianapolis, IN 46250 USA  
[www.stanleysecuritysolutions.com](http://www.stanleysecuritysolutions.com)

© 2009-2012 Stanley Security Solutions, Inc. and Stanley Logistics, Inc.

172713-S3