

Update Portal Firmware

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

- 1 Navigate to the Gateway menu option in the WQXM-PG webpage.
- 2 Click on the Update button towards the bottom of the Gateway page.

Figure 57 Gateway Configuration Page

The screenshot shows the 'Gateway' configuration page with a red header bar containing navigation icons for STATUS, GATEWAY, INTERFACE, and LOGOUT. The 'GATEWAY' tab is selected. The page title is 'Gateway'. Below the title is a 'CONFIGURATION' section with various settings:

- MAC ADDRESS: 0014F5208C06
- DHCP: ☐
- IPv4 Address: 10.189.17.16
- IPv4 Address(Link Local): fe80::0:0:0:0::214::PSK::fe20::8c06
- IPv4 Address(Global): 0:0:0:0:0:0:0:0
- Subnet Mask: 255.255.255.0
- Gateway: 10.189.17.1
- Portal Service Port: 8000
- WiFi SSID:
- WiFi IP Address: 192.168.3.200
- WiFi Password: password
- WiFi Security: WPA2-PSK [AES]
- Enable SSL: ☐ GET CERTIFICATE
- Portal Firmware Version: 4.0.2.0 UPDATE ☒

At the bottom, there are buttons for SAVE, CANCEL, and REBOOT GATEWAY.

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

Figure 58 Gateway Configuration Page

The screenshot shows a pop-up window titled 'Select the update file to be applied'. It contains three buttons: 'Browse' (highlighted with a red box), 'APPLY' (disabled), and 'CANCEL' (highlighted with a red box).

- 4 Browse to the previously extracted .gzhe portal firmware file and click the Open button to upload the file.
- 5 The selected file will be listed in the pop-up window. Verify it is correct and click the Apply button.
- 6 The firmware will be applied to the Gateway. The Gateway's LED will flash aqua when it downloads the firmware.

Reboot Gateway

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

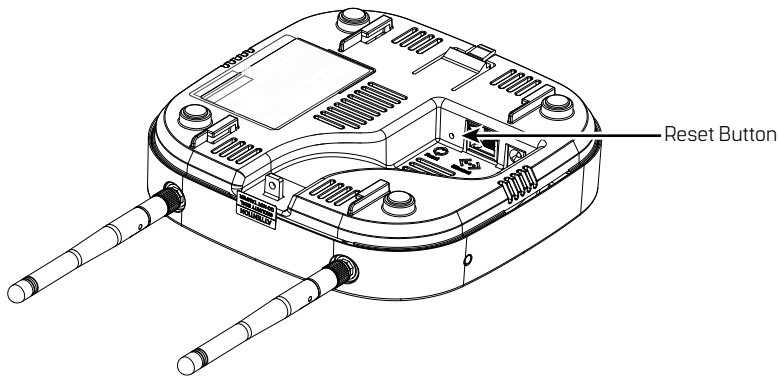
- 1 Navigate to the Gateway menu option of the Gateway.
- 2 Scroll to the bottom of the screen.
- 3 Click the Reboot Gateway button.
- 4 A pop-up window will appear asking if you are sure you want to reboot the Gateway. Any changes made and that have not been saved will be lost. Click the Reset button to continue.
- 5 The Gateway will reboot immediately. During a reboot, the Gateway will flash purple. Once it reconnects to the ACS, the LED will display a solid green light.

Factory Reset the Gateway

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

- 1 Remove Gateway from enclosure or from the mounted location.
- 2 On the back of the Gateway locate the Deep Reset button next to the Ethernet inlet. The Deep Reset button is a recessed button accessible from a pin hole. [See Figure 60.](#)
- 3 Push and hold the Deep Reset button using a small implement such as a paper clip for more than 10 seconds.

Figure 59 Wi-Fi Reset Button



Interface Menu

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

Adding Wi-Q Gateways to AMS

Portals can be added to your system in two ways:

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

Adding Wi-Q Gateways One at a Time

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

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

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

Figure 60 Configure New Wi-Q Gateway screen

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

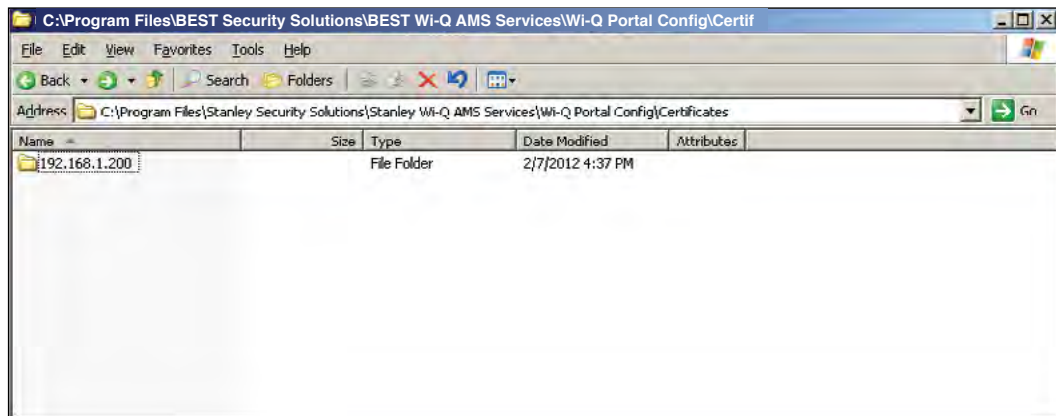
- 7 Click the ellipsis button next to the Channels field and select at least two channels that the Wi-Q Gateway will use to communicate. Check with your network administrator to make sure the channels are available. Click the ellipsis button next to the Update Interval field. Here you can set how often the system will update the Wi-Q Gateway with changes you've made to users, readers, timezones, and other functional changes to the database.
- 8 Click the ellipsis button next to the Transactions field to select which, if any, Wi-Q Gateway transactions you want to enable and which you want to make a priority. Priority transactions will be uploaded immediately rather than waiting for the next update interval that was set in the field above. Two transactions are available:

- Portal Firmware Update
- Portal Radio Start Failed

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

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

Figure 61 Path to Certificate File



10 Click Finish.

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

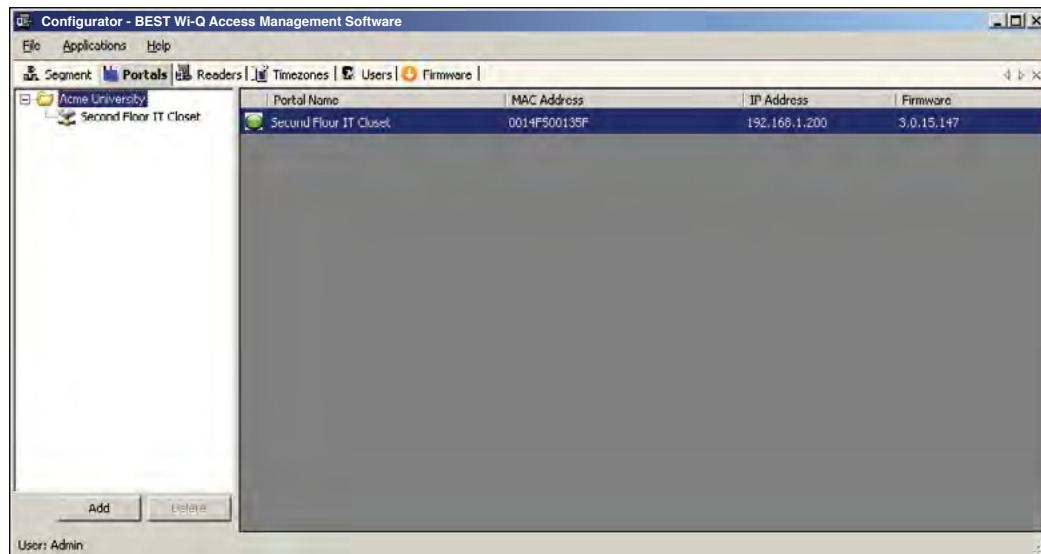
Wi-Q Gateway Operational Status

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

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

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

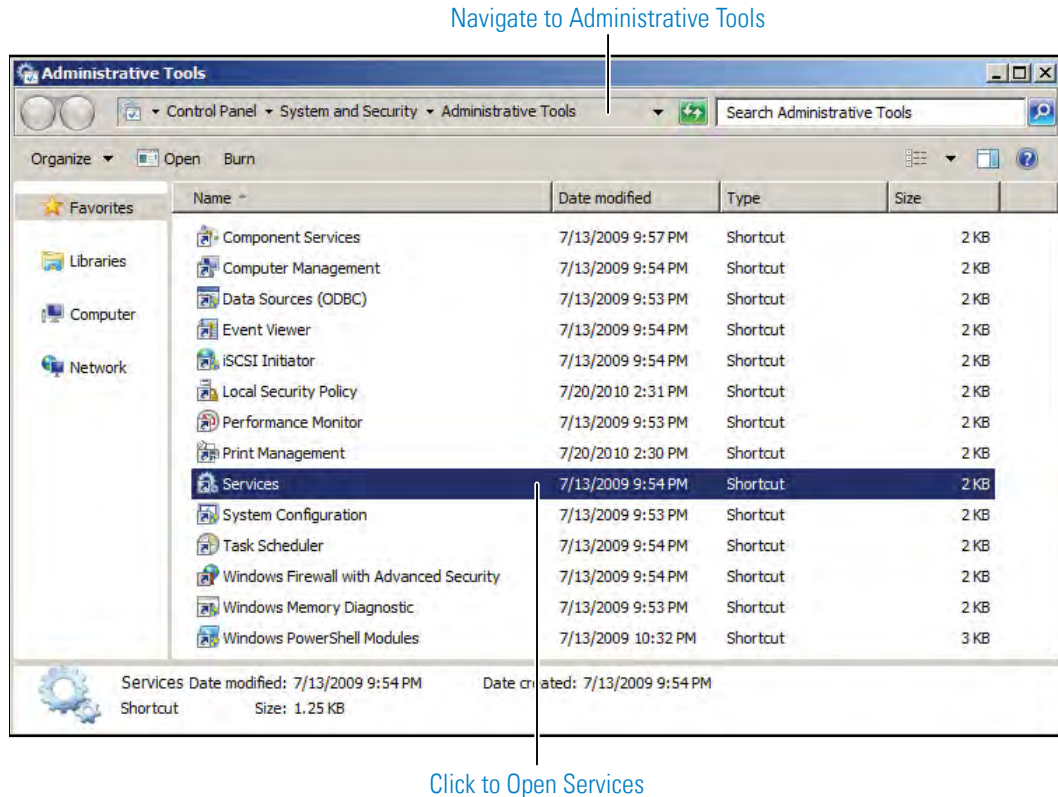
Figure 62 Wi-Q Gateway with Green Circle Icon



Restarting your Communication Server

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

Figure 63 Navigate to Services



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

Importing Wi-Q Gateways in Bulk

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

Generating an XML Bulk Import File

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

- 1 Select all the Portals you wish to add to your AMS software using Select All button.
- 2 Click on Export Portal IP Configurations ([See Figure 47](#)).
- 3 Choose a location to save your XML file, and click Save. [Figure 64](#) shows a sample XML file.

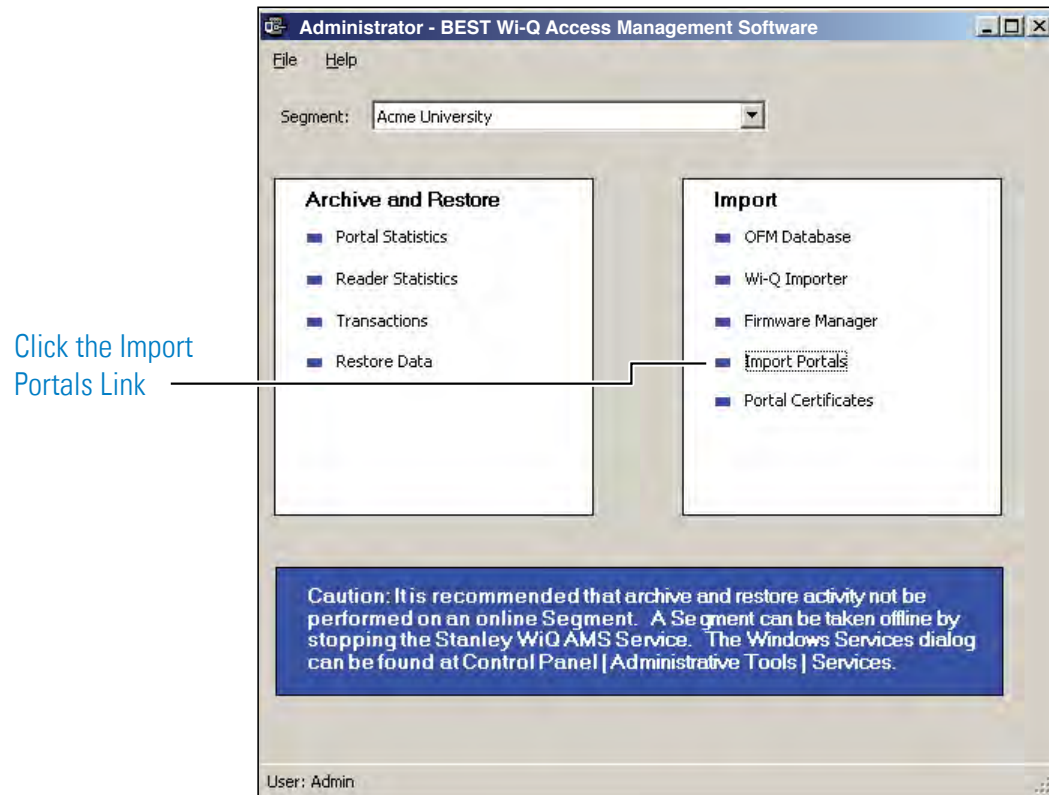
Figure 64 Sample XML file

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

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

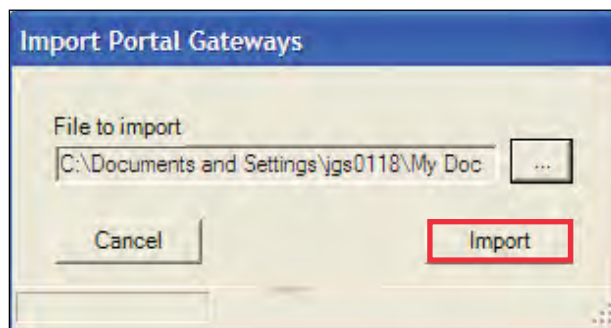
- 1 Start the System Administrator module (Applications dropdown menu inside Configurator).
- 2 Click the Import Portals link from the Import pane. [See Figure 65](#).

Figure 65 System Administrator Wi-Q Gateway Import



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

Figure 66 Import Wi-Q Gateways



- 6 Click Import.

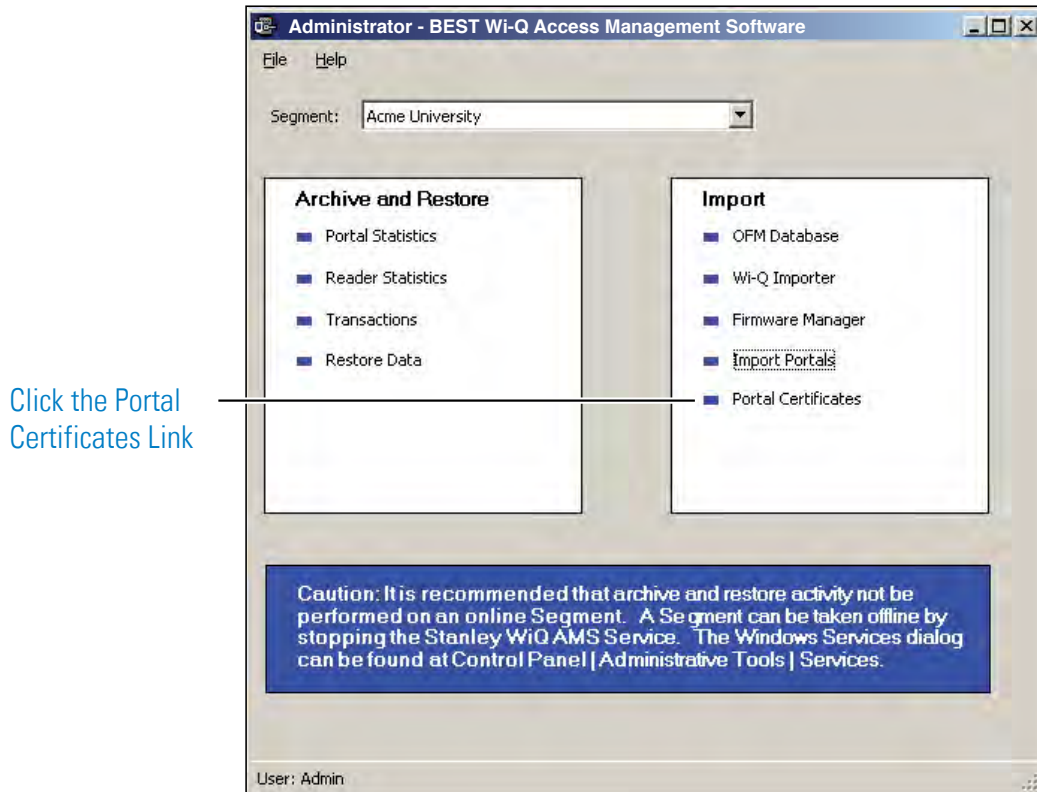
Note The Portals are imported (or updated) and a results box details the import. Workstation needs to be allocated and the MAC addresses should automatically show up in Wi-Q Gateways' properties.

Importing Portal SSL Certificates

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

- 1 From the System Administrator application, click the Portal Certificates link under the Import pane. [See Figure 67.](#)

Figure 67 System Administrator Portal Certificates link



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

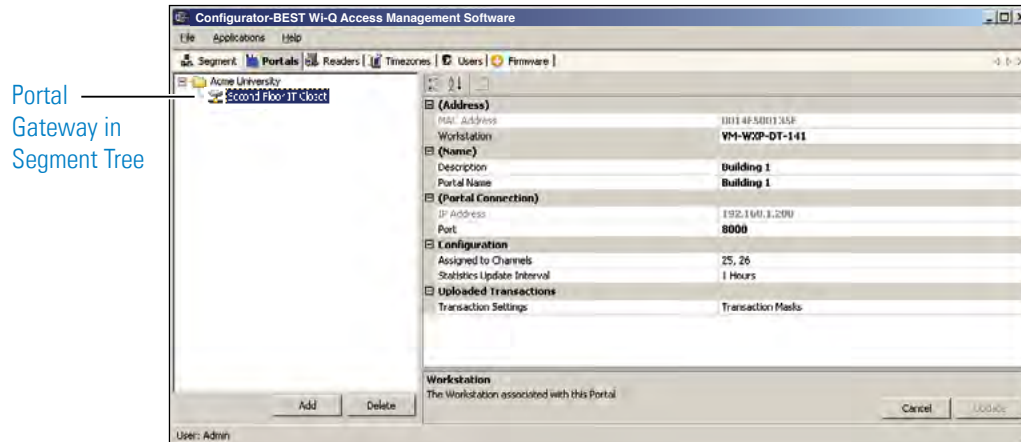
The Portals you have added will now be visible in the Segment Tree. See "Viewing the Segment Tree". You may now check the operational status of your Wi-Q Gateways. See "The Portal(s) you have added will now be visible in the Segment Tree. See "Viewing the Segment Tree" on . You can check the operational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

Viewing the Segment Tree

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

[Figure 68](#) shows an example Wi-Q Gateway in the Segment Tree.

Figure 68 Wi-Q Gateway visible in Segment Tree



To view the Segment Tree

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

The Segment Tree is also viewable from within the Readers tab. [See “Adding Controllers to the Segment Tree”.](#)

Organizing your Segment Tree

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

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

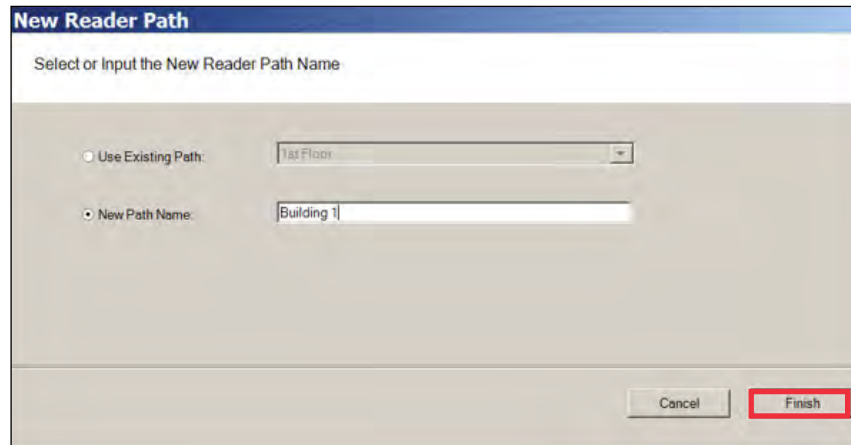
Note To delete a folder, you must already have moved any devices in that folder to a different location.

To create a new segment item folder

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

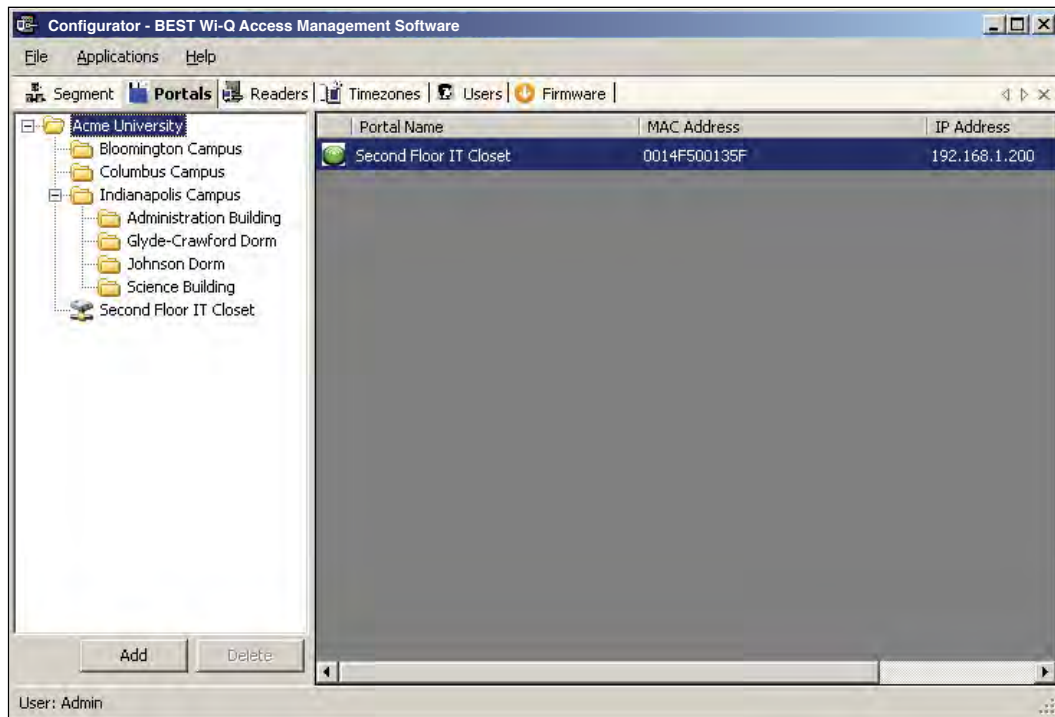
Figure 69 Defining a New Reader Path

Select New Path Name and enter a name

The image shows a dialog box titled "New Reader Path". Inside the dialog, there is a label "Select or Input the New Reader Path Name". Below this, there are two options: "Use Existing Path:" with a dropdown menu showing "1st Floor", and "New Path Name:" with a text input field containing "Building 1". At the bottom right of the dialog, there are two buttons: "Cancel" and "Finish". The "Finish" button is highlighted with a red border.

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

Figure 70 Folders and Sub-Folders in the Segment Tree



Moving Wi-Q Gateways within the Segment Tree

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

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

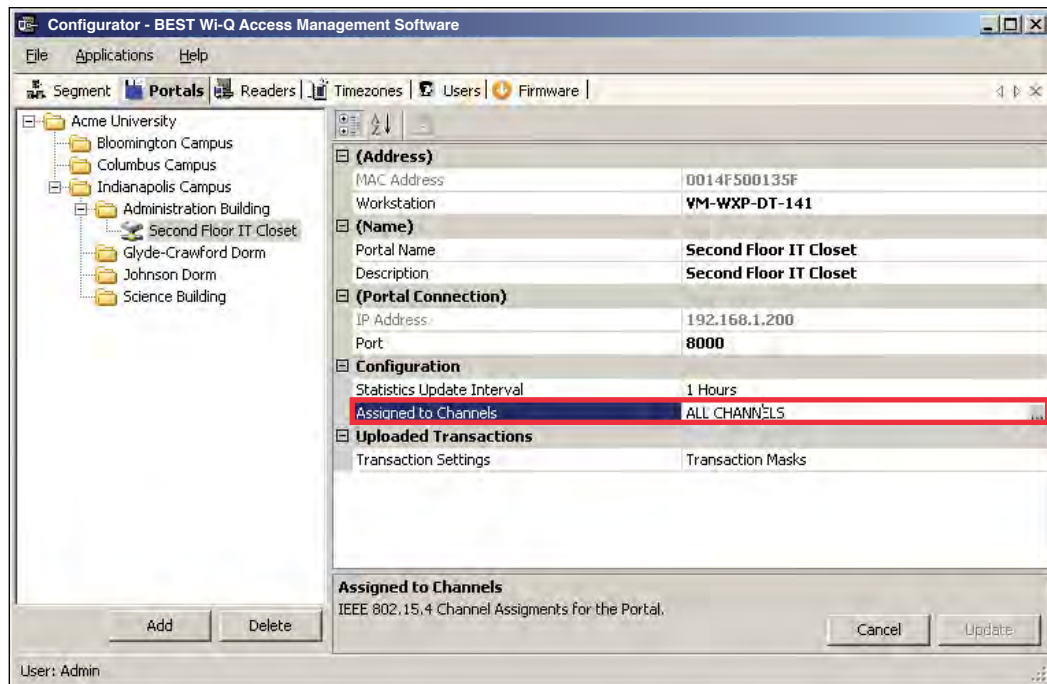
Assign Portal Channels

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

To assign Portal channels

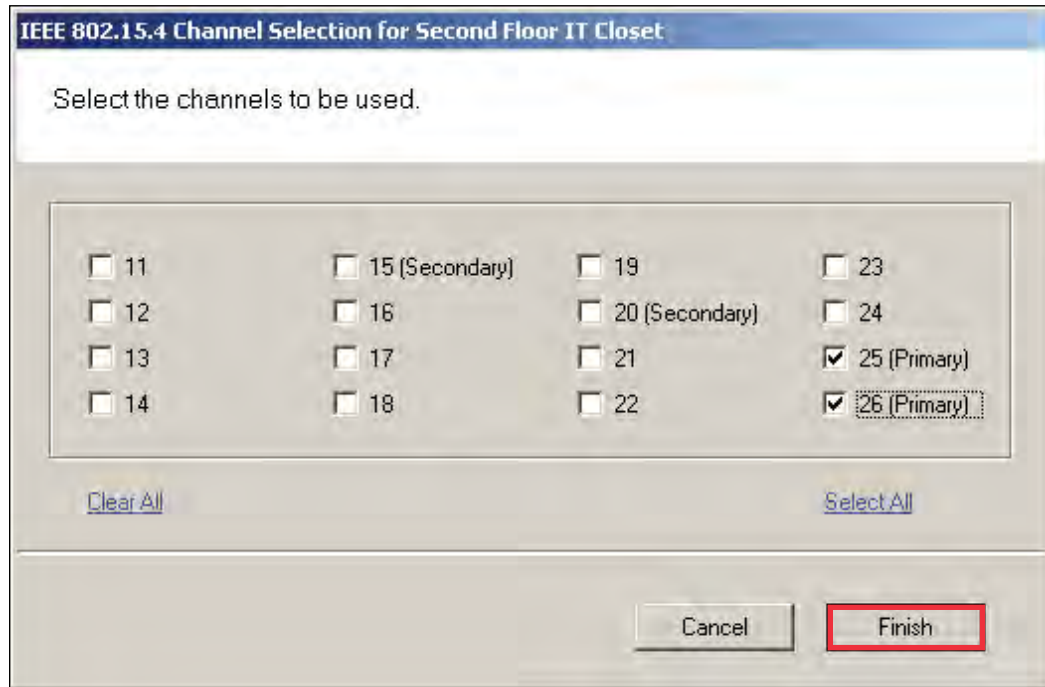
- 1 Click on the Portal tab, and select the desired Portal from the Segment Tree. Clicking on a Portal will display Portal properties on the left.

Figure 71 Portal Properties



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

Figure 72 Portal Channel Selection



The dialog box is titled "IEEE 802.15.4 Channel Selection for Second Floor IT Closet". It contains a text label "Select the channels to be used." followed by a grid of 16 checkboxes arranged in four columns and four rows. The first three columns have checkboxes for channels 11, 12, 13, 14, 15 (Secondary), 16, 17, 18, 19, 20 (Secondary), 21, and 22. The fourth column has checkboxes for channels 23, 24, 25 (Primary), and 26 (Primary). The checkboxes for 25 and 26 are checked. Below the grid are two links: "Clear All" and "Select All". At the bottom right are two buttons: "Cancel" and "Finish". The "Finish" button is highlighted with a red border.

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

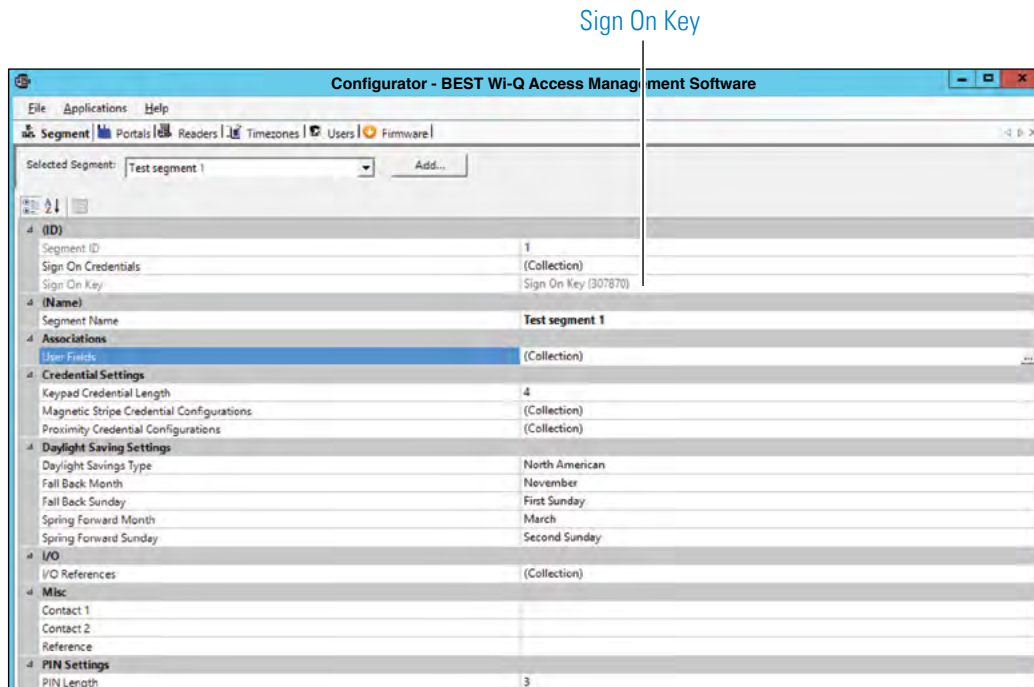
- 3 Enable or disable channels as needed (at least one channel must be selected).
- 4 Click Finish to save your settings.

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

Sign on and Configure Controllers (Task 10)

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

Figure 73 Signing on readers from the Segment tab



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

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

Signing on Keypad Controllers

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

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

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

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

Signing on Card Readers

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

- 1 In the Configurator's Segment tab, select the segment to which the readers belong.
- 2 In the ID Category, click in the Sign On Credentials field and select the ellipsis button at the far right of the field. The Segment Credentials Setup property sheet opens.

The screenshot shows the "Segment (Acme University) Credentials Setup" window. The title bar reads "Segment (Acme University) Credentials Setup". Below the title bar is a subtitle "Add, Delete, and Modify Segment Credentials". On the left is a tree view with "Proximity Card" selected. The main area displays details for the selected credential:

- (ID)**: Credential ID is 2; Credential Type is Proximity Card.
- (Name)**: Credential Name is Proximity Card.
- Credential**: Issue Number is 0; Number is 00000000000000000000003456.
- Proximity Card**: Enforce Expiration Date is False; Hot Stamp Number is blank; Proximity Card Type is Prox 26-Bit Card.

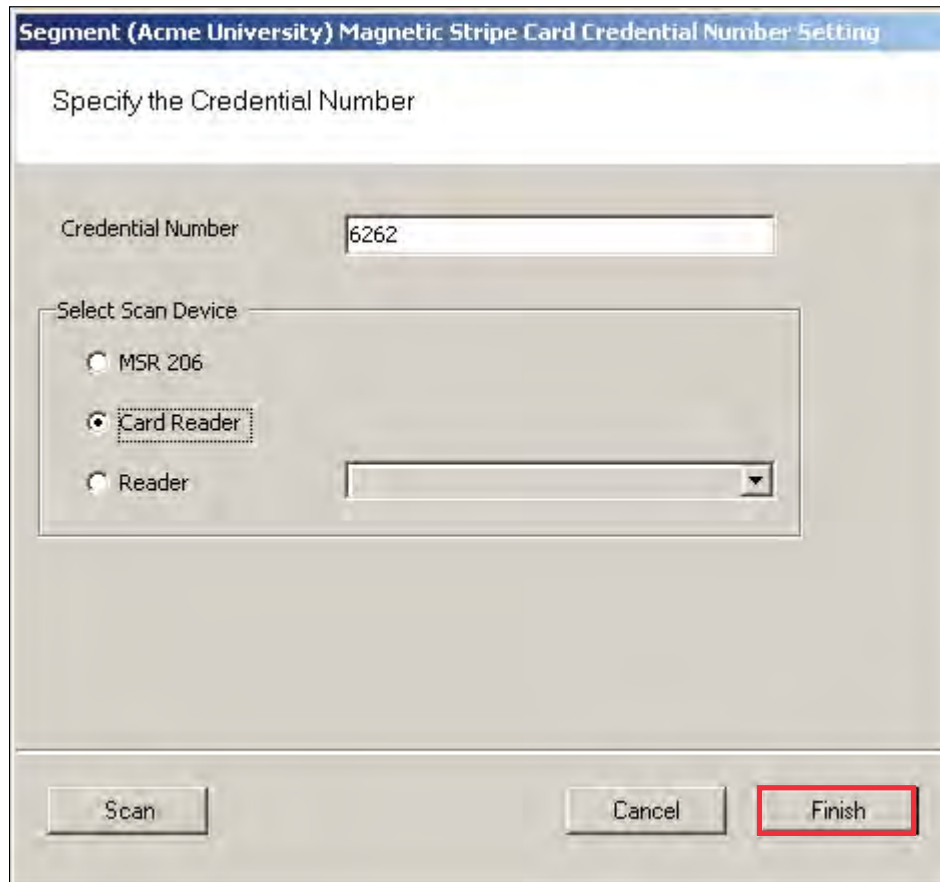
Below the details is a section titled "Credential ID" with the text "The User Credential's ID Number." At the bottom are four buttons: "Add" (highlighted with a red rectangle), "Delete", "Update", and "OK".

- Figure 75 Add Credential to Segment



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

Figure 76 MAG Card Settings



The dialog box is titled "Segment (Acme University) Magnetic Stripe Card Credential Number Setting". It contains a section titled "Specify the Credential Number" with a text input field labeled "Credential Number" containing the value "6262". Below this is a section titled "Select Scan Device" with three radio button options: "MSR 206", "Card Reader" (which is selected and highlighted with a dashed border), and "Reader". To the right of the "Reader" option is a drop-down menu. At the bottom of the dialog are three buttons: "Scan", "Cancel", and "Finish". The "Finish" button is highlighted with a red rectangular border.

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

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

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

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

Completing the Credential for a Prox card

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

To sign on card readers

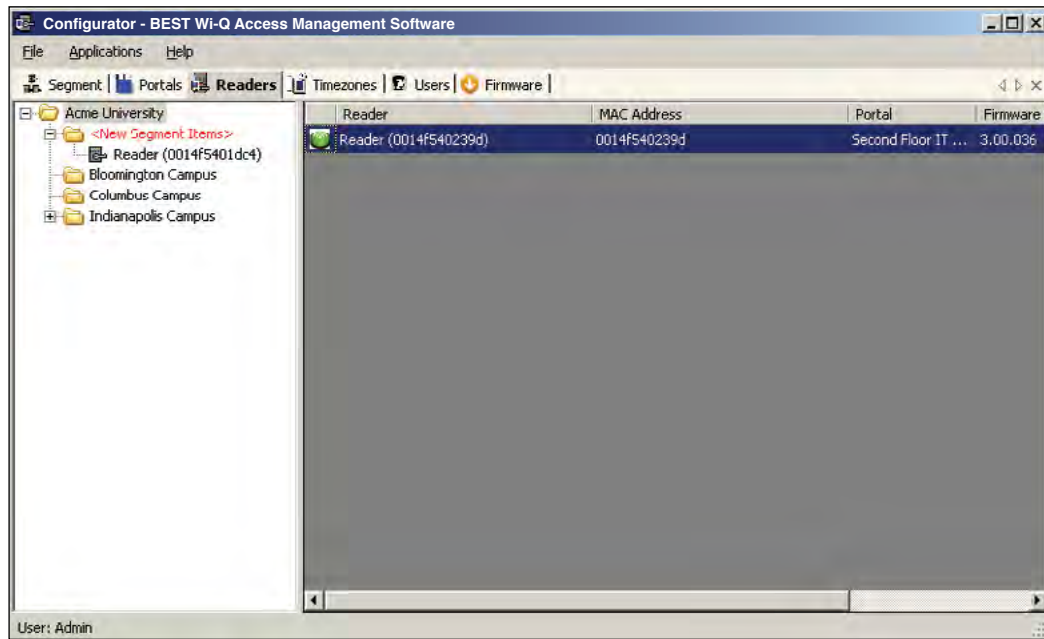
- 1 At each card reader, scan the card you registered with the segment credential.
- 2 Once this is done, the readers will appear in the <New Segment Items> folder, viewable in the Readers tab Segment Tree.

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

Adding Controllers to the Segment Tree

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

Figure 77 <New Segment Items>



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

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

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

Copying Reader Parameters

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

Configuring New Controllers

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

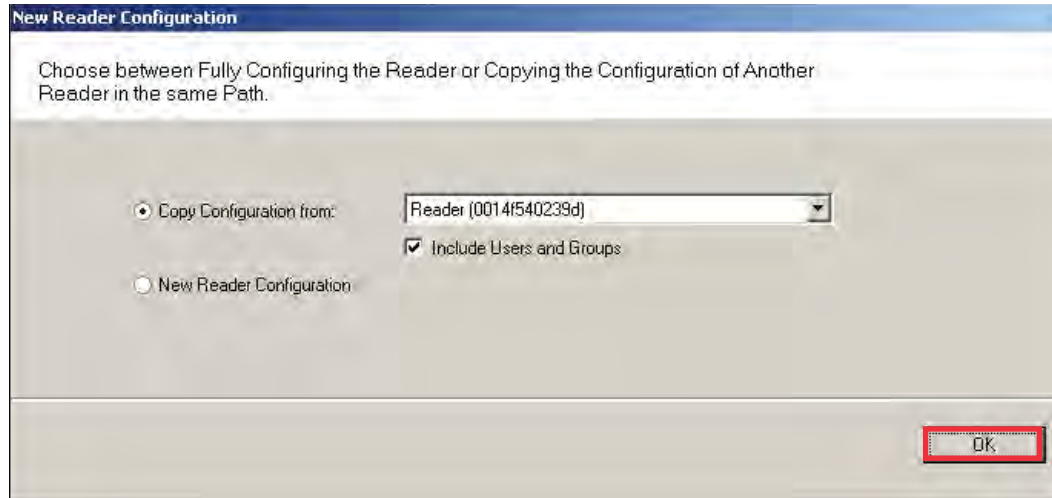
To configure a new Controller

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

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

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

Figure 78 New Reader Configuration



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

Field Category Definitions

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

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

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

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

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

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

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

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

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

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

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

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

Wiegand Device — Define if applicable.

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

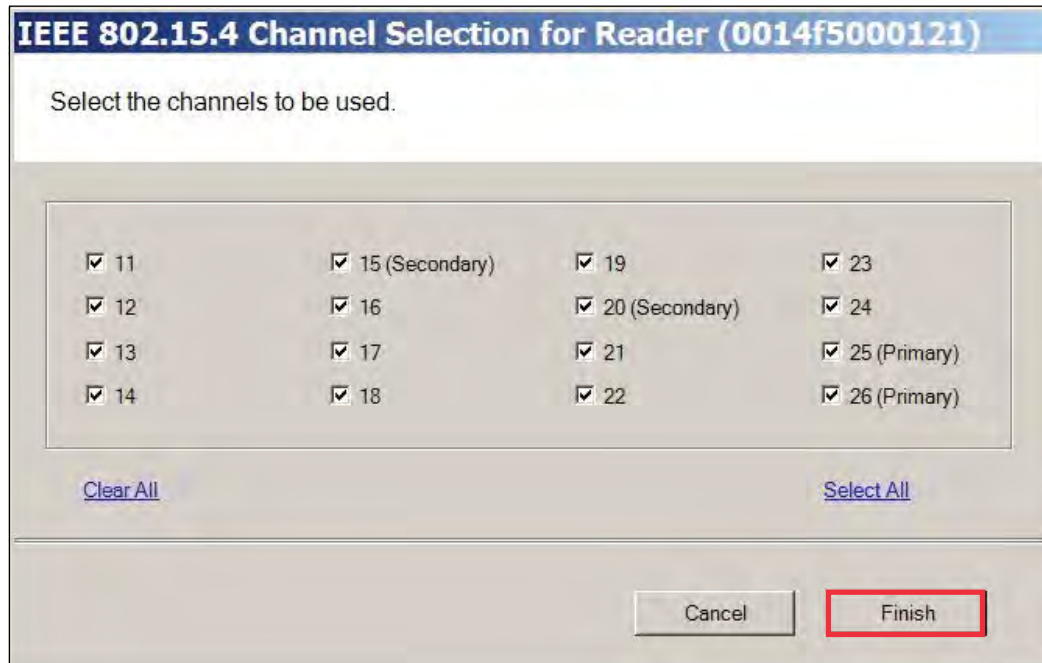
Card Formats Assignments — Assign card formats to the reader.

Assigning Reader Channels

Perform the following steps to assign reader channels.

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

Figure 79 Reader Channel Selection



The dialog box is titled "IEEE 802.15.4 Channel Selection for Reader (0014f5000121)". It contains a text label "Select the channels to be used." followed by a list of 16 channels arranged in a 4x4 grid. Each channel has a checked checkbox. The channels are: 11, 12, 13, 14, 15 (Secondary), 16, 17, 18, 19, 20 (Secondary), 21, 22, 23, 24, 25 (Primary), and 26 (Primary). Below the grid are two links: "Clear All" and "Select All". At the bottom right are two buttons: "Cancel" and "Finish". The "Finish" button is highlighted with a red border.

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

- 4 Select your desired channels.
- 5 Click Finish to save your settings.

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

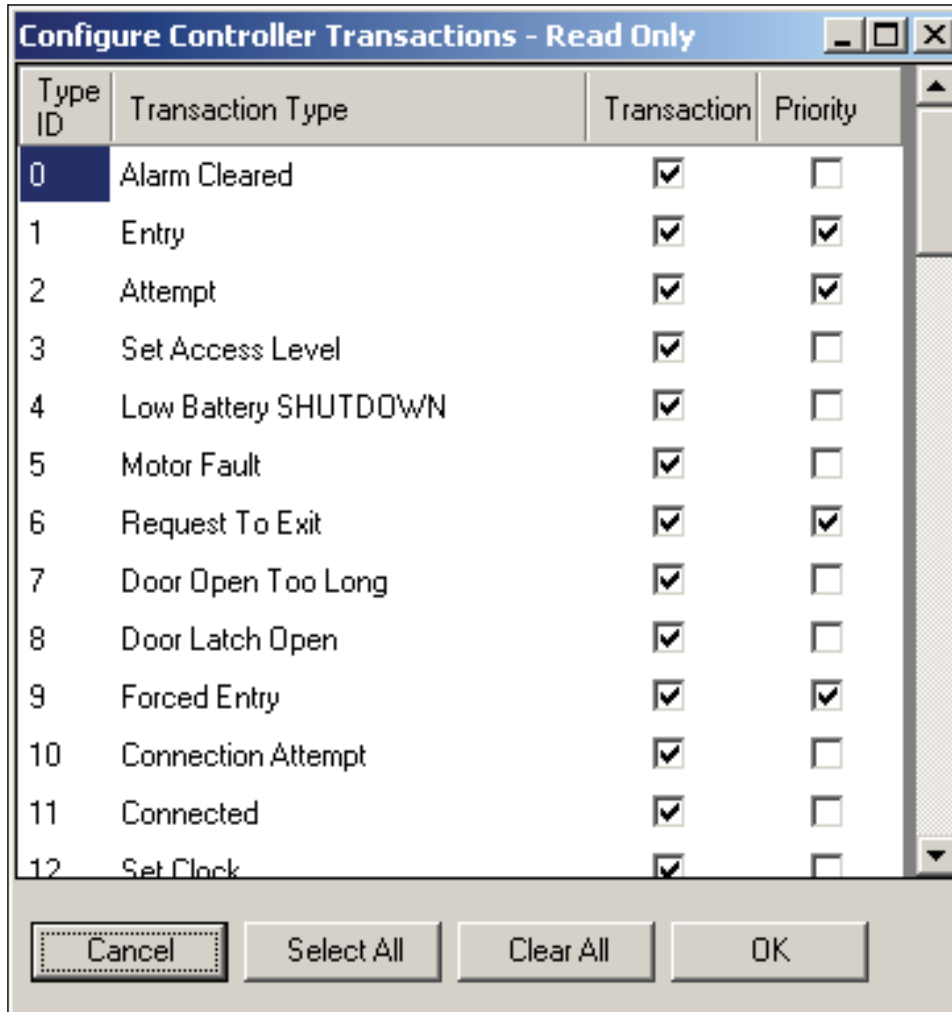
Reader Control

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

Uploaded Transactions

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

Figure 80 Configure Controller Transactions



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

5 Configure AMS Software (Task 11)

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

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

Associations

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

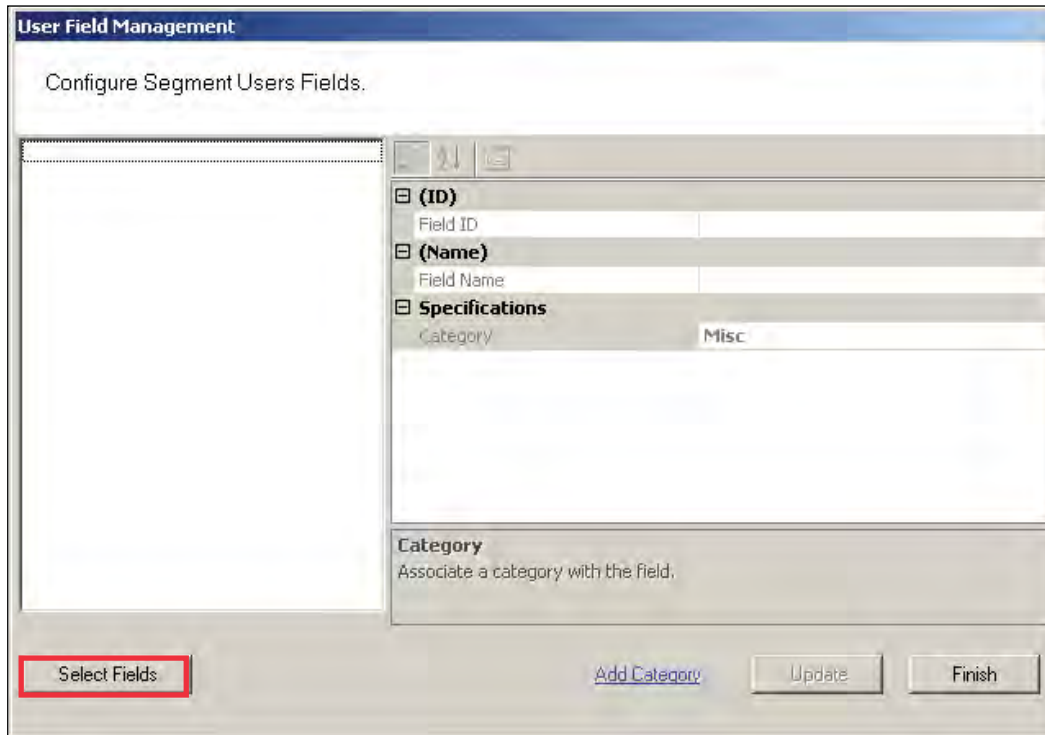
User Fields

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

Adding Additional User Fields

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

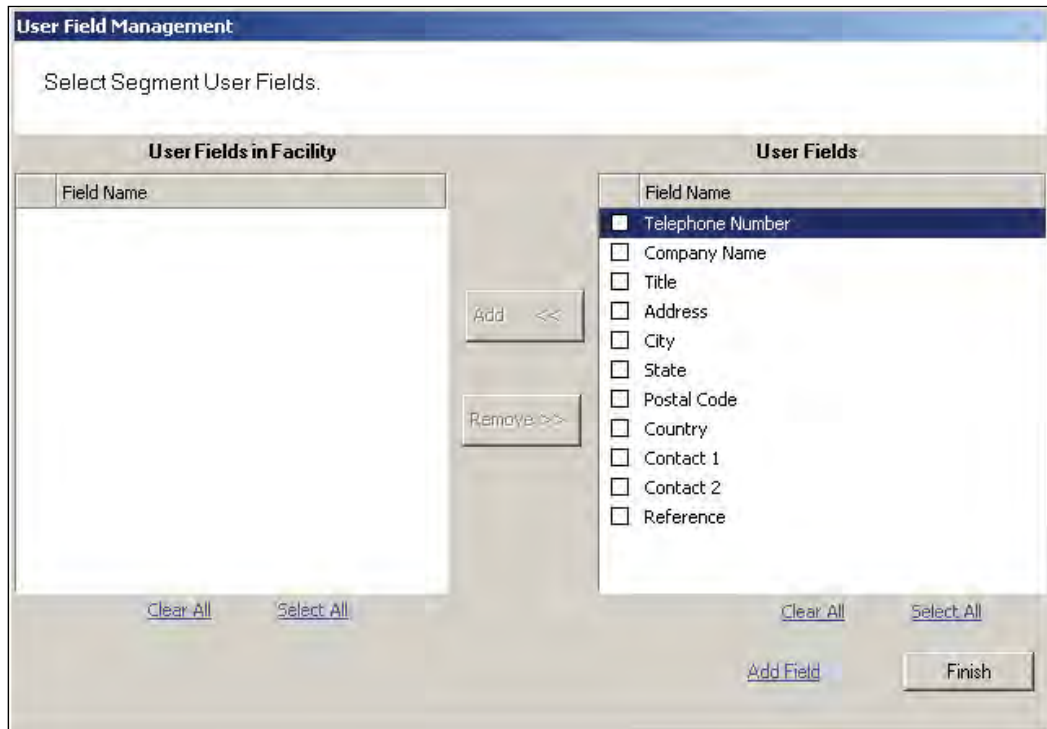
Figure 81 User Field Management



The image shows a 'User Field Management' dialog box. The title bar is blue with the text 'User Field Management'. Below the title bar, the text 'Configure Segment Users Fields.' is displayed. The dialog is divided into two main sections. The left section is a large, empty white area. The right section contains a list of fields with expandable sections. The first section is '(ID)' with a 'Field ID' input field. The second section is '(Name)' with a 'Field Name' input field. The third section is 'Specifications' with a 'Category' dropdown menu set to 'Misc'. Below these sections is a 'Category' label and the text 'Associate a category with the field.' At the bottom of the dialog, there are four buttons: 'Select Fields' (highlighted with a red rectangle), 'Add Category' (with a blue underline), 'Update', and 'Finish'.

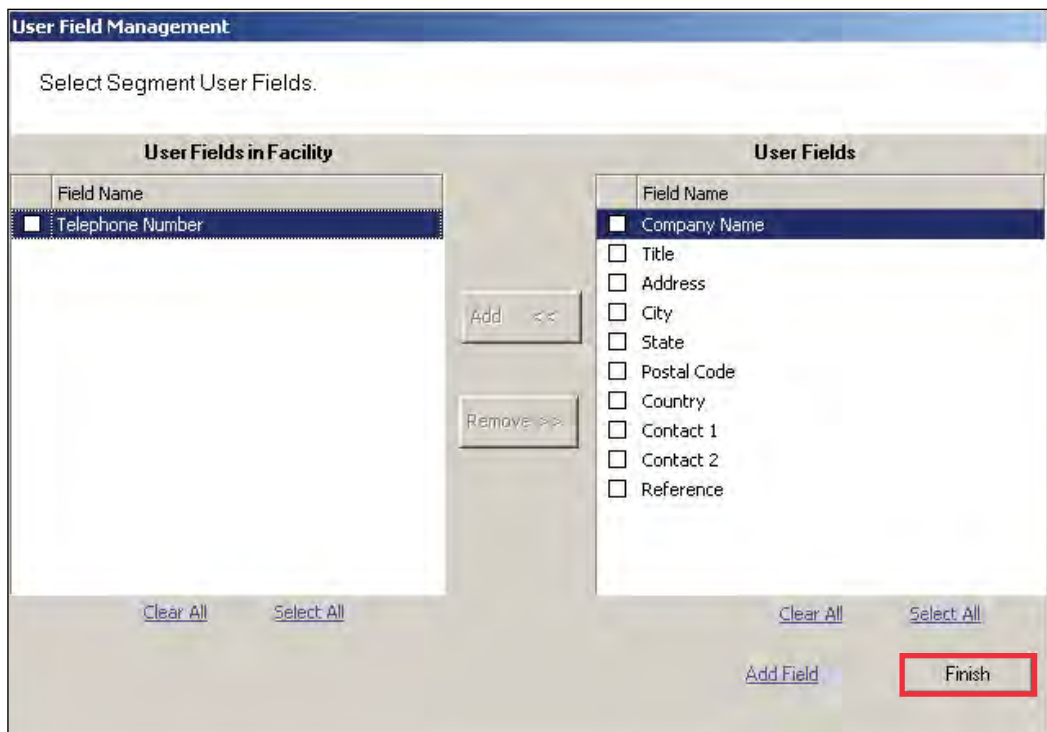
- 2 Click the Select Fields button at the bottom of the dialog box. The Select Segment User Fields dialog box opens. Additional pre-defined User Fields are listed on the right.

Figure 82 Select Segment User Fields



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

Figure 83 User Fields in Facility



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

Creating New User Fields

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

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

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

Figure 84 Add, Remove and Configure System User Fields

User Field Management
Add, Remove, and Configure System User Fields.

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

(ID)
Field ID 26

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

Specifications
Category **Statistics**

Field Name
The Field's Name.

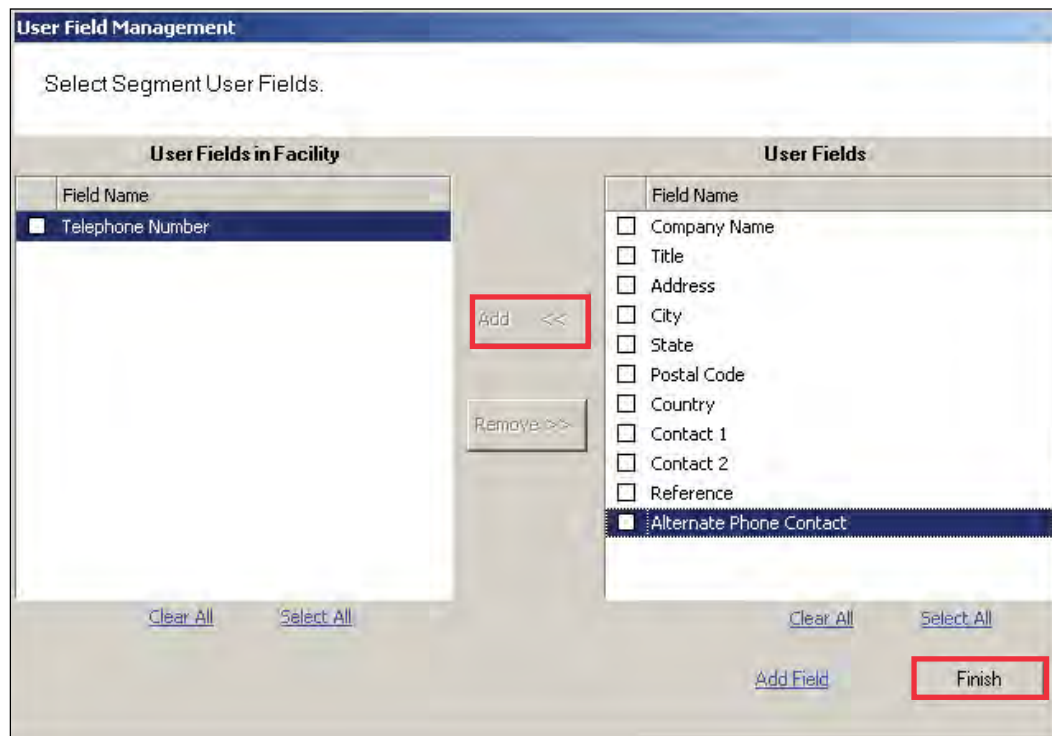
Add Remove Add Category Update **Finish**

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

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

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

Figure 85 User Field added to list

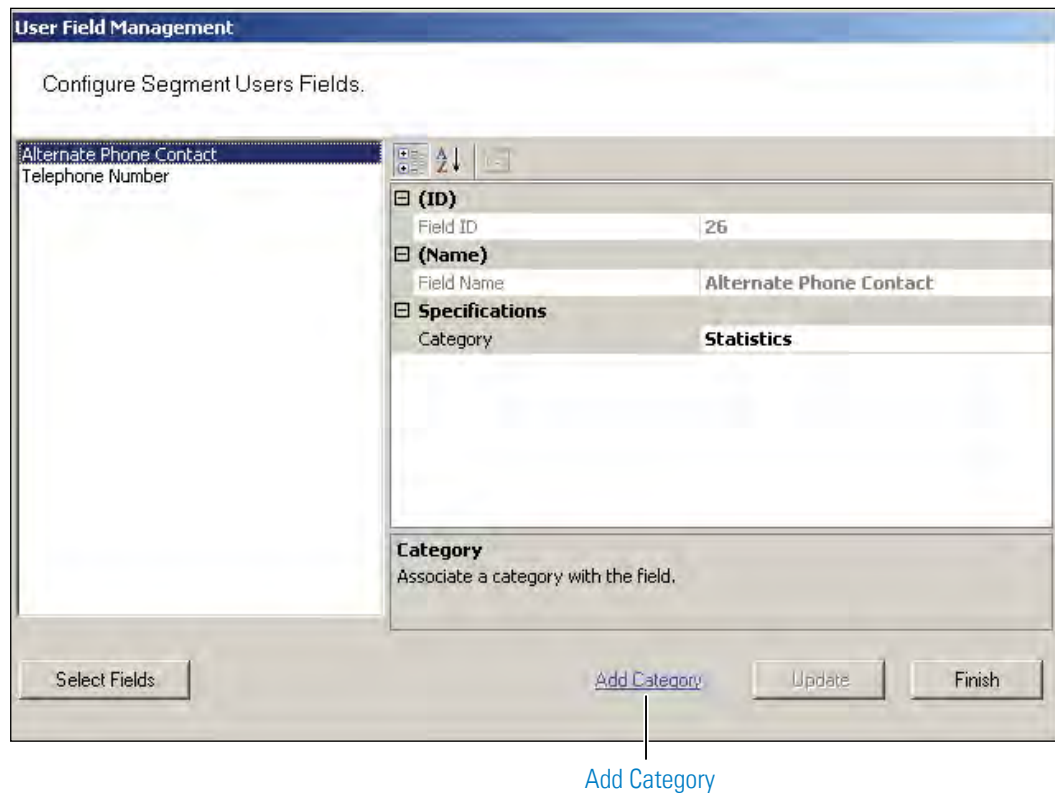


- 5 Select the Checkbox next to the field and click <<Add. The field is transferred to the User Fields in Segment box on the left.
- 6 Select Finish. The new field is now added to the User Field Management dialog box.

Adding a New User Fields Category

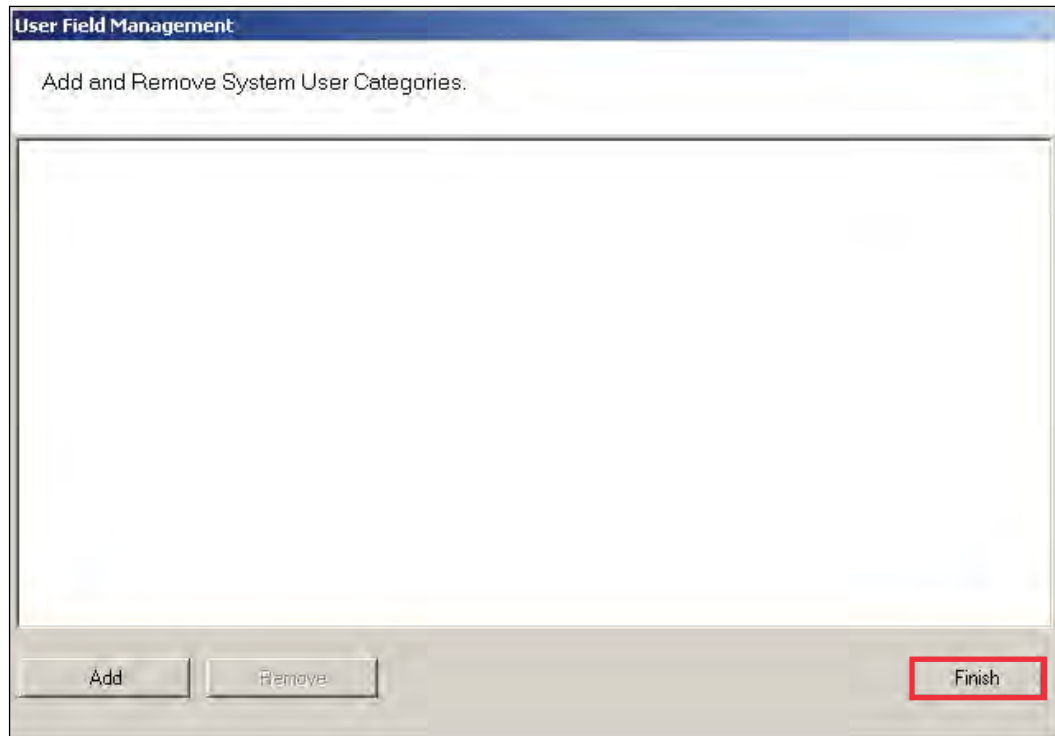
- 1 In the User Field Management of Segment dialog box, click the Add Category Link at the bottom of the dialog box.

Figure 86 Add Category



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

Figure 87 Adding and Remove System User Categories



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

Removing User Fields and Categories

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

To remove User Fields from the system

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

To remove added Categories from the system

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

User Groups

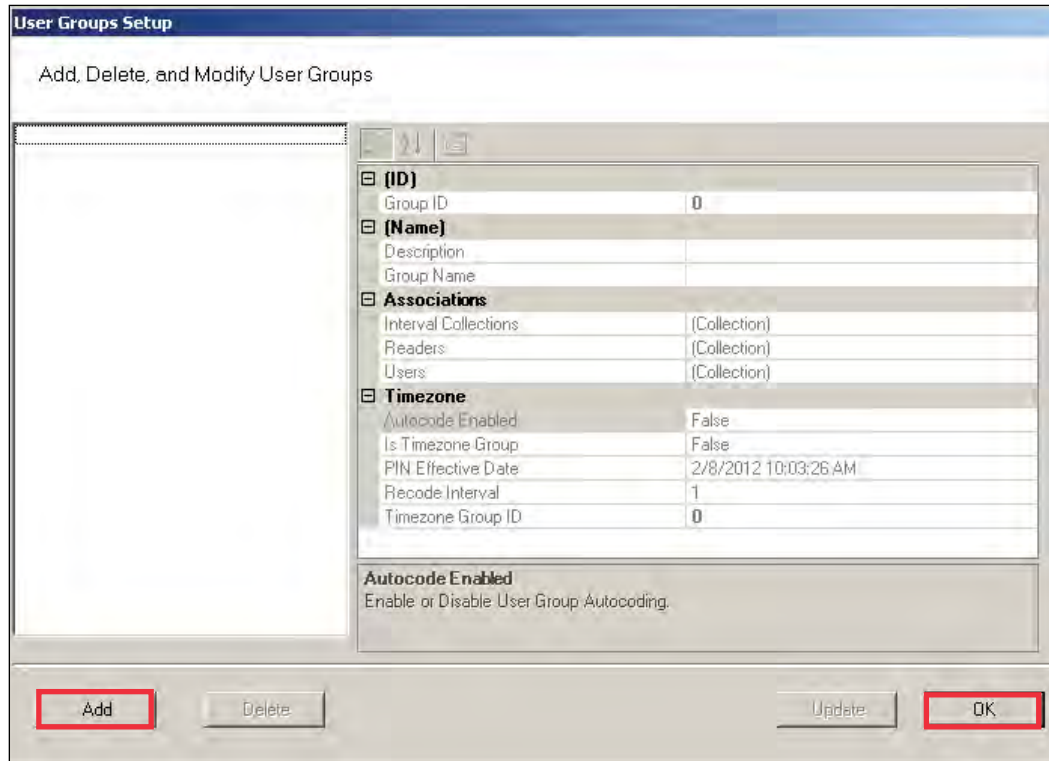
User Groups are a convenient way to define properties that will affect certain groups of individuals in your system. For example, if your Administrative personnel have different hours or entry parameters, you can create an Administrative group, make that group a Timezone Group and assign administrative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

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

Adding User Groups

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

Figure 88 User Groups Setup



The dialog box is titled "User Groups Setup" and has a subtitle "Add, Delete, and Modify User Groups". It is divided into two main sections. The left section is a list box for displaying created groups. The right section contains a form for defining a new group, with fields organized into four expandable categories: (ID), (Name), Associations, and Timezone. The (ID) category has a "Group ID" field with the value "0". The (Name) category has "Description" and "Group Name" fields. The Associations category has "Interval Collections", "Readers", and "Users" fields, all with "(Collection)" as the value. The Timezone category has "Autocode Enabled" (False), "Is Timezone Group" (False), "PIN Effective Date" (2/8/2012 10:03:26 AM), "Recode Interval" (1), and "Timezone Group ID" (0). Below these fields is a section labeled "Autocode Enabled" with the instruction "Enable or Disable User Group Autocoding." At the bottom of the dialog are four buttons: "Add", "Delete", "Update", and "OK". The "Add" and "OK" buttons are highlighted with red rectangles.

User Groups Setup	
Add, Delete, and Modify User Groups	
List of User Groups	(ID)
	Group ID
	0
	(Name)
	Description
	Group Name
	Associations
	Interval Collections
	(Collection)
	Readers
	(Collection)
	Users
	(Collection)
	Timezone
	Autocode Enabled
False	
Is Timezone Group	
False	
PIN Effective Date	
2/8/2012 10:03:26 AM	
Recode Interval	
1	
Timezone Group ID	
0	
Autocode Enabled	
Enable or Disable User Group Autocoding.	
Add Delete Update OK	

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

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

Removing User Groups

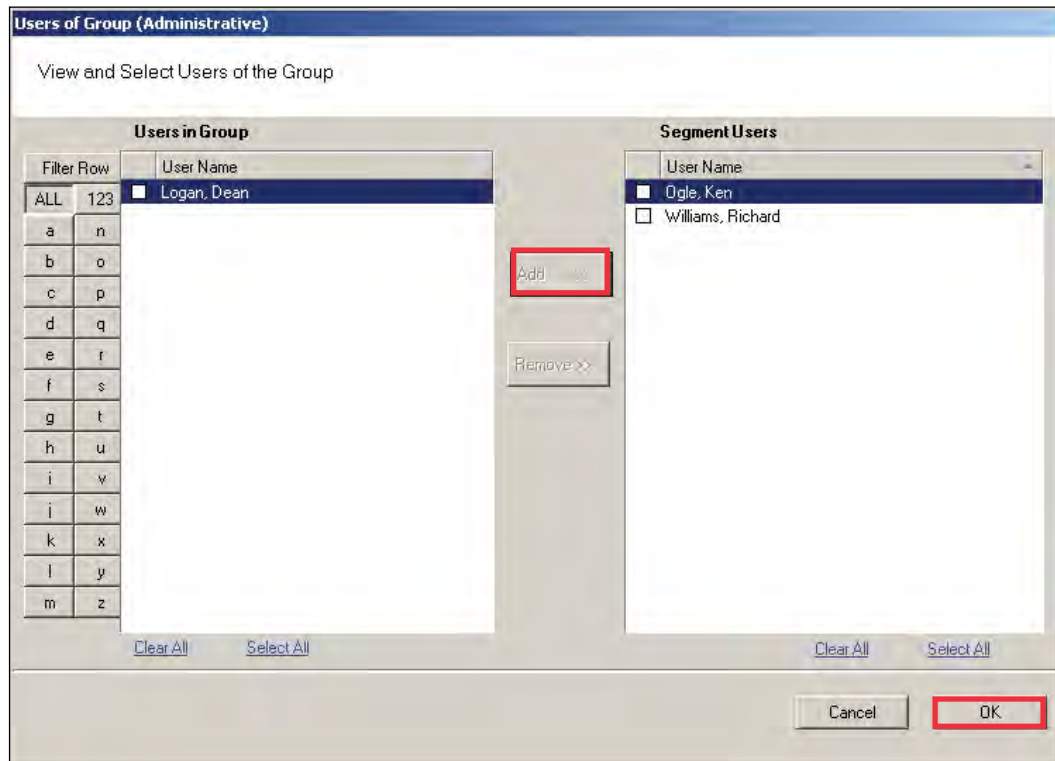
In the User Group Setup dialog box, select the group you wish to remove and select the Delete button. The group is immediately removed from the list, along with its associations.

Associating Users with User Groups

- 1 In the Segment Tab, Associations category, click the User Groups field.
- 2 Select the ellipsis button at the far right of the field.

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

Figure 89 Users of Group



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

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

Removing Users from User Group

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

Timezone User Groups

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

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

Figure 90 Creating a Timezone User Group

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

Once you have created a Timezone group, you will need to set up access times to apply to that group. For more information about Timezones and Timezone User Groups, see “Configuring Timezones” on [page 154](#).

Credential Settings

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

Keypad Credential Length

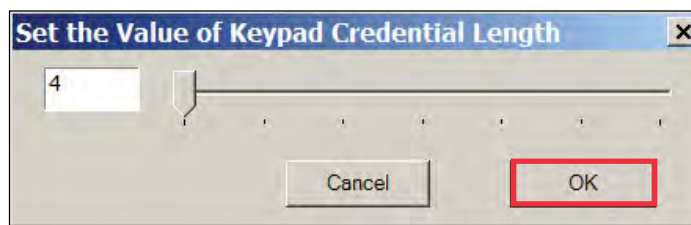
If your access system will have or currently has cards encoded with keypad credentials, you may set the number of digits required here.

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

Perform the following steps to set the Keypad Credential Length.

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

Figure 91 Setting the Credential Length



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

Magnetic Stripe Credential Configurations

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

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

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

Figure 92 Magnetic Stripe Credential Configurations

Magnetic Stripe Credential Configurations

Add, Delete, and Modify Magnetic Stripe Credential Configurations

(Name)

Configuration Name

Credential Settings

Card Track: Track 2

Number of Characters in the Credential: 80

Expiration Date Settings

Expiration Date Position Type: Not Used

Expiration Date Format: DDMMYY

Expiration Date Position: 1

Expiration Date Valid: Thru Expiration Date

Facility Code Settings

Facility Code Position Type: Not Used

Facility Code

Facility Code Length: 0

Facility Code Position: 1

Issue Number Settings

Issue Number Position Type: Not Used

Issue Number Length: 0

Issue Number Look Ahead Enable: False

Issue Number Position: 1

User ID Settings

User ID Length: 80

User ID Position: 1

User ID Position Type: Character

Number of Characters in the Credential

Set the Maximum Number of Characters on the Credential.

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

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

Credential Settings

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

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

Card Track Limits

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

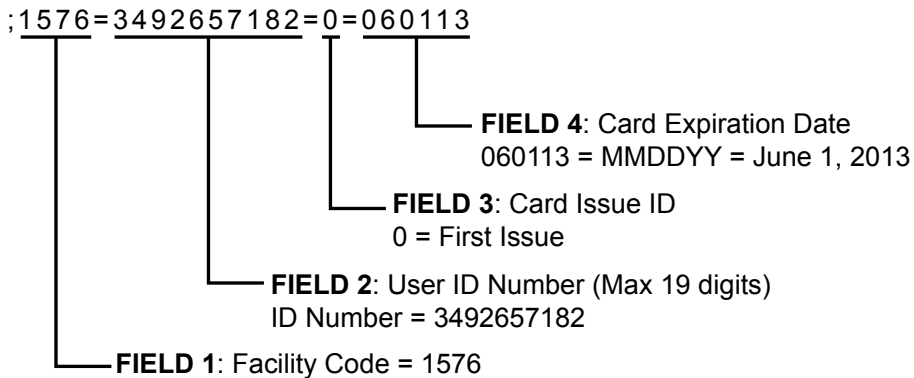
Character codes and counts

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

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

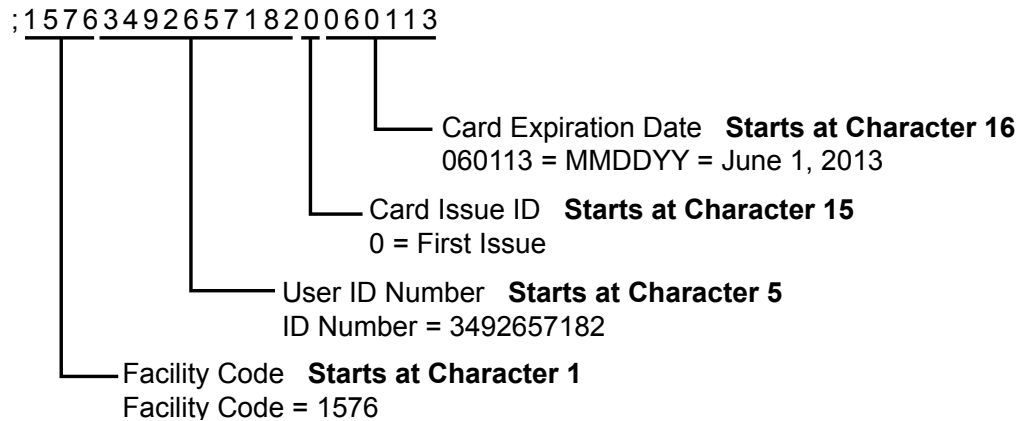
Following is an example of encoded data using field separators on Track 2.

Figure 93 Data Fields



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

Figure 94 Character count fields



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

Expiration Date Settings

Perform the following steps to define a card expiration date.

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

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

Facility Code Settings

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

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

Issue Number Settings

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

Perform the following steps to define an issue number position.

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

User ID Settings

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

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

Proximity Credential Configurations

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

Figure 95 Proximity Credential Configurations

Proximity Credential Configurations	
Add, Delete, and Modify Proximity Credential Configurations	
Configuration Name	
Credential Settings	
Number of Bits in the Credential	60
Facility Code Settings	
*Facility Code Position Type	Not Used
Facility Code	
Facility Code Length	0
Facility Code Position	1
Issue Number Settings	
*Issue Number Position Type	Not Used
Issue Number Length	0
Issue Number Look Ahead Enable	False
Issue Number Position	1
User ID Settings	
User ID Length	60
User ID Position	1
User ID Position Type	Active

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

Buttons: Add (highlighted), Delete, Cancel, OK

To add a card configuration, perform the following steps.

- 1 Click Add. Give your new configuration a name in the Configuration Name field.
- 2 Under Credential Settings, select Number of Bits in the Credential. Change the number to the right (default 60) to match the number of bits on your card.
- 3 If your card is configured to include the facility code, change Facility Code Position type to Active. The facility code fields below will activate.
 - a Enter your facility code in the Facility Code field.
 - b Change the Facility Code Length to match the number of bits in your facility code.
 - c Change the Facility Code Position to match your card.

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

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

Daylight Saving Settings

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

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

I/O

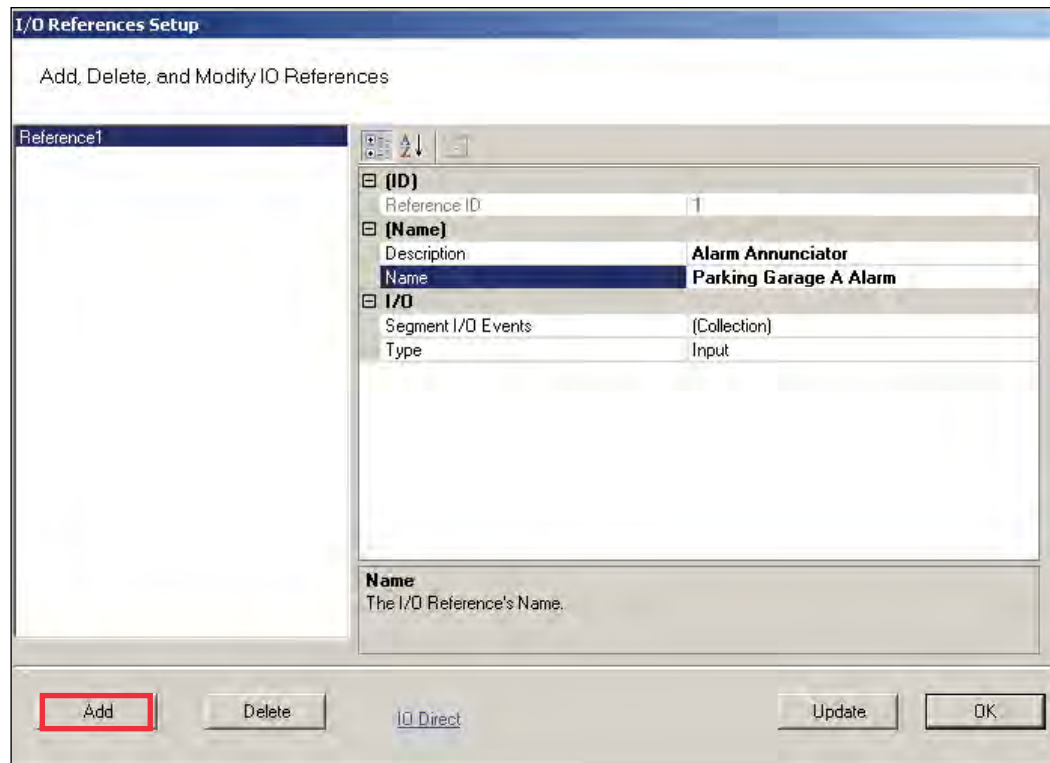
If you are using input/output devices in your system, they are recognized and defined similar to a Controller.

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

Adding and Modifying I/O References

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

Figure 96 I/O References Setup



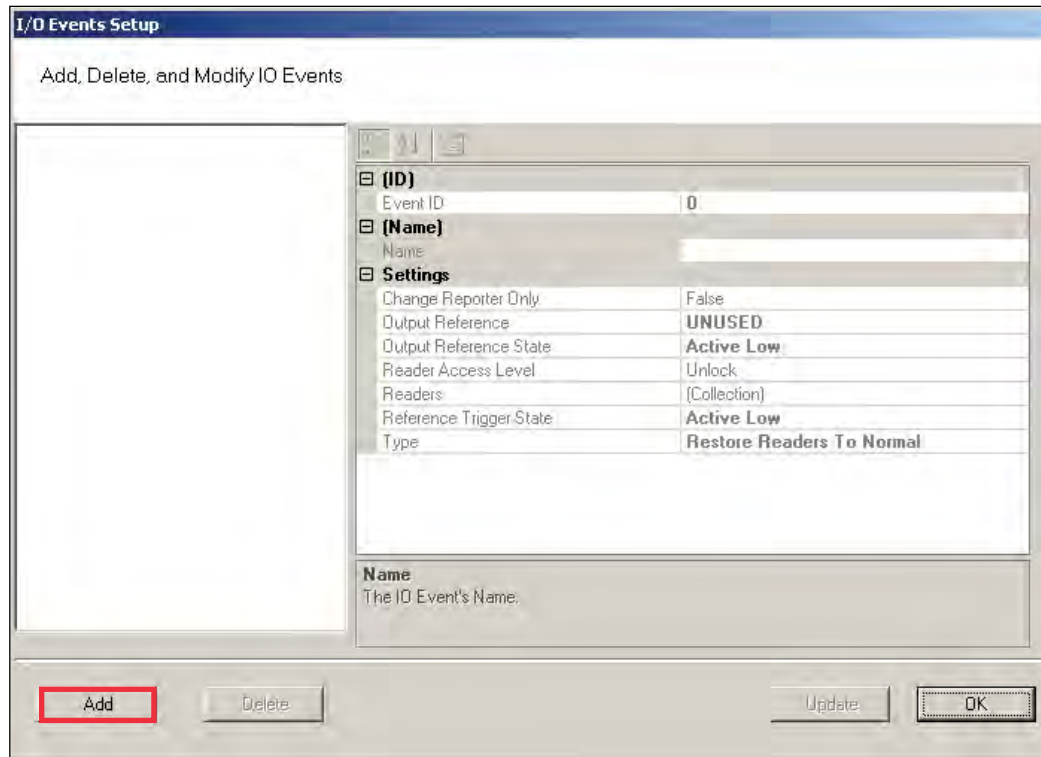
The dialog box is titled "I/O References Setup" and contains the subtitle "Add, Delete, and Modify IO References". On the left, a list box labeled "Reference1" is empty. On the right, there are three expandable sections: (ID), (Name), and I/O. The (ID) section has a "Reference ID" field with the value "1". The (Name) section has a "Description" field with the value "Alarm Annunciator" and a "Name" field with the value "Parking Garage A Alarm". The I/O section has a "Segment I/O Events" field with the value "(Collection)" and a "Type" field with the value "Input". At the bottom, there are four buttons: "Add" (highlighted with a red rectangle), "Delete", "IO Direct", and "Update". An "OK" button is also present at the bottom right.

I/O References Setup	
Add, Delete, and Modify IO References	
Reference1	
(ID)	
Reference ID	1
(Name)	
Description	Alarm Annunciator
Name	Parking Garage A Alarm
I/O	
Segment I/O Events	(Collection)
Type	Input
Name The I/O Reference's Name.	
Add	Delete
IO Direct	Update
OK	

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

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

Figure 97 I/O Events Setup



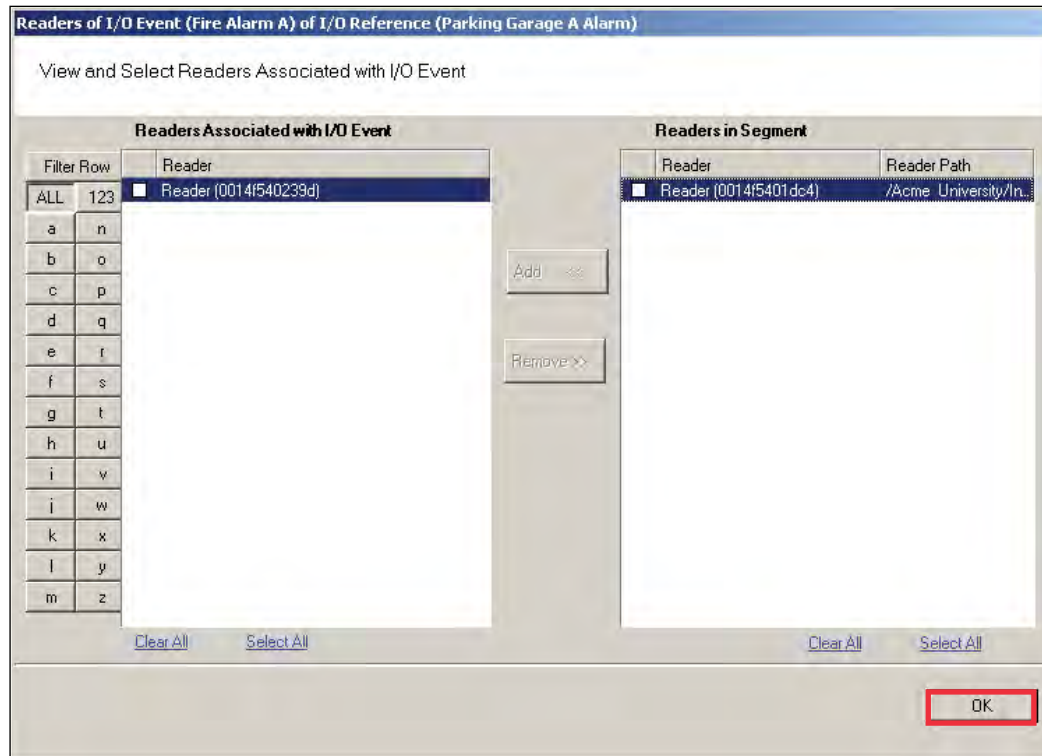
The I/O Events Setup dialog box is titled "I/O Events Setup" and contains the subtitle "Add, Delete, and Modify IO Events". It features a large empty list on the left for event entries. On the right, there are three expandable sections: (ID), (Name), and Settings. The (ID) section has an "Event ID" field with the value "0". The (Name) section has a "Name" field. The Settings section contains several fields: "Change Reporter Only" (False), "Output Reference" (UNUSED), "Output Reference State" (Active Low), "Reader Access Level" (Unlock), "Readers" ((Collection)), "Reference Trigger State" (Active Low), and "Type" (Restore Readers To Normal). Below these sections is a "Name" label and a text field containing "The IO Event's Name:". At the bottom, there are four buttons: "Add" (highlighted with a red rectangle), "Delete", "Update", and "OK".

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

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

- 6 Click the Add button. The system creates an Event ID and adds it to the list in the left hand column.
- 7 Enter a name for the event, such as Fire Alarm A.
- 8 Under the Settings Category, click the Readers field and click the ellipsis button.
- 9 This will open up a new window. [See Figure 98](#). Select a device from the Readers in Segment section that will be associated with the event.
- 10 Click Add << to add it to the list of Readers Associated with I/O Event list.

Figure 98 Associating an I/O event with a Reader



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

Misc

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

PIN Settings

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

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

Figure 99 Set the Value of PIN Length



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

Adding Users to the Segment

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

Before You Begin

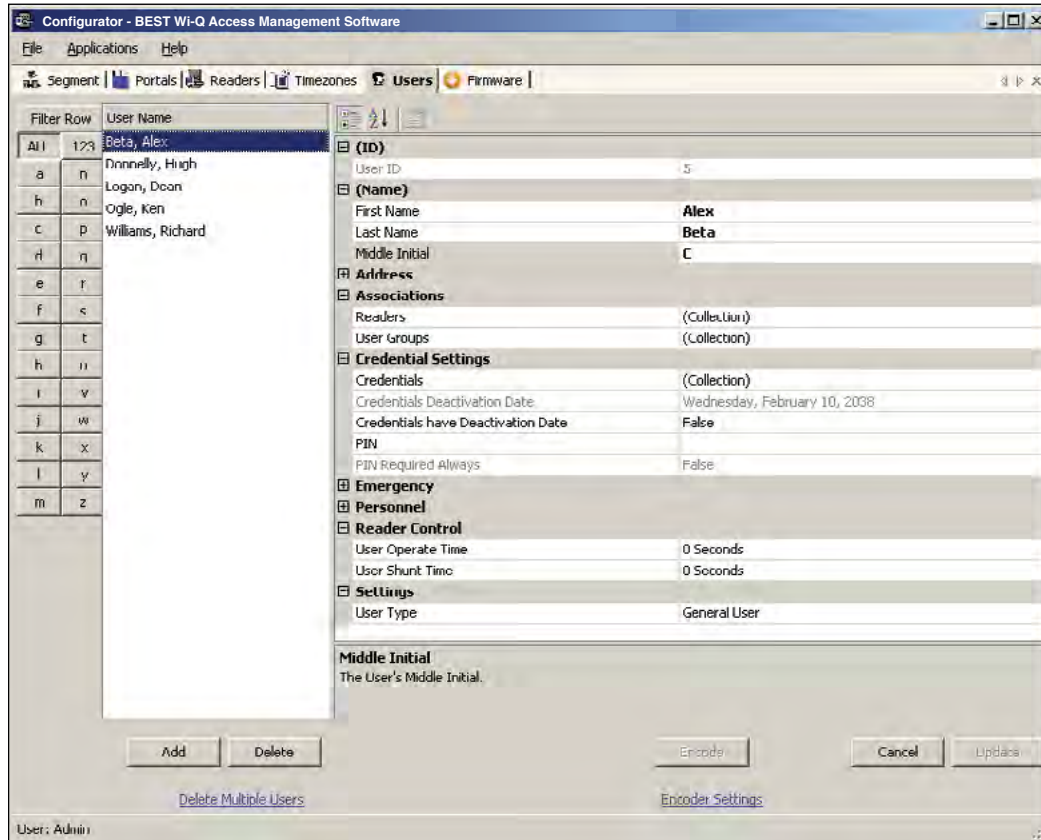
Before you begin adding users to the system for the first time, be prepared to address the following items:

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

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

Users Tab Overview

Figure 100 Users Tab



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

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

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

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

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

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

Adding a User Name

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

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

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

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

To associate a user with readers

- 1 In the Associations category, click inside the Readers field, and select the ellipsis button at the far right.
- 2 The Readers of User dialog box opens and displays a list of readers available to the User.

Figure 101 Readers of User

Readers of User (Alex Beta)

View and Select Readers Associated with User

Readers Associated with User

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

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

Readers in Facility

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

[Add <<](#)

[Remove >>](#)

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

[Finish](#)

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

Figure 102 Selecting a reader to associate with a user

The screenshot shows a window titled "Readers of User (Alex Beta)" with the subtitle "View and Select Readers Associated with User". The window is divided into two main sections: "Readers Associated with User" on the left and "Readers in Facility" on the right. In the "Readers Associated with User" section, there is a table with a "Filter Row" column and a "Reader" column. The "Filter Row" column has a grid of buttons labeled with letters and numbers (a-n, b-o, c-p, d-q, e-r, f-s, g-l, h-u, i-v, j-w, k-x, l-y) and a "ALL" button. The "Reader" column has a single entry: "Reader (0014f5001534)". Below this table are "Clear All" and "Select All" buttons. In the "Readers in Facility" section, there is a table with "Reader" and "Reader Path" columns, which is currently empty. Below this table are "Clear All" and "Select All" buttons. Between the two sections are "Add <<" and "Remove >>" buttons. At the bottom right of the window is a "Finish" button.

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

User Groups

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

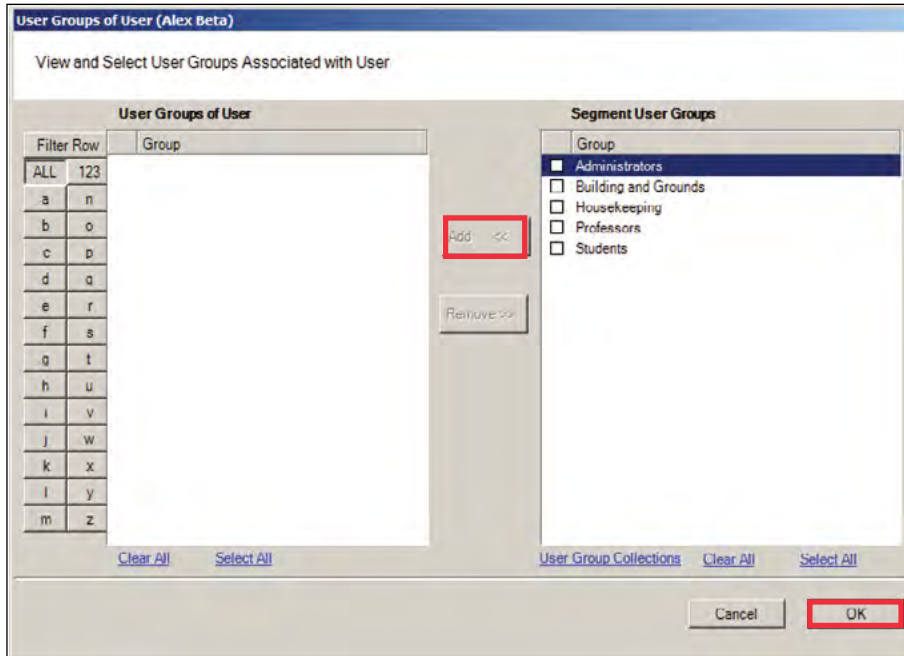
A User Group may also be defined as a Timezone Group. Timezone User Groups further define access levels for the Master Timezone. You can restrict access of certain groups of employees to a specific time period. For example, you may have a housekeeping group designated as a Timezone Group with restricted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

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

To add a user to a User Group

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

Figure 103 User Groups of User



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

Credential Settings

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

enter them here. Credential setup is a two-step process: First, you will select the credential type to be used, then you will register the credential.

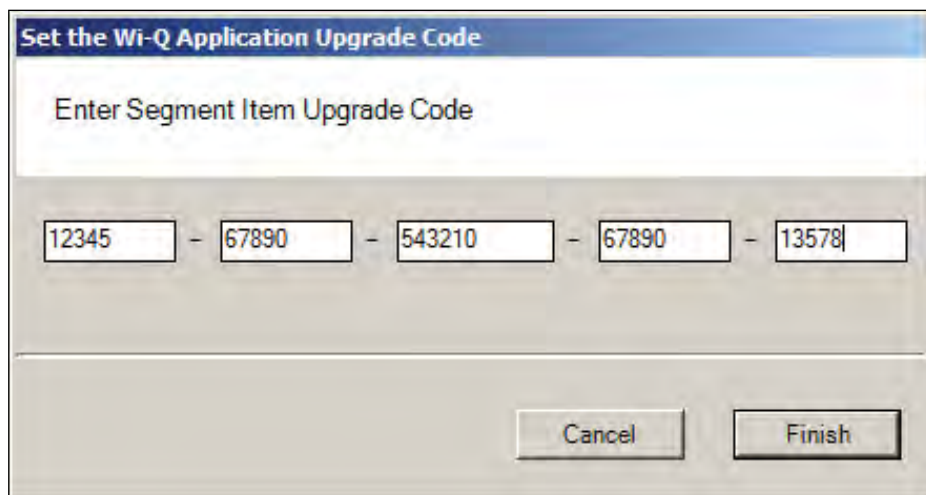
Keypad Type — The default credential type in AMS is Keypad. When you add a user to the system, the software assigns them a unique keypad credential number, then automatically registers it with the system. If your segment uses only keypads, once you add the new user name, you can skip to Adding PINs and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

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

To select the card type

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

Figure 104 Selecting a User Credential type



Set the Wi-Q Application Upgrade Code

Enter Segment Item Upgrade Code

12345 - 67890 - 543210 - 67890 - 13578

Cancel Finish

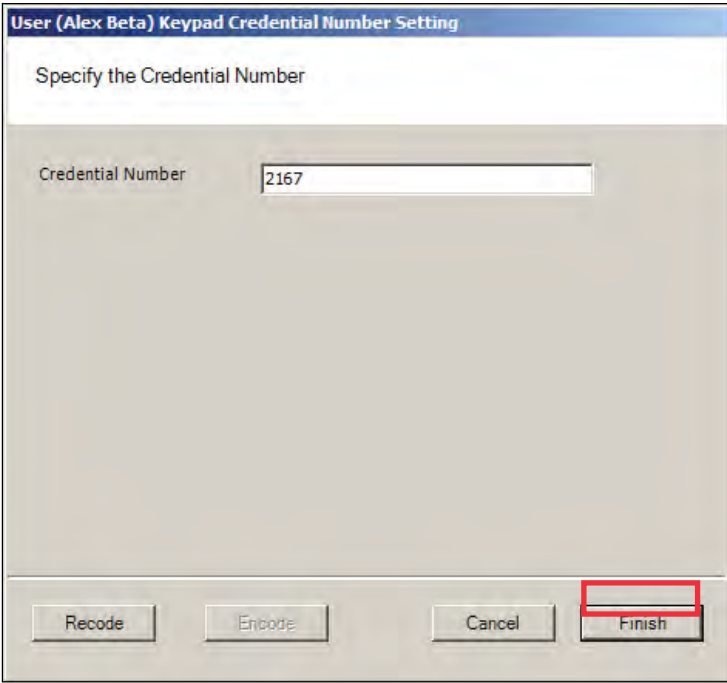
- 2 Select the type of credential the reader will use, for example, Keypad. The credential options in the categories on the right will change, depending on the type selected.

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

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

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

Figure 105 Enter a user credential number



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

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

Credentials Deactivation Date — You can define whether a user's credentials can be automatically de-activated based on an expiration date. This is useful, for example,

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

Registering the Credential

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

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

To register a Keypad credential

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

To register a Magnetic Stripe Card credential

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

Figure 106 Entering a Magnetic Card credential number

User (Alex Beta) Magnetic Stripe Card Credential Number Setting

Specify the Credential Number

Credential Number 0000000000006161

Select Scan Device

☐ MSR 2016

☒ Card Reader

☐ Reader

Scan Encode Cancel Finish

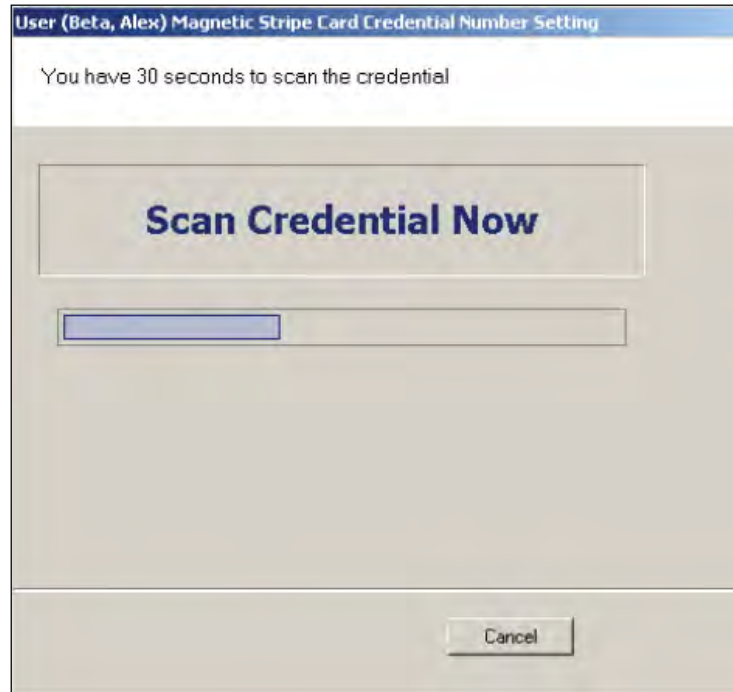
- 3 Enter a Credential Number manually (must be less than 16 characters, zeros will be appended) or select a scan device.

Using a scanning device to register a credential

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

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

Figure 107 Scan Credentials



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

Using a local reader

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

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

Note You may need to expand the drop-down list to view all available readers. Use the

highlighted area in the lower right corner.

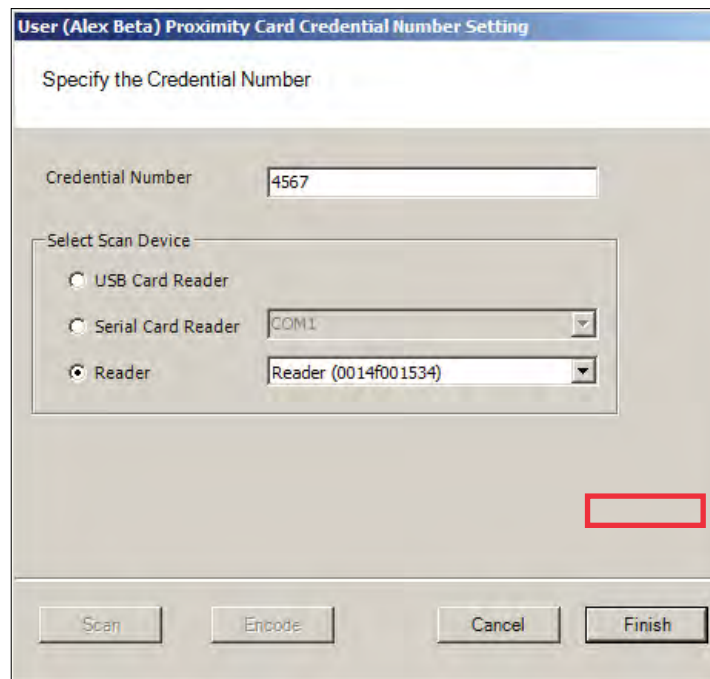
Registering a Prox card credential

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

To register a Prox Card Credential

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

Figure 108 Entering a Proximity Card credential number



The dialog box is titled "User (Alex Beta) Proximity Card Credential Number Setting". It contains a section "Specify the Credential Number" with a text box labeled "Credential Number" containing the value "4567". Below this is a section "Select Scan Device" with three radio buttons: "USB Card Reader", "Serial Card Reader", and "Reader". The "Reader" option is selected. Next to "Serial Card Reader" is a dropdown menu showing "COM1". Next to "Reader" is a dropdown menu showing "Reader (0014f001534)". At the bottom right of the dialog box, there is a red rectangular box. At the bottom of the dialog box are four buttons: "Scan", "Encode", "Cancel", and "Finish".

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

USB Card Reader

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

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

Serial Card Reader

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

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

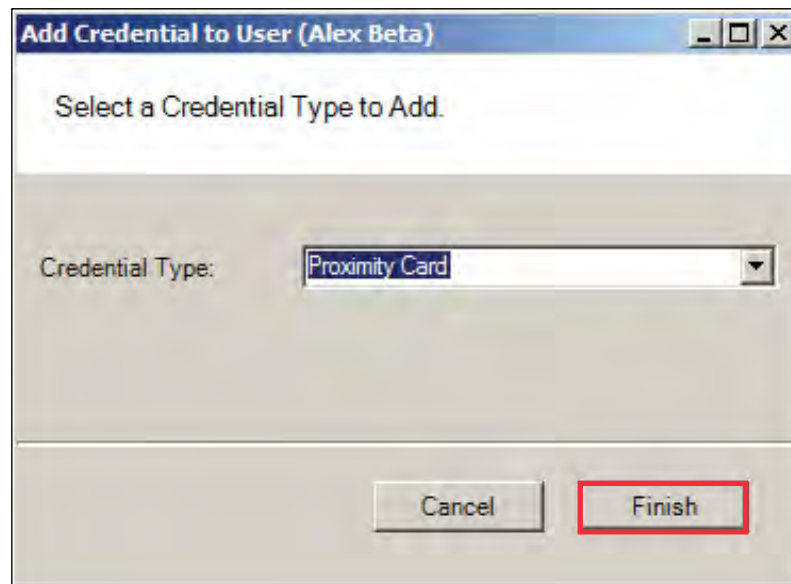
Adding a Credential Type

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

To add a card type to the list

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

Figure 109 Add Credential to User



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

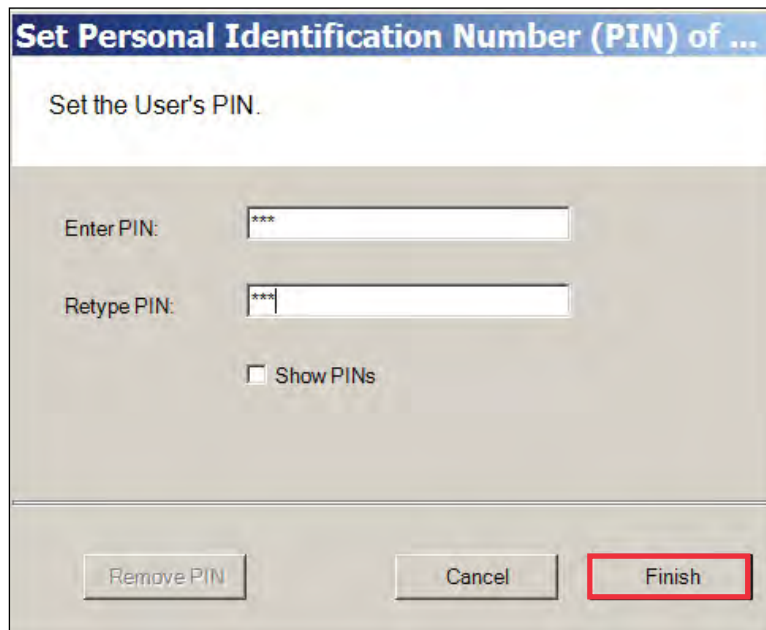
PIN

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

To add a PIN Number for a User

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

Figure 110 Set PIN of User

The image shows a dialog box titled "Set Personal Identification Number (PIN) of ...". Inside the dialog, the text "Set the User's PIN." is displayed. There are two input fields: "Enter PIN:" and "Retype PIN:", both containing three asterisks. Below these fields is a checkbox labeled "Show PINs" which is currently unchecked. At the bottom of the dialog, there are three buttons: "Remove PIN", "Cancel", and "Finish". The "Finish" button is highlighted with a red rectangular border.

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

Reader Control

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

To modify User Operate Time

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

To modify User Shunt Time

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

Settings

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

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

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

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

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

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

To assign User Type

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

Wi-Q Gateway and Reader Control and Messaging

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

Wi-Q Gateway Controls

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

To access right-click Wi-Q Gateway messaging

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