BEST
dormakaba Group

Wi-Q
wireless technology

BEST WI-Q™
ACCESS MANAGEMENT SYSTEM

Appendix B

Credits/Copyright

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

This publication is intended to be an accurate description and set of instructions pertaining to its subject matter. However, as with any publication of this complexity, errors or omissions are possible. Please call dormakaba USA Inc. at 1-855-365-2407 if you see any errors or have any questions. No part of this manual and/or databases may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose, without the express written permission of dormakaba USA Inc.

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

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

T85202_Appendix B February 2022

Contents

Overview

Installation

Configuring Segments, Virtual Portal Gateways and Controllers

User Interface for Wi-Q Virtual Portal

Overview

This document shows how to use the offline Omnilock 2000 features in Wi-Q–AMS.

Definitions

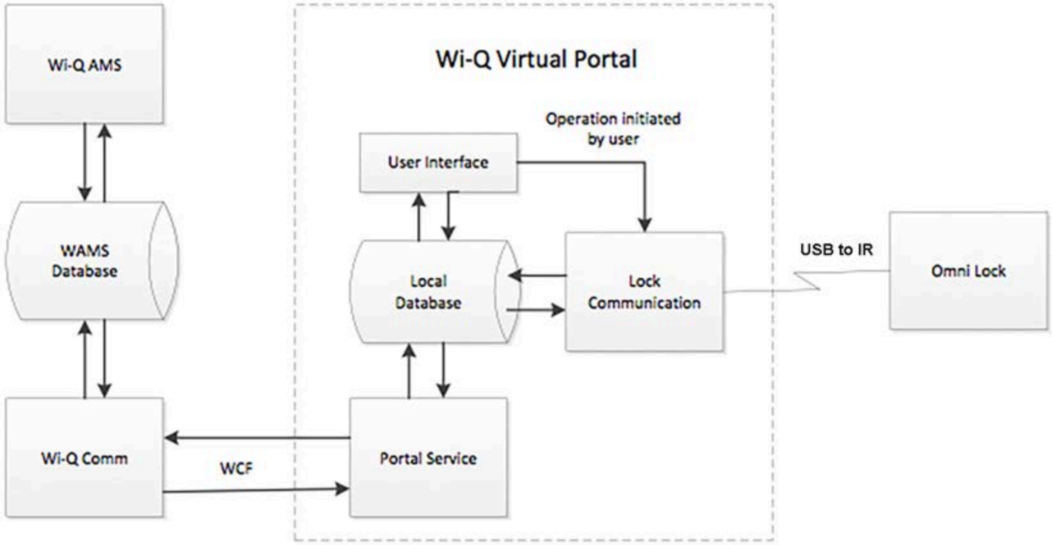
The following definitions are used throughout this document and are described below.

- **PG—** Portal Gateway.
- **Wi-Q Comm—**application that transfers data from the Wi-Q AMS to Portal Gateways through a service interface.
- **Wi-Q AMS—**Access Management System used to define the schedules and credentials that are transferred to controllers and govern who is allowed to get through a door and when.
- **Controller—**also referred to as a lock or reader.
- **Omnilock—**the offline lock that receives data either through a serial connection or an IR transceiver.
- **OFM—**(Offline Facility Manager) – legacy software used to configure Omnilock. This software will be replaced by the Virtual Portal and changes to Wi-Q AMS.

Architecture

The basic architecture of the application consists of a Portal Service to send and receive data to and from Wi-Q Comm, a local database to store that information, a user interface and a lock communication layer to send and receive data to and from the Omnilock.

Figure 1 Wi-Q Virtual Portal System Diagram



Installation

Setup Checklist

- ❑ Installed AMS system
- ❑ IR Dongle
- ❑ Virtual Portal Software Installed
- ❑ Optional USB extension cable (for lock programming)
- ❑ Optional Prox Wedge Reader

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 (Telnet - Optional)
- Port 80 (HTTP)
- Port 1433 (Default SQL Server)
- Port 1434 (Default SQL Server)
- Port 8000 (Communication)
- Port 11000 (Wi-Q Com Service)
- Port 5353 (Bonjour)

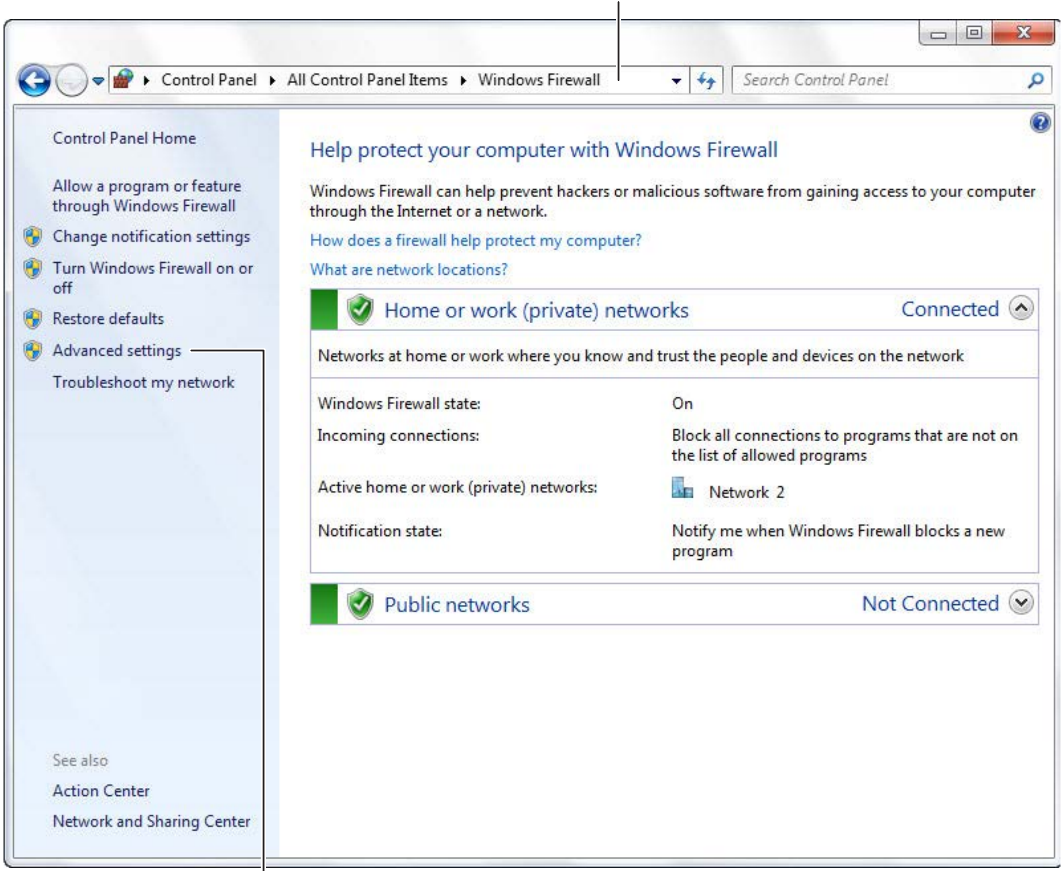
If your firewall is disabled, then all ports are open by default. If the firewall is on, perform the following in order to add the required ports.

Note The following reflects 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 2. Then, click on Advanced settings.

Figure 2 Windows Firewall

Navigate to Windows Firewall


Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

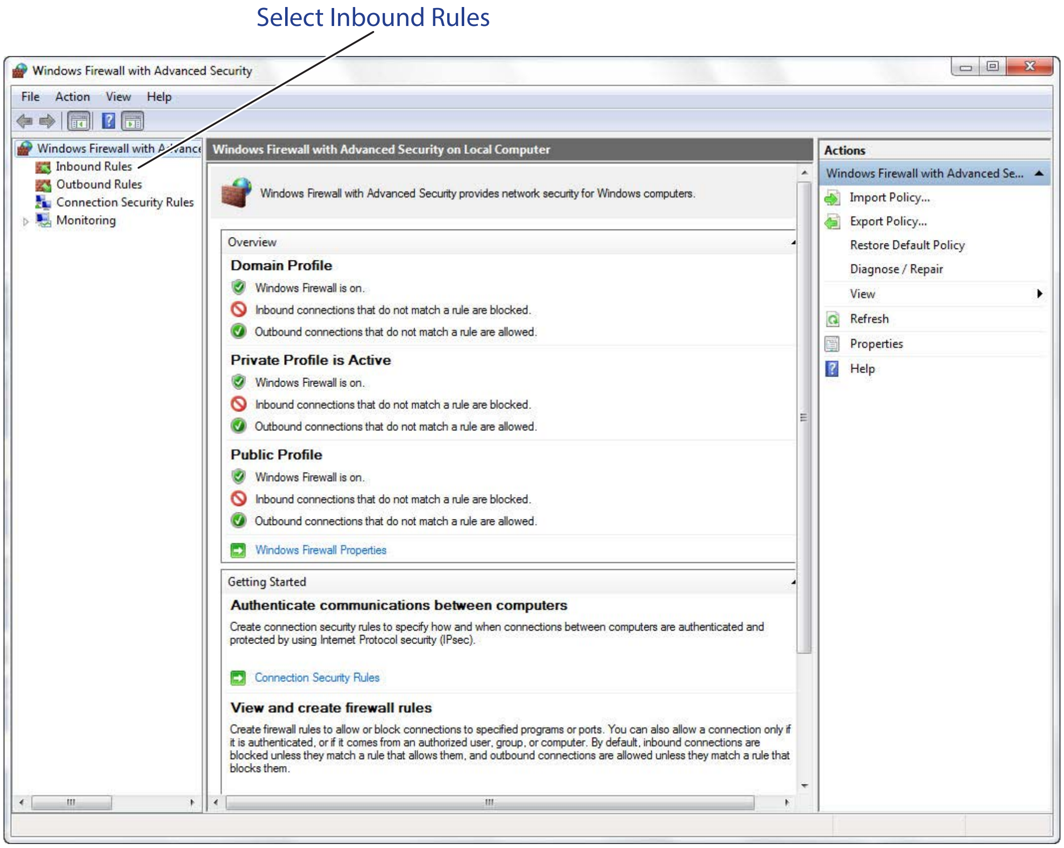
Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network 2
Notification state:	Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

Click on Advanced settings

2 Select Inbound Rules.

Figure 3 Inbound Rules



Select Inbound Rules

Windows Firewall with Advanced Security on Local Computer

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

Overview

Domain Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile is Active

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile

- Windows Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

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

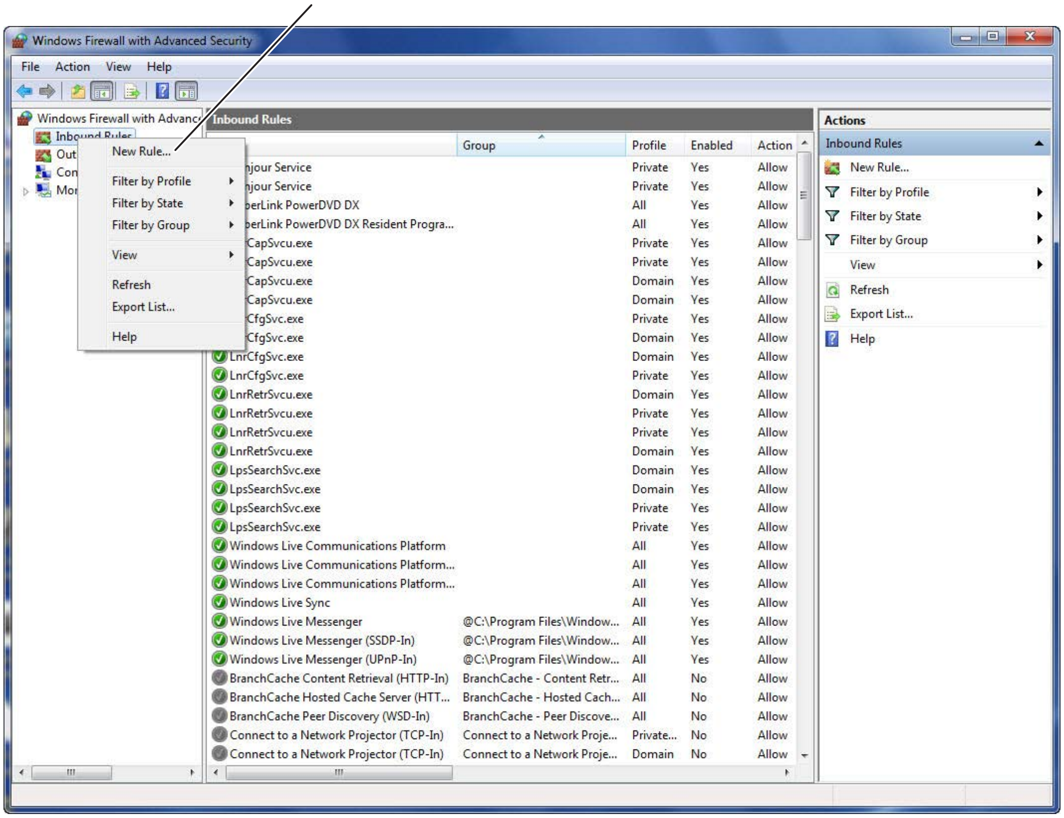
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

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

Figure 4 New Rule

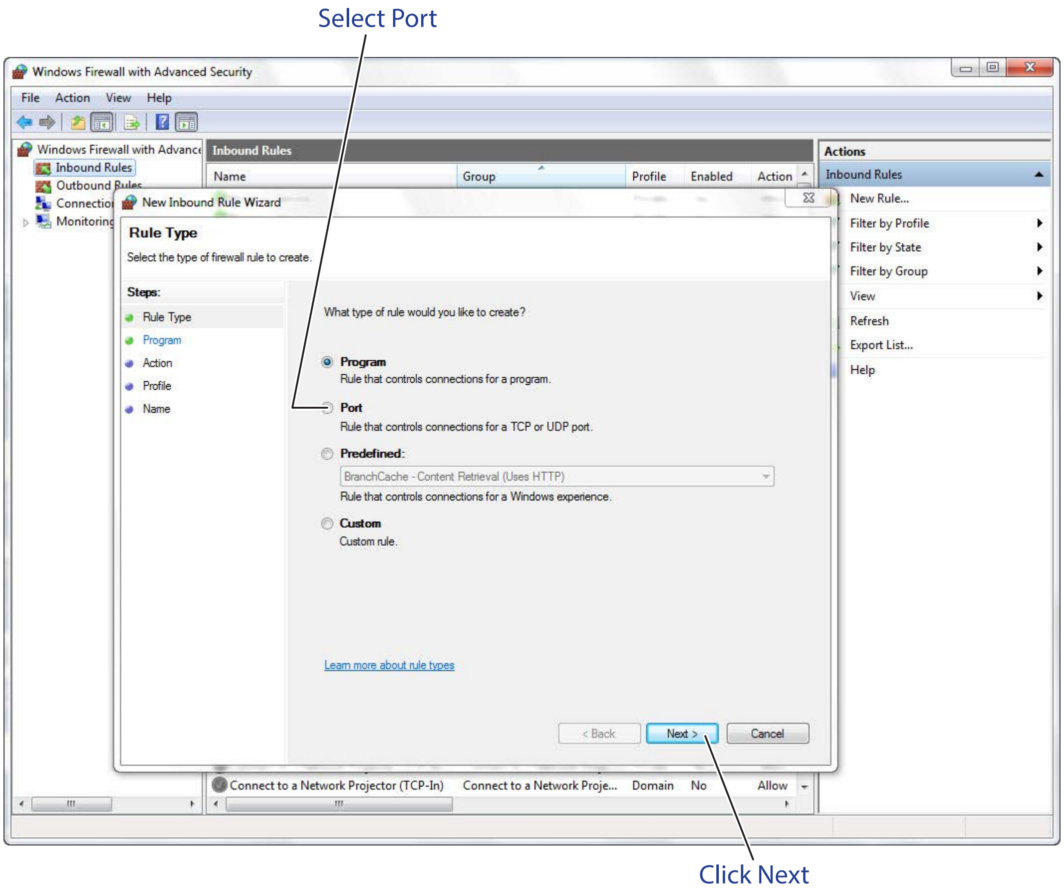


Select New Rule

	Group	Profile	Enabled	Action
njour Service		Private	Yes	Allow
njour Service		Private	Yes	Allow
berLink PowerDVD DX		All	Yes	Allow
berLink PowerDVD DX Resident Progra...		All	Yes	Allow
CapSvcu.exe		Private	Yes	Allow
CapSvcu.exe		Private	Yes	Allow
CapSvcu.exe		Domain	Yes	Allow
CapSvcu.exe		Domain	Yes	Allow
CfgSvc.exe		Private	Yes	Allow
CfgSvc.exe		Domain	Yes	Allow
LnrCfgSvc.exe		Domain	Yes	Allow
LnrCfgSvc.exe		Private	Yes	Allow
LnrRetrSvcu.exe		Domain	Yes	Allow
LnrRetrSvcu.exe		Private	Yes	Allow
LnrRetrSvcu.exe		Private	Yes	Allow
LnrRetrSvcu.exe		Domain	Yes	Allow
LpsSearchSvc.exe		Domain	Yes	Allow
LpsSearchSvc.exe		Domain	Yes	Allow
LpsSearchSvc.exe		Private	Yes	Allow
LpsSearchSvc.exe		Private	Yes	Allow
Windows Live Communications Platform		All	Yes	Allow
Windows Live Communications Platform...		All	Yes	Allow
Windows Live Communications Platform...		All	Yes	Allow
Windows Live Sync		All	Yes	Allow
Windows Live Messenger	@C:\Program Files\Window...	All	Yes	Allow
Windows Live Messenger (SSDP-In)	@C:\Program Files\Window...	All	Yes	Allow
Windows Live Messenger (UPnP-In)	@C:\Program Files\Window...	All	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow

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

Figure 5 Create Port Rule



Select Port

Click Next

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

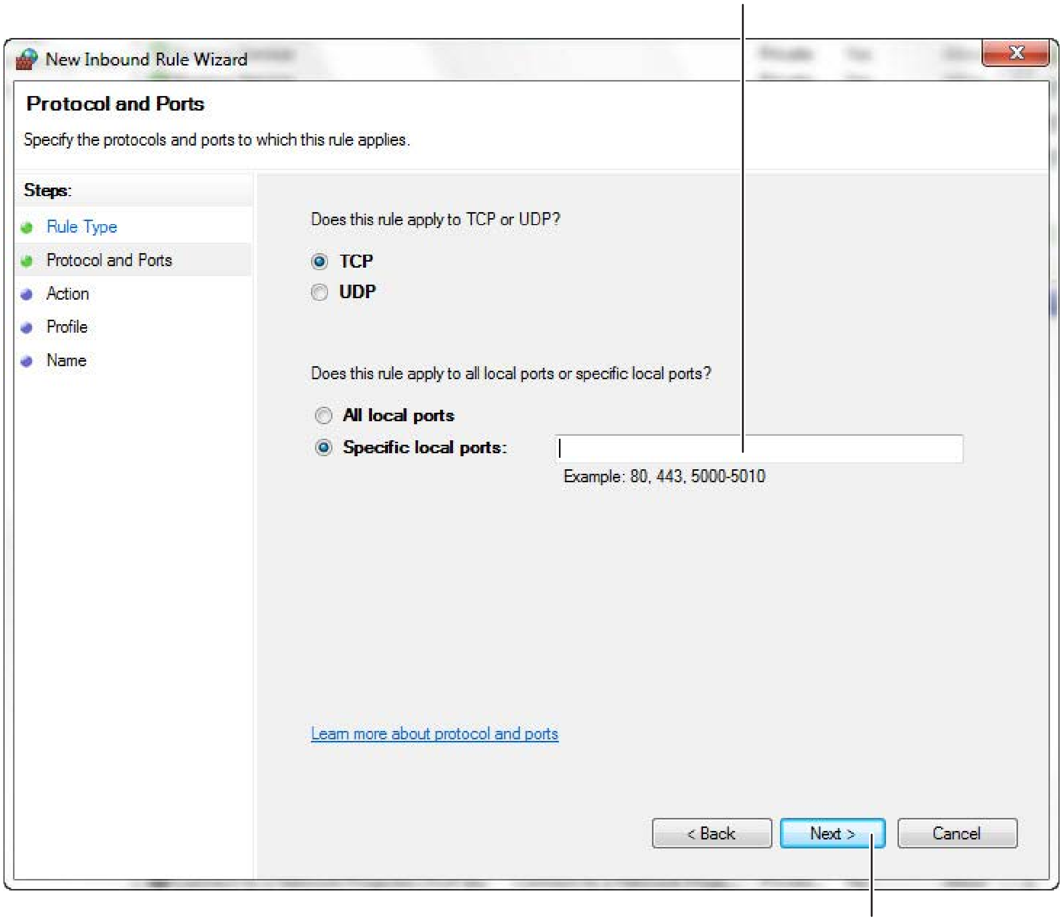
○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

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

Figure 6 Enter Ports

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



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:**

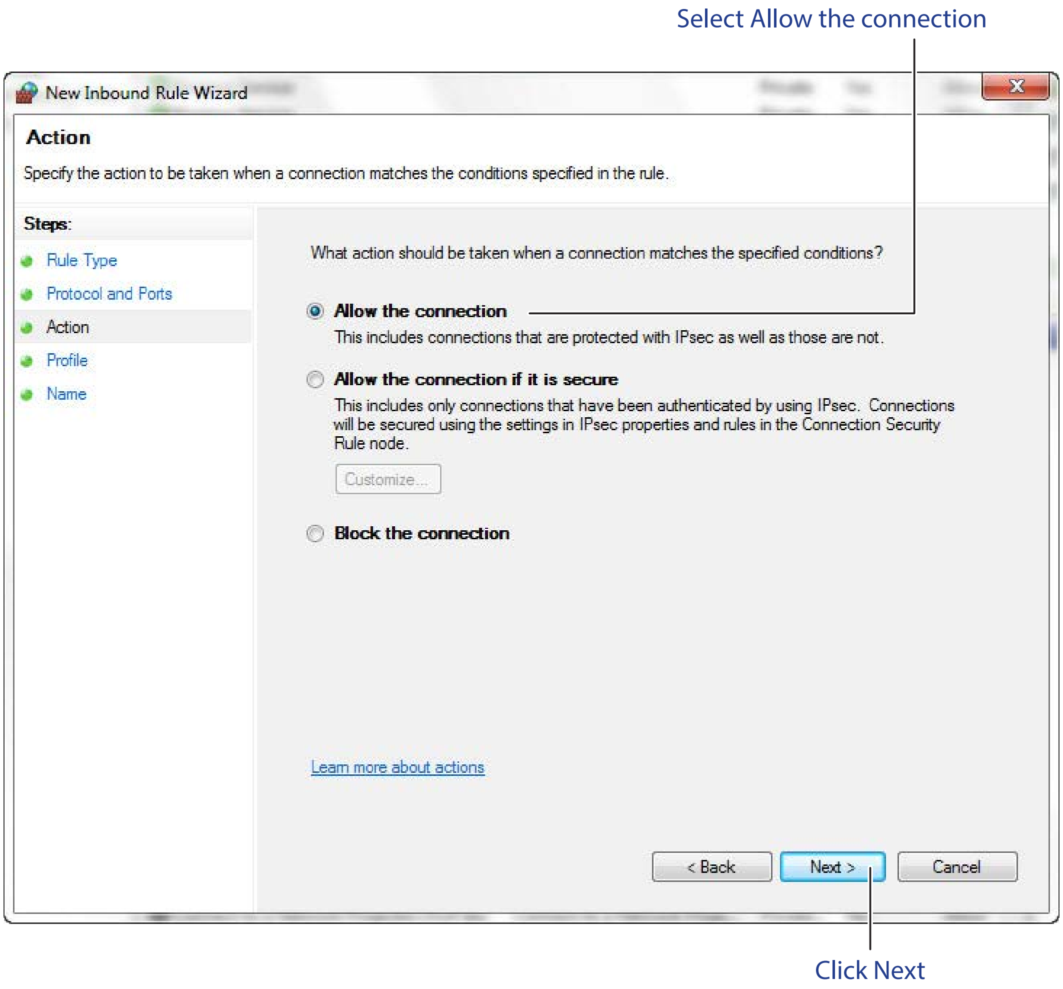
Example: 80, 443, 5000-5010

Learn more about protocol and ports

Click Next

6 Select Allow the connection. Click Next to continue. See Figure 7.

Figure 7 Allow the Connection



Select Allow the connection

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

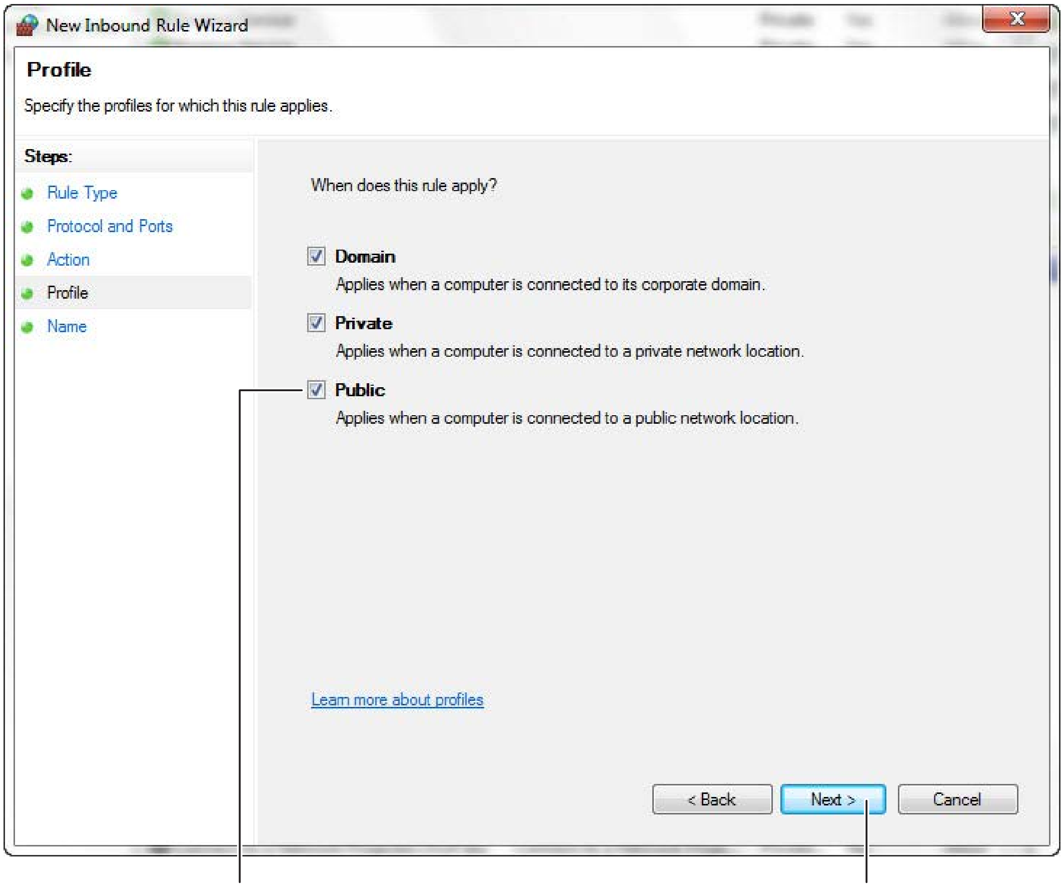
○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Click Next

7 De-select the Public option. Click Next.

Figure 8 De-select Public



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

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

☑ **Private**
Applies when a computer is connected to a private network location.

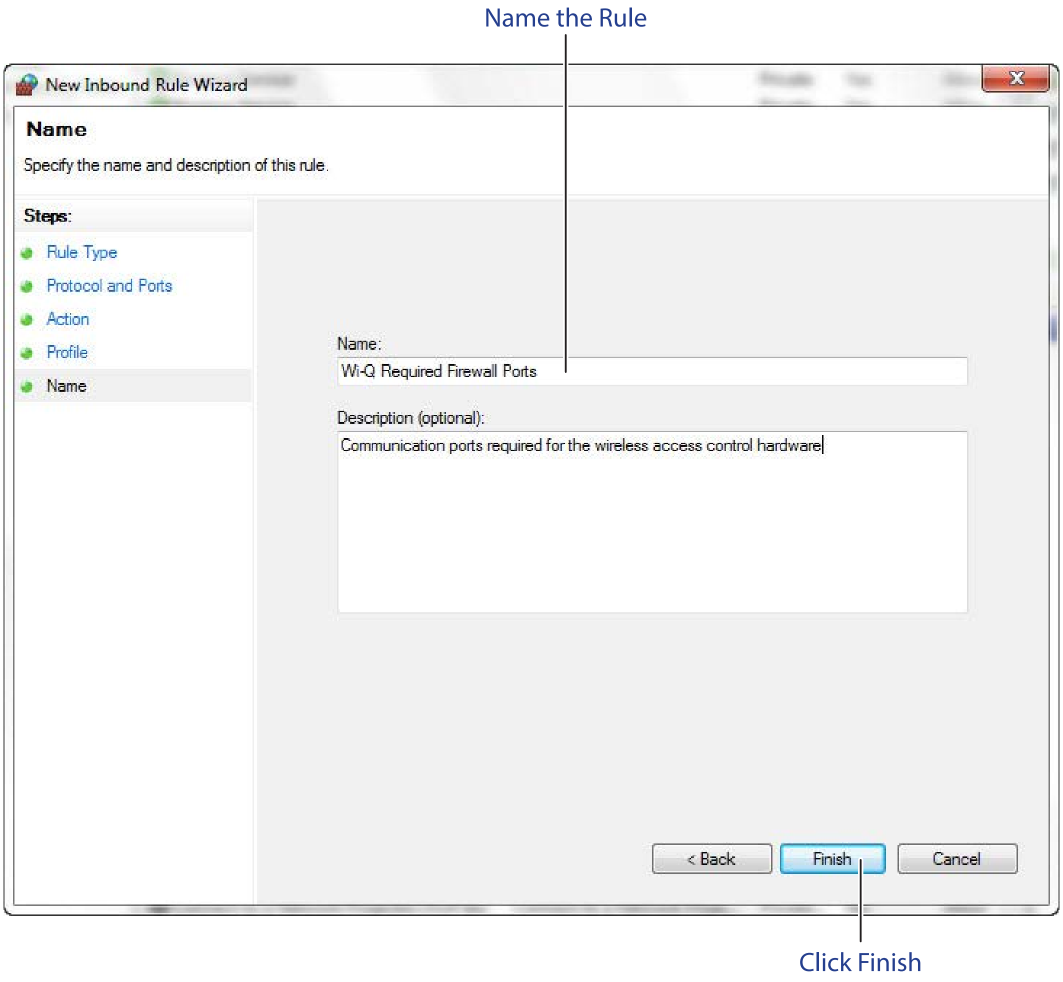
☑ **Public**
Applies when a computer is connected to a public network location.

De-Select Public

Click Next

8 Give the new rule a name that can be easily identified by an administrator. Once finished, click Finish. See Figure 9.

Figure 9 Name the Rule



Name:

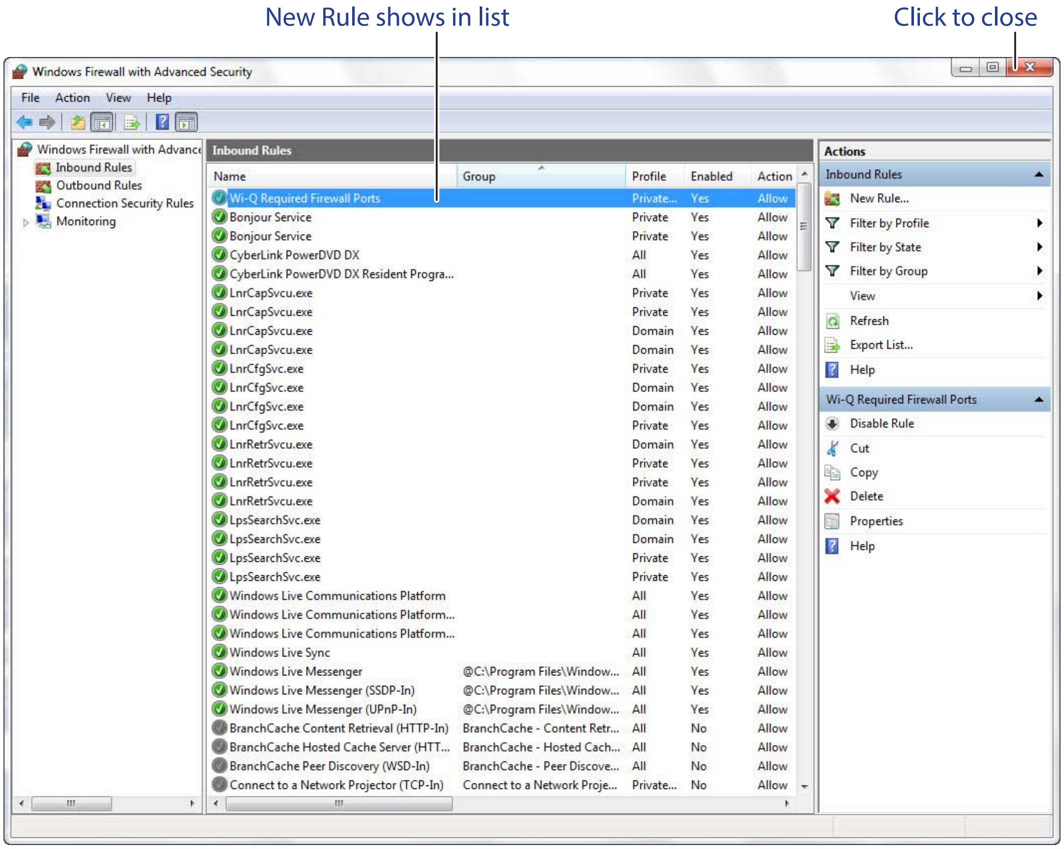
Wi-Q Required Firewall Ports

Description (optional):

Communication ports required for the wireless access control hardware

9 The new rule now appears in the list. The Firewall Settings module may now be closed. See Figure 10.

Figure 10 Inbound Rules List



Name	Group	Profile	Enabled	Action
Wi-Q Required Firewall Ports		Private...	Yes	Allow
Bonjour Service		Private	Yes	Allow
Bonjour Service		Private	Yes	Allow
CyberLink PowerDVD DX		All	Yes	Allow
CyberLink PowerDVD DX Resident Progra...		All	Yes	Allow
LnrCapSvcu.exe		Private	Yes	Allow
LnrCapSvcu.exe		Private	Yes	Allow
LnrCapSvcu.exe		Domain	Yes	Allow
LnrCapSvcu.exe		Domain	Yes	Allow
LnrCfgSvc.exe		Private	Yes	Allow
LnrCfgSvc.exe		Domain	Yes	Allow
LnrCfgSvc.exe		Domain	Yes	Allow
LnrCfgSvc.exe		Private	Yes	Allow
LnrRetrSvcu.exe		Domain	Yes	Allow
LnrRetrSvcu.exe		Private	Yes	Allow
LnrRetrSvcu.exe		Private	Yes	Allow
LnrRetrSvcu.exe		Domain	Yes	Allow
LpsSearchSvc.exe		Domain	Yes	Allow
LpsSearchSvc.exe		Domain	Yes	Allow
LpsSearchSvc.exe		Private	Yes	Allow
LpsSearchSvc.exe		Private	Yes	Allow
Windows Live Communications Platform		All	Yes	Allow
Windows Live Communications Platform...		All	Yes	Allow
Windows Live Communications Platform...		All	Yes	Allow
Windows Live Sync		All	Yes	Allow
Windows Live Messenger	@C:\Program Files\Window...	All	Yes	Allow
Windows Live Messenger (SSDP-In)	@C:\Program Files\Window...	All	Yes	Allow
Windows Live Messenger (UPnP-In)	@C:\Program Files\Window...	All	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow

Gather and Organize Segment Data

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 device names and physical locations of all readers 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.

Install Software

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)).

Beginning Installation

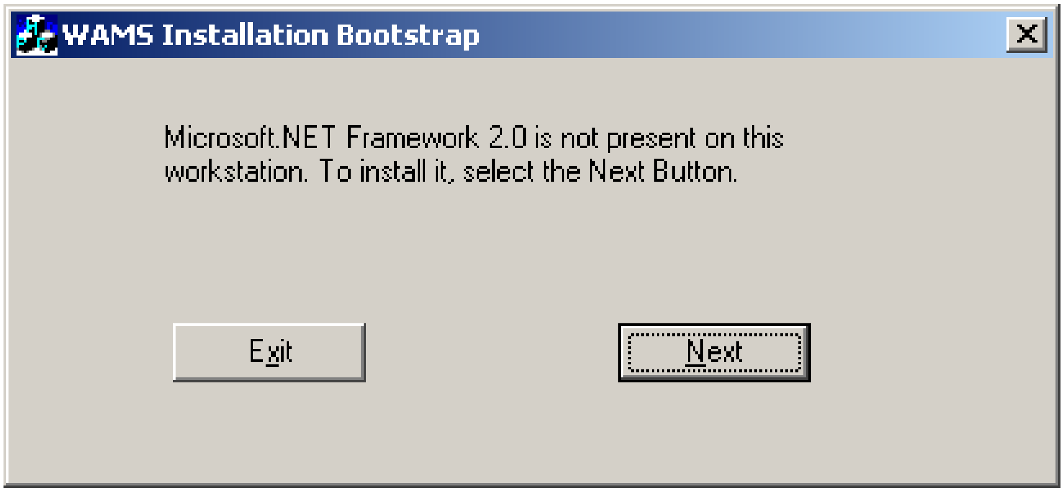
1 If you have not already done so, download the Wi-Q AMS Software from the Technical Support website.

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: WIQSetup.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 11 Installation of WIQSetup.exe



Microsoft.NET Framework 2.0 is not present on this workstation. To install it, select the Next Button.

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 “WIQSetup.exe” file again.

4 The AMS Setup Main page opens, Figure 12. It is important to perform the steps in the sequence presented.

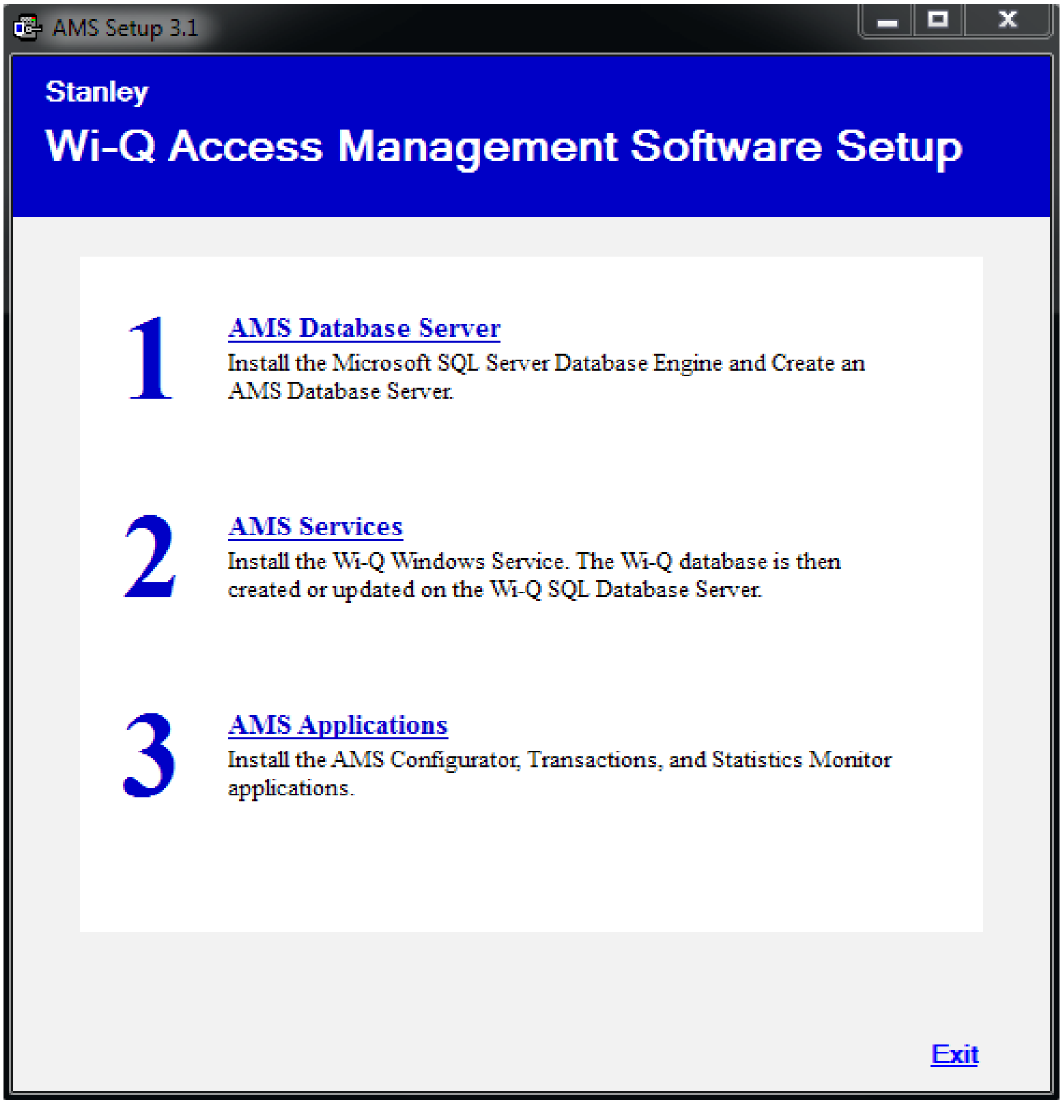
Note You may wish to install the services and database on one machine (such as the Host) and the AMS Applications only at other machines. This can be done by selecting the appropriate application from the System Setup windows.

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

Step 1

1 Click the AMS Database Server link.

Figure 12 AMS Setup



Stanley

Wi-Q Access Management Software Setup

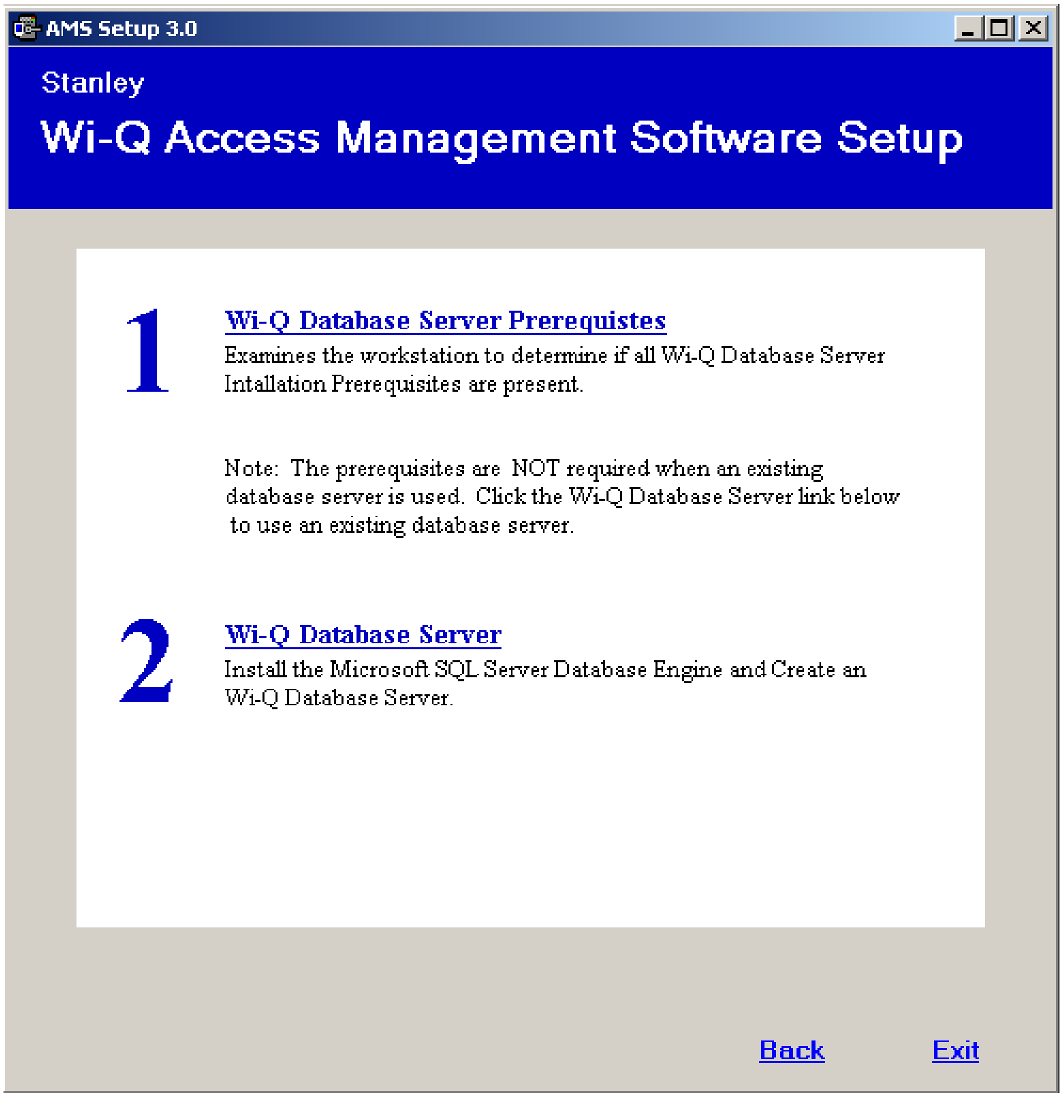
1 AMS Database Server
Install the Microsoft SQL Server Database Engine and Create an AMS Database Server.

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

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

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

Figure 13 Database Server Prerequisites



AMS Setup 3.0

Stanley

Wi-Q Access Management Software Setup

1 Wi-Q Database Server Prerequistes

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

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

2 Wi-Q Database Server

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

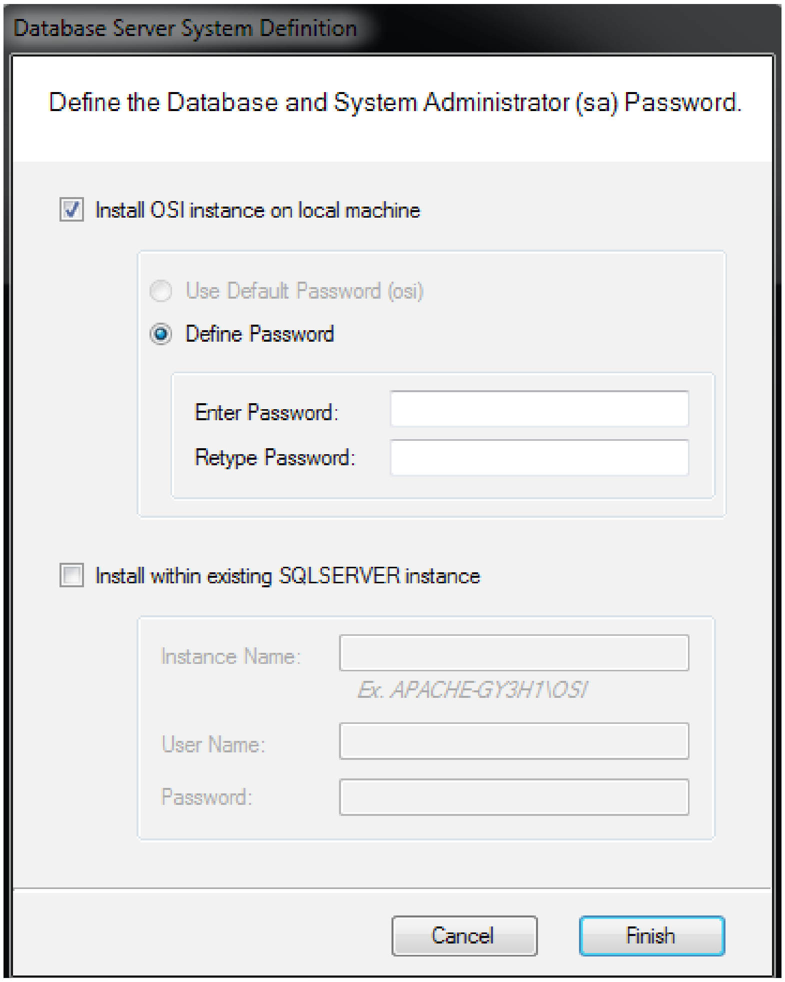
3 You may be prompted to install a number of prerequisites, including Microsoft Windows Installer and Windows PowerShell. To install the latest versions of these prerequisites, it is recommended that you click the website links provided and download directly from the Microsoft website. Once you've downloaded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

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

5 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 within an existing server, enter the instance name and associated user name and password. Then click Finish.

Figure 14 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

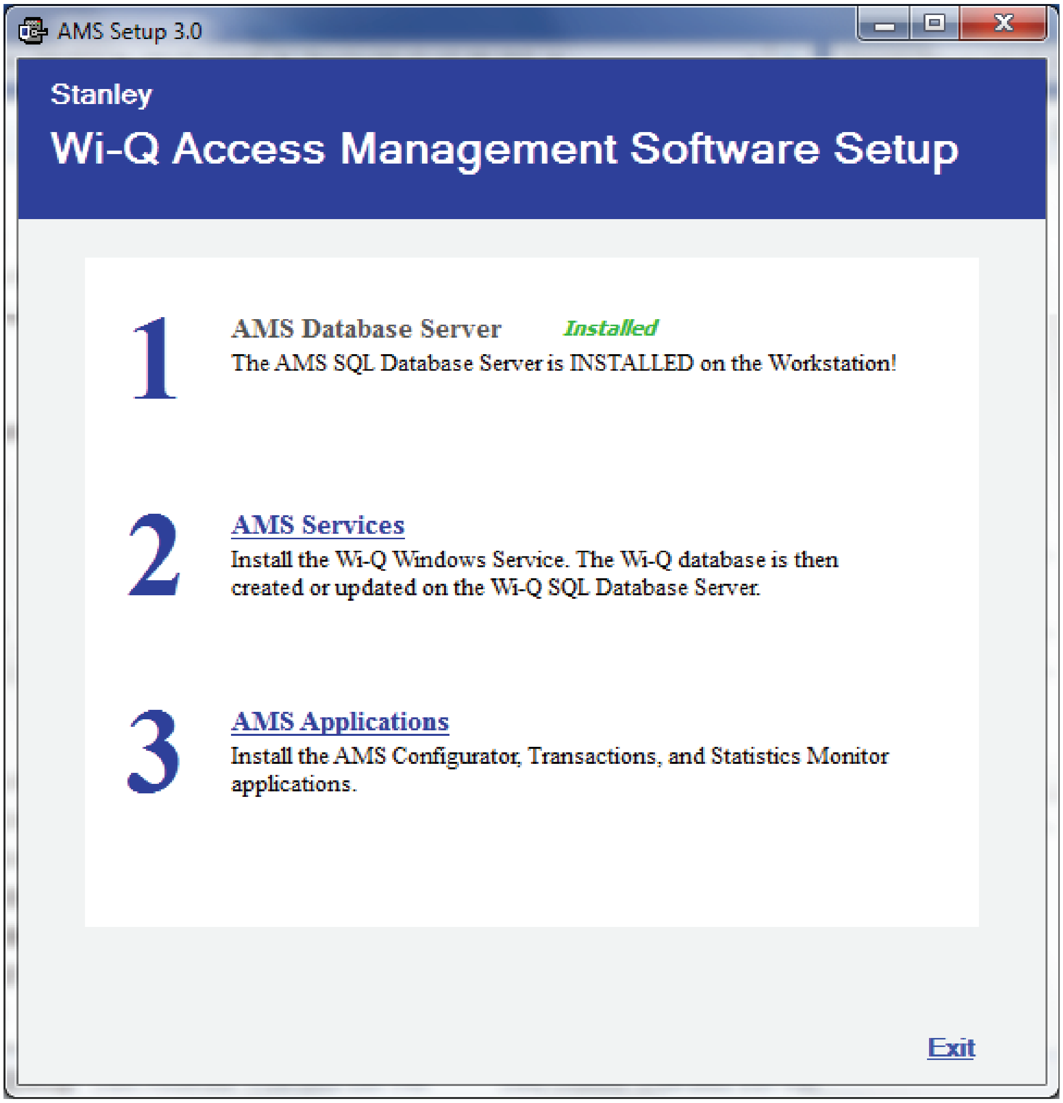
User Name:

Password:

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

7 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 15 AMS Database Server Successfully Installed



Stanley

Wi-Q Access Management Software Setup

1 AMS Database Server *Installed*

The AMS SQL Database Server is INSTALLED on the Workstation!

2 AMS Services

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

3 AMS Applications

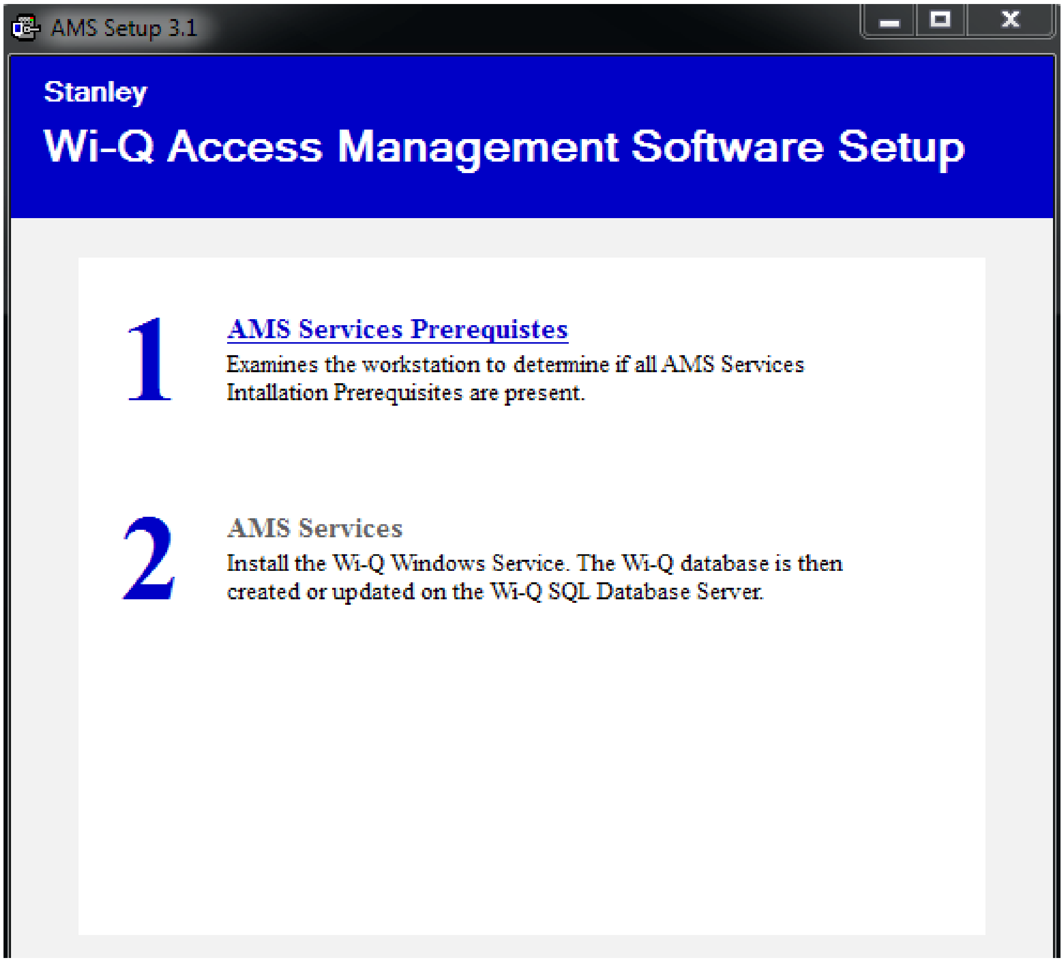
Install the AMS Configurator, Transactions, and Statistics Monitor applications.

Step 2

1 On the Setup main page (see Figure 12), click the AMS Services link.

2 If a similar dialog box opens with a link to install Prerequisites, click the link. See Figure 16.

Figure 16 Install Prerequisites



AMS Setup 3.1

Stanley

Wi-Q Access Management Software Setup

1 AMS Services Prerequistes

Examines the workstation to determine if all AMS Services Intallation Prerequisites are present.

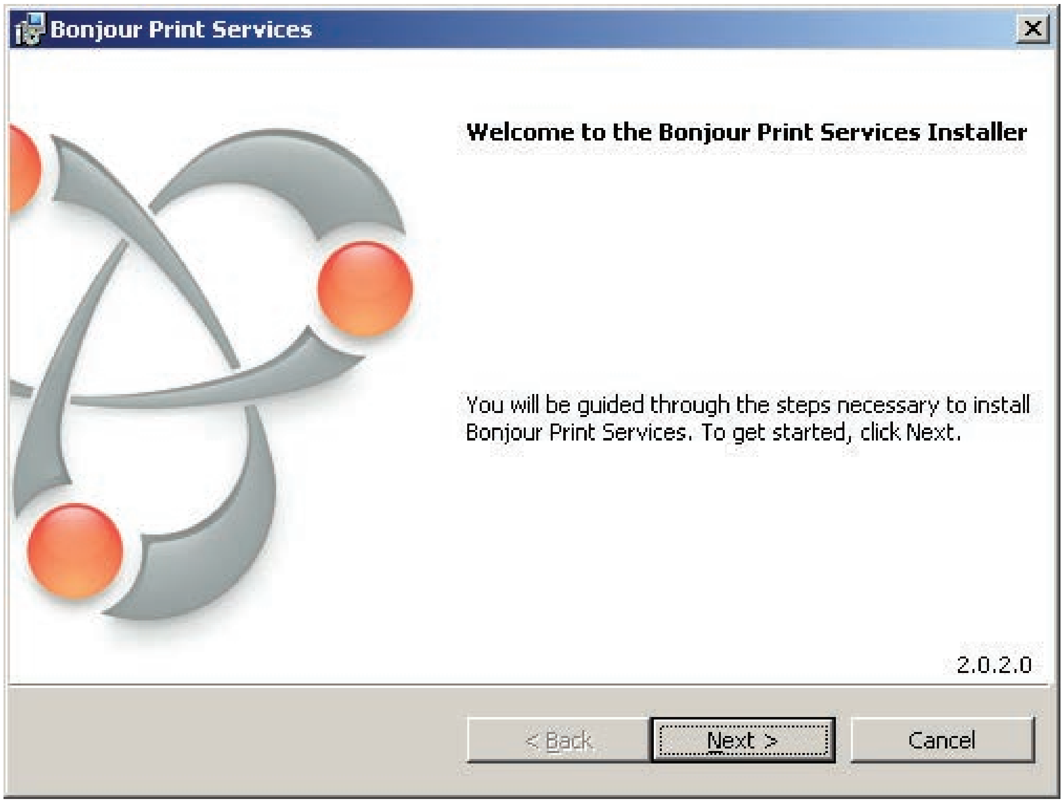
2 AMS Services

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

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

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

Figure 17 Bonjour Print Services Installer



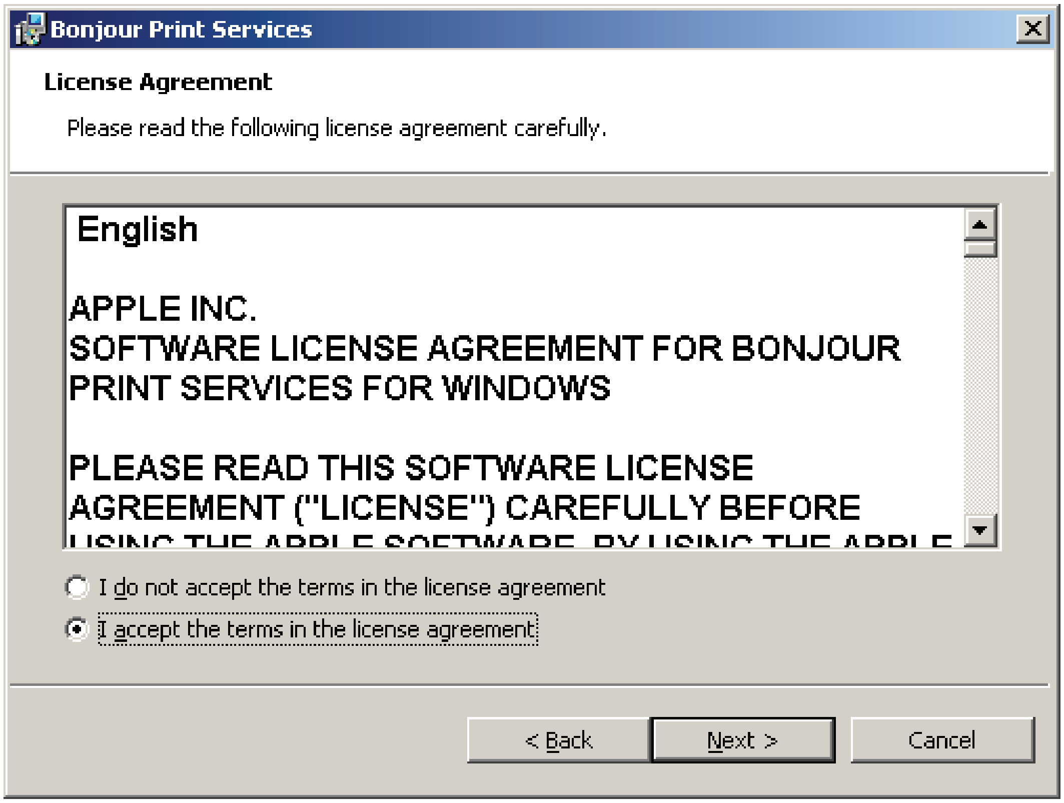
Welcome to the Bonjour Print Services Installer

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

2.0.2.0

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

Figure 18 Bonjour Print Services License Agreement



License Agreement

Please read the following license agreement carefully.

English

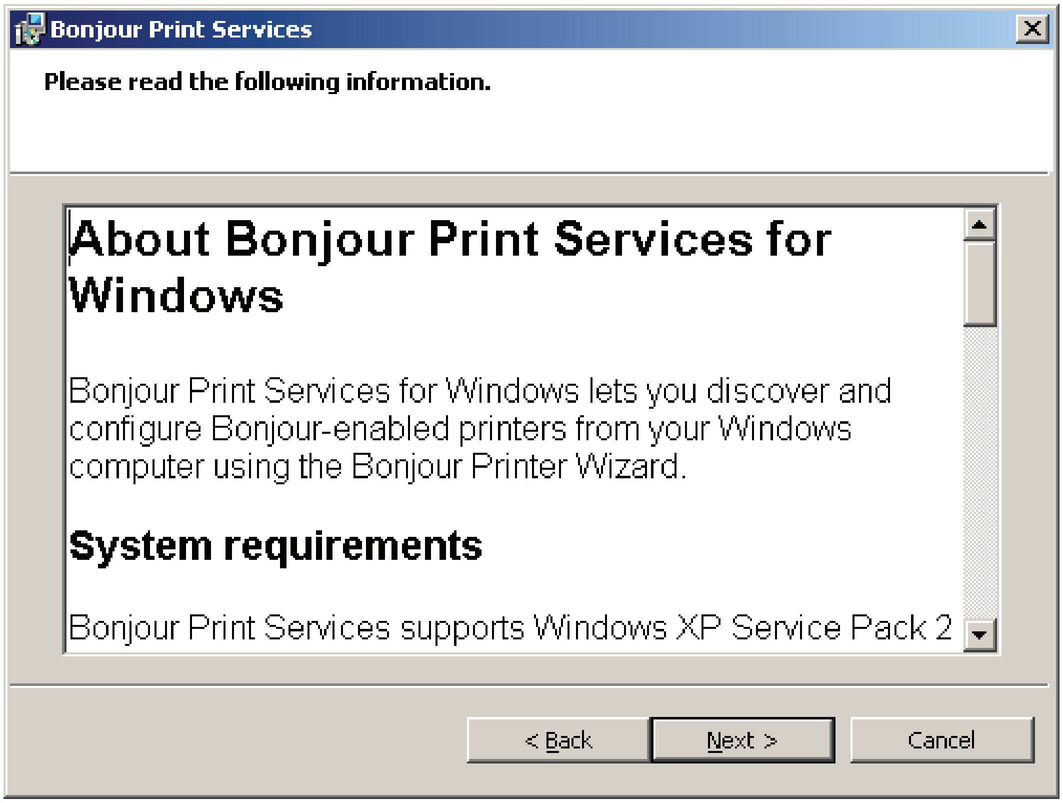
APPLE INC.
SOFTWARE LICENSE AGREEMENT FOR BONJOUR PRINT SERVICES FOR WINDOWS

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

○ I do not accept the terms in the license agreement

● I accept the terms in the license agreement d Read the information about Bonjour Print Services. Then press Next.

Figure 19 Bonjour Print Services Information



Please read the following information.

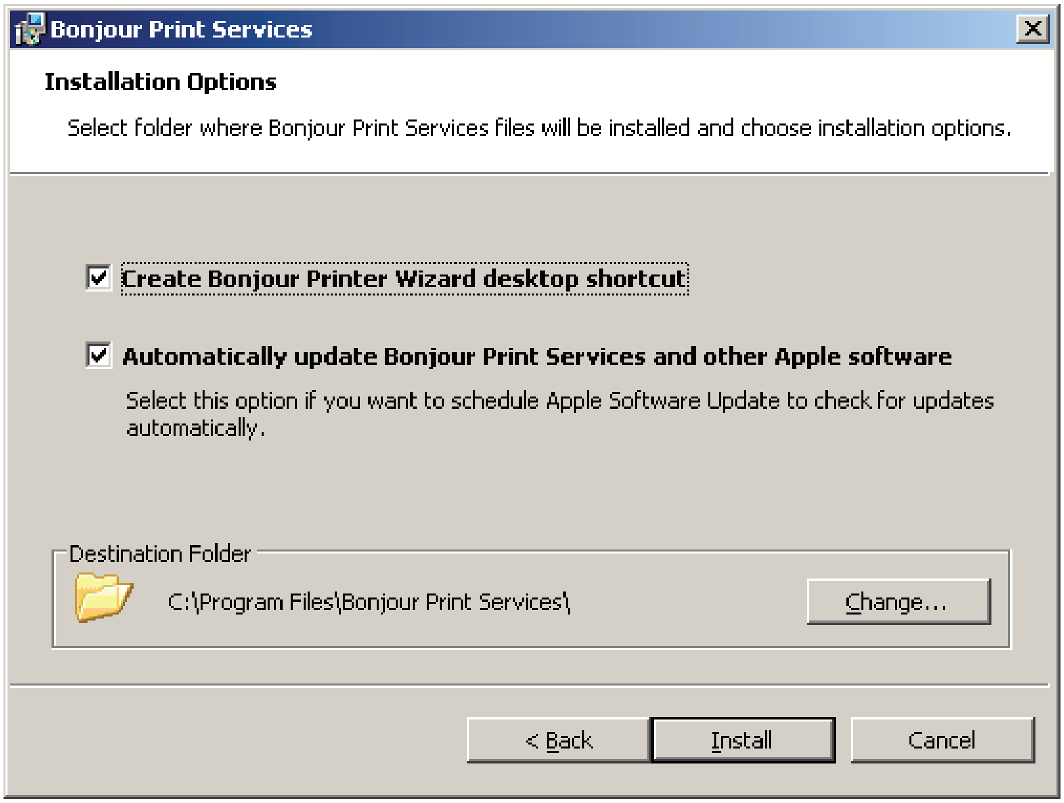
About Bonjour Print Services for Windows

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

System requirements

Bonjour Print Services supports Windows XP Service Pack 2 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 20 Bonjour Installation Options



Bonjour Print Services

Installation Options

Select folder where Bonjour Print Services files will be installed and choose installation options.

☑ **Create Bonjour Printer Wizard desktop shortcut**

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

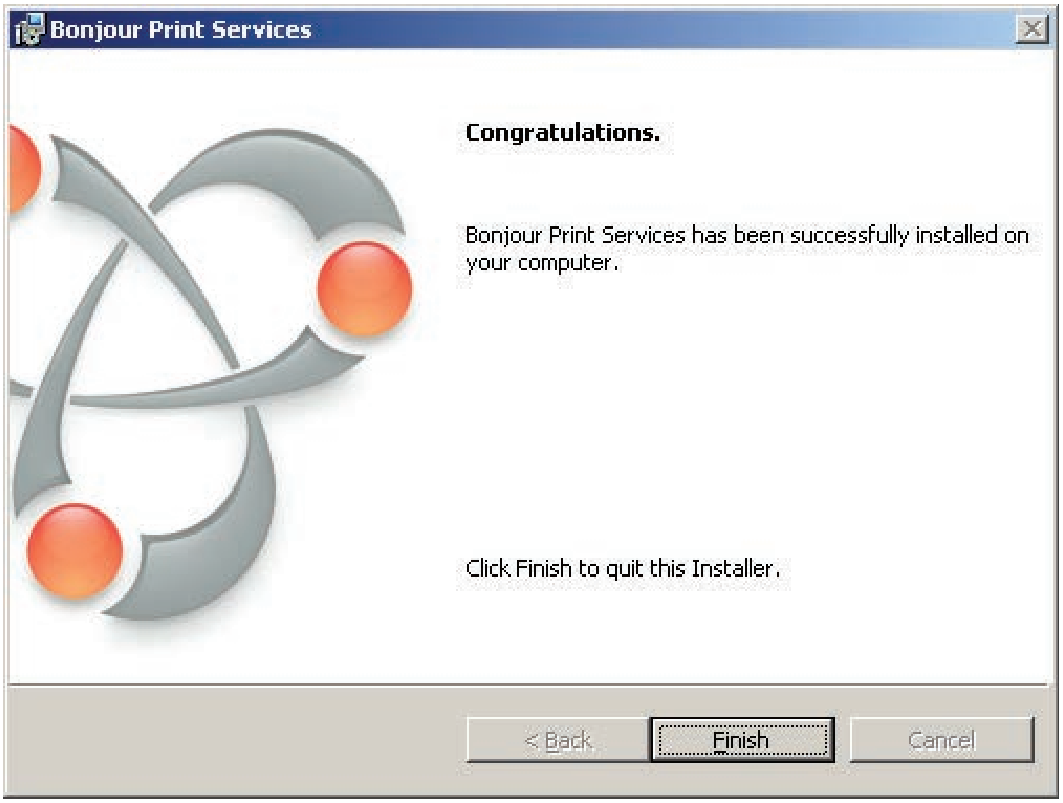
Select this option if you want to schedule Apple Software Update to check for updates automatically.

Destination Folder

C:\Program Files\Bonjour Print Services\

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

Figure 21 Bonjour Print Services Installation Complete



Bonjour Print Services

Congratulations.

Bonjour Print Services has been successfully installed on your computer.

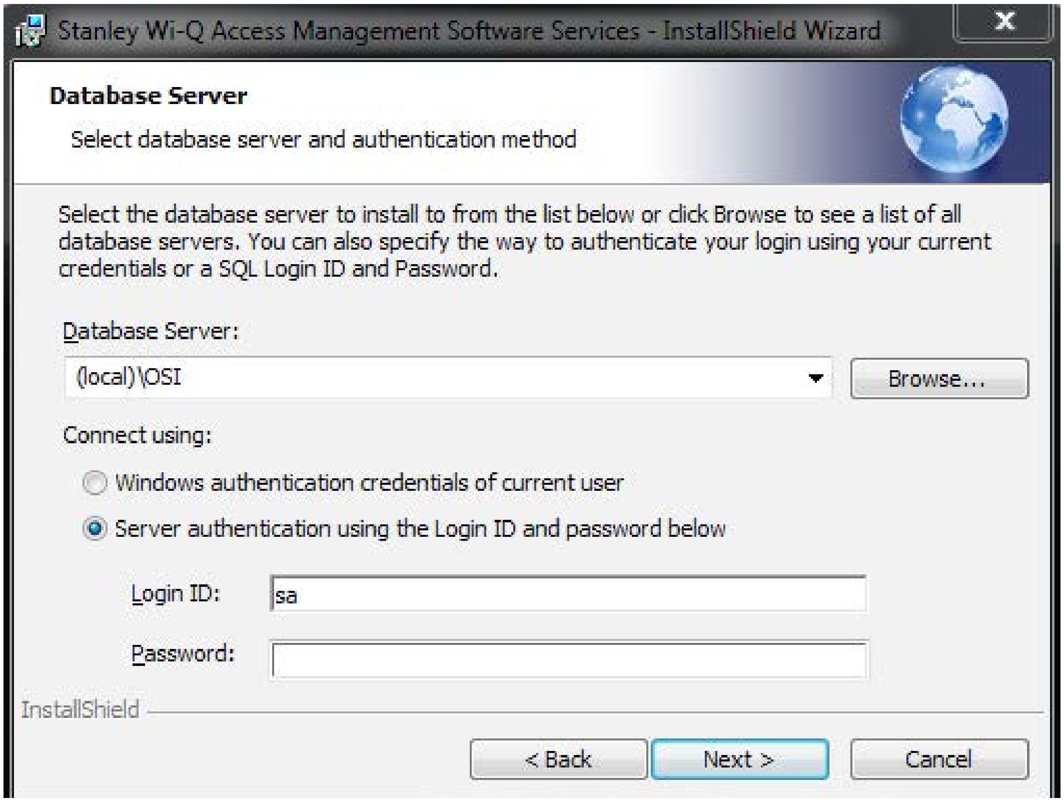
Click Finish to quit this Installer.

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

4 Click Next to continue past the Welcome page.

5 On the Database Server dialog box, browse to your database server and select your connection method. In the Connect Using section, choose your connection method. If you choose Server authentication, provide the Login ID and Password for the server. See Figure 22.

Figure 22 InstallShield Wizard Database Server



Stanley Wi-Q Access Management Software Services - InstallShield Wizard

Database Server

Select database server and authentication method

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

Database Server: (local)\OSI

Connect using:

○ Windows authentication credentials of current user

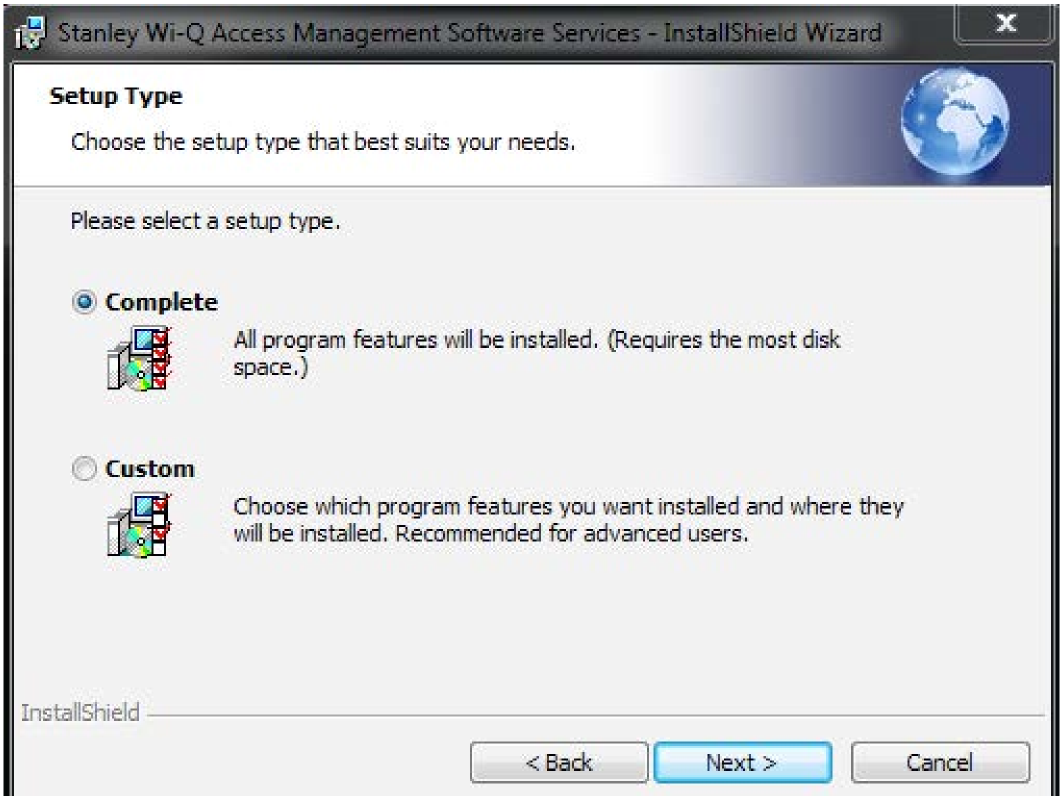
● Server authentication using the Login ID and password below

Login ID: sa

Password:

6 In the Setup Type dialog box (Figure 23), 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 23 Setup Type



Stanley Wi-Q Access Management Software Services - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Complete**

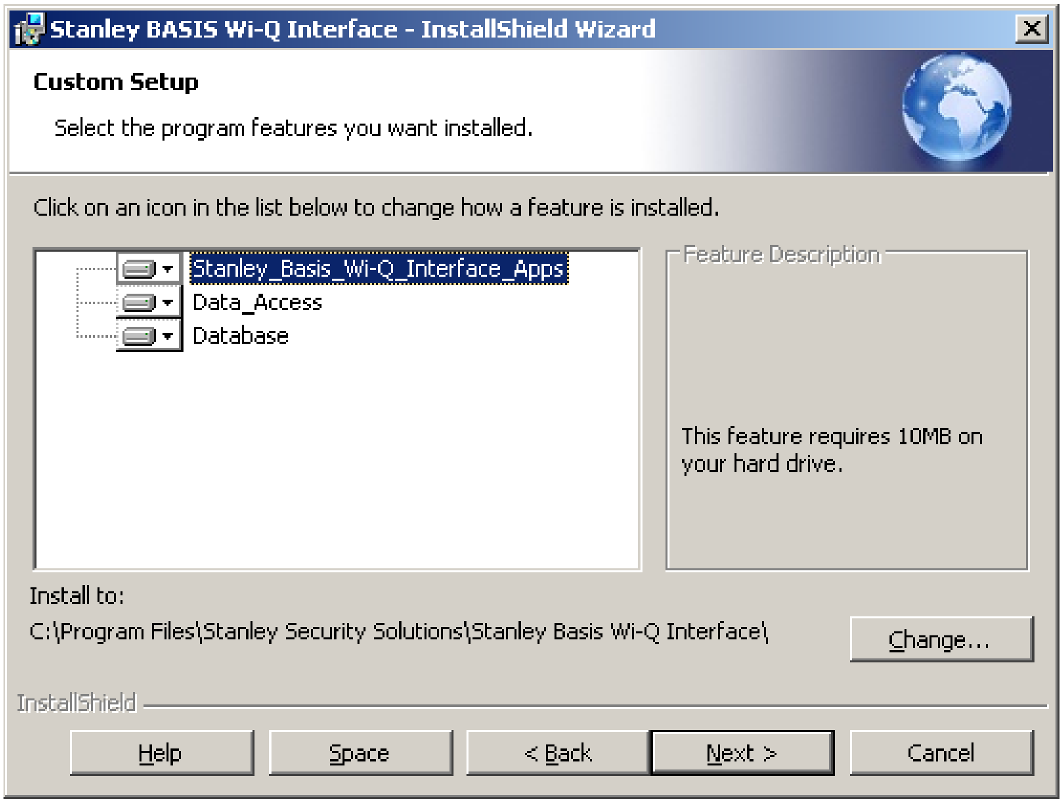
All program features will be installed. (Requires the most disk space.)

○ **Custom**

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

Figure 24 shows the installation components available in a Custom Setup.

Figure 24 Custom Setup



Stanley BASIS Wi-Q Interface - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Stanley_Basis_Wi-Q_Interface_Apps
- Data_Access
- Database

Feature Description

This feature requires 10MB on your hard drive.

Install to:

C:\Program Files\Stanley Security Solutions\Stanley Basis Wi-Q Interface\

7 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.

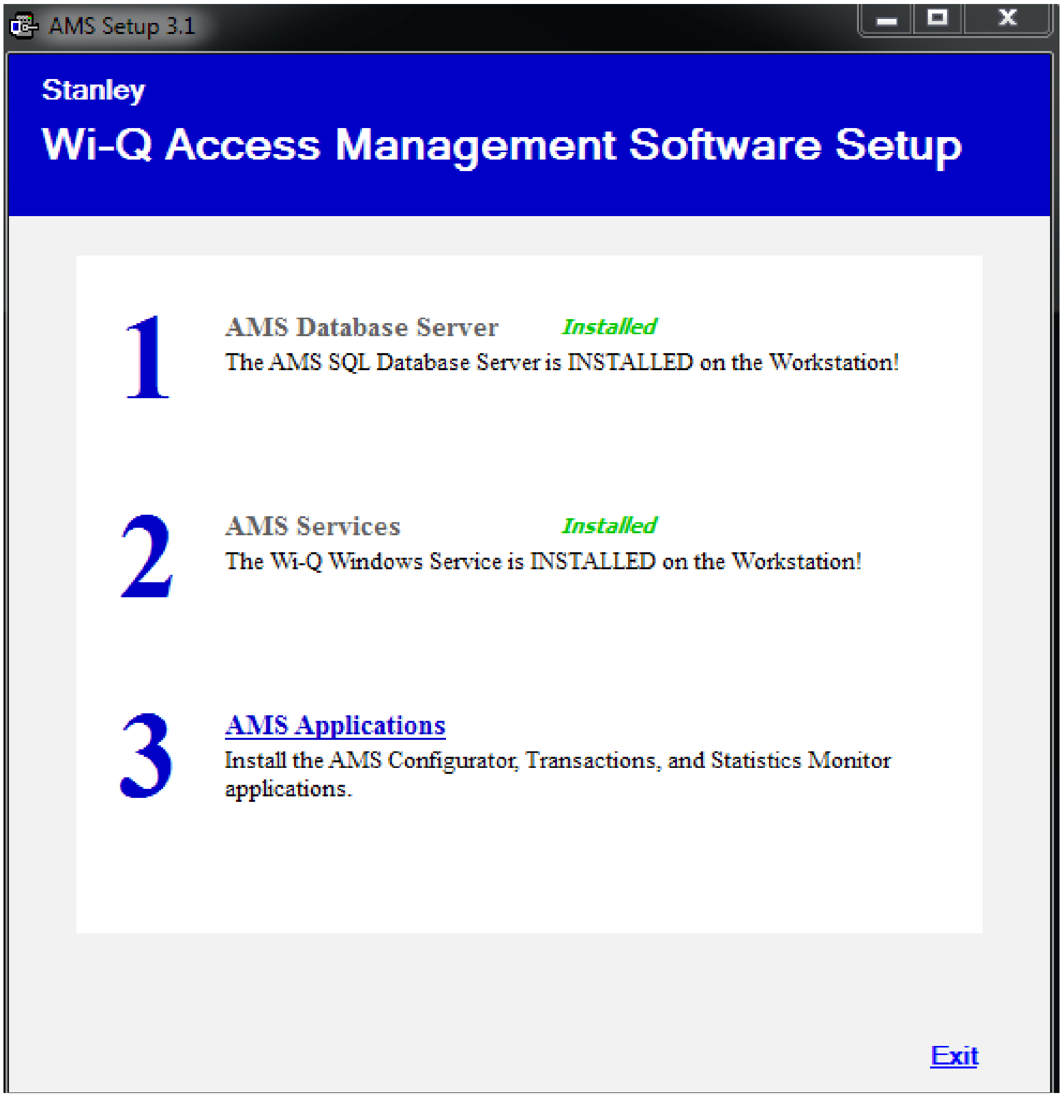
8 The wizard is now ready to begin installation. Click Install.

9 Once the installation is complete, click Finish.

Step 3

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

Figure 25 Install AMS Applications



Stanley

Wi-Q Access Management Software Setup

1 AMS Database Server Installed

The AMS SQL Database Server is INSTALLED on the Workstation!

2 AMS Services Installed

The Wi-Q Windows Service is INSTALLED on the Workstation!

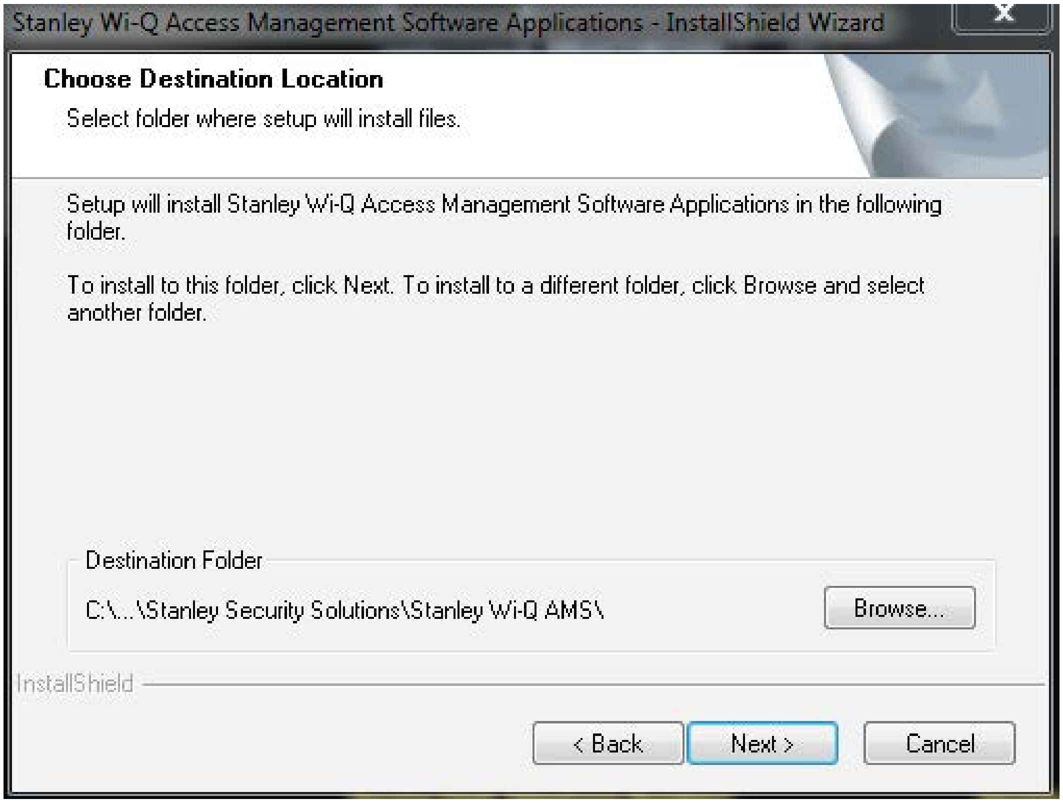
3 AMS Applications

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

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

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

Figure 26 Destination Folder



Stanley Wi-Q Access Management Software Applications - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

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

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

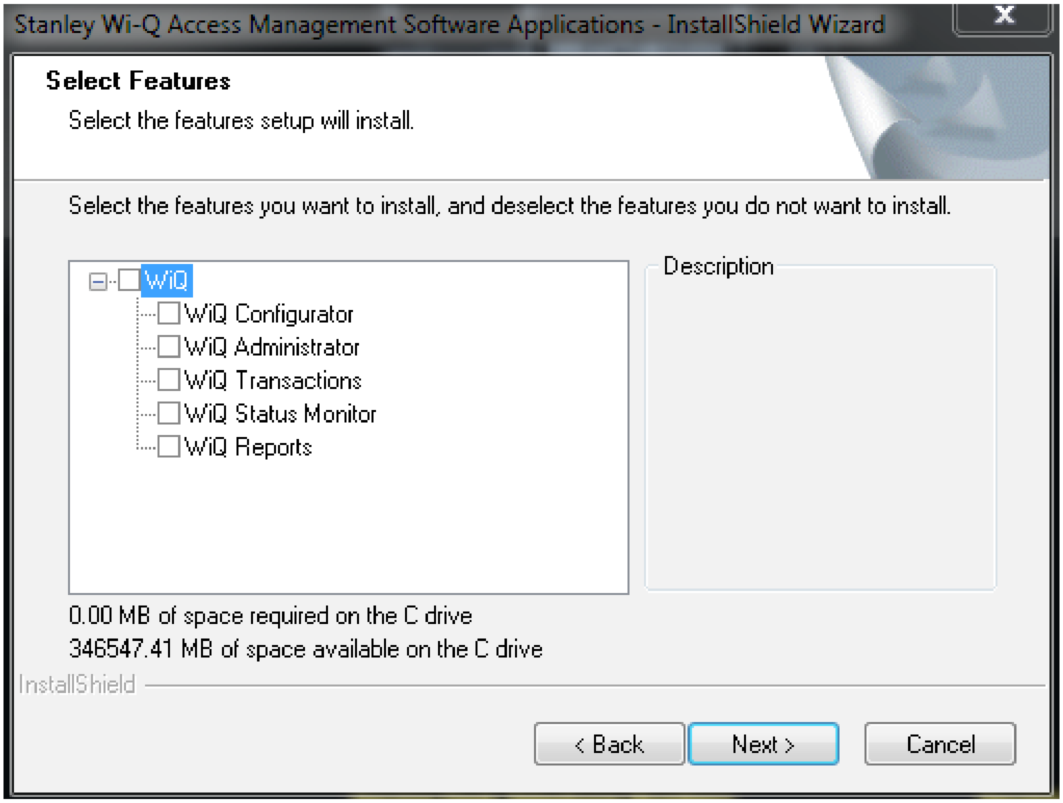
Destination Folder

C:\...\Stanley Security Solutions\Stanley Wi-Q AMS\

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

Figure 27 shows the installation components available in a Custom Setup.

Figure 27 Custom Setup



Stanley Wi-Q Access Management Software Applications - InstallShield Wizard

Select Features

Select the features setup will install.

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

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

Description

0.00 MB of space required on the C drive

346547.41 MB of space available on the C drive

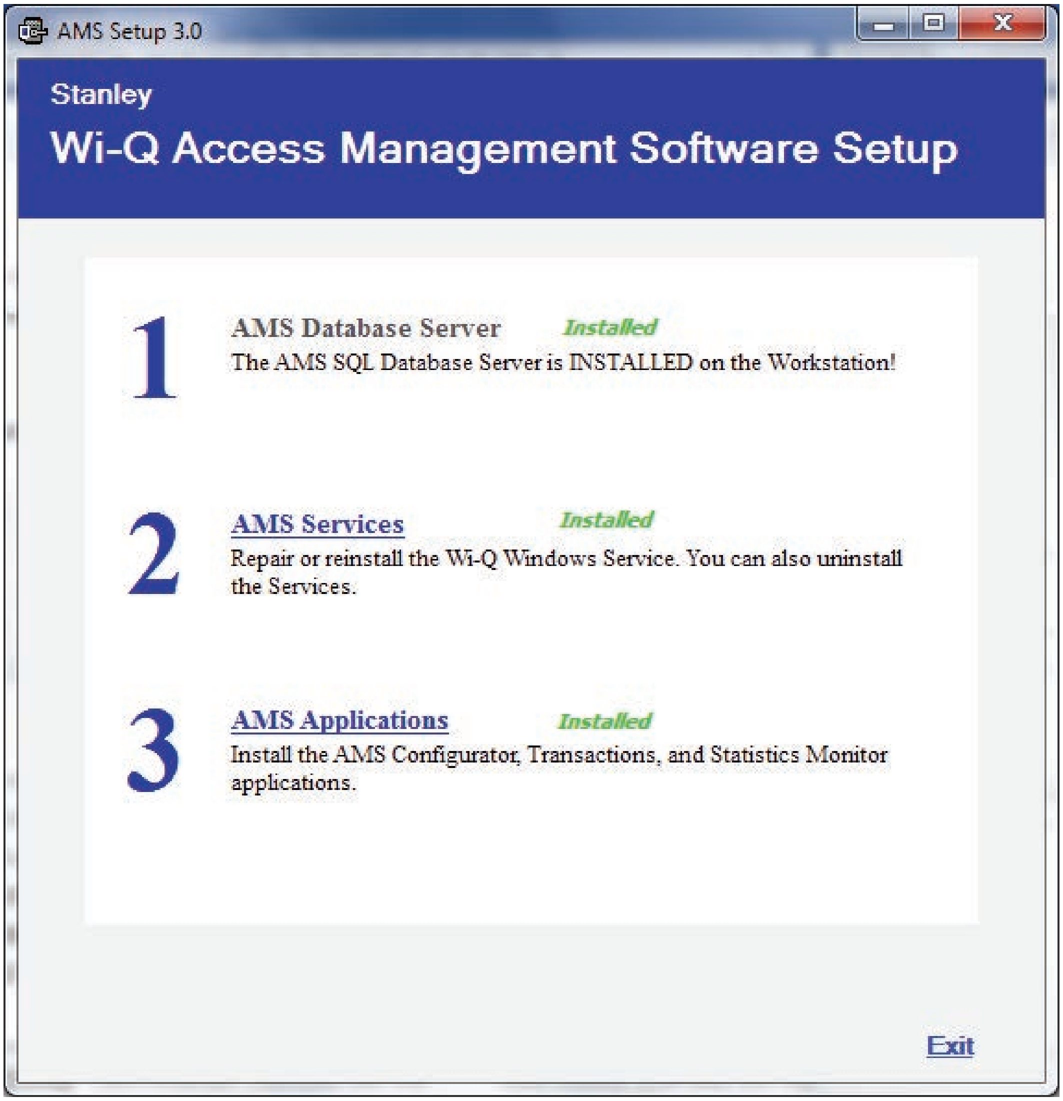
5 Clicking on the icons to the left of each component will bring up installation options. If you decide on a Custom Setup, you must select an installation option for each component. Then click Next to continue.

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

7 Once the installation is complete, click Finish.

The installation of all three components is now complete.

Figure 28 Successful System Setup



AMS Setup 3.0

Stanley

Wi-Q Access Management Software Setup

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

2 AMS Services Installed
Repair or reinstall the Wi-Q Windows Service. You can also uninstall the Services.

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

8 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.

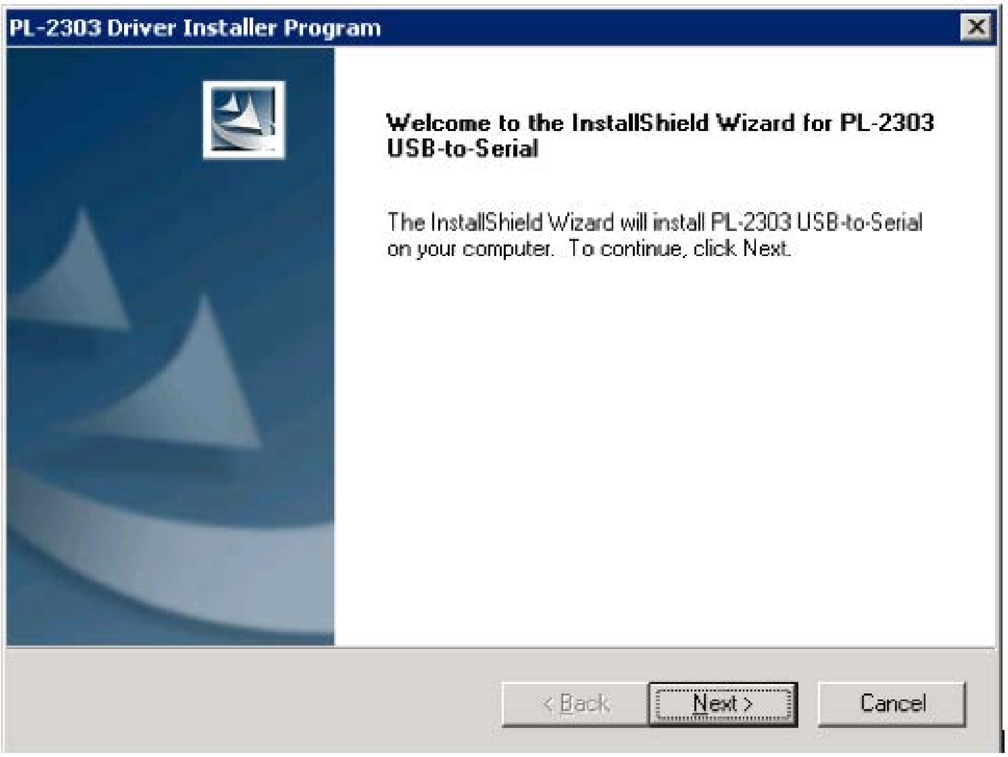
Infrared Dongle

The application runs on any PC running Windows 7, Windows 8, or Windows Server 2012. The PC must have either a serial port or USB port.

Locks communicate through an IR interface, a USB to raw SIR serial adapter is required. The dongle used for development and testing is the Actisys ACT-IR424UN.

1. Run ACT_IR224UN_DriverInstaller_xxx.exe. vis-
2. Install Shield Wizard will install PL-2303 USB-to-Serial on your computer.

Figure 29 InstallShield Wizard



PL-2303 Driver Installer Program

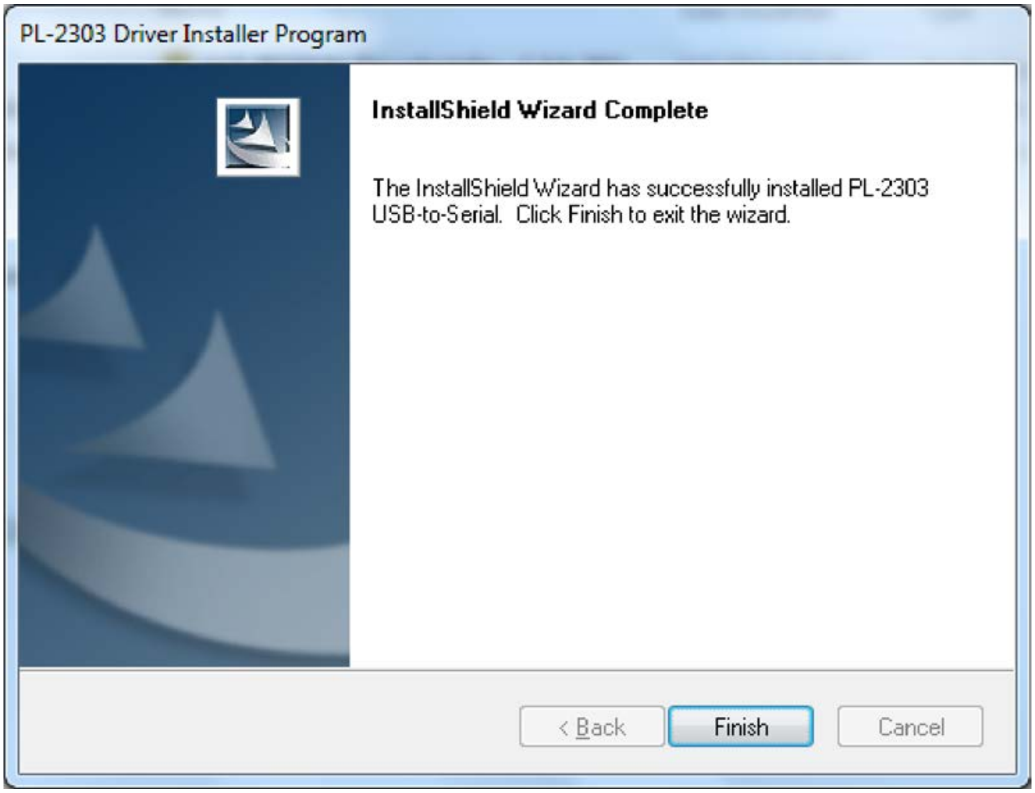
Welcome to the InstallShield Wizard for PL-2303 USB-to-Serial

The InstallShield Wizard will install PL-2303 USB-to-Serial on your computer. To continue, click Next.

3. Select Next.

4 Select Finish.

Figure 30 InstallShield Wizard



PL-2303 Driver Installer Program

InstallShield Wizard Complete

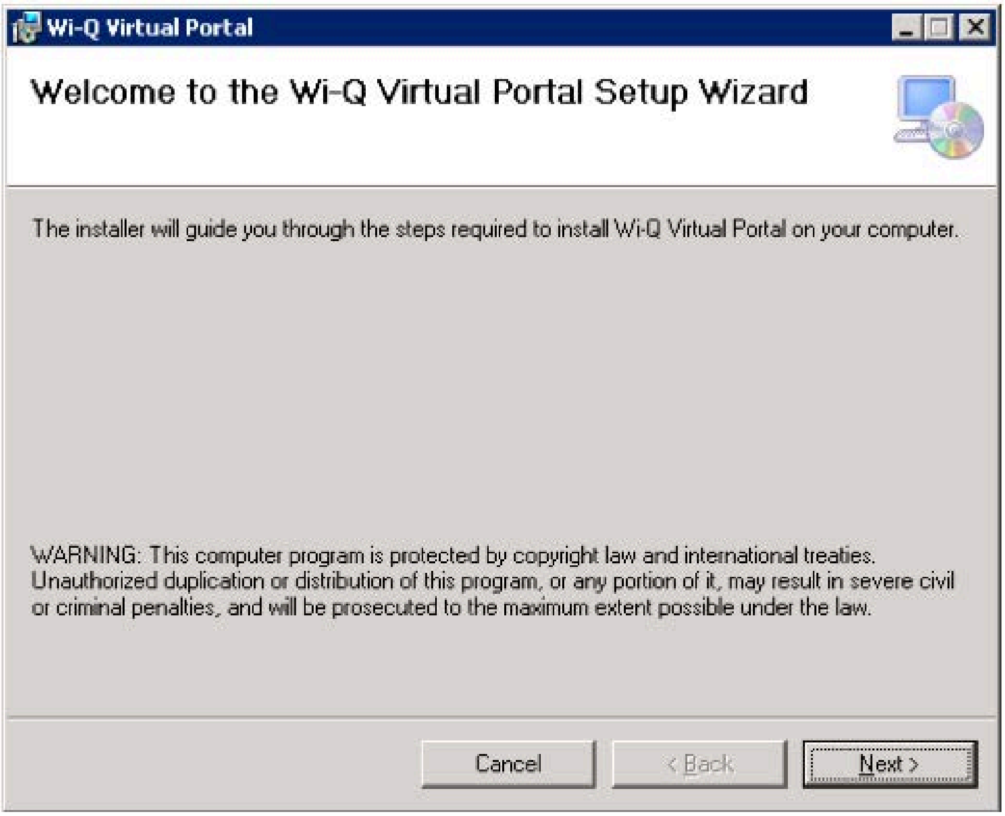
The InstallShield Wizard has successfully installed PL-2303 USB-to-Serial. Click Finish to exit the wizard.

Wi-Q Virtual Portal Installation

This will install the Wi-Q Virtual Portal software needed to connect to the offline OM2000 locksets. Run setup.exe under virtual portal installer folder.

1 Select Next.

Figure 31 Wi-Q Virtual Portal Setup Wizard



Welcome to the Wi-Q Virtual Portal Setup Wizard

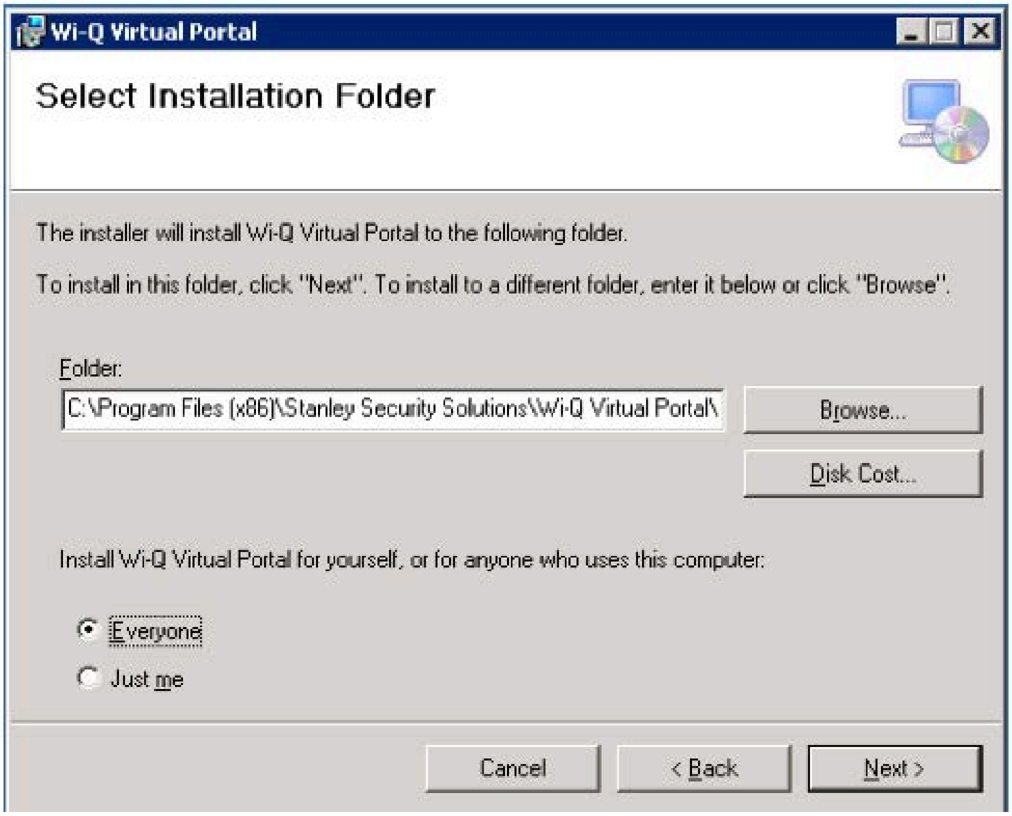
The installer will guide you through the steps required to install Wi-Q Virtual Portal on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

2 Enter the installation path or browse to a path location. Choose installation for everyone or just the current user. Select Next.

Note Recommended settings are displayed.

Figure 32 Select Installation Folder



Wi-Q Virtual Portal

Select Installation Folder

The installer will install Wi-Q Virtual Portal to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:

C:\Program Files (x86)\Stanley Security Solutions\Wi-Q Virtual Portal\

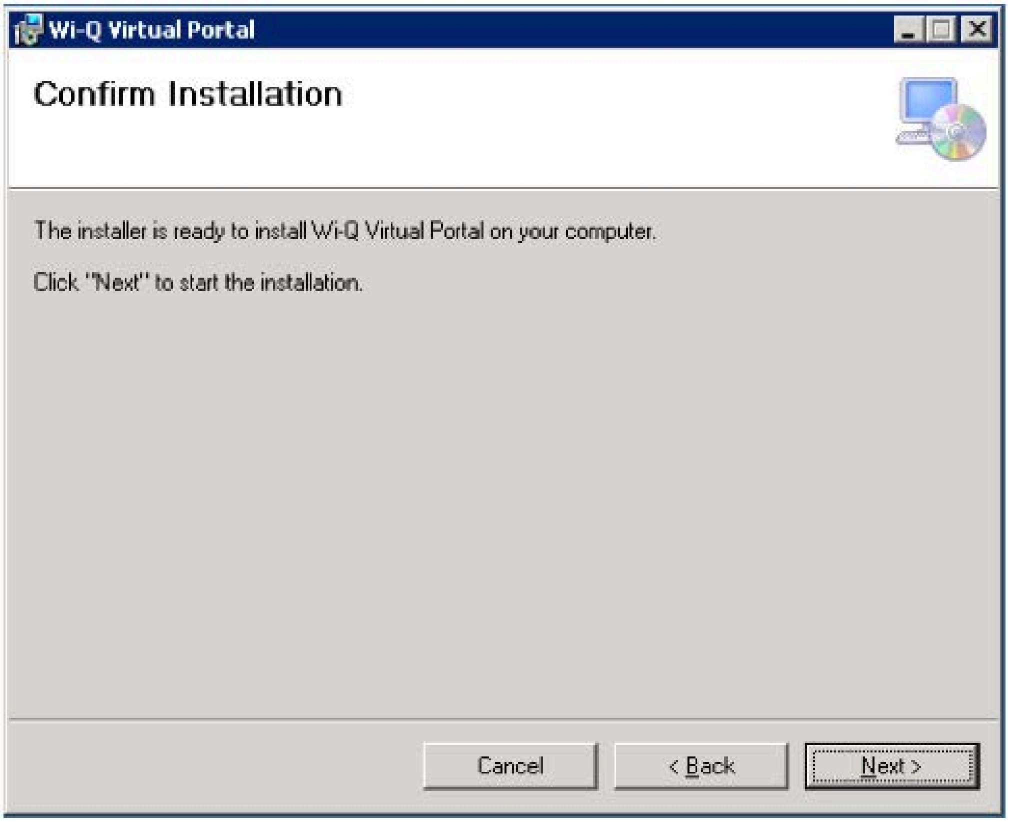
Install Wi-Q Virtual Portal for yourself, or for anyone who uses this computer:

● Everyone

○ Just me

3 Select Next.

Figure 33 Confirm Installation



Wi-Q Virtual Portal

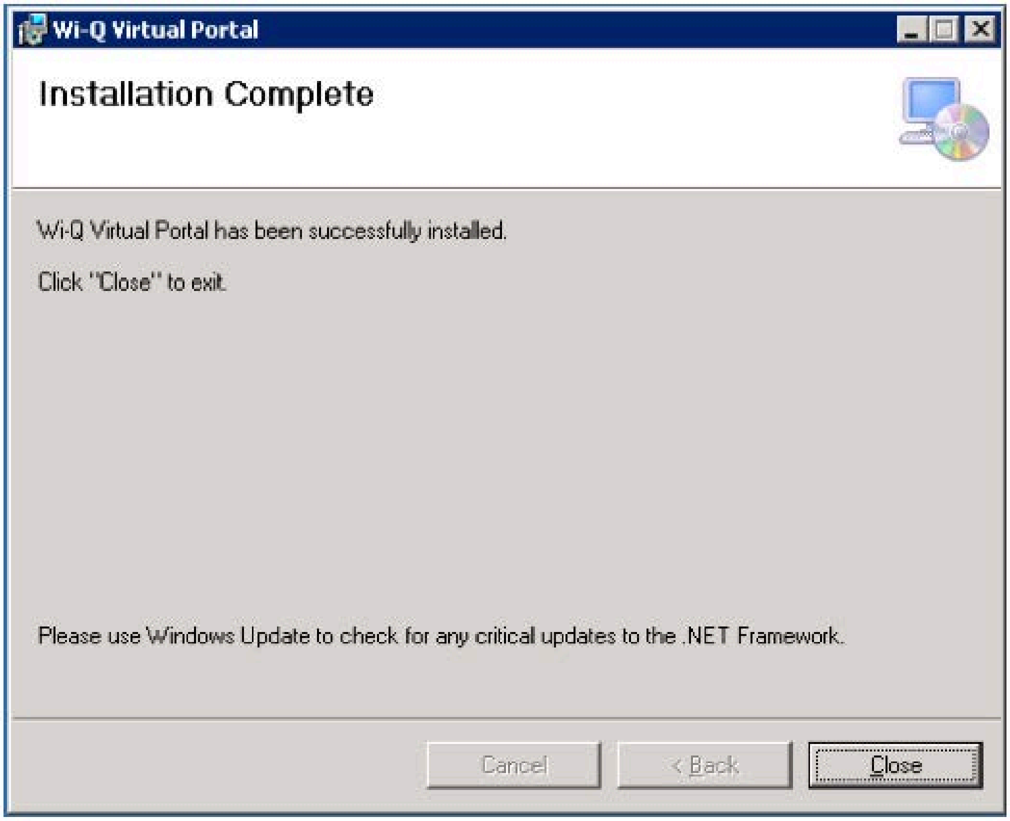
Confirm Installation

The installer is ready to install Wi-Q Virtual Portal on your computer.

Click "Next" to start the installation.

4 Installation will complete. Select Close to exit installation.

Figure 34 Installation Complete



Wi-Q Virtual Portal

Installation Complete

Wi-Q Virtual Portal has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

Configuring Segments, Virtual Portal Gateways and Controllers

Create Your Segment

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

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

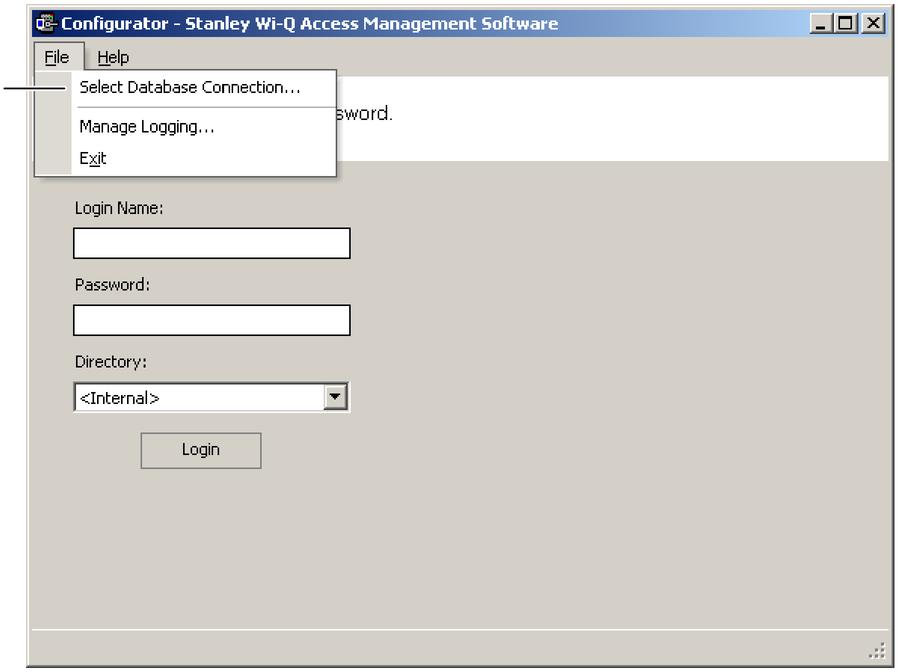
Selecting the Database Connection

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 35 Select Database Connection



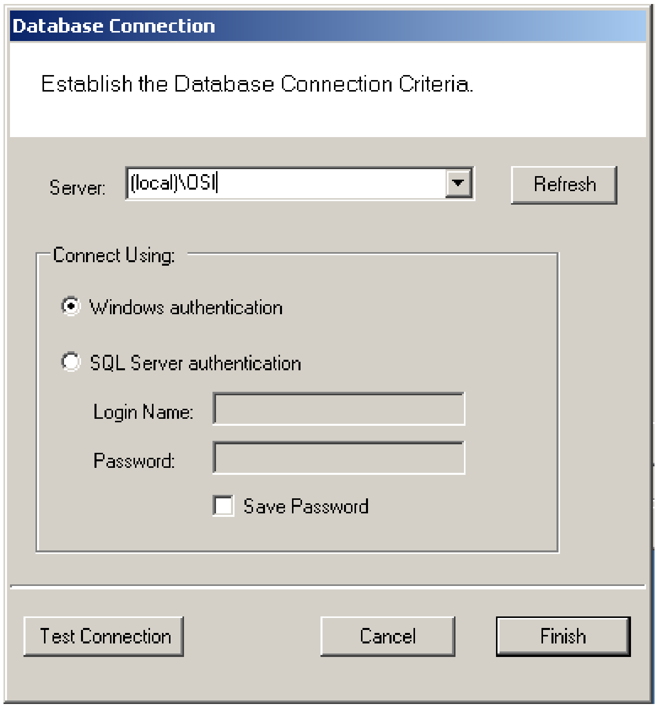
Configurator - Stanley Wi-Q Access Management Software
File
Help
Select Database Connection...
Manage Logging...
Exit
sword.
Login Name:
Password:
Directory:
Login

Directory: <Internal>

Click on Select Database Connection

The Database Connection dialog box opens. See Figure 36.

Figure 36 Database Connection Window



Establish the Database Connection Criteria.

Server: (local)\OSI

Connect Using:

● Windows authentication

○ SQL Server authentication

Login Name:

Password:

□ Save Password

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

3 Under Connect Using, select either Windows authentication or SQL Server authentication. If you select SQL Server Authentication, 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.

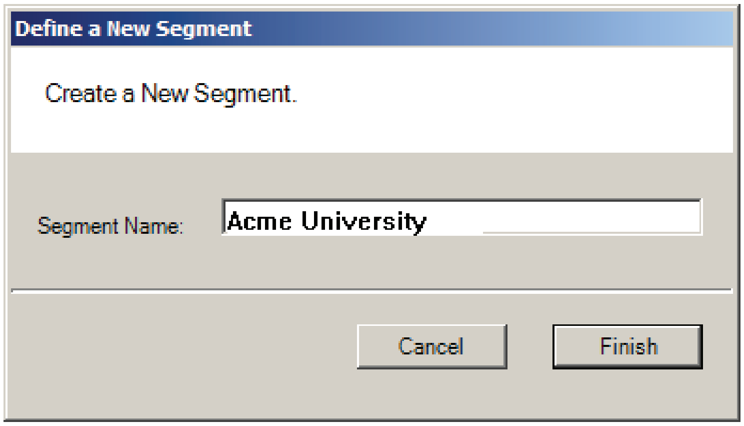
2 Select Login. You are ready to start setting up your new segment.

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 37 Define a New Segment



Define a New Segment

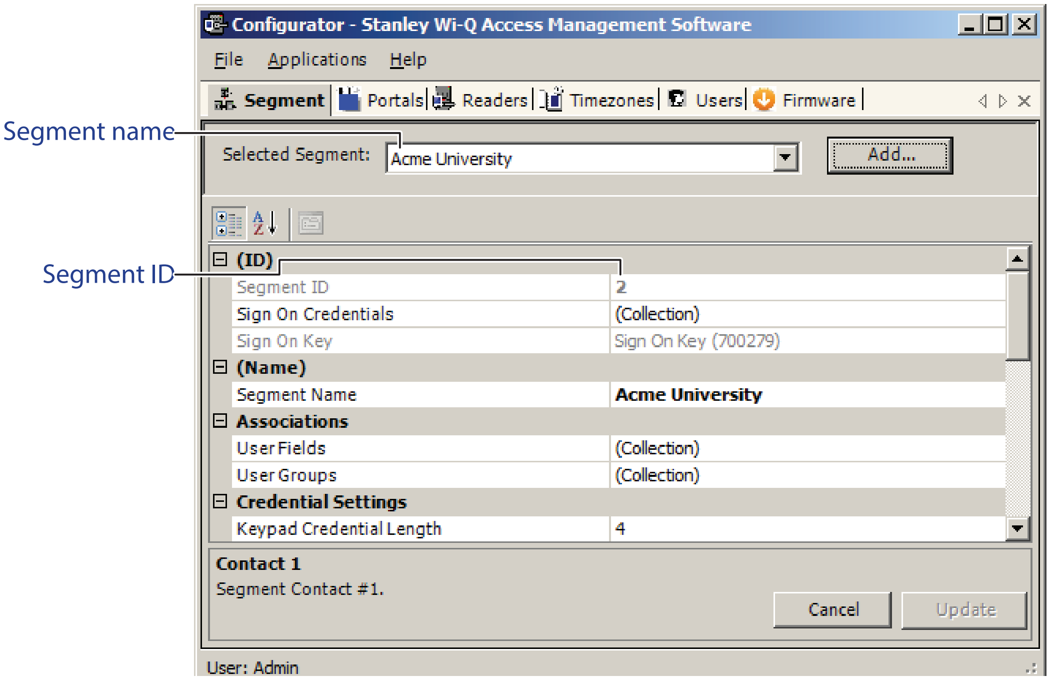
Create a New Segment.

Segment Name: Acme University

2 Select Finish.

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

Figure 38 Identifying the Segment name and ID



Selected Segment: Acme University

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

Contact 1
Segment Contact #1.

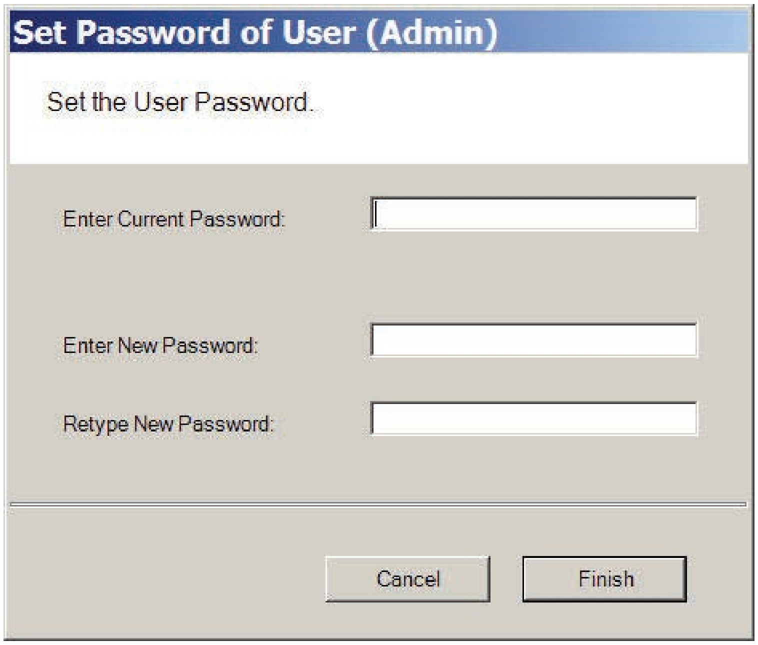
User: Admin

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

To change the Password

1 At the top left corner of the Configurator dialog box, select File>Change Password. The Set Password of User dialog box opens (Figure 39 on page 41).

Figure 39 Set Password of User



Set Password of User (Admin)

Set the User Password.

Enter Current Password:

Enter New Password:

Retype New Password:

2 Enter the new password.

3 Retype the new password.

4 Select Finish.

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

Credential Settings

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

Note Proximity card configurations are supported, but not configurable.

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.

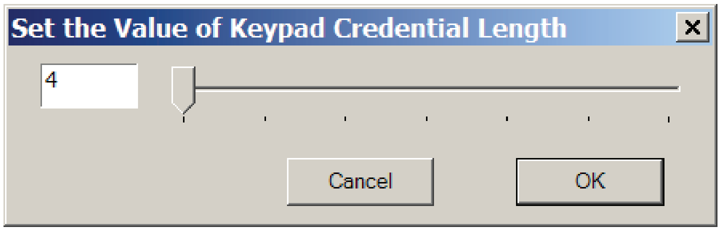
Note Keypad credential length must be set before you add users to the system.

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 40 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.

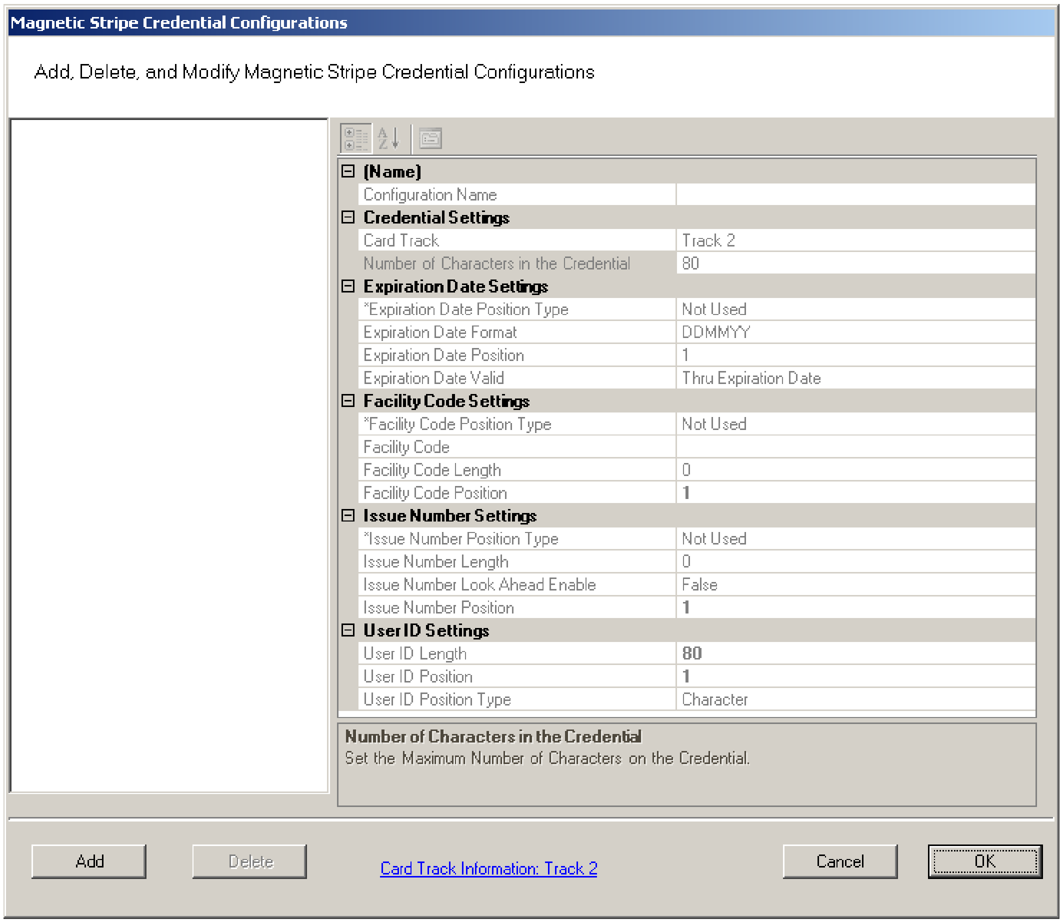
Magnetic Stripe Credential Configurations

Before Magnetic cards can be used in the system, you must configure AMS to accept the card types and settings. Figure 41 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 defaults Expiration Date, Segment Code, and Issue Number settings to Not Used, and no other changes need to be made.

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

Figure 41 Magnetic Stripe Credential Configurations



Magnetic Stripe Credential Configurations

Add, Delete, and Modify Magnetic Stripe Credential Configurations

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

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

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

Credential Settings

Wi-Q AMS can be configured to accept coding from existing Track 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 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 dormakaba Knowledge Base or contact Technical Support for controller hardware track limits.

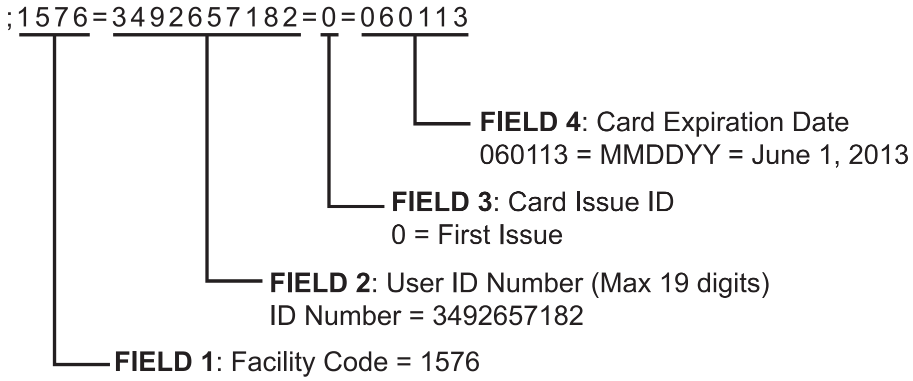
Character codes and counts

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.

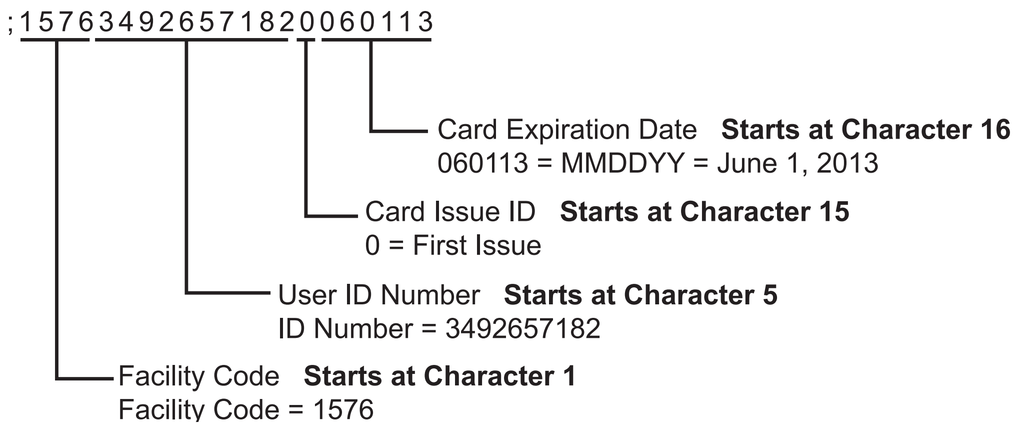
Following is an example of encoded data using field separators on Track 2.

Figure 42 Data Fields


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

Character Count — You can set up a character count from the beginning of each ID. For example, the Segment ID could start at the beginning of the data stripe, digit count of 1. If the Segment ID has eight digits, the User ID would be set to start at digit count of 9. This method requires all data groups with exception of the last one, to have a fixed number of digits. Following is an example of encoded data using character counts on Track 2. User ID Number has a maximum of ten characters (Figure 43 on page 45).

Figure 43 Character Count Fields


;1576349265718200060113
Card Expiration Date Starts at Character 16
060113 = MMDDYY = June 1, 2013
Card Issue ID Starts at Character 15
0 = First Issue
User ID Number Starts at Character 5
ID Number = 3492657182
Facility Code Starts at Character 1
Facility Code = 1576

Note If you are not using the default settings for Magnetic Stripe Credential Configurations, make sure that Expiration Date Position Type, Facility Code Position Type, Issue Number Position Type and User ID Position Type are all set the same. They must be set either 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 44 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.

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 de-faults 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.

Misc

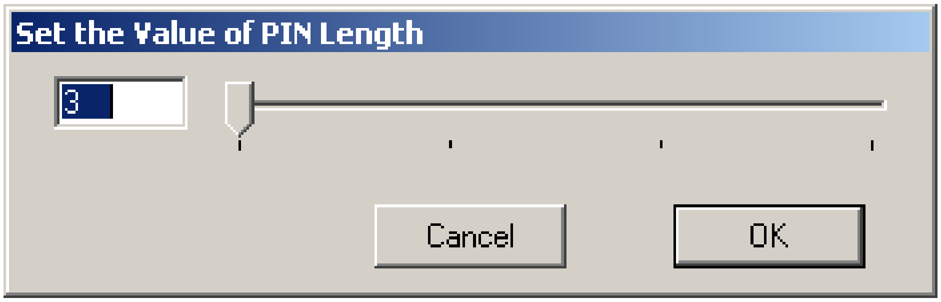
This category contains three fields (Contact 1, Contact 2, and Reference) that you can use to store any miscellaneous information you that will be helpful to you and your system. For example, you may decide to enter the phone number or email address for dormakaba Technical Support in case you experience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

PIN Settings

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

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

Figure 44 Set the Value of PIN Length



Set the Value of PIN Length

3

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.

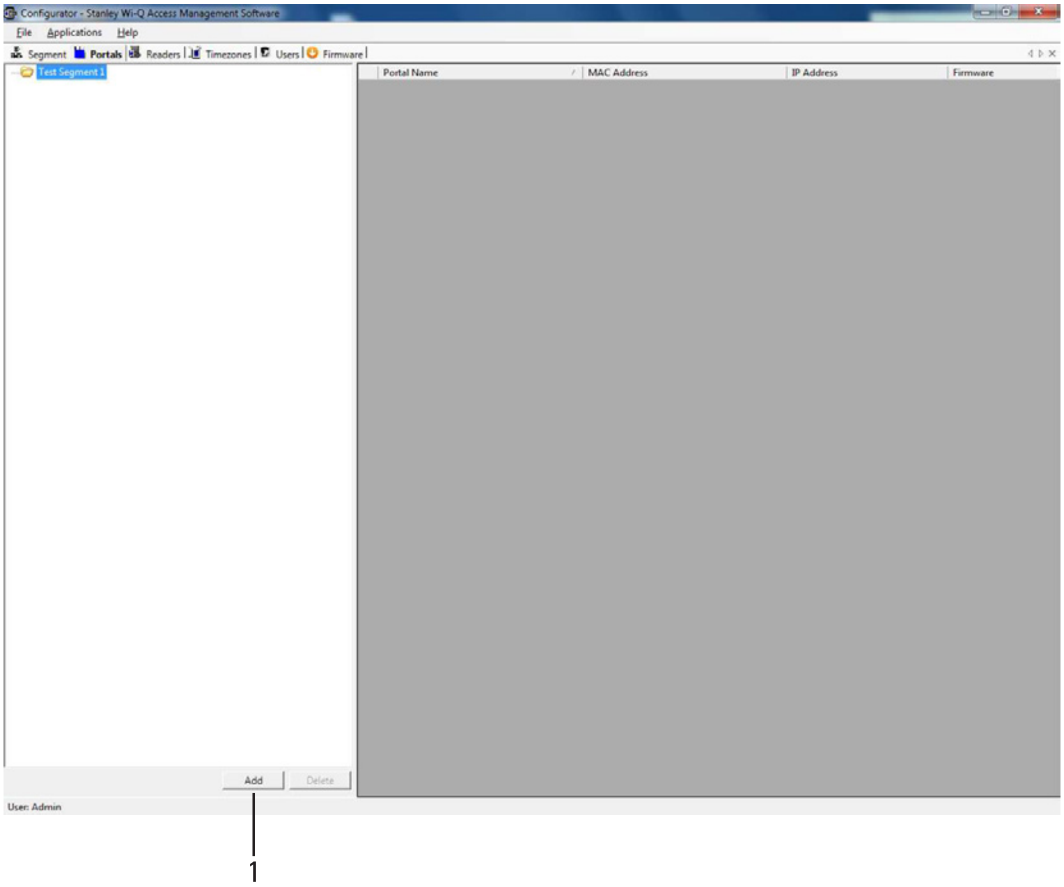
Note Sign on credential and I/O references are not supported for offline controllers.

Creating a Virtual Portal

Open Wi-Q Access Management (Configurator) and select the ‘Portals’ tab.

1 Click Add.

Figure 45 Configurator



The Configure New Portal Gateway window opens (Figure 46 on page 49).

2 Name new portal in Name field.

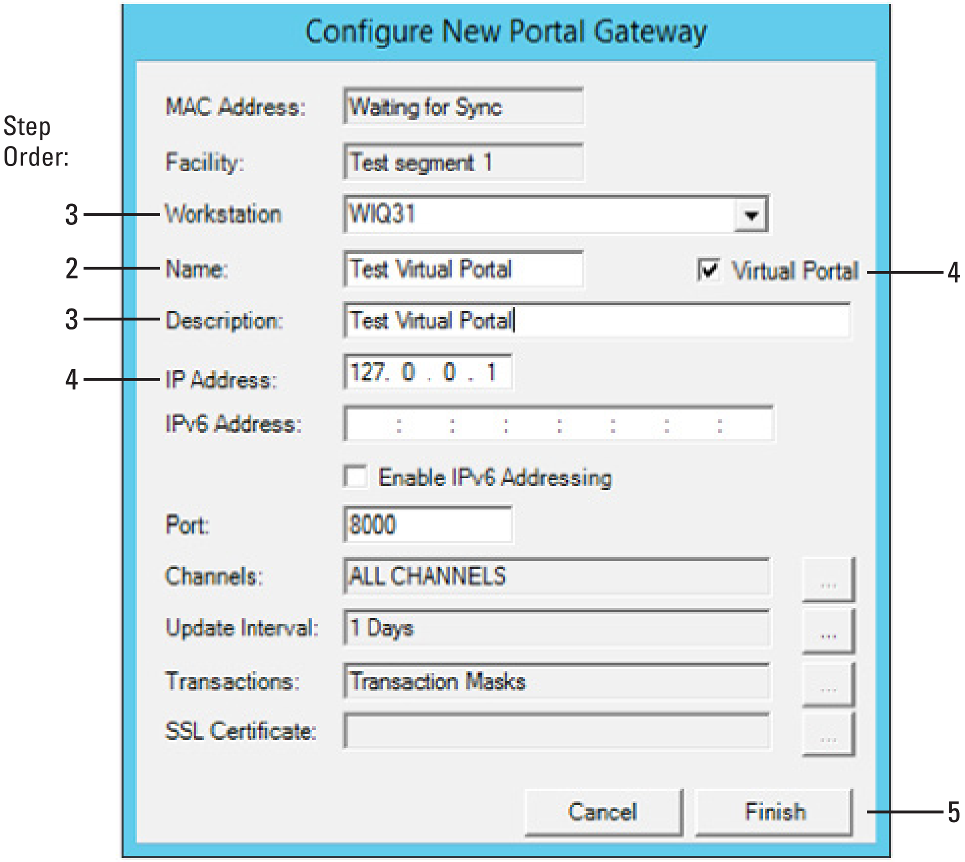
3 Select ‘Workstation’ and add ‘Description’.

4 Check Virtual Portal checkbox. IP Address should be host loopback address (127.0.0.1).

5 Click Finish.

Note When the Virtual Portal checkbox is checked, the Channels and Transactions dialog buttons are disabled.

Figure 46 Configure New Portal Gateway



Configure New Portal Gateway

MAC Address: Waiting for Sync

Facility: Test segment 1

Workstation WIQ31

Name: Test Virtual Portal

☑ Virtual Portal

Description: Test Virtual Portal

IP Address: 127. 0 . 0 . 1

IPv6 Address: : : : : : : :

□ Enable IPv6 Addressing

Port: 8000

Channels: ALL CHANNELS

Update Interval: 1 Days

Transactions: Transaction Masks

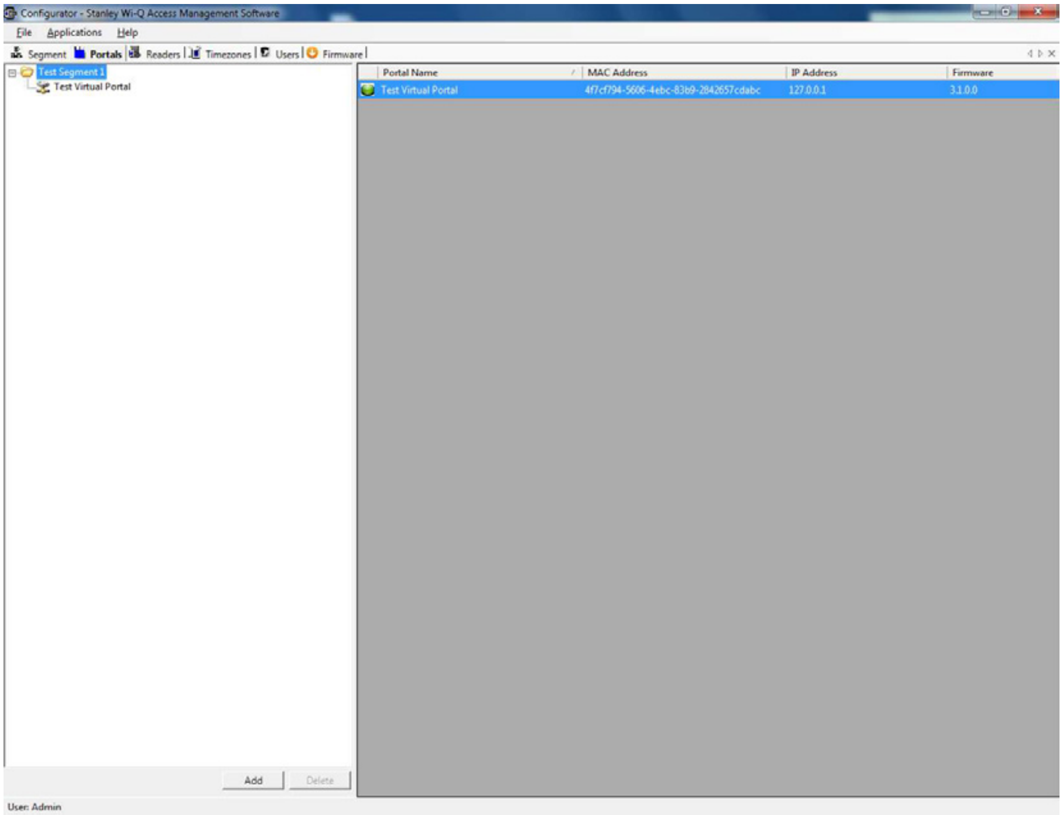
SSL Certificate:

Note A checkbox has been added to the Portal Add dialog to indicate that the new portal is a Virtual Portal.

Note Once a Virtual Portal is created, new options are added in Configurator:

- OM2000 Holiday - found in ‘Timezones’ tab
- OM2000 User Groups - found in ‘Users’ tab
- 'Add Offline' Controllers - found in ‘Readers’ tab

Figure 47 Configurator

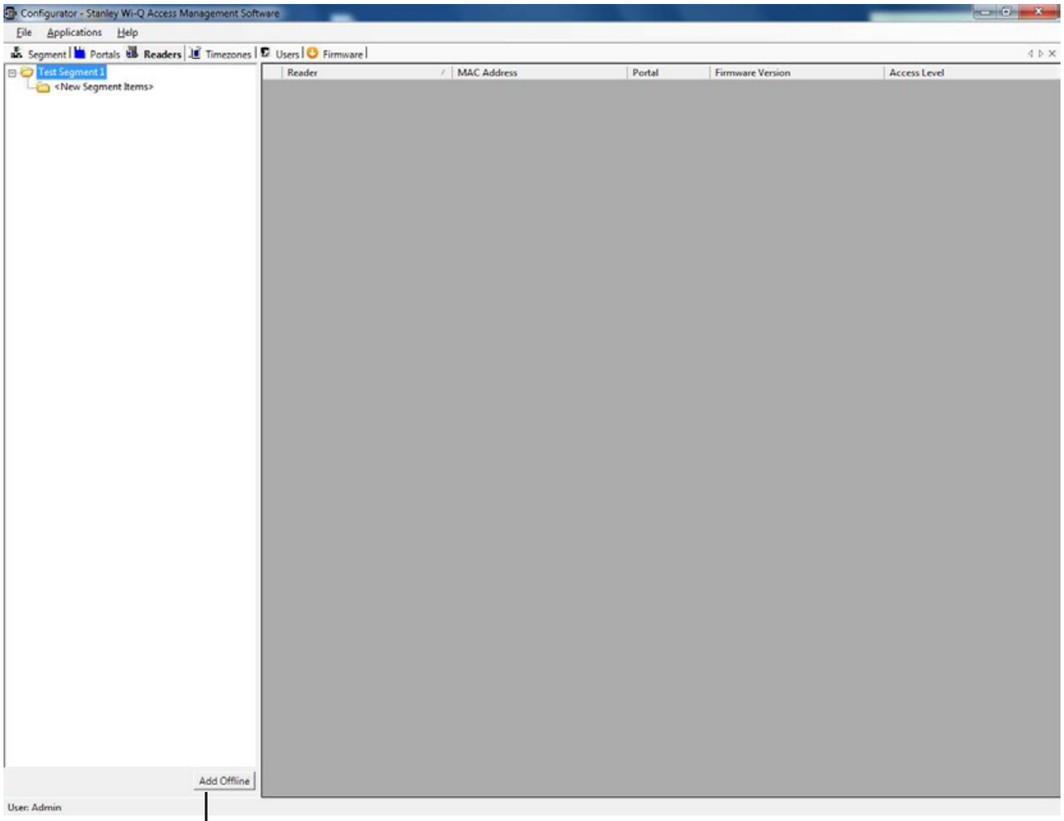


Portal Name	MAC Address	IP Address	Firmware
Test Virtual Portal	4f7cf794-5606-4ebc-83b9-2842657cdabc	127.0.0.1	3.1.0.0

Creating an OM2000 Offline Reader

1. Select Readers tab in Configurator.
2. Click Add Offline, the Configure New Offline Reader window opens.

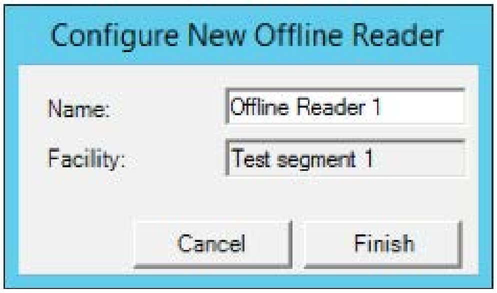
Figure 48 Configurator—With Add Offline Button



Not shown until virtual portal added

3. Enter a name for the reader to add an offline reader. Click Next.

Figure 49 Configure New Offline Reader

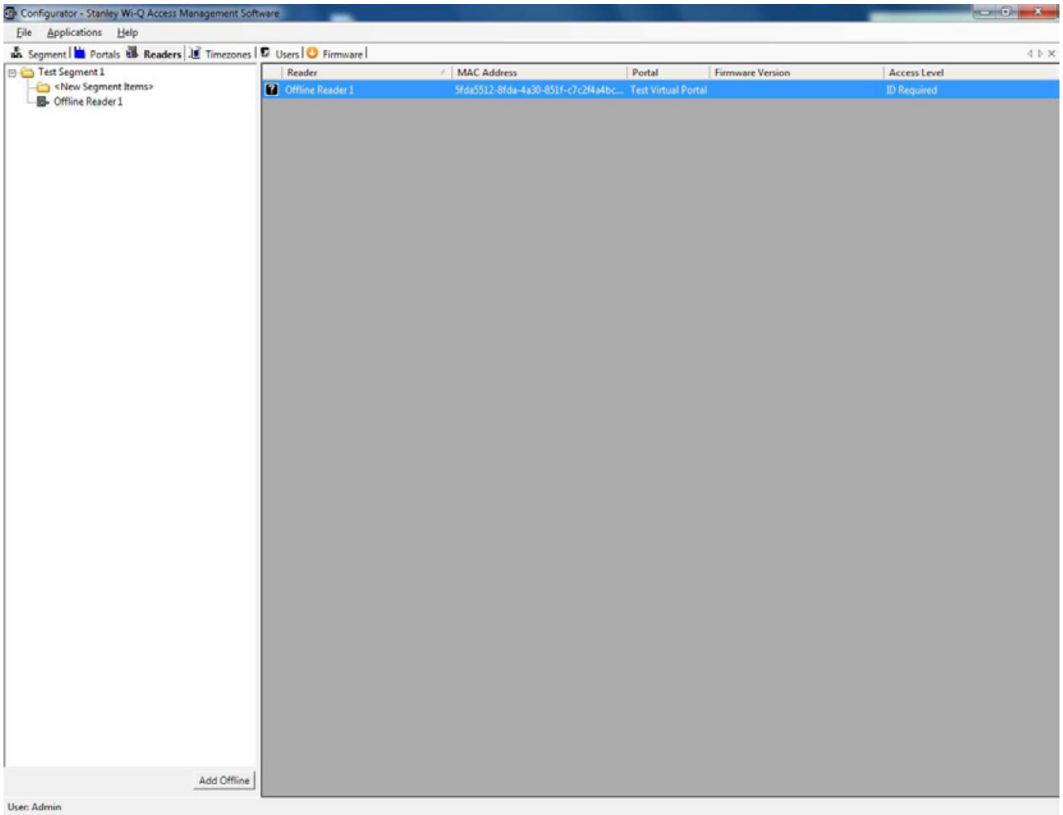

Configure New Offline Reader

Name: Offline Reader 1

Facility: Test segment 1

Once the reader has been manually added, it will show up in the Wi-Q readers tree.

Figure 50 Configurator—Showing Offline Reader



Reader	MAC Address	Portal	Firmware Version	Access Level
Offline Reader 1	5fda5512-8fda-4a30-851f-c7c2f4a4bc...	Test Virtual Portal		ID Required

Assign Card Formats to Readers

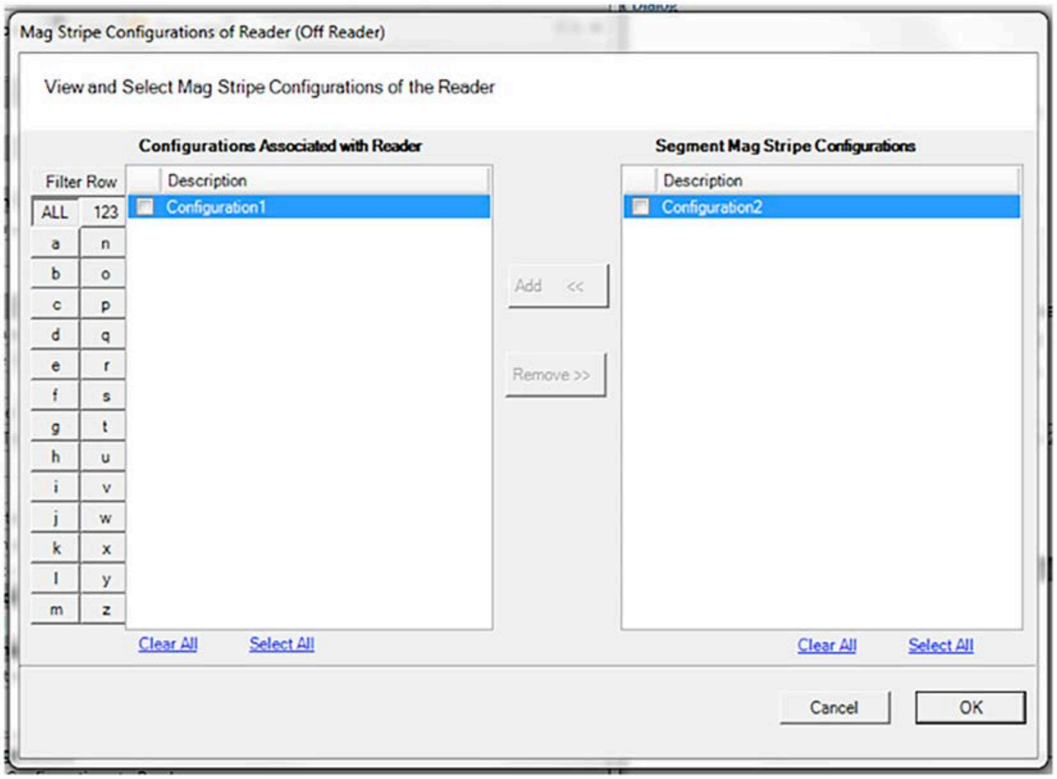
Refer to Wi-Q AMS User Guide, Section 5 Credential Settings.

1 Select Offline Reader.

2 Click button under Mag Stripe Configuration.

3 Click the box for the appropriate Mag configuration from list under Segment Mag Stripe Configurations.

Figure 51 Mag Stripe Configurations of Reader


Mag Stripe Configurations of Reader (Off Reader)
View and Select Mag Stripe Configurations of the Reader
Configurations Associated with Reader
Segment Mag Stripe Configurations
Filter Row
ALL
123
a
b
c
d
e
f
g
h
i
j
k
l
m
n
o
p
q
r
s
t
u
v
w
x
y
z
Description
□ Configuration1
Description
□ Configuration2
Add <<
Remove >>
Clear All
Select All
Clear All
Select All
Cancel
OK

Note Two new items have been added to the Associations sections in Wi-Q AMS 3.1 – Mag Configurations and Prox Configurations. Since offline readers can have at most one mag card configuration assigned to them, a mechanism to associate a mag card configuration to a reader is needed. Offline readers do not require a proximity card format to be assigned because the offline reader uses just the raw prox data as it is read from the card for comparison. **However, since it is desirable to allow assignment of card configurations (both mag and prox) to readers rather than all card configurations being assigned to every reader, the feature is implemented for both types of card configurations for all readers (both offline and online).**

Note For offline readers, one magnetic card configuration can be assigned.

Note Proximity card configurations are supported, but not configurable.

Creating TimeZone Intervals

The Offline reader does not allow timezone intervals that:

- Have a start date/time in the future
- Have an end date/time set
- Do not recur
- Are not a weekly recurrence or are not a daily recurrence that recurs every 1 day

If an Interval Collection containing an interval that is not compatible with the virtual portal is assigned to a Reader Control with an offline reader assigned to it, a message box is displayed alerting the user that the Interval Collection cannot be assigned to the Reader Control.

Also, if a Reader Control with an Interval Collection which includes an incompatible interval is assigned an offline reader, a message box is displayed alerting the user that the assignment cannot be made.

And finally, if an interval that is assigned to an Interval Collection that is assigned to a Reader Control containing an offline reader is modified so that it is no longer compatible with the virtual portal, a message box is displayed alerting the user that the change cannot be made.

- Every lock has a Reader Control assigned which has a default mode. Any period of time not covered by an Interval Collection, is set to the default mode just like in Wi-Q.

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. Sub-tabs exist inside the Timezone tab:

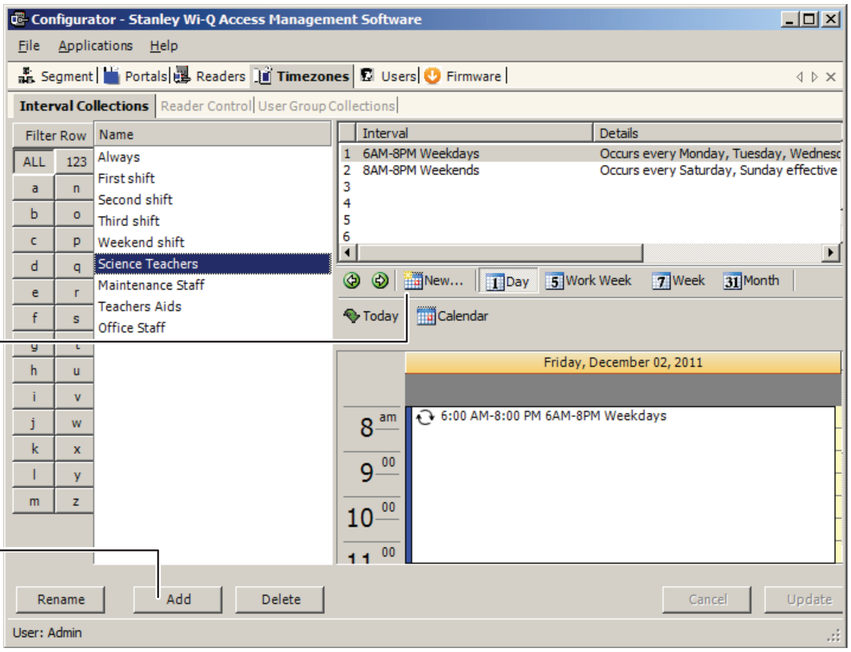
- Interval Collections — this is a collection of recurring ranges of time and days of the week, such as 6:00 am to 6:00 pm weekdays AND 8:00 am to 8:00 pm weekends.
- Reader Control — this is where you assign access levels to readers and determine how the reader will operate during assigned timezone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

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 52 Interval Collection



Name
Always
First shift
Second shift
Third shift
Weekend shift
Science Teachers
Maintenance Staff
Teachers Aids
Office Staff

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

Friday, December 02, 2011

6:00 AM-8:00 PM 6AM-8PM Weekdays

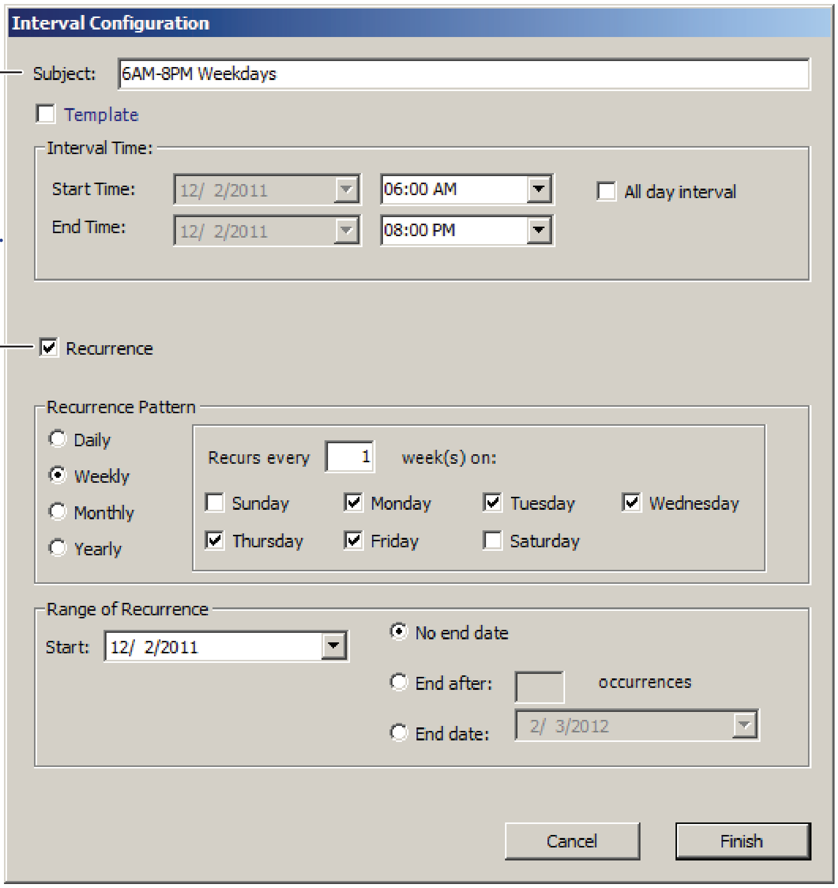
User: Admin

Click New to create a new interval.

Click Add to create an Interval Collection.

The Interval Configuration window opens.

Figure 53 Interval Configuration



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

Click Recurrence if the interval repeats.

Interval Configuration

Subject: 6AM-8PM Weekdays

□ Template

Interval Time:

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

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

☑ Recurrence

Recurrence Pattern

○ Daily
● Weekly
○ Monthly
○ Yearly

Recurs every 1 week(s) on:

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

Range of Recurrence

Start: 12/ 2/2011

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

4 Enter a brief name for the Interval.

5 Select the Start and End Time of the Interval.

6 Click the Recurrence check box.

7 Select the Recurrence Pattern of the Interval.

8 Select the Range of Recurrence for the Interval.

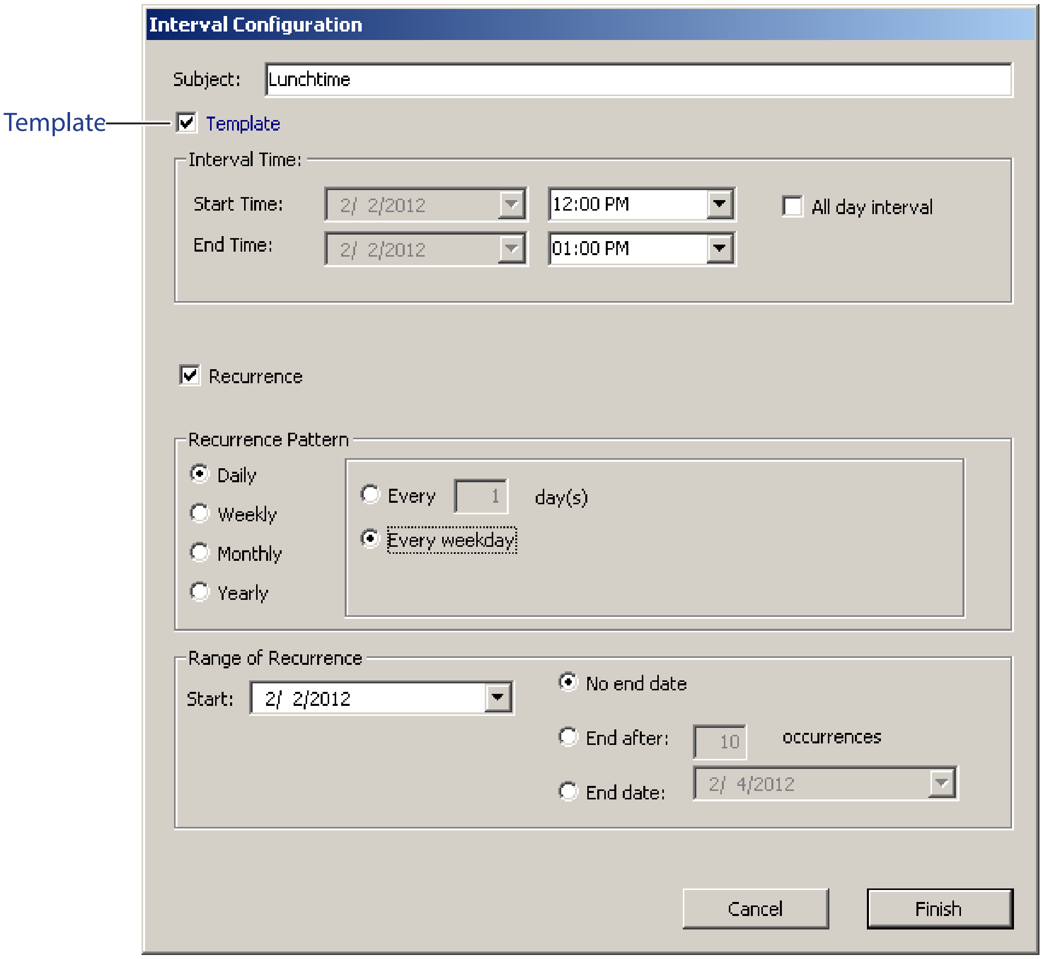
9 Click Finish to save your new Interval. This Interval is now listed as one of the intervals for the Interval Collection.

10 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" check box. 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" check box (Figure 54), you can add that interval to an existing collection.

Figure 54 Interval Configuration Template



Interval Configuration

Subject: Lunchtime

☑ Template

Interval Time:

Start Time: 2/ 2/2012 12:00 PM

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

☐ All day interval

☑ Recurrence

Recurrence Pattern

● Daily
○ Weekly
○ Monthly
○ Yearly

○ Every 1 day(s)
● Every weekday

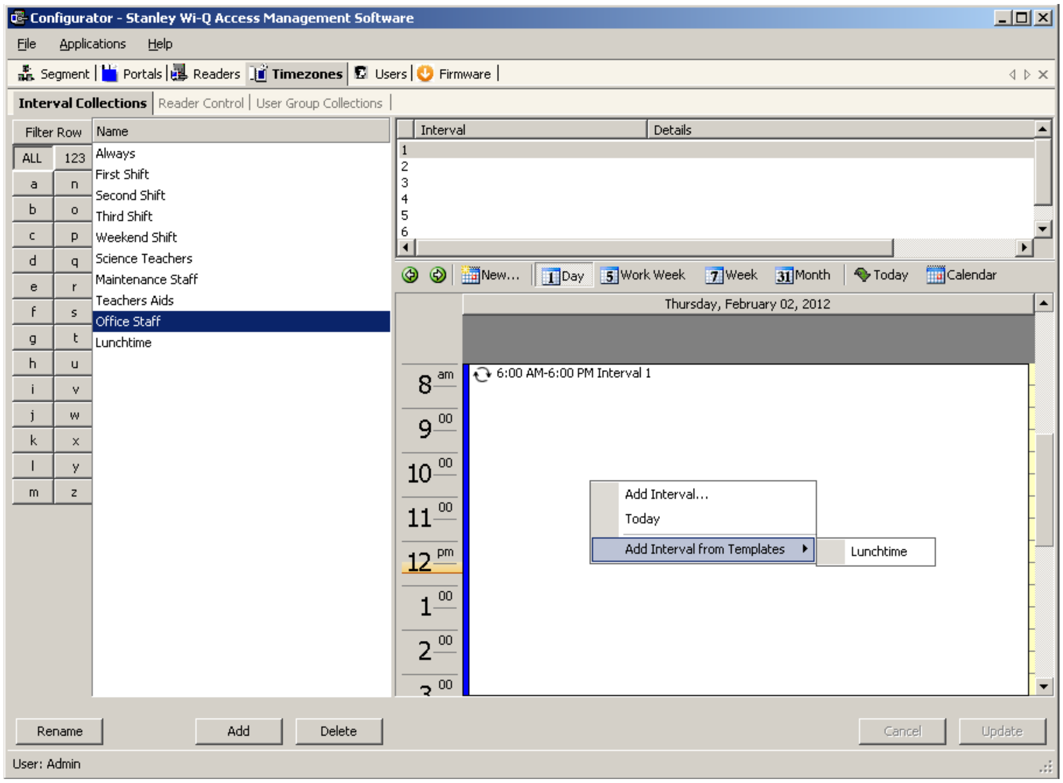
Range of Recurrence

Start: 2/ 2/2012

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

To add the "Lunchtime" interval to another collection , select the existing interval collection from the list at the left, right-click in the calendar area, and select "Lunchtime" from the Add Interval from Templates options. In our example, we add the Lunchtime interval to the Office Staff Interval Collection. See Figure 55.

Figure 55 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.

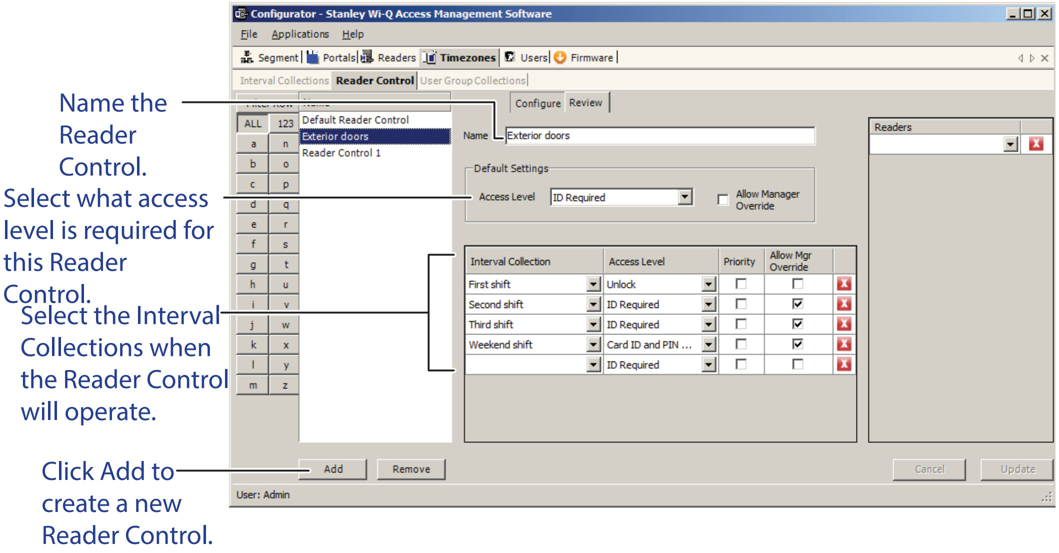
5 Select the Interval Collections when the Reader Control will operate.

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 56 Reader Control



Default Reader Control
Exterior doors
Reader Control 1

Name: Exterior doors

Default Settings
Access Level: ID Required
□ Allow Manager Override

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

Name the Reader Control.

Select what access level is required for this Reader Control.

Select the Interval Collections when the Reader Control will operate.

Click Add to create a new Reader Control.

Note If an Interval Collection containing an interval that is not compatible with the virtual portal is assigned to a Reader Control with an offilne reader assigned to it, a message box is displayed alerting the user that the Interval Collection cannot be assigned to the Reader Control.

Note If a Reader Control with an Interval Collection which includes an incompatible interval is assigned an offline reader, a message box is displayed alerting the user that the assignment cannot be made.

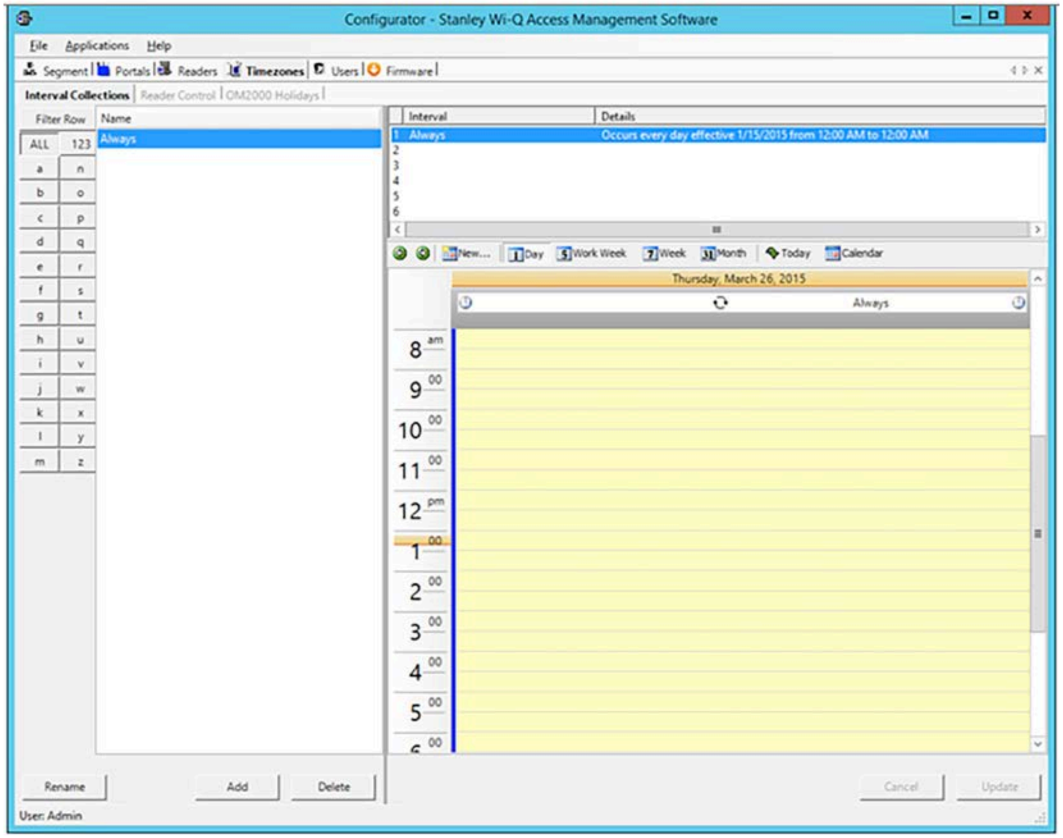
Note If an interval that is assigned to an Interval Collection that is assigned to a Reader Control containing an offline reader is modified so that it is no longer compatible with the virtual portal, a message box is displayed alerting the user that the change cannot be made.

Note Every lock has a Reader Control assigned which has a default mode. Any period of time not covered by an Interval Collection, is set to the default mode just like in Wi-Q.

Creating OM2000 Holidays

1 Click Timezones Tab in Configurator.

Figure 57 Interval Collections Tab



Configurator - Stanley Wi-Q Access Management Software

Name
Always

	Interval	Details
1	Always	Occurs every day effective 1/15/2015 from 12:00 AM to 12:00 AM
2		
3		
4		
5		
6		

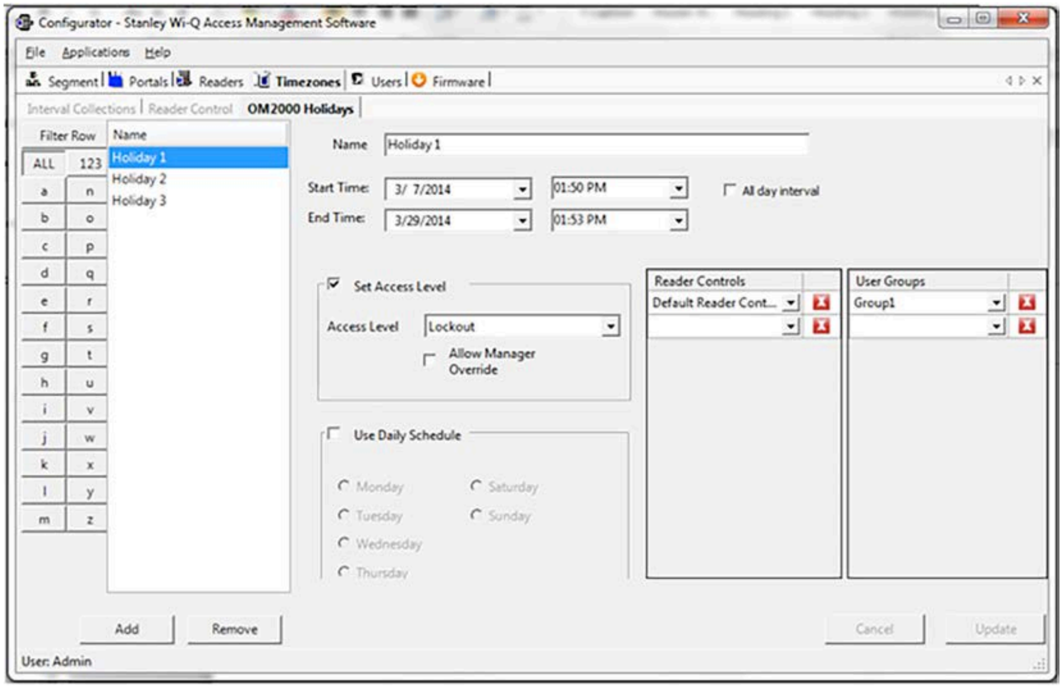
Thursday, March 26, 2015

Always

User: Admin

2 Click OM2000 Holidays sub-tab.

Figure 58 OM2000 Holidays Tab



Configurator - Stanley Wi-Q Access Management Software

Name
Holiday 1
Holiday 2
Holiday 3

Name: Holiday 1

Start Time: 3/ 7/2014 01:50 PM

End Time: 3/29/2014 01:53 PM

□ All day interval

☑ Set Access Level

Access Level: Lockout

□ Allow Manager Override

□ Use Daily Schedule

○ Monday ○ Saturday
○ Tuesday ○ Sunday
○ Wednesday
○ Thursday

Reader Controls
Default Reader Cont...

User Groups
Group1

User: Admin

3 Click "Add".

4 Set “Name” (descriptive name for the Holiday).

5 Set “Start Time” (date and time the holiday is to begin).

6 Set “End Time” (date and time the holiday is to end).

7 A Holiday is a deviation from the configured timezone. After setting the start and end time, you are able to select from one of two Holiday modes , “Set Access Level” or “Use Daily Schedule”.

Set “Access Level” (access level is in effect during the entire holiday period).

a Offline readers included in the selected reader control will follow the new selected access level during the holiday timeframe.

b User groups selected will have access during the holiday timeframe.

c If required check “Allow Manager Override” (manager override setting is in effect during the entire holiday period).

Or when using “Daily schedule” as an option, set “Day of Week”.

a The access level settings for the selected day is used for the duration of the Holiday.

b If a group has access on the selected day, then that group will have access for the duration of the Holiday.

8 Set "Reader Controls" (all readers assigned to the selected reader controls will be subject to the holiday setting).

9 Set "User Groups" (the user groups that are allowed access during the holiday period).

- Every OM2000 controller has a Reader Control assigned which has a default mode. Any period of time not covered by an Interval Collection, is set to the default mode.
- When timezones are translated for OM2000 controllers, a schedule is built for each day of the week and if there are no intervals assigned for a day, then that day is the default mode from 12 am to midnight.
- The offline reader allows a maximum of 255 offline holidays per reader. This limit is enforced at the segment level so the AMS allows a maximum of 255 offline holidays per Segment. If the limit is exceeded, a message box is displayed alerting the user and the offline holiday is not saved.
- The offline reader allows a maximum of 255 schedule events. As described earlier, the conversion of Wi-Q reader controls and user group timezone settings to offline schedule events, is quite complex. Due to this complexity, it does not make sense to duplicate the conversion logic that exists in the Virtual Portal application in the Wi-Q Configurator application. The limit of 255 schedule events per reader is validated in the Virtual Portal application.

Creating OM2000 User Groups

A new tab, entitled OM2000 User Groups, is visible only when a virtual portal exists for the segment.

1 Select the Users Tab in Configurator. Click the User Groups sub-tab.

2 Click Add.

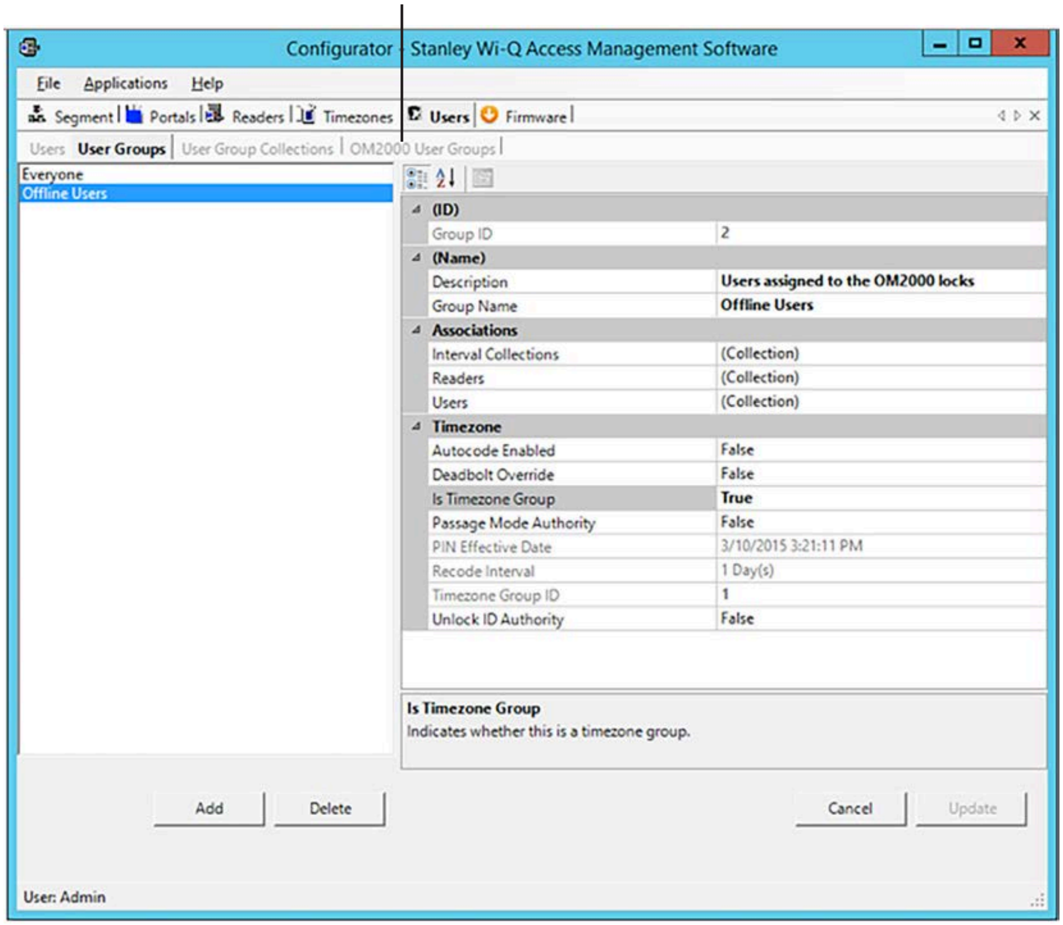
3 Fill in details for new user group.

4 Change Timezone Group to True.

5 Assign Users to group by clicking the ellipsis … button in the users field under Associations. One User MUST be of a Programmer type or downloading to Offline Reader will fail later.

6 Click OM2000 User Group sub-tab.

Figure 59 Configurator



Not shown until virtual portal added

(ID)	
Group ID	2
(Name)	
Description	Users assigned to the OM2000 locks
Group Name	Offline Users
Associations	
Interval Collections	(Collection)
Readers	(Collection)
Users	(Collection)
Timezone	
Autocode Enabled	False
Deadbolt Override	False
Is Timezone Group	True
Passage Mode Authority	False
PIN Effective Date	3/10/2015 3:21:11 PM
Recode Interval	1 Day(s)
Timezone Group ID	1
Unlock ID Authority	False

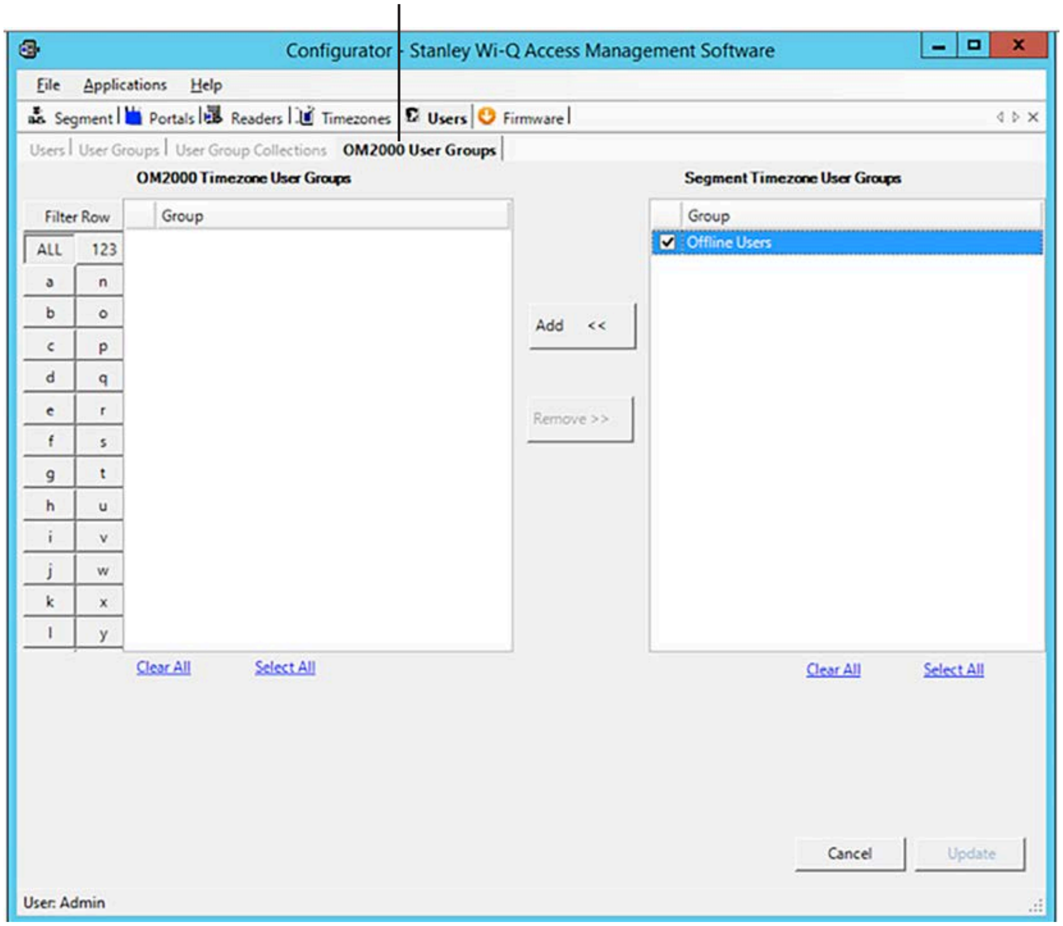
Is Timezone Group
Indicates whether this is a timezone group.

7 Select Segment Timezone User Groups from right pane.

8 Click Add to assign to OM2000 Timezone User Groups.

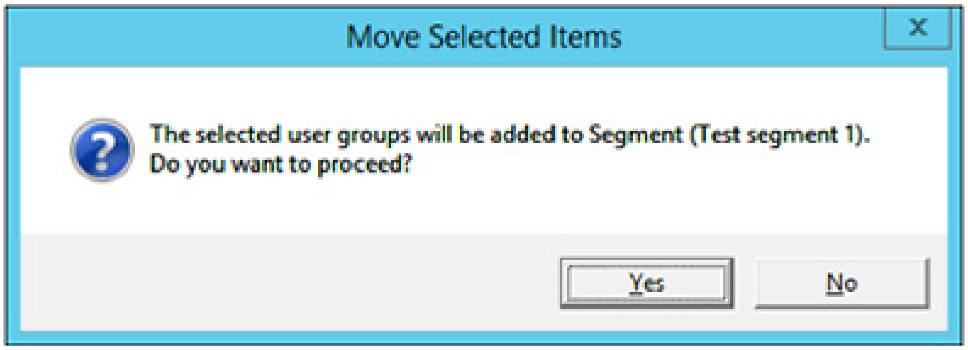
9 Click Update.

Figure 60 Configurator


Not shown until virtual portal added

10 Confirmation window will open. Select Yes.

Figure 61 Confirm


Move Selected Items

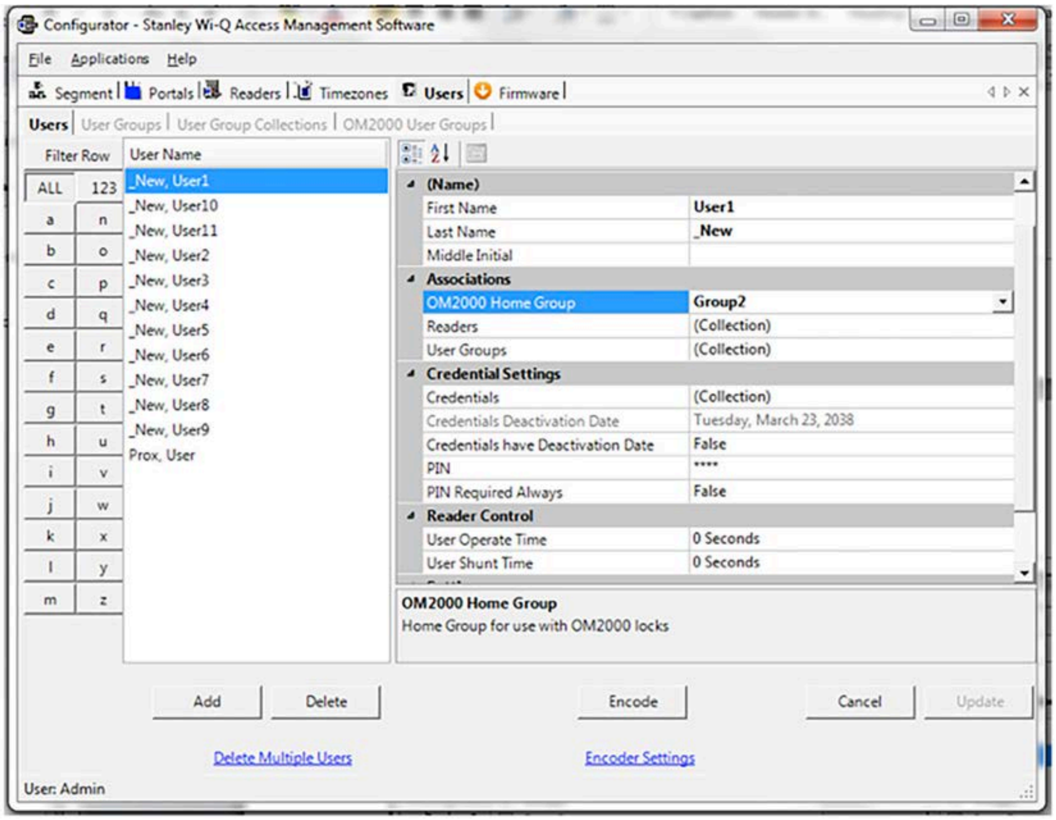
The selected user groups will be added to Segment (Test segment 1).
Do you want to proceed?

An offline reader may have at most eight timezone user groups assigned to it. The only way to assign a user to an Offline reader is through an OM2000 timezone group. Users may not be assigned directly to a reader neither through a direct assignment to the reader nor through a non-timezone user group.

- Only user groups that are designated as timezone user groups are available in the Segment Timezone User Groups listing to be assigned to the offline reader. A timezone user group can be assigned to both online and offline readers. Offline readers require a Home Group to be set for each user. A new user property, entitled OM2000 Home Group, is included in the Associations category of user properties when a virtual portal is present in a segment. The available groups to be assigned as a user's home group are the configured OM2000 User Groups.

11 Assign OM2000 home group to offline reader users.

Figure 62 Users Tab Showing OM2000 Home Group Setting



(Name)	
First Name	User1
Last Name	_New
Middle Initial	
Associations	
OM2000 Home Group	Group2
Readers	(Collection)
User Groups	(Collection)
Credential Settings	
Credentials	(Collection)
Credentials Deactivation Date	Tuesday, March 23, 2038
Credentials have Deactivation Date	False
PIN	****
PIN Required Always	False
Reader Control	
User Operate Time	0 Seconds
User Shunt Time	0 Seconds

OM2000 Home Group
Home Group for use with OM2000 locks

User: Admin

- Offline readers do not allow users to be directly assigned to them. Therefore, when selecting a user's Readers Associations, only wireless readers are available.
- When assigning users to a user group, if a user that does not have a Home Group assigned is assigned to an OM2000 User Group, a message box is displayed indicating that the assignment is not allowed because the user does not have a Home Group assigned and the assignment is not made.

Creating Users

For full User creation details please refer to "Details on Adding Users to the Segment" on page 66.

1 Click the Users Tab.

2 Click Add Button.

3 Edit First Name, Last Name to the User’s name.

4 Click Update Button.

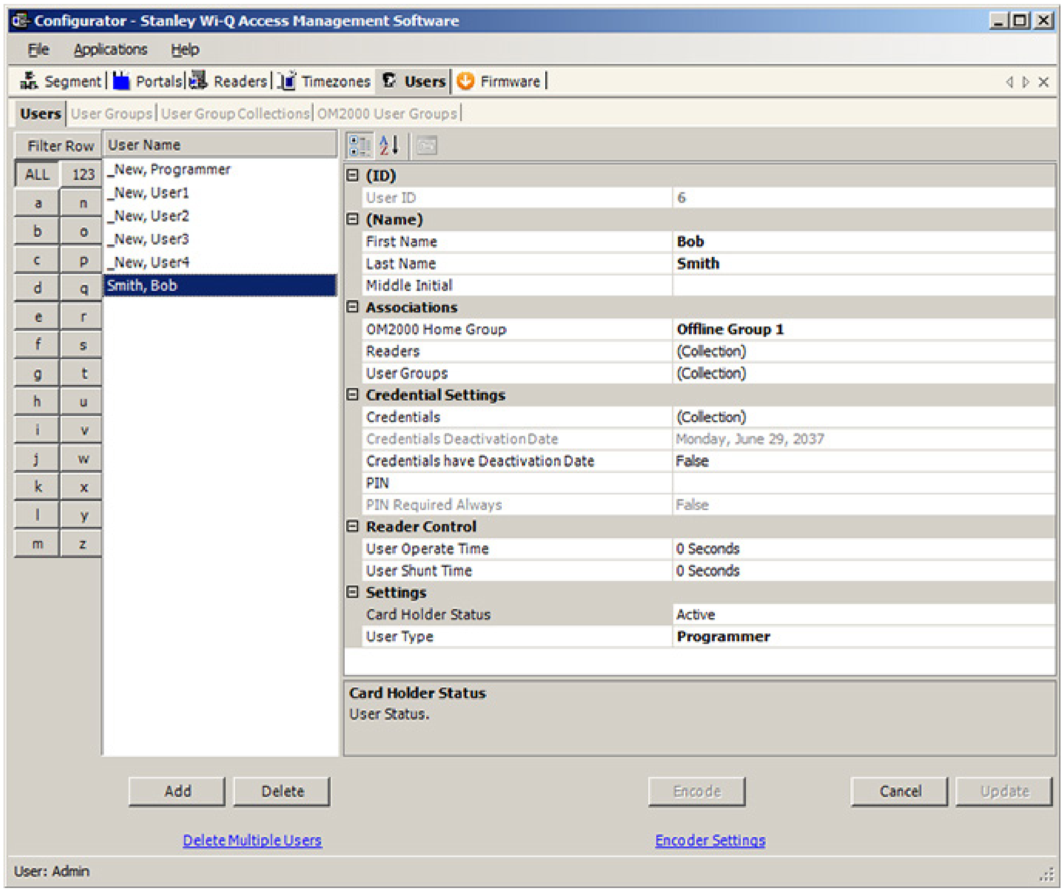
5 Give the User the desired credentials by clicking the ellipsis ... button in Credentials field.

6 Set User Type.

7 Set the OM2000 Home Group from the drop down selection. For OM2000 group set up, see next section.

8 Click Update Button.

Figure 63 Creating Users



_New, Programmer
_New, User1
_New, User2
_New, User3
_New, User4
Smith, Bob

(ID)	
User ID	6
(Name)	
First Name	**Bob**
Last Name	**Smith**
Middle Initial	
Associations	
OM2000 Home Group	**Offline Group 1**
Readers	(Collection)
User Groups	(Collection)
Credential Settings	
Credentials	(Collection)
Credentials Deactivation Date	Monday, June 29, 2037
Credentials have Deactivation Date	False
PIN	
PIN Required Always	False
Reader Control	
User Operate Time	0 Seconds
User Shunt Time	0 Seconds
Settings	
Card Holder Status	Active
User Type	**Programmer**

Card Holder Status
User Status.

Details on 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

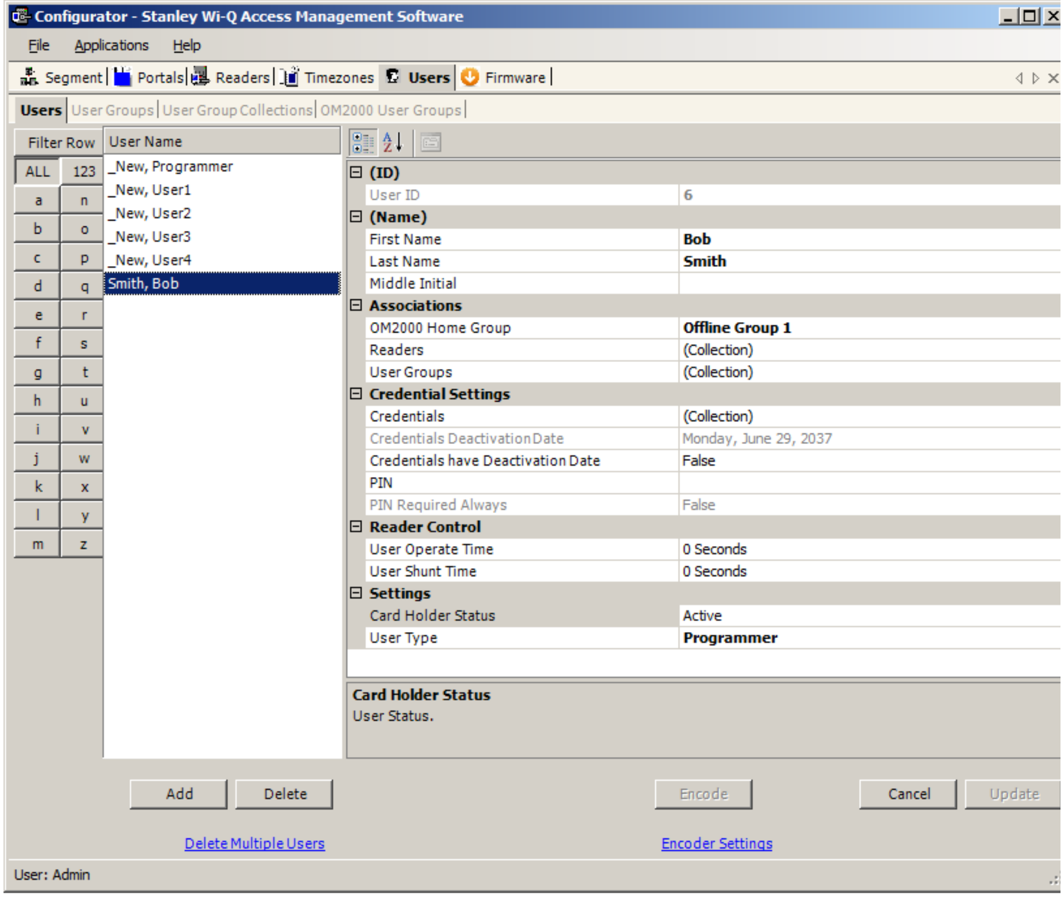
Before you begin adding users to the system for the first time, be prepared to address the following items:

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 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 64 Users Tab



User Name

_New, Programmer
_New, User1
_New, User2
_New, User3
_New, User4
Smith, Bob

(ID)	
User ID	6
(Name)	
First Name	**Bob**
Last Name	**Smith**
Middle Initial	
Associations	
OM2000 Home Group	**Offline Group 1**
Readers	(Collection)
User Groups	(Collection)
Credential Settings	
Credentials	(Collection)
Credentials Deactivation Date	Monday, June 29, 2037
Credentials have Deactivation Date	False
PIN	
PIN Required Always	False
Reader Control	
User Operate Time	0 Seconds
User Shunt Time	0 Seconds
Settings	
Card Holder Status	Active
User Type	**Programmer**

Card Holder Status
User Status.

User: Admin

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

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

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

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

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

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

Adding a User Name

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

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

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

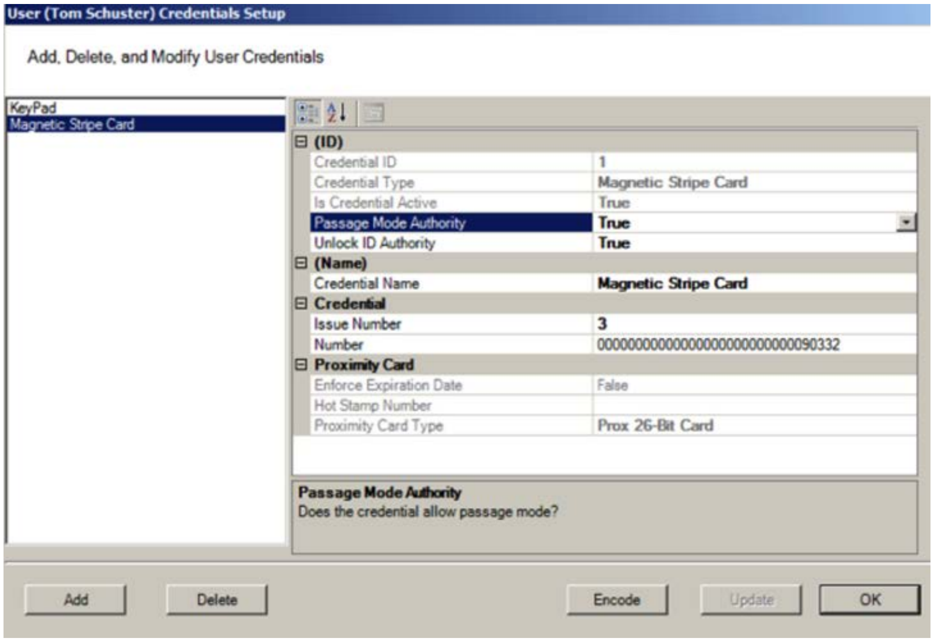
Keypad Type — The default credential type in AMS is Keypad. When you add a user to the system, the software assigns them a unique keypad credential number, then automatically registers it with the system. If your segment uses only keypads, once you add the new user name, you can skip to Adding PINs and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

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

To select the card type

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

Figure 65 Selecting a User Credential type



User (Tom Schuster) Credentials Setup

Add, Delete, and Modify User Credentials

- KeyPad
- Magnetic Stripe Card

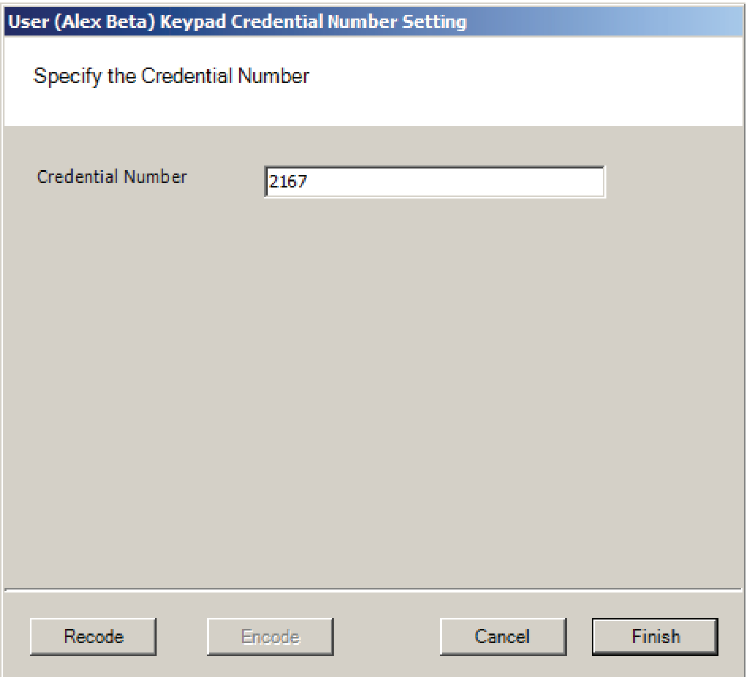
⊟ **(ID)**	
Credential ID	1
Credential Type	Magnetic Stripe Card
Is Credential Active	True
Passage Mode Authority	**True**
Unlock ID Authority	**True**
⊟ **(Name)**	
Credential Name	**Magnetic Stripe Card**
⊟ **Credential**	
Issue Number	**3**
Number	0000000000000000000000000090332
⊟ **Proximity Card**	
Enforce Expiration Date	False
Hot Stamp Number	
Proximity Card Type	Prox 26-Bit Card

Passage Mode Authority
Does the credential allow passage mode?

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.

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

Figure 66 Enter a user credential number



User (Alex Beta) Keypad Credential Number Setting

Specify the Credential Number

Credential Number: 2167

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

5 Now you are ready to register the credential.

Note If the credential type you need is not in the list of card types on the left, you can add one. See "Adding a Credential Type" on page 73.

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

Registering the Credential

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

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

To register a Keypad credential

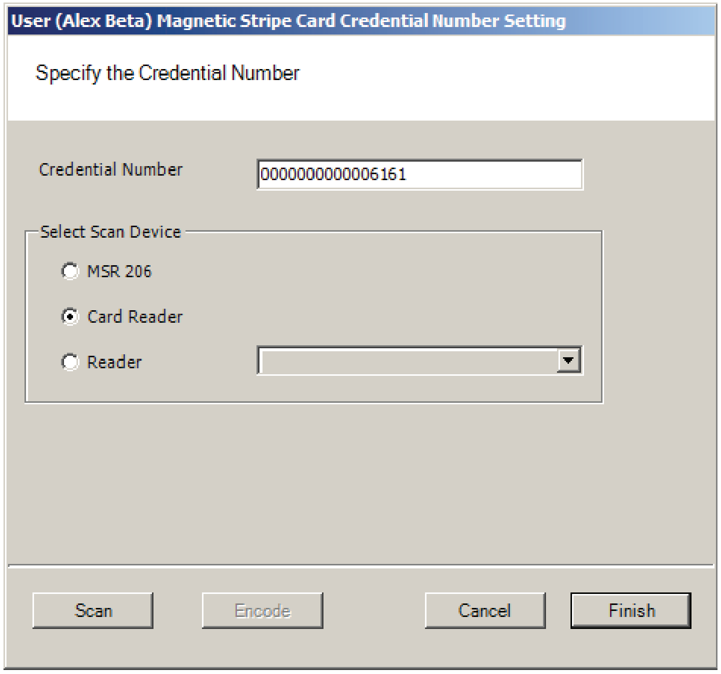
1 Keypad credentials are automatically registered by the system, and no further steps are required.

To register a Magnetic Stripe Card credential

1 From the User Credential Setup dialog box, select Mag Card from the list.

2 Click in the Number field and select the ellipsis ... button. The Users Magnetic Stripe Card Credential Number Setting dialog box opens.

Figure 67 Entering a Magnetic Card credential number



User (Alex Beta) Magnetic Stripe Card Credential Number Setting

Specify the Credential Number

Credential Number: 0000000000006161

Select Scan Device

○ MSR 206

● Card Reader

○ Reader

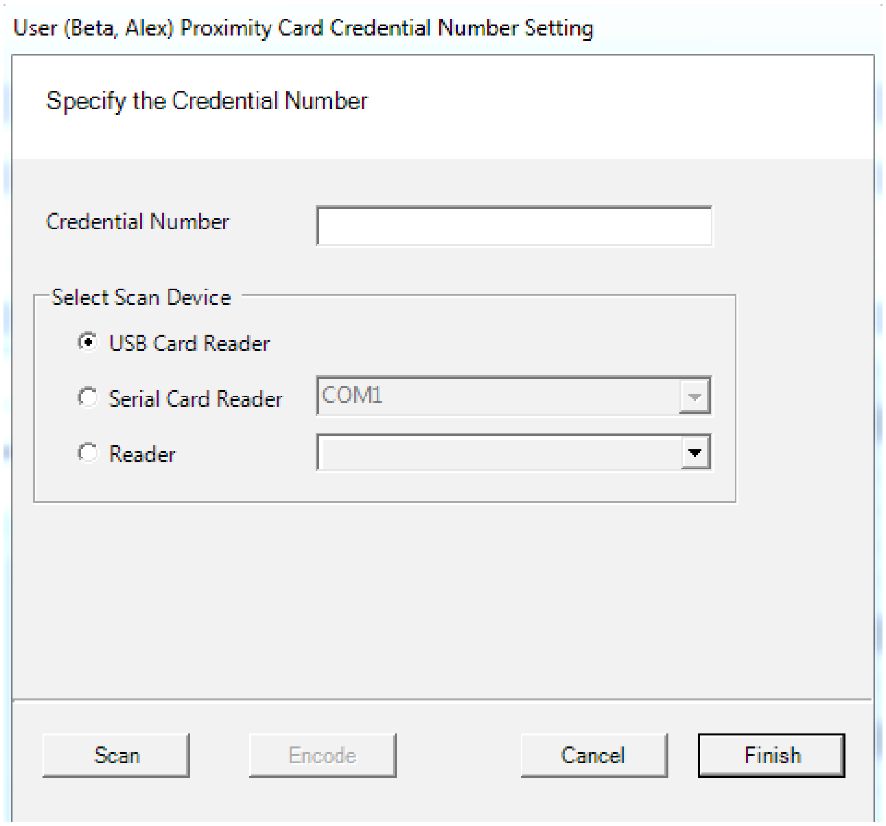
3 Enter a Credential Number manually (must be less than 16 characters, zeros will be appended) or select a scan device.

Using a scanning device to register a credential

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

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

Figure 68 Scan Credentials



User (Beta, Alex) Proximity Card Credential Number Setting

Specify the Credential Number

Credential Number

Select Scan Device

● USB Card Reader

○ Serial Card Reader COM1

○ Reader

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

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

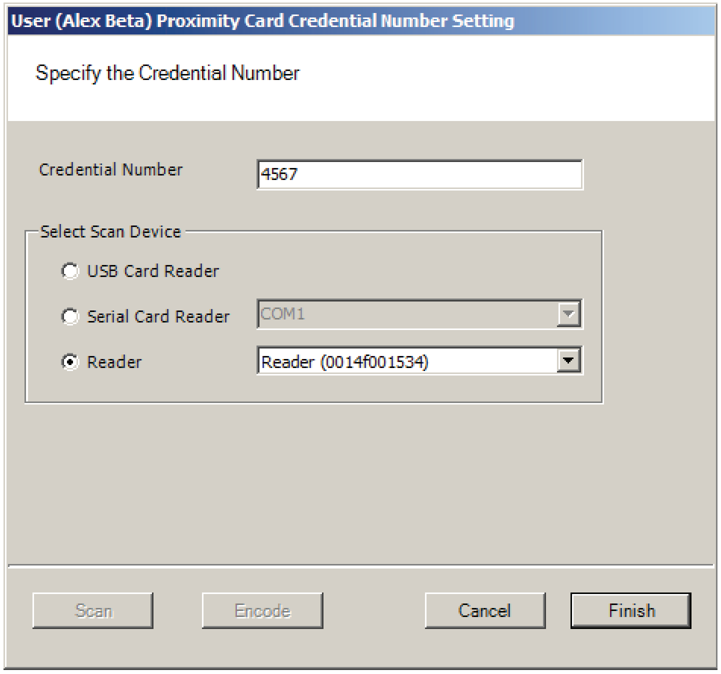
Registering a Prox card credential

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 … button in the Number field, under the Credential category. The User Proximity Card Credential Number Setting dialog box opens.

Figure 69 Entering a Proximity Card credential number



User (Alex Beta) Proximity Card Credential Number Setting

Specify the Credential Number

Credential Number: 4567

Select Scan Device

○ USB Card Reader

○ Serial Card Reader: COM1

● Reader: Reader (0014f001534)

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

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.

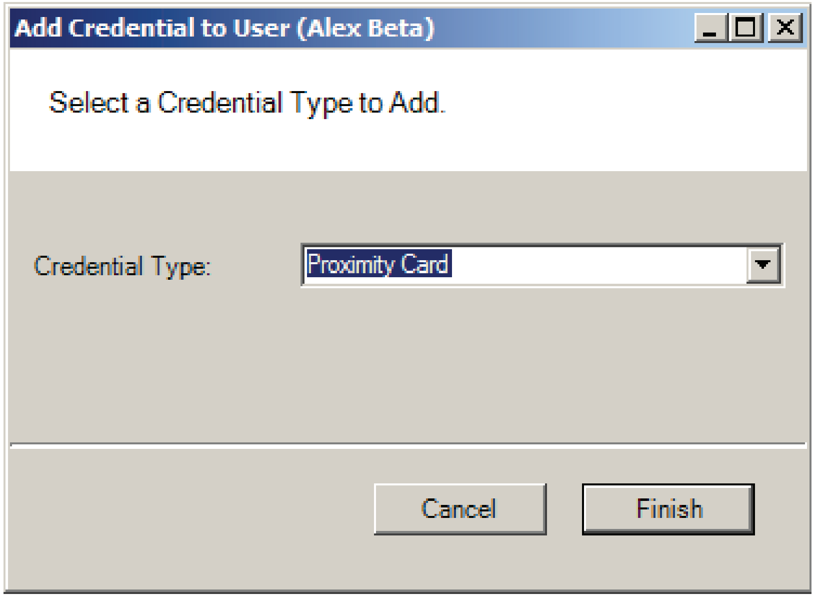
Adding a Credential Type

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 70 Add Credential to User



Add Credential to User (Alex Beta)

Select a Credential Type to Add.

Credential Type: Proximity Card

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

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

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

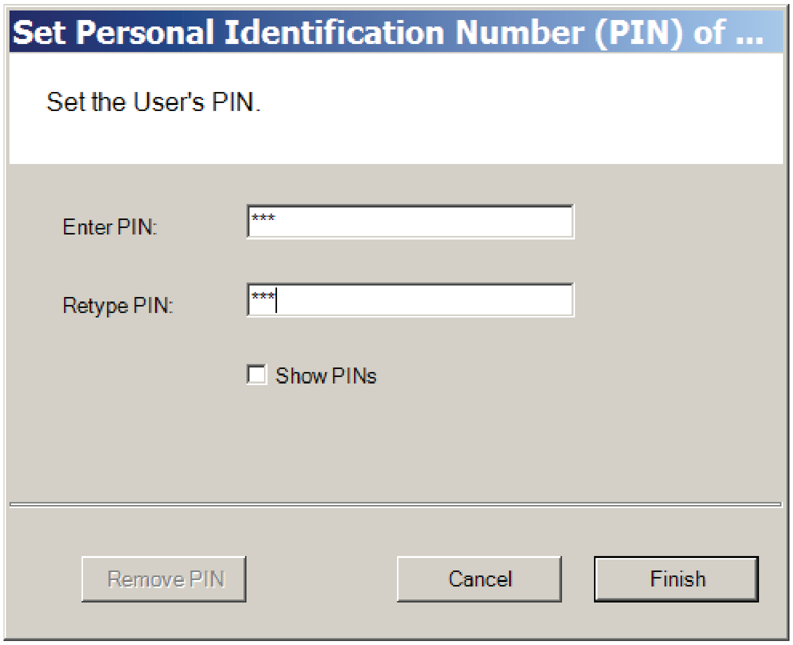
PIN

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

To add a PIN Number for a User

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

Figure 71 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.

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 — In most applications, the vast majority of system users are General Users. The General Users are only allowed entry when the access level is set to Enrolled ID Required or Facility Card. General Users never have access when the reader is in Lockout or Shutdown. There are no privileges or other rights to be granted to General Users. They are the most basic and most common of user types.

Manager — Managers are one of the most useful types of IDs. Managers may be given the unique capability of changing the access level of the lock with a few simple key presses. It should be noted, however, that any changes that a manager makes to the access level can and will be overridden by the time schedule or another manager or programmer. Another benefit of the Manager is that managers are always allowed access to a lock. For those facilities that require an individual to have access at all hours of the day without giving any extra privileges, Mangers can fill that need.

Manager privileges are described below:

1 Supervise Home Group - This allows managers to enable or disable only their home group.

2 Pin required - This is an optional restriction to enable extra security.

3 Passage Mode Toggle - This setting restricts the manager so that the manager can only set the access level to Unlocked or ID Required. All other Access levels are then denied to the Manager.

Programmer — The Programmer ID is the only User type that can program changes into the lock. The Programmer ID is the only ID that will initiate the communication between the programming device and the lockset; therefore, **each lock must have at least one Programmer enrolled.** Programmers can have certain restrictions that must be assigned to them during the enrollment process. This allows the administrator to delegate the tasks of walking through the building to someone else without having to compromise the building security.

Programmers have four different restrictions that can be assigned to them:

1 Entry - This privilege allows the programmer entry through the lock. Without it, the lock will not unlock.

2 Run Diagnostic - This privilege allows the user to run computer diagnostics at the lock. This privilege requires that the Entry privilege also be assigned.

3 Set Access Level - This privilege allows the user to set various access levels at the lock by using the programming device as an interface. This privilege requires Entry and Run Diagnostics privileges also be assigned.

4 PIN Required - This is an optional restriction to enable extra security.

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

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.

Table 1 Manager Override Codes

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.

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.

Notes

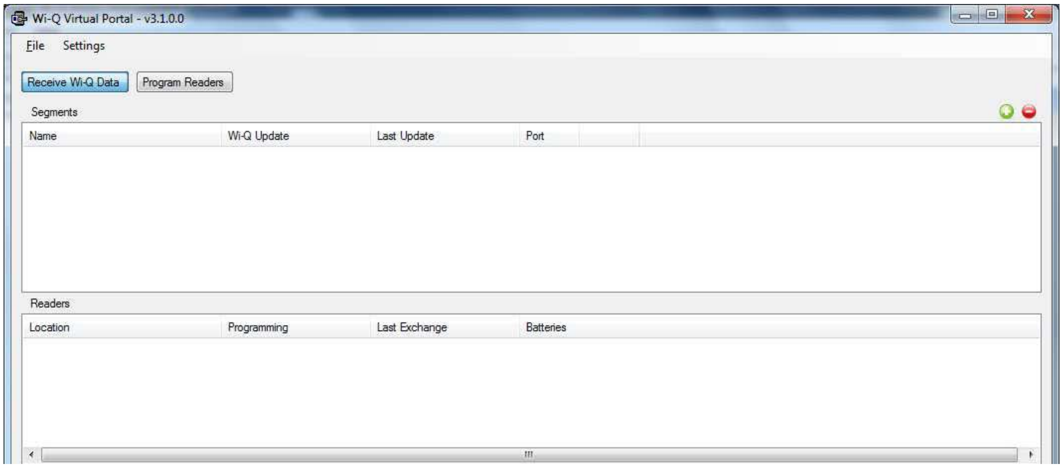
User Interface for Wi-Q Virtual Portal

This section describes the User Interface of the Virtual Portal application and how it is used.

Wi-Q Virtual Portal

Open Wi-Q Virtual Portal application to show the configured Segments/Virtual Portals. When a Segment is selected in the Segments list view, that Segment's directories and Readers are displayed in the lower list view.

Figure 72 Wi-Q Virtual Portal



The Virtual Portal Application is actually a container for any number of Virtual Portals defined in the Wi-Q AMS. Each Segment in Wi-Q is allowed to have at most one Virtual Portal assigned to it so in essence a Segment in the Virtual Portal application is synonymous with a Virtual Portal in the Wi-Q AMS.

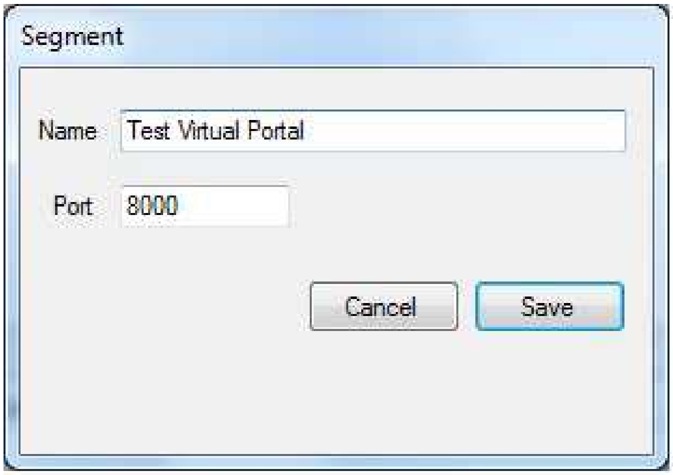
The Virtual Portal application can be in one of two states: Receive Mode or Programming Mode.

In Receive Mode, selected by clicking the “Receive Wi-Q Data” toggle button, the Portal Service for each Segment is open allowing Wi-Q Comm to make a connection to it. Programming locks is not allowed.

In Programming Mode, selected by clicking the Program Readers toggle button, the Portal Service for each Segment is closed. Programming locks is allowed by right-clicking the desired lock and selecting an action from the context menu.

1 Click the green plus (+) icon to the right and above the segments list in the virtual portal window, see "Wi-Q Virtual Portal" on page 79.

Figure 73 Segment



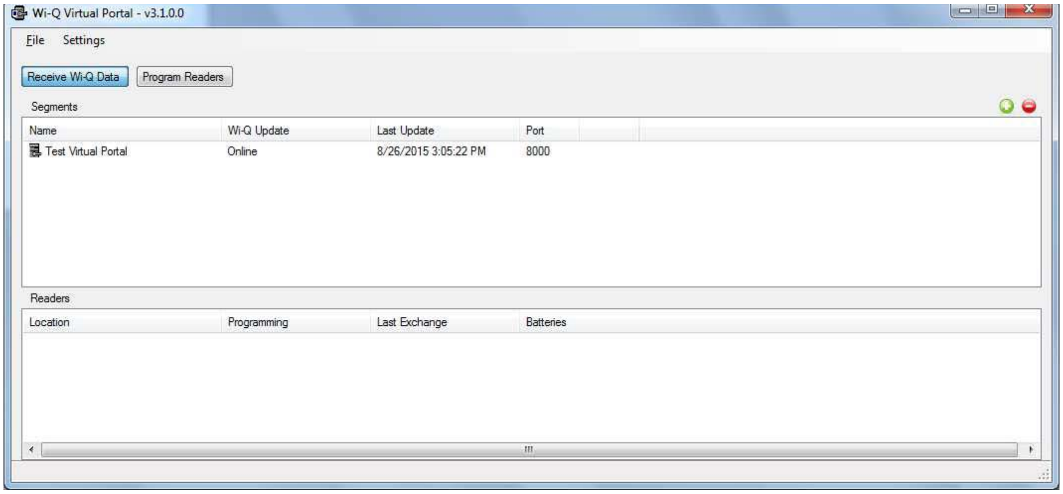
Segment

Name: Test Virtual Portal

Port: 8000

2 Type a name, Click Save.

Figure 74 Virtual Portal



Wi-Q Virtual Portal - v3.1.0.0

Segments

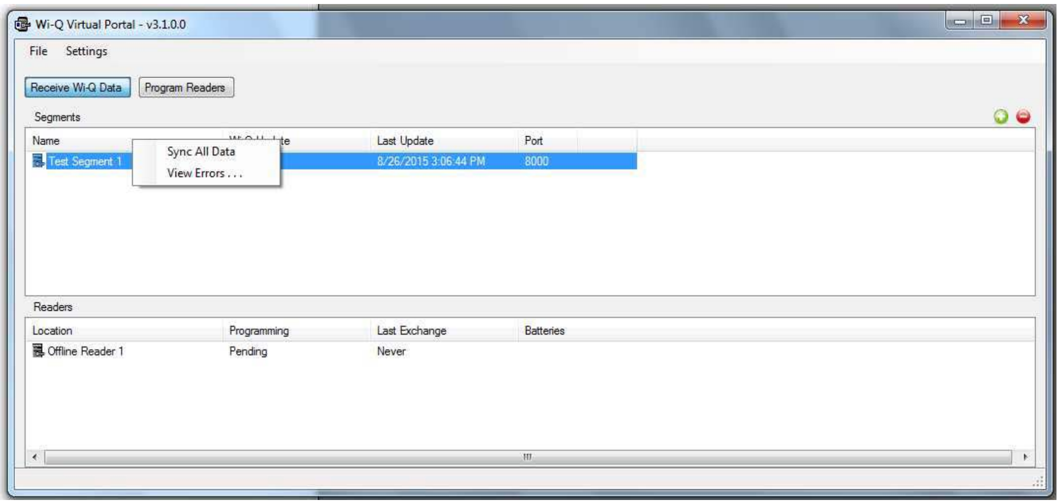
Name	Wi-Q Update	Last Update	Port
Test Virtual Portal	Online	8/26/2015 3:05:22 PM	8000

Readers

Location	Programming	Last Exchange	Batteries

3 Right Click the segment and Click ‘sync all data’ (this pulls all info set up in configurator and the segment assumes the name of the segment set up in configurator).

Figure 75 Sync All Data



Name	Wi-Q Update	Last Update	Port
Test Segment 1		8/26/2015 3:06:44 PM	8000

Location	Programming	Last Exchange	Batteries
Offline Reader 1	Pending	Never	

Segments

The following information is displayed for each Segment:

Wi-Q Update — Indicates if the Portal Service for the Segment is online.

Last Update — The timestamp of the last data or request received from Wi-Q Comm.

Port — The port the Segment’s Portal Service is listening on. This is the port that should be used to configure the Virtual Portal in the Wi-Q AMS.

Error Status — If an error occurs in the Portal Service, this column will show “!Error”.

Right-clicking a segment will display context menu with the following options:

Sync All Data — this option sets the status flags for the portal and all of its controllers to indicate to Wi-Q Comm that they need to be configured. This will cause Wi-Q Comm to do a full data download.

View Errors — this option displays the View Errors form to allow the user to view the list of errors that have occurred in the Portal Service. The errors are not saved to the database and are only available until the application closes.

Segments are added by clicking the green plus (+) icon above the Segments list view.

Clicking the red minus (-) icon will remove the selected Segment. All data for the Segment is removed including Transactions that have not been transferred to Wi-Q.

Readers

The following information is displayed for each Reader:

Programming — The Reader's programming status. Complete means that there is no new data to be sent to the Reader. Pending means that new data has been received for the Reader since the last programming session.

Last Exchange — The timestamp of the last successful programming session with the reader.

Batteries — Status of the Reader's battery as of the last programming session.

Readers are added through Wi-Q AMS and transferred to the Virtual Portal by Wi-Q Comm as explained later in this document.

When in Programming mode, right –clicking a reader will display a context menu with the following options:

Update — sends to the reader changes since the last reader programming session.

Full Download — sends all data to the reader.

Access Levels — allows the user to manually override the access level and groups allowed.

Diagnostics — allows the user to view diagnostic information for the lock including current access level, battery level, drive count and current time.

Settings Menu

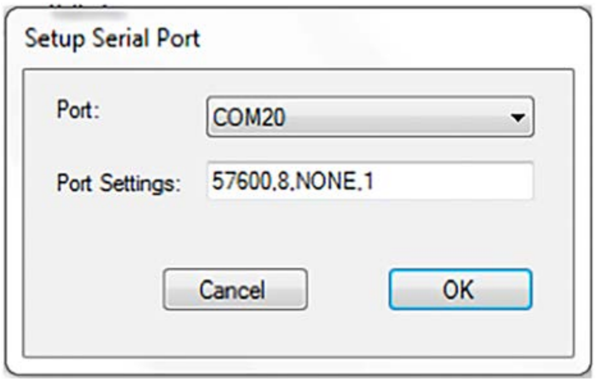
The Settings menu contains one item - "Reader Connection . . ."

Selecting this menu item opens the Serial Port Setup dialog where the COM Port and other serial settings are configured.

Setup Serial Port Dialog

This dialog allows setting up the COM port and port settings for the serial connection to readers. The Port settings field should never change. The COM port should be set to the COM port on the local PC to which the serial cable or IR dongle is connected.

Figure 76 Setup Serial Port Dialog



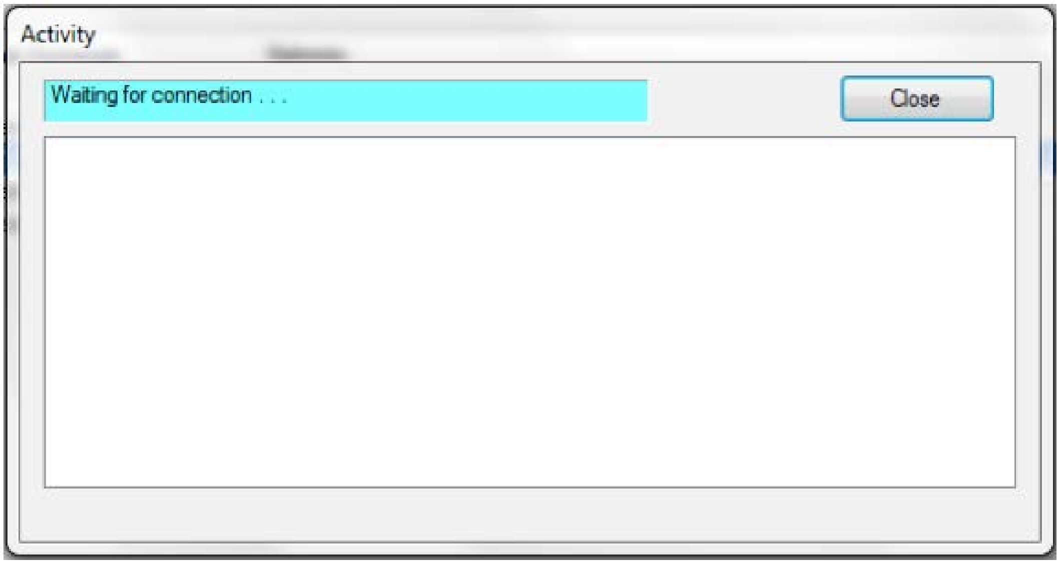
Port: COM20

Port Settings: 57600,8,NONE,1

Programming Activity Dialog

This dialog is displayed when the user selects either Update of Full Download from the Reader context menu.

Figure 77 Programming Activity Dialog



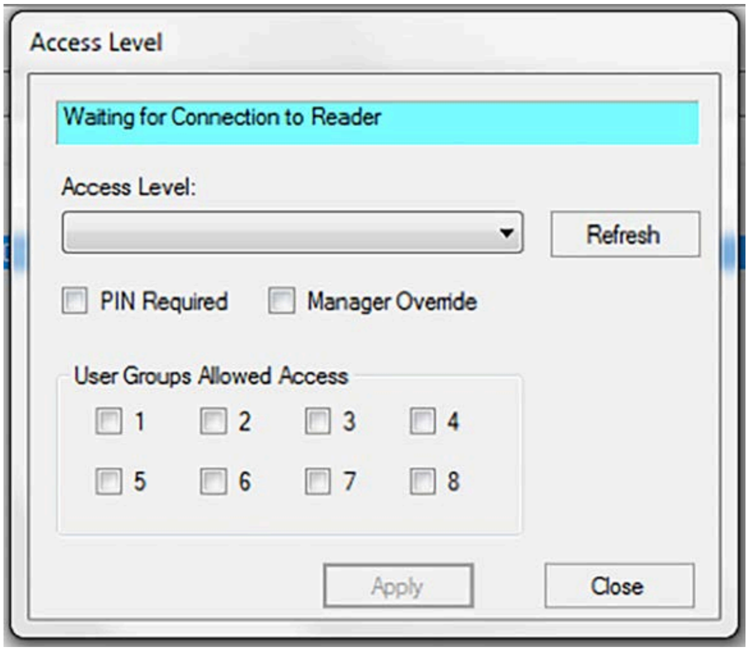
Waiting for connection . . .

Once the connection is established, programing will begin and messages will be displayed indicating the information being sent to the reader.

Access Levels Dialog

This dialog is displayed when the user selects Access Levels from the Reader context menu.

Figure 78 Access Level Dialog



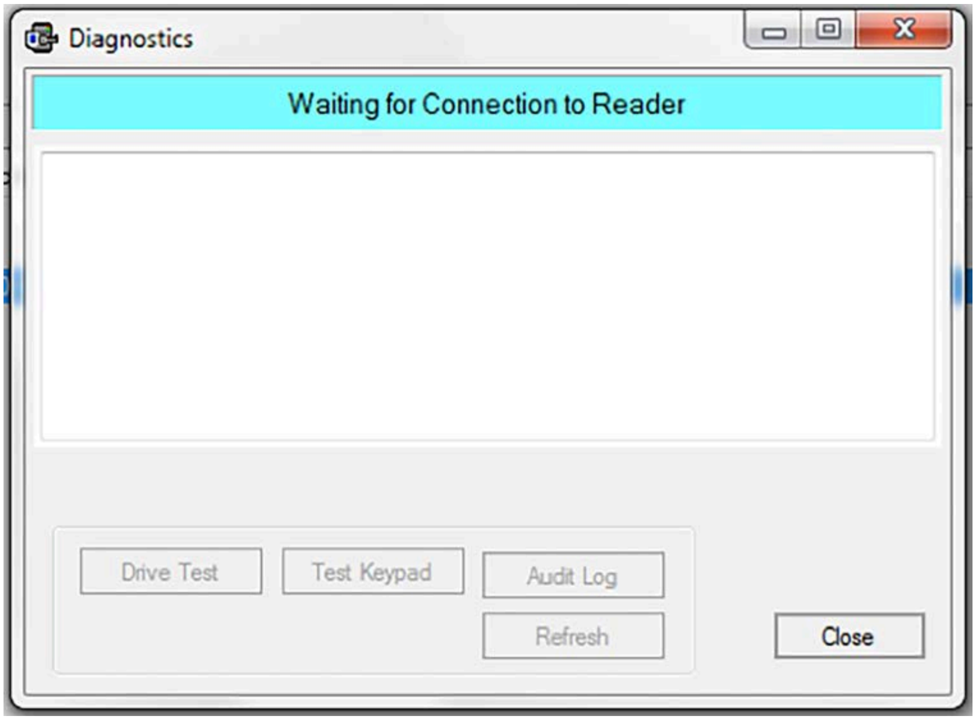
Waiting for Connection to Reader

Once the connection with the reader is established, this form will show the current Access Level, PIN Required setting, Manager Override setting and the Groups that are currently allowed access. Changing any of these settings and then clicking the Apply button will send the new settings to the Reader which will override the current reader Access Level settings.

Diagnostics Dialog

This dialog is displayed when the user selects Diagnostics from the Reader context menu.

Figure 79 Diagnostics



Waiting for Connection to Reader

- Once reader connection is established, diagnostic information will be displayed for the reader. The diagnostic information includes the current access level information (including PIN Required and Manager Override), the battery level, firmware version, battery level and current time.
- Clicking the Drive Test button will perform a drive test sequence for the reader.
- Clicking the Test Keypad button will allow the user to click keypad buttons on the reader to test that they are functioning properly.
- Clicking the Audit Log button will download the audit log from the reader.
- Clicking the Refresh button will pull diagnostic for the reader and update the display with the new information received.
- Clicking the Close button will send a log off message to the lock and close the dialog.
- Once a Schedule Event starts, it is in effect until another Schedule Event starts. This is in contrast to Wi-Q where a start and end time are set for an Interval and when the Interval ends, the default Access Level goes into effect.
- The equivalent of an OFM Schedule in Wi-Q is the Reader Control.
- The equivalent of an OFM Schedule Event in Wi-Q is a combination of Intervals, Interval Collections and Controller Interval Collection Assignments.

To translate a Wi-Q Reader Control to an Omni Lock Schedule, requires the following steps for each Interval assigned to the controller:

1 Create a Schedule Event for the start of the interval with the Access Level from the Interval Collection / Controller assignment.

2 Create a Schedule Event for the end of the interval with the Access Level set to the Default Access Level for the Reader Control assigned to the Controller.

Group Access schedules in the Omni Lock are set up for each of the allowed eight Timezone User Groups for each day of the week. Each Group Schedule Event is made up of the following fields: Start Time and an Allow/Deny Access flag.

Once a Group Schedule Event starts, it is in effect until another Group Schedule Event Starts.

The equivalent of a Group Schedule Event is the combination of Intervals, Interval Collections and User Group Interval Collection Assignments.

To translate a Wi-Q User Group Assignment to an Omni Lock Group Schedule, requires the following steps for each Interval assigned to the User Group:

1 Create a Group Schedule Event starting at the Interval start time and with group access allowed for the timezone user group.

2 Create a Group Schedule Event starting at the Interval end time and with group access disallowed for the timezone user group.

There are two complicating factors to this translation – intervals that overlap and the fact that the OFM Schedules and OFM Group Schedules are both sent to the lock using the same programming block (PGMWriteSchedule).