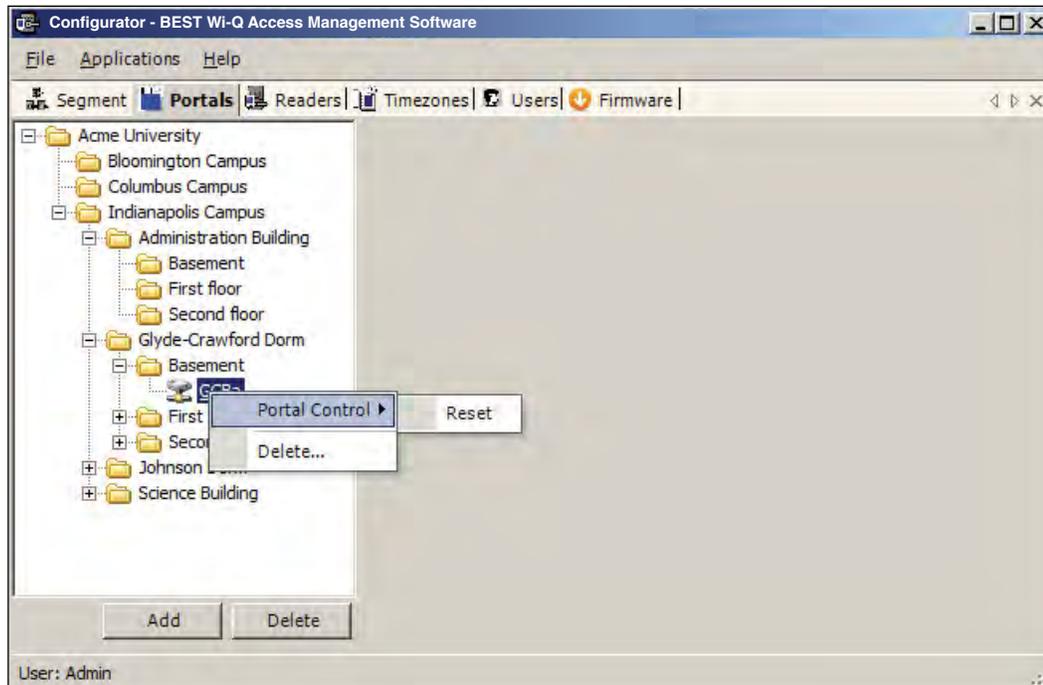


Figure 111 Right-click Portal messaging options



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

Reader Controls

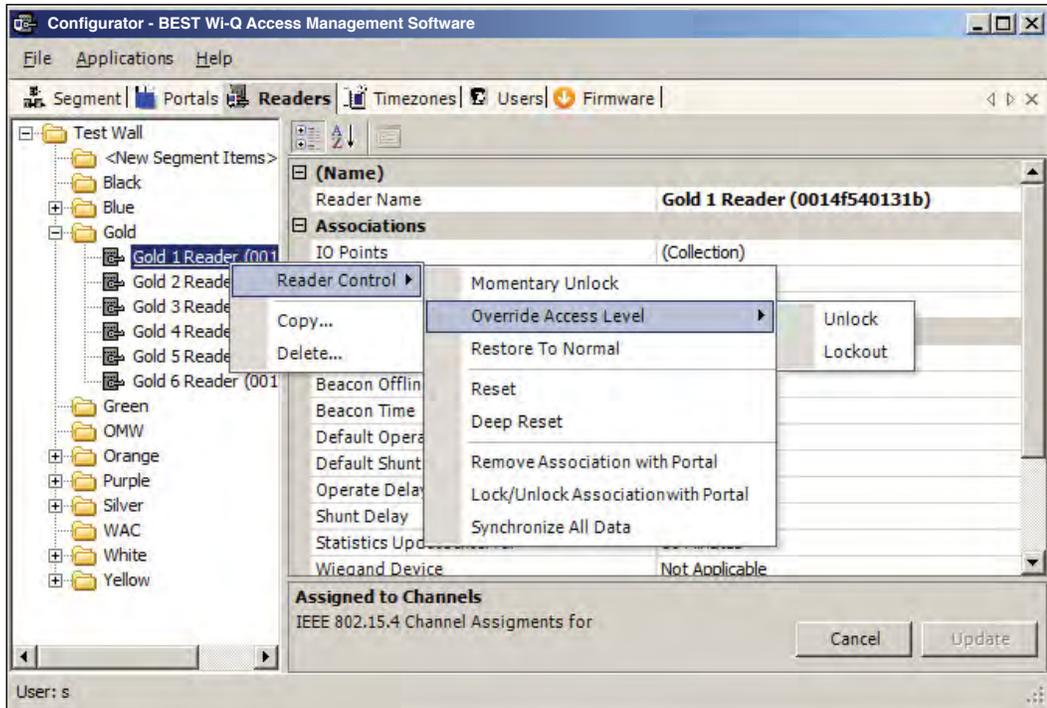
You can delete, reset and restore a reader to normal operation without going to the physical location of the reader. In addition to these commands, you can momentarily unlock, override the access level, perform a deep reset and remove the reader's association to a Portal all from within the software.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

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

To Access Right-Click Reader Messaging

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

Figure 112 Right-click reader messaging options



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

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

Restore to Normal — Immediately restores all standard normal operation.

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

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

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

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

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

Configuring Timezones

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

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

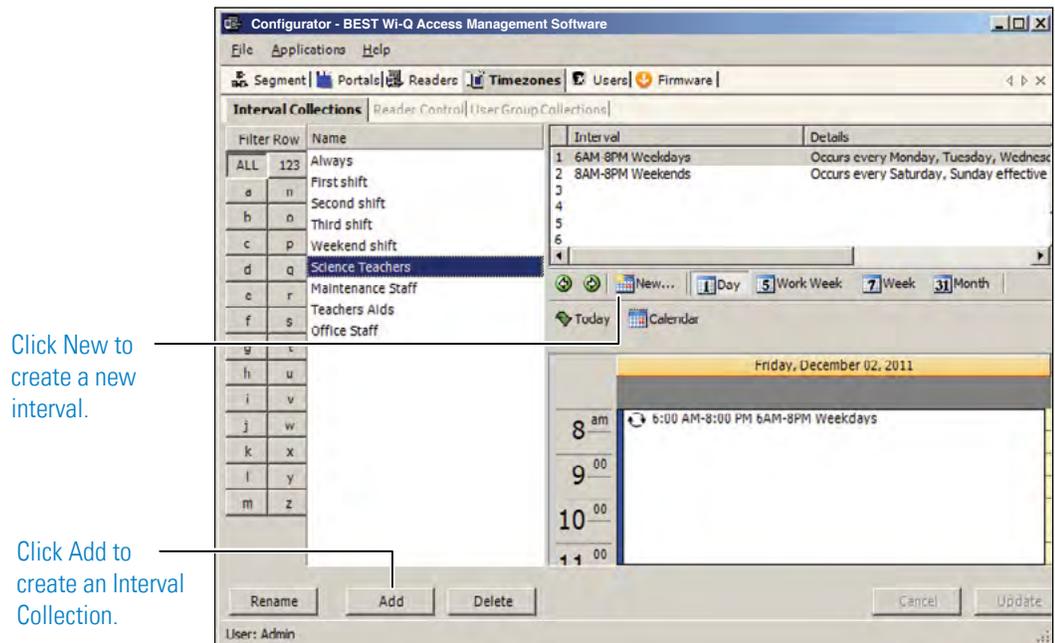
- Interval Collections — this is a collection of recurring ranges of time and days of the week, such as 6:00 am to 6:00 pm weekdays AND 8:00 am to 8:00 pm weekends.
- Reader Control — this is where you assign access levels to readers and determine how the reader will operate during assigned timezone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

Note Readers can be assigned to only one Timezone.

To create a Timezone Interval Collection

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

Figure 113 Interval Collection



- 4 The Interval Configuration window opens.

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

Figure 114 Interval Configuration

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

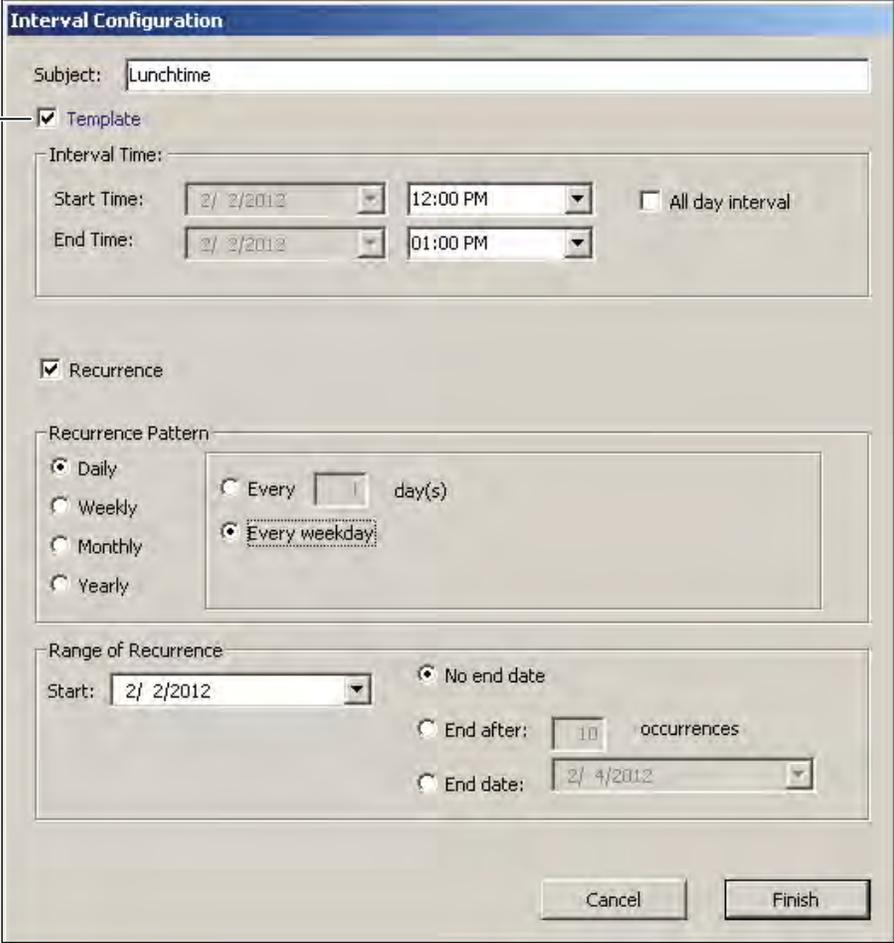
Click Recurrence if the interval repeats.

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

Timezone Interval Template Feature

At the top of the Interval Configuration window, there is a “Template” checkbox. Selecting this box will allow the timezone interval you configure to be used as a template for other intervals. For example, if you create a “Lunchtime” interval collection between 12 pm and 1 pm, and you select the “Template” checkbox ([Figure 115](#)), you can add that interval to an existing collection.

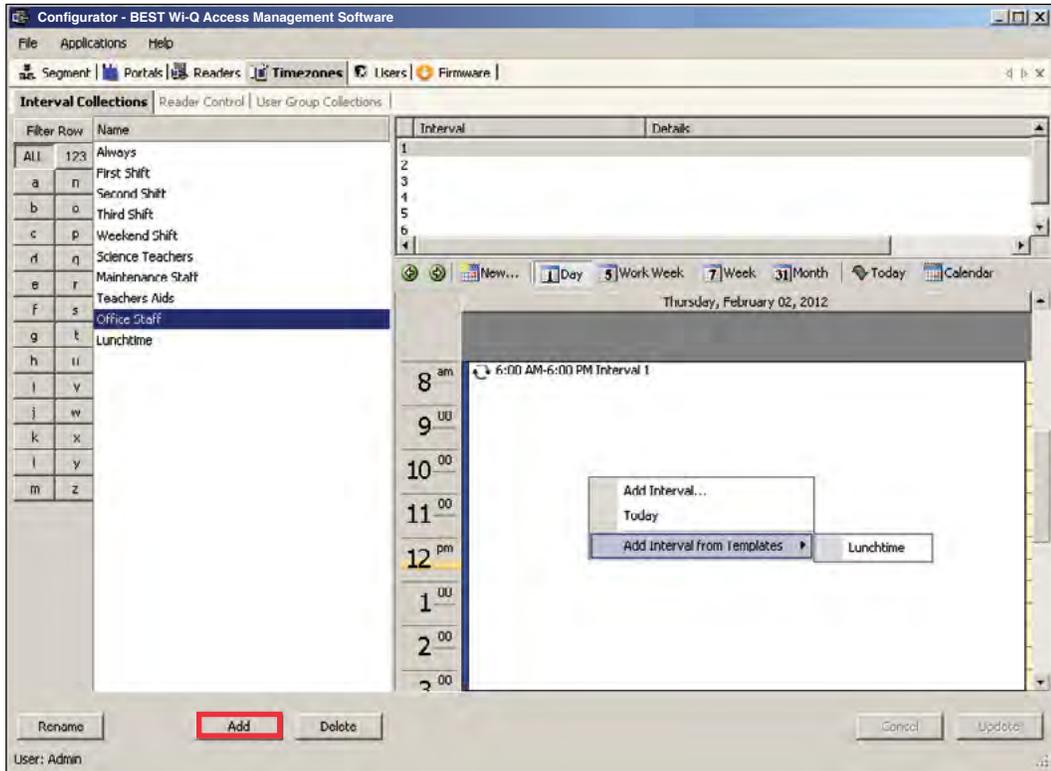
Figure 115 Interval Configuration Template



The screenshot shows the "Interval Configuration" dialog box. The "Subject" field is set to "Lunchtime". The "Template" checkbox is checked and highlighted with a blue arrow and the label "Template". The "Interval Time" section shows a start time of 12:00 PM and an end time of 01:00 PM on 2/2/2012. The "All day interval" checkbox is unchecked. The "Recurrence" section is checked, and the "Recurrence Pattern" is set to "Every weekday". The "Range of Recurrence" section shows a start date of 2/2/2012, with "No end date" selected. The "Cancel" and "Finish" buttons are at the bottom right.

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 116](#).

Figure 116 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 117 Reader Control

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.

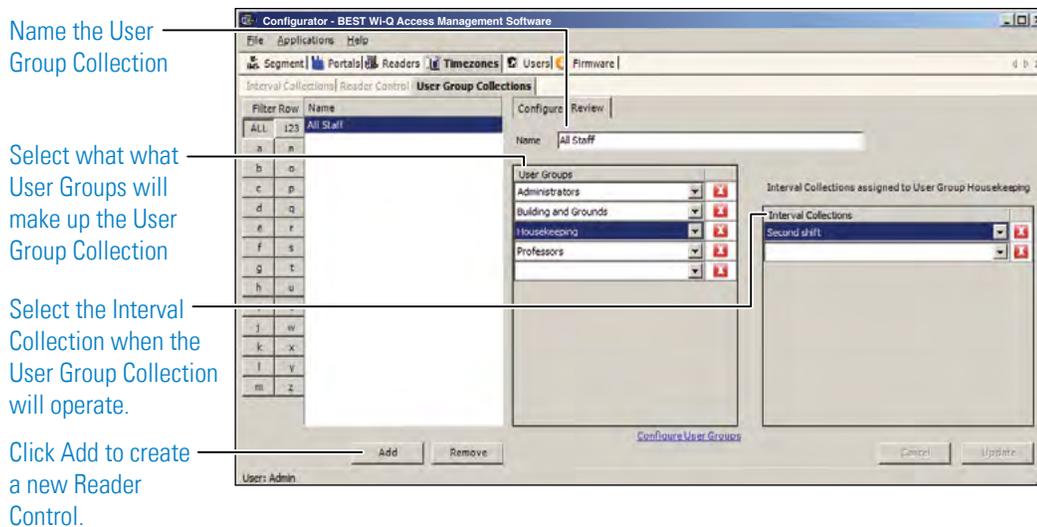
Timezone User Group Collections

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

To create the Timezone User Group Collection

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

Figure 118 Creating the timezone user group collection



6 Using and Managing the System

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

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

Wi-Q AMS and Omnilock Configurator

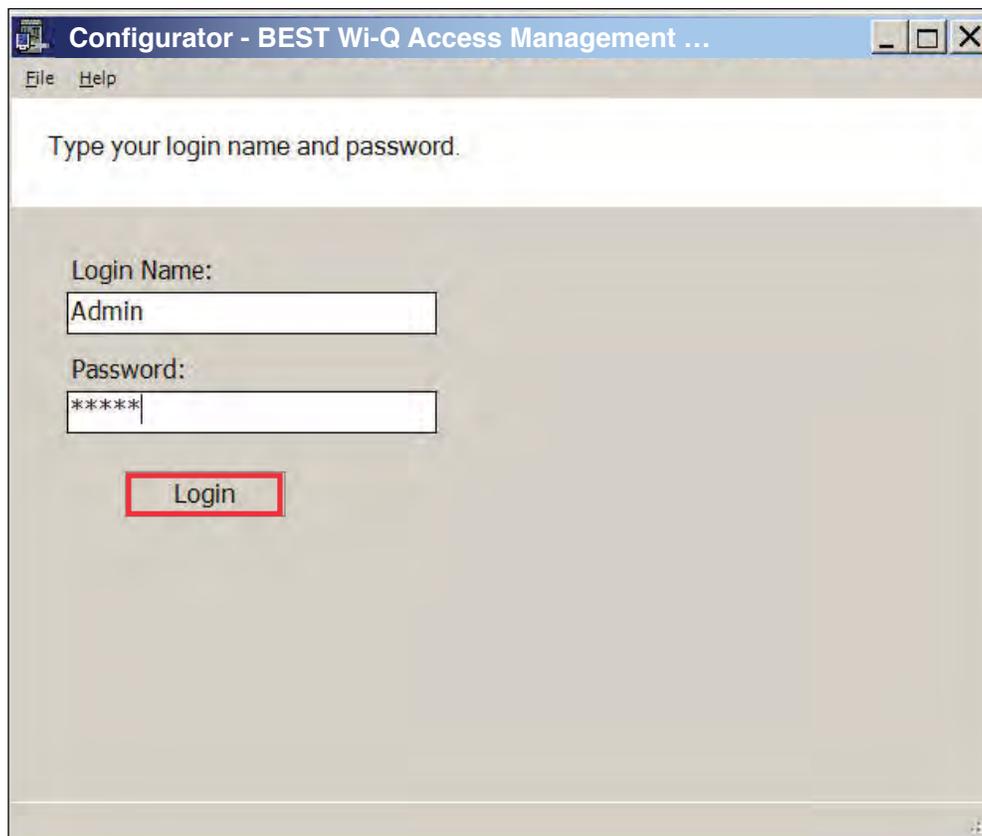
The following sections describe the essential functions you can perform using Configurator.

Launching Wi-Q AMS Configurator

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

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

Figure 119 Logging in to Configurator



If you are a AMS User, your System Administrator or IT representative must provide you a Login Name and Password. You will need this to login to the Configurator. If you are a System Administrator, see "Logging in to Configurator" on [page 65](#) for more information about launching the software for the first time.

To Login to the Wi-Q AMS Configurator:

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

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

Managing Application Users

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

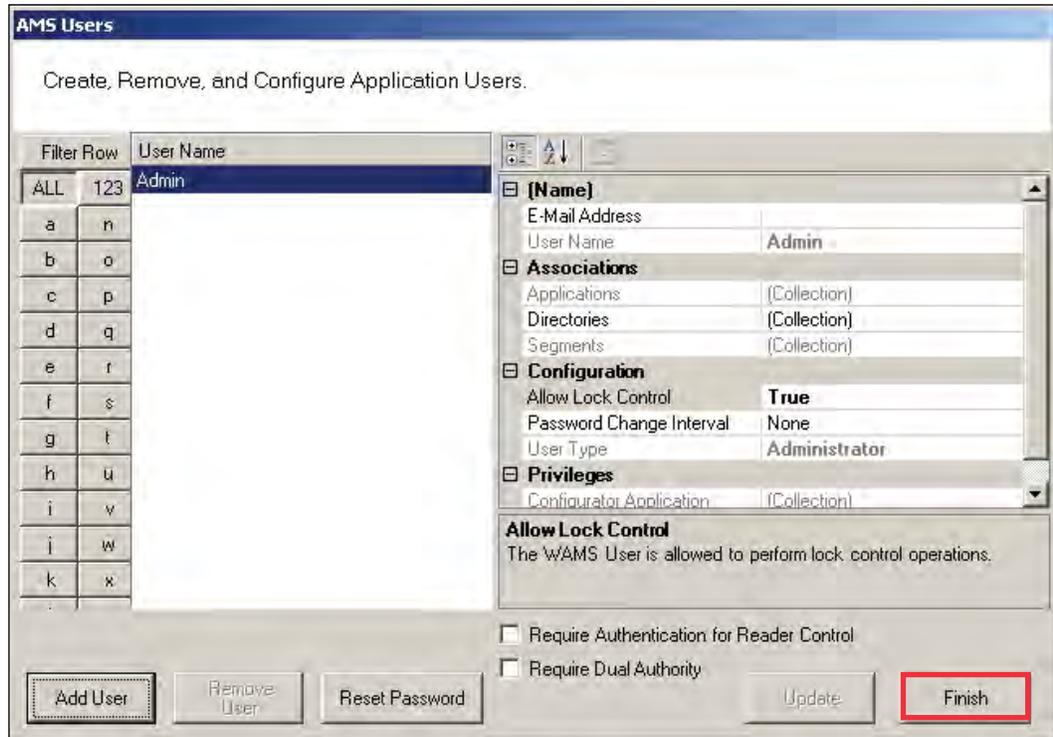
AMS Users must be added to the system as cardholders because they will require some type of physical access to the segment. However, they must also be assigned as AMSUsers and be given User names and Passwords if they are to access and operate application software.

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

To Manage Applications Users:

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

Figure 120 AMS Users



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

To add an AMS User:

- 1 In the AMS Users dialog box, click Add User. The system creates "User1" in the left column.
- 2 In the Name category on the right, enter an e-mail address (optional), and the user name.
- 3 Under Associations, click the Applications field, then click the ellipsis button at the far right.
- 4 Select which application(s) the User will have access to. Then click Finish.
- 5 In the Directories field, click the ellipsis button. Select the directories linked to the User. Then, click Finish.
- 6 In the Segments field, click the ellipsis button. Select which segments the User will have access to and supply contact information as needed.
- 7 Under the Configuration category, in the Allow Lock Control field, select either True or False from the drop-down list.

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

User Types

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

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

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

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

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

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

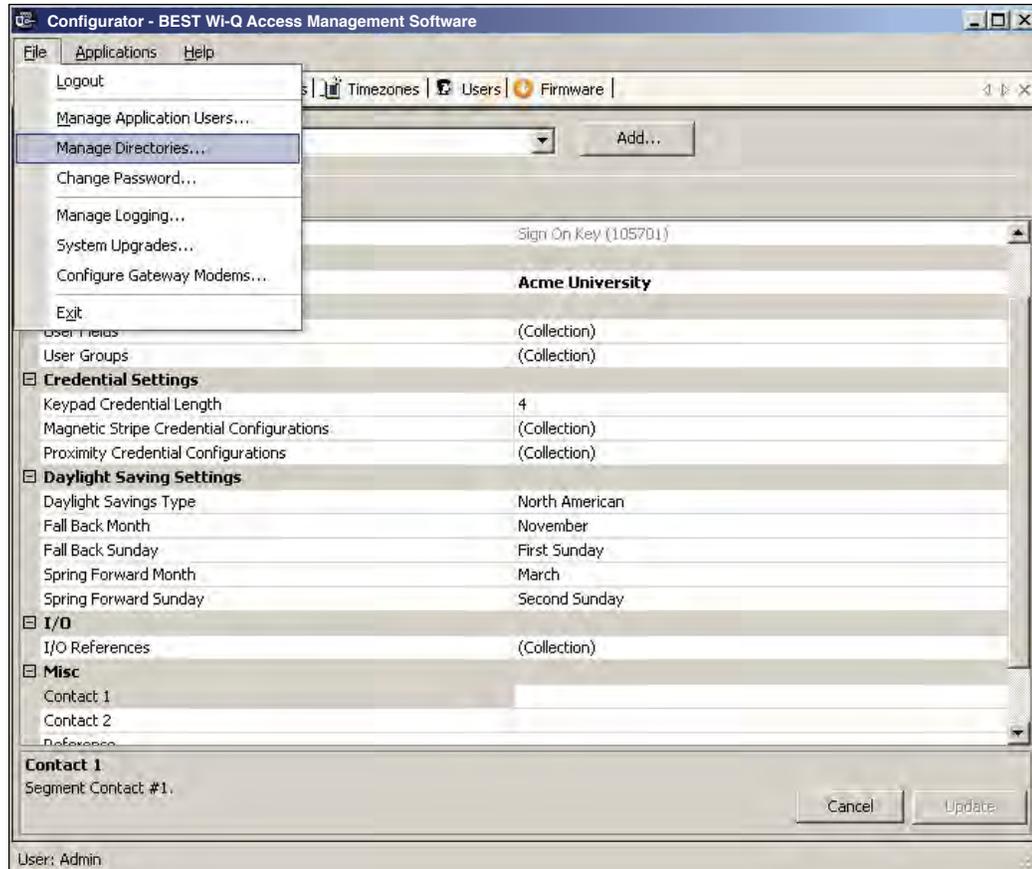
Linking AMS Users' Windows Accounts to Configurator

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

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

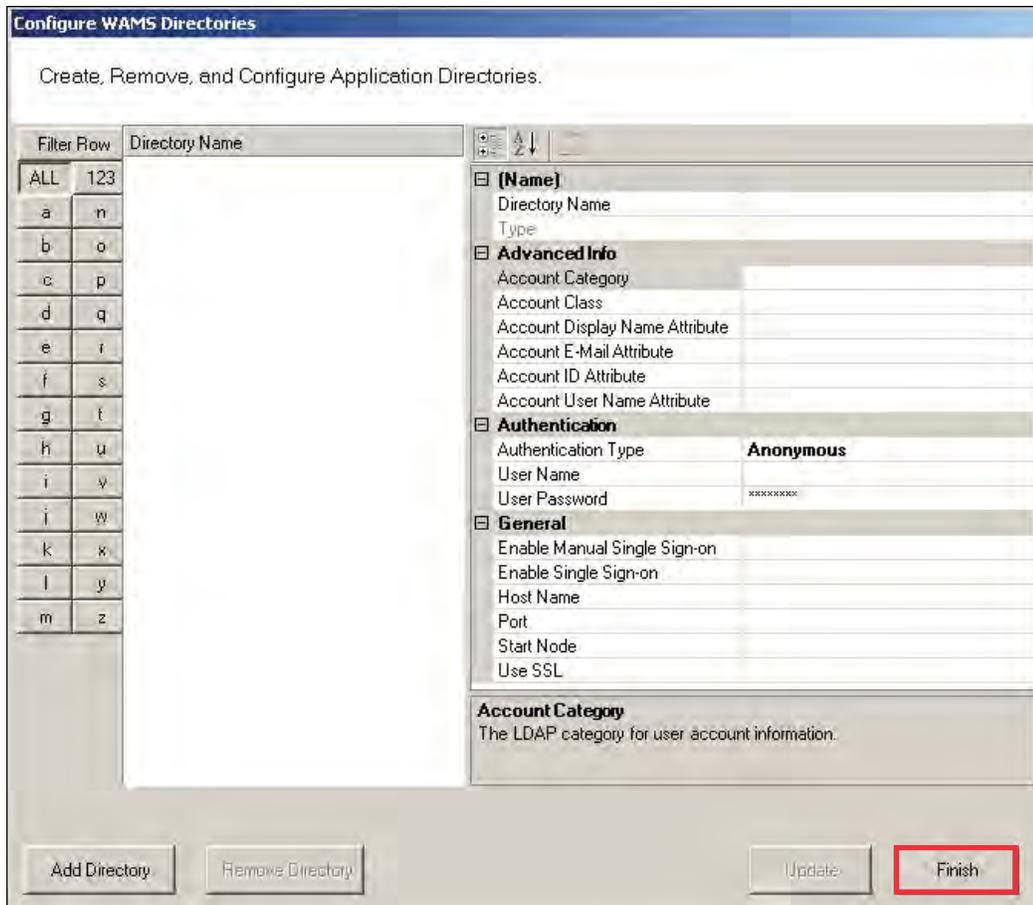
- 1 From the Configurator File menu, select Manage Directories.

Figure 121 Manage Directories



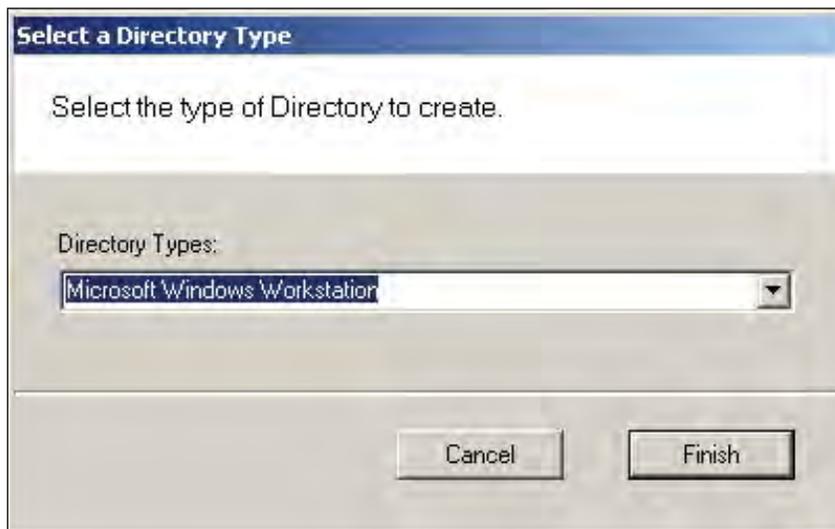
- 2 The Configure Directories dialog box opens. Click on Add Directory.

Figure 122 Configure Directories



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

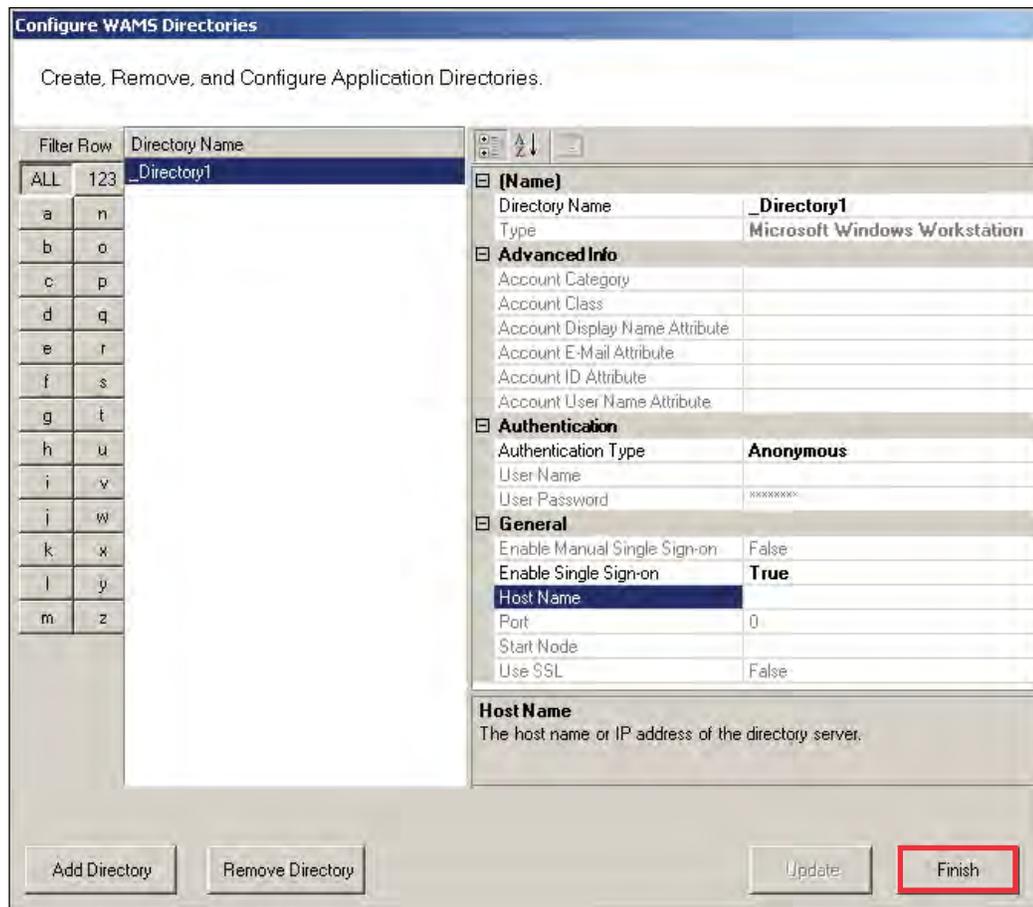
Figure 123 Select a Directory Type



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

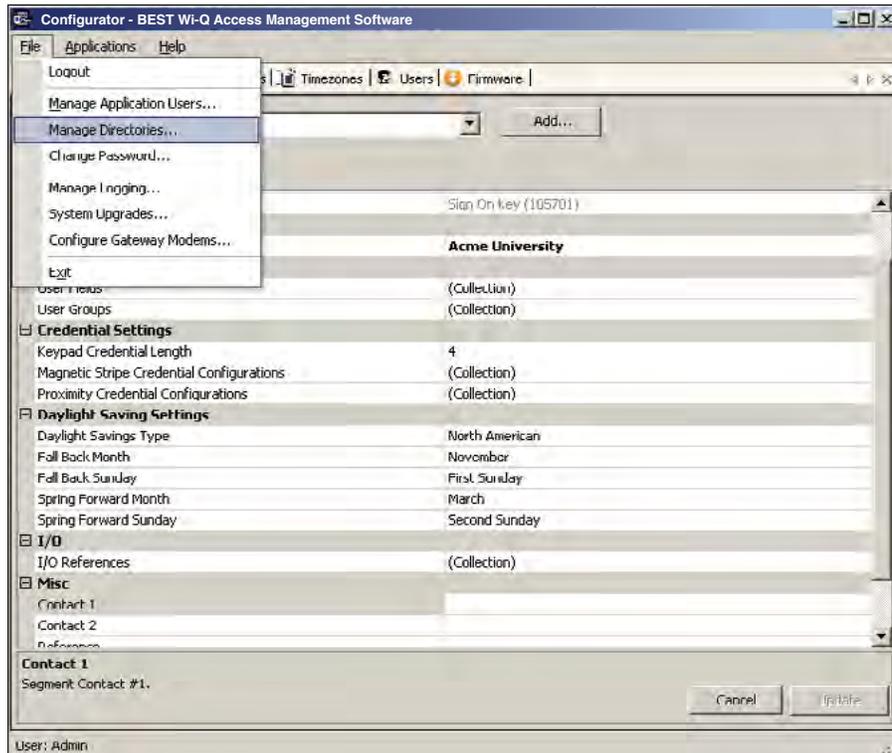
name. In the Host Name field, under the General category, type in the computer name of the host. Then, click Finish.

Figure 124 Directory and Host Names



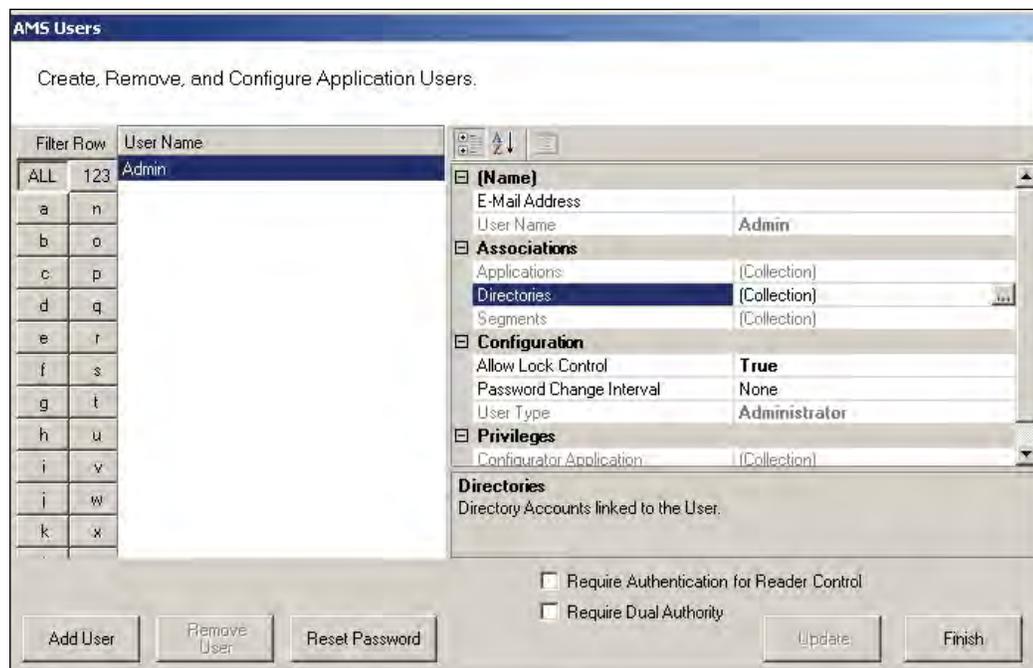
5 From the Configurator File menu, select Manage Application Users.

Figure 125 Manage Application Users



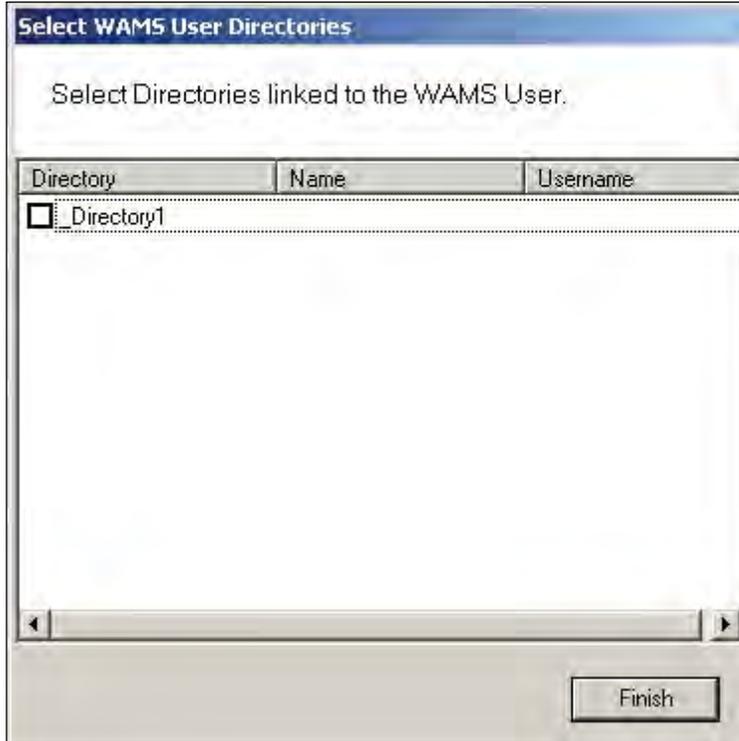
6 The AMS Users dialog box opens. Click in the Directories field, under the Associations column, and select the ellipsis button.

Figure 126 AMS Users



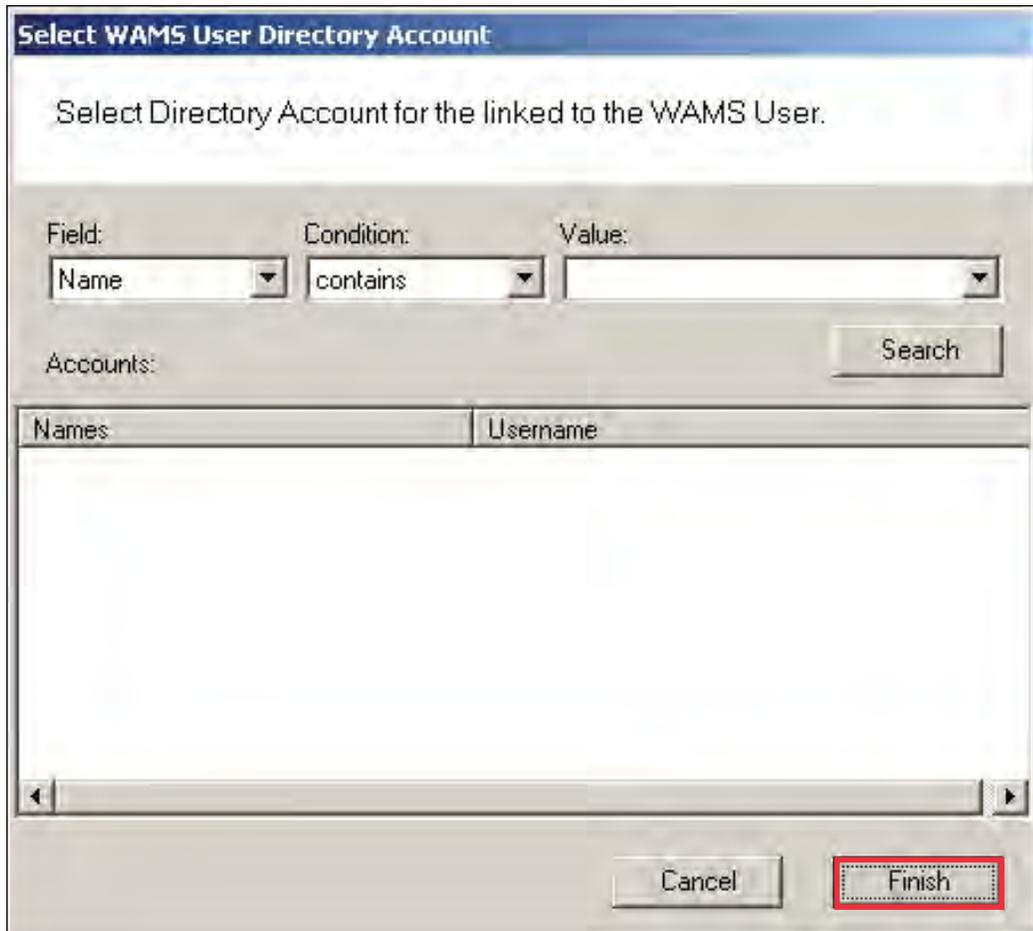
7 The Select User Directories window opens. Select the directory you created previously.

Figure 127 Select User Directories



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

Figure 128 Select User Directory Account



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

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

Configurator Overview

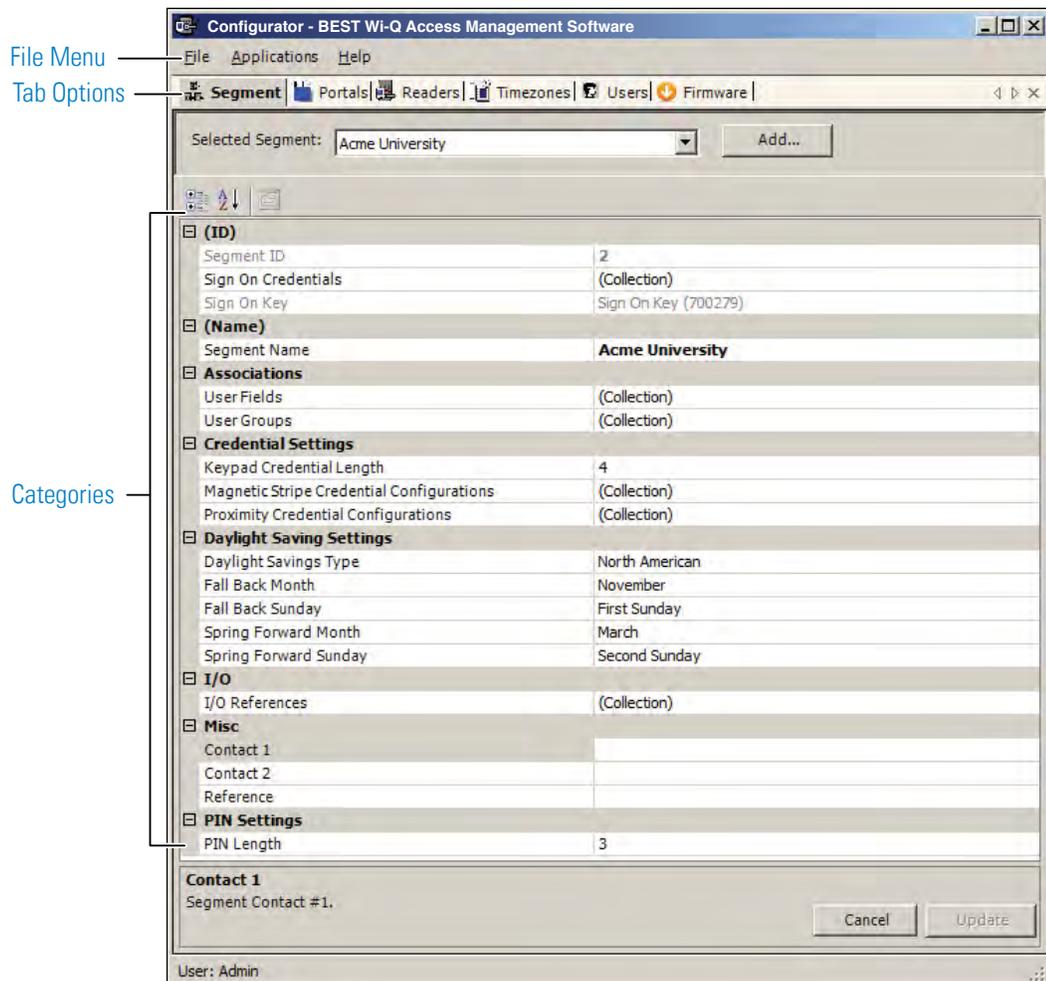
The following sections provide a brief overview of the Configurator module's Display and Tab options.

Display Options

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

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

Figure 129 Segment Tab



In the Segment and Users Tabs, you can display items by category or sort alphabetically. This is useful when displaying the Configurator in full-screen view. A number of global

operations are also available from the program File menu.

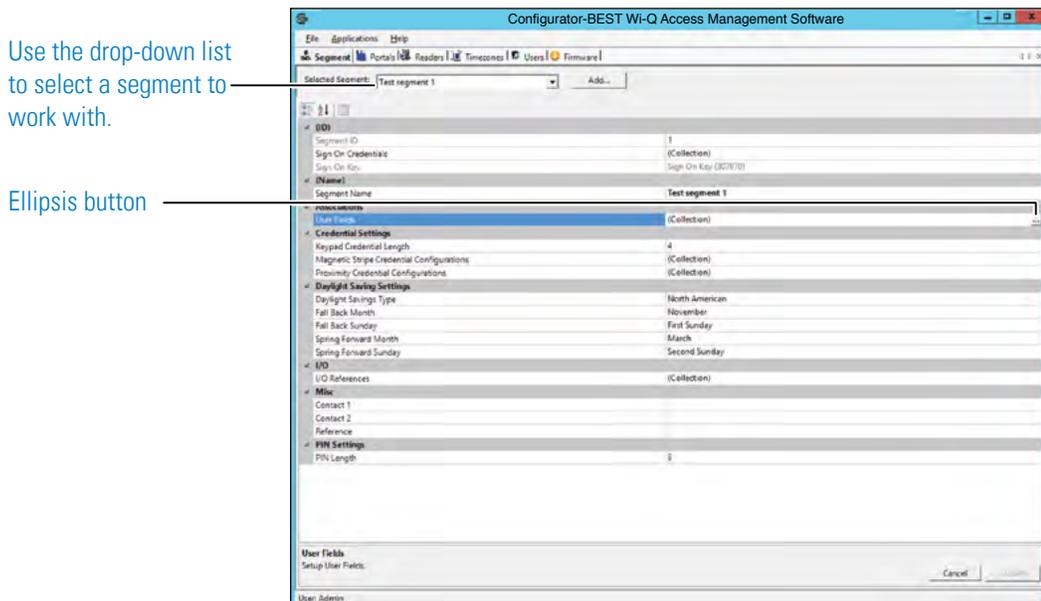
Segment Tab

Most Segment set up tasks are performed in the Segment Tab, [Figure 130](#). Here, the Program Administrator will create User Groups and configure the software to work with the type of segment access cards or keypad credentials you will use.

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

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

Figure 130 Segment Tab Categories

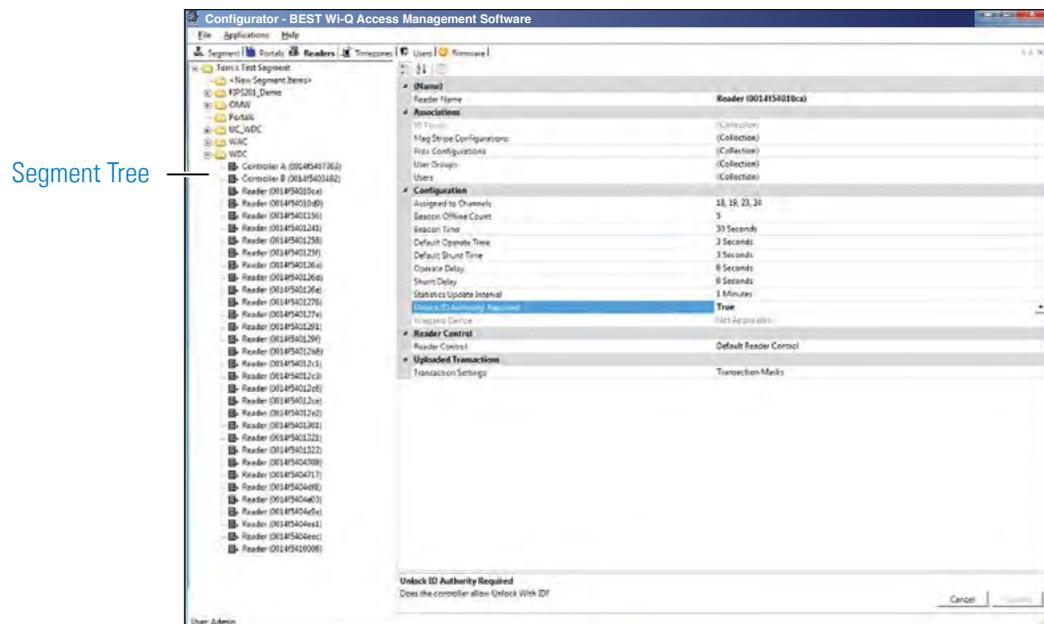


Portals and Readers Tabs

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

Information about creating the Segment Tree and assigning devices to the various folders in the tree is presented in Chapter 4, “Configuring Segments, Wi-Q Gateways and Controllers” . Typically, only the Program Administrator will perform tasks using the Readers Tab, [Figure 131](#).

Figure 131 Readers Tab



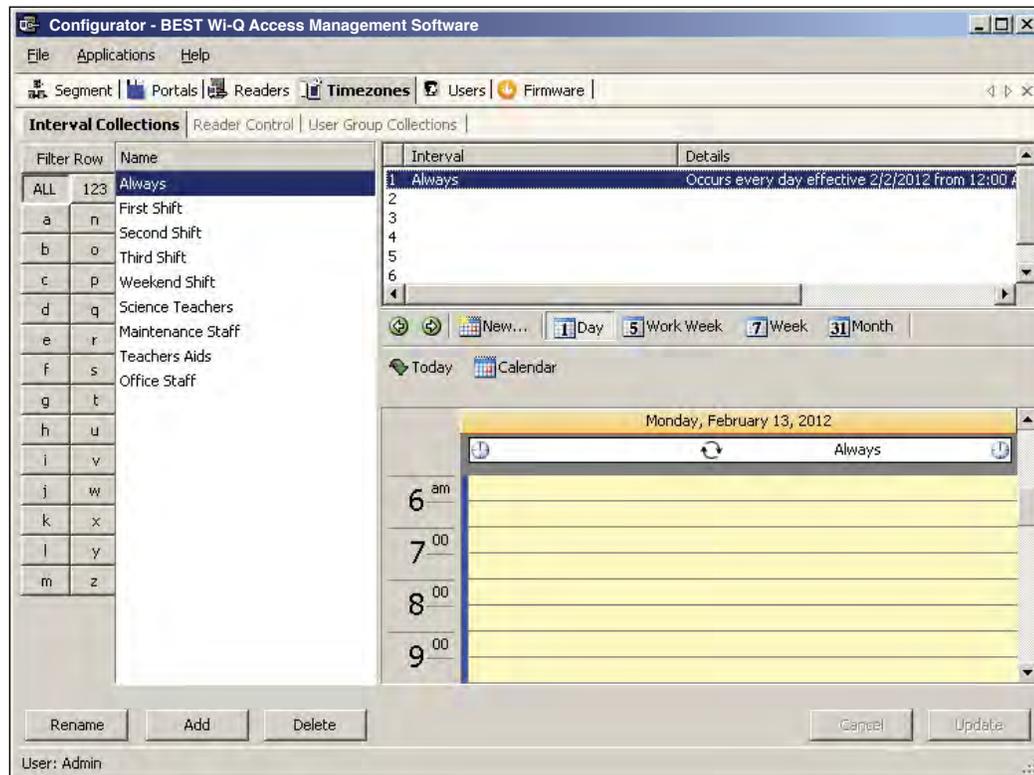
Timezones Tab

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

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

More information about creating Timezone Intervals and Timezone Groups is presented in later in Chapter 5, "Configure AMS Software (Task 11)" on [page 112](#).

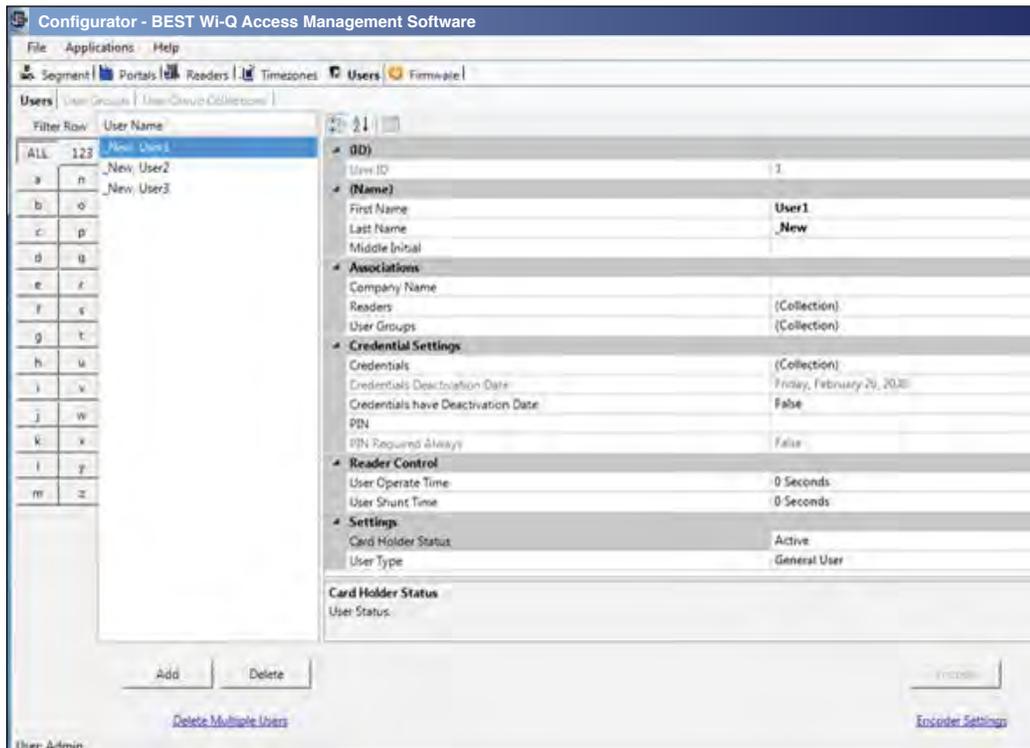
Figure 132 Setting up the Timezones



Users Tab

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

Figure 133 Users Tab



More information about adding users to the system is presented in Chapter 5, "Configure AMS Software (Task 11)" on [page 112](#).

Firmware Tab

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

System Overrides

Manager Override at Keypad Controller

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

Note MC refers to Manager Credential.

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

Programmer Override at Keypad Reader

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

Note PC refers to Programmer Credential.

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

Deep Reset

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

To Perform a Deep Reset from within Configurator

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

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

Segment Item Upgrades

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

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

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

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

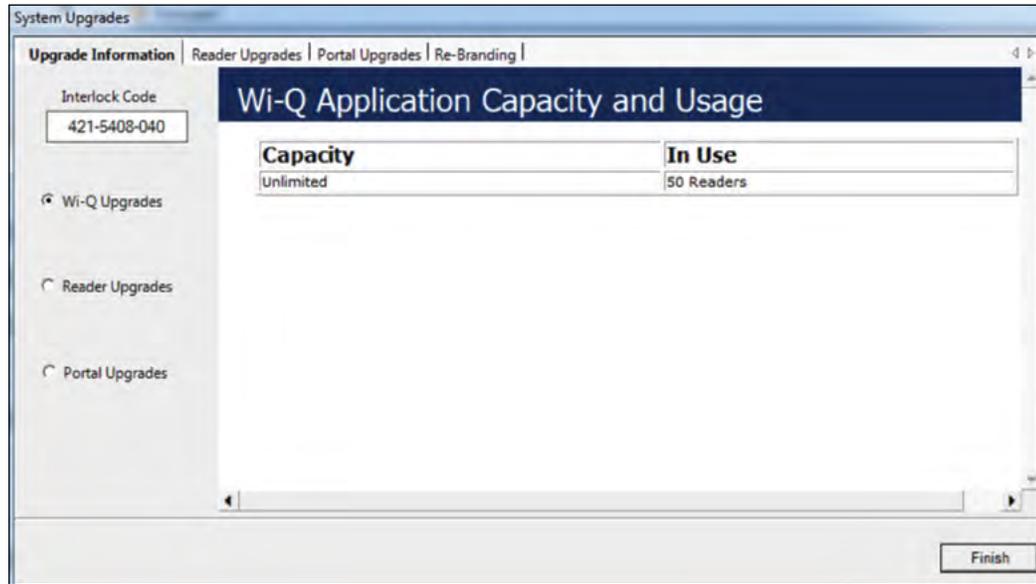
Determine Segment Reader and Portal Capacity

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

To view Wi-Q AMS and Omnilock Upgrade use

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

Figure 134 Upgrading your system capacity



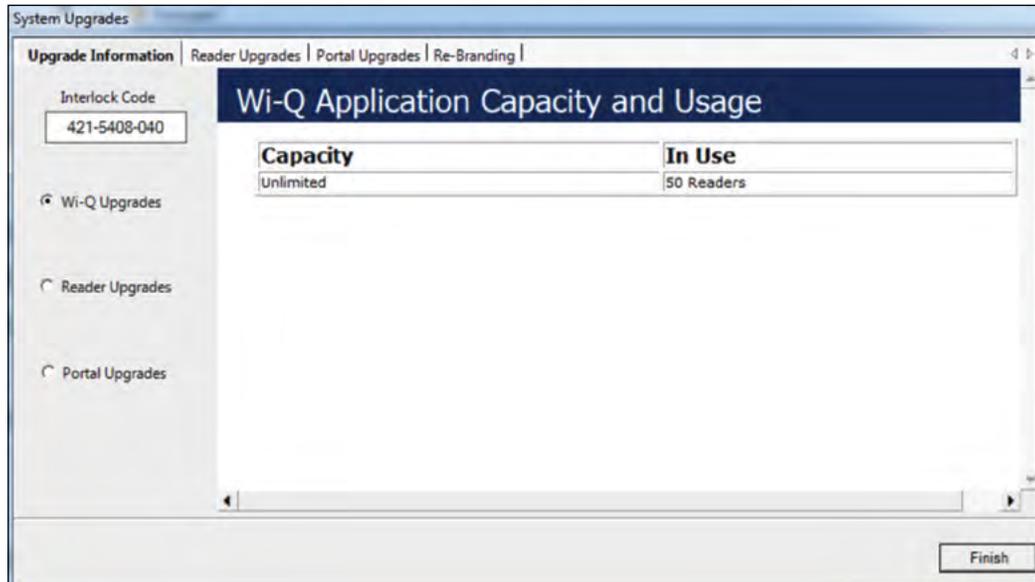
AMS Upgrades

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

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

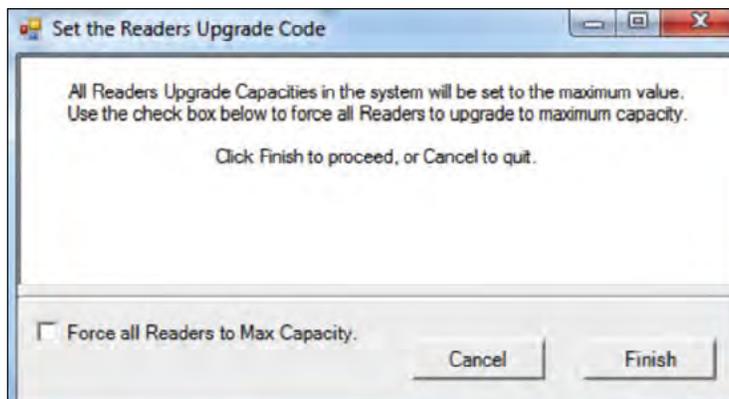
Reader Licenses in Use — With the Reader Upgrades radio button selected on the left, the property sheet displays the number of Licensed Upgrades in each user capacity value, and how many of those Licensed Upgrades are currently in use.

Figure 135 Upgrading your system capacity



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

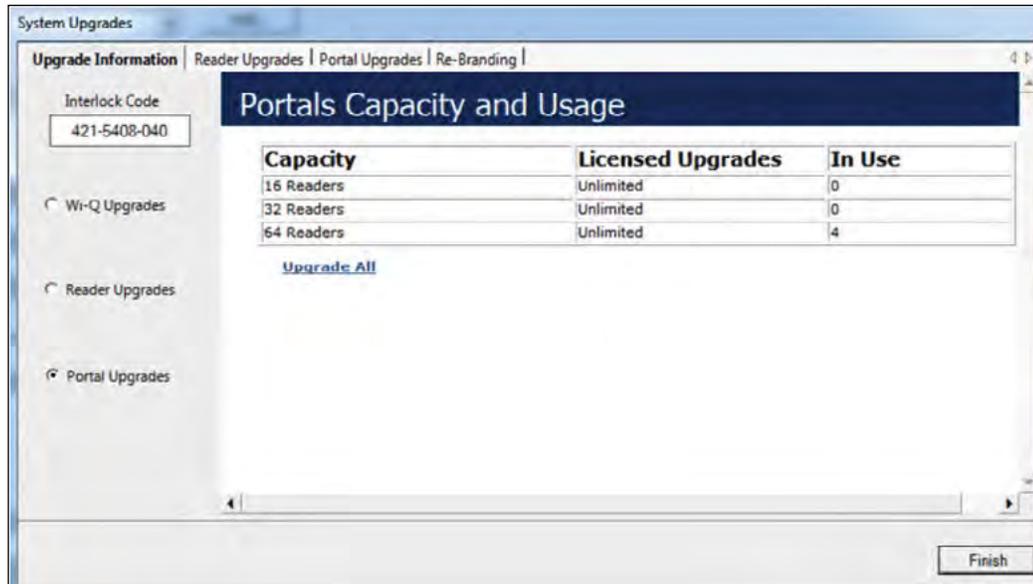
Figure 136 Set the Readers Upgrade Code



Select force all readers to max capacity and click finish.

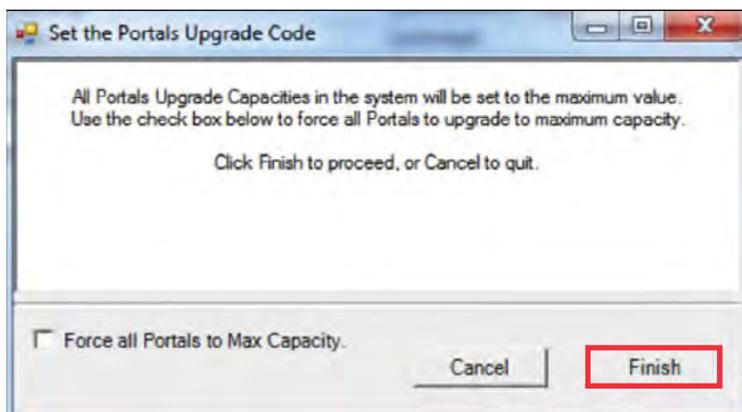
Portal Licenses in Use — With the Portal Upgrades radio button selected on the left, the property sheet displays the number of Licensed Upgrades in each reader capacity value, and how many of those Licensed Upgrades are currently in use.

Figure 137 Upgrading your system capacity



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

Figure 138 Upgrading your system capacity



Select force all portals to max capacity and click finish.

System Administrator

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

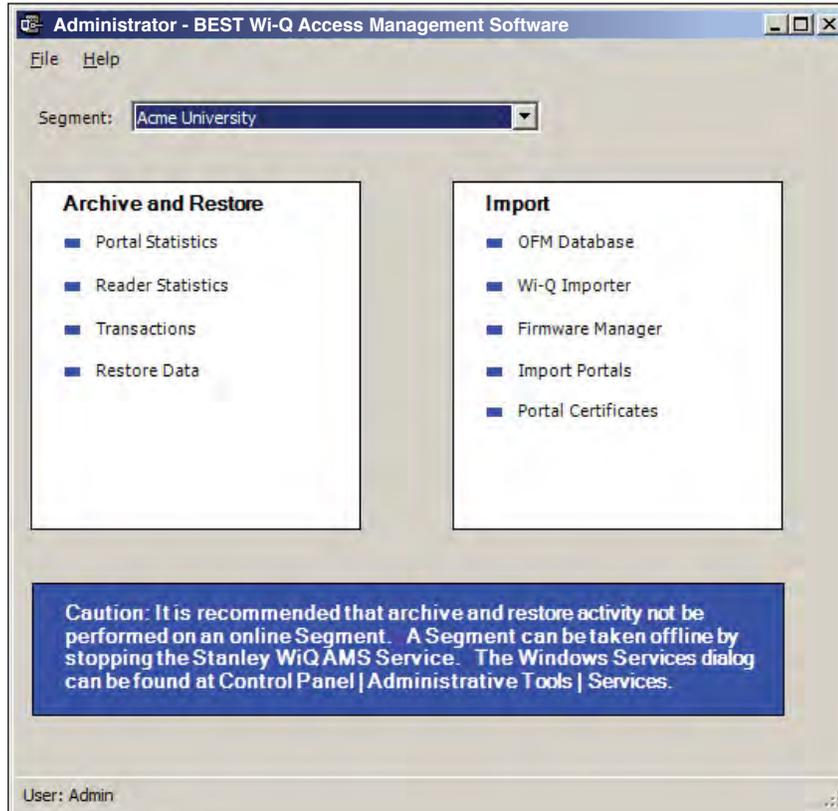
Note Archiving and restoring transactions and statistics is not the same as performing a full AMS database back up. Full back up and restore is performed using Microsoft SQL Server Management Studio Express (installed with AMS). Complete steps are described later in this chapter.

Establish an Archive Protocol

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

Using System Administrator

Figure 139 System Administrator



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

Archiving Statistics in the AMS Database

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

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

Once you've selected the Portal or reader to archive, you can also select what statistics to archive; for example, all statistics, only those statistics greater than a specific ID, or specify a range of statistics older than a specific date.

To Archive Statistics

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

Figure 140 Portal Statistics Archival for Segment

Portal Statistics Archival for Segment (Acme University)

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

Portal Selection

All Portals

Selected Portal GC2 (0014f5001605)

Statistics Selection

Archive All Statistics

Archive Statistics with IDs less than 1

Archive Statistics older than Monday, December 05, 2011

Archive Finish

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

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

Restoring Data to the Database

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

To Restore Data to AMS

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

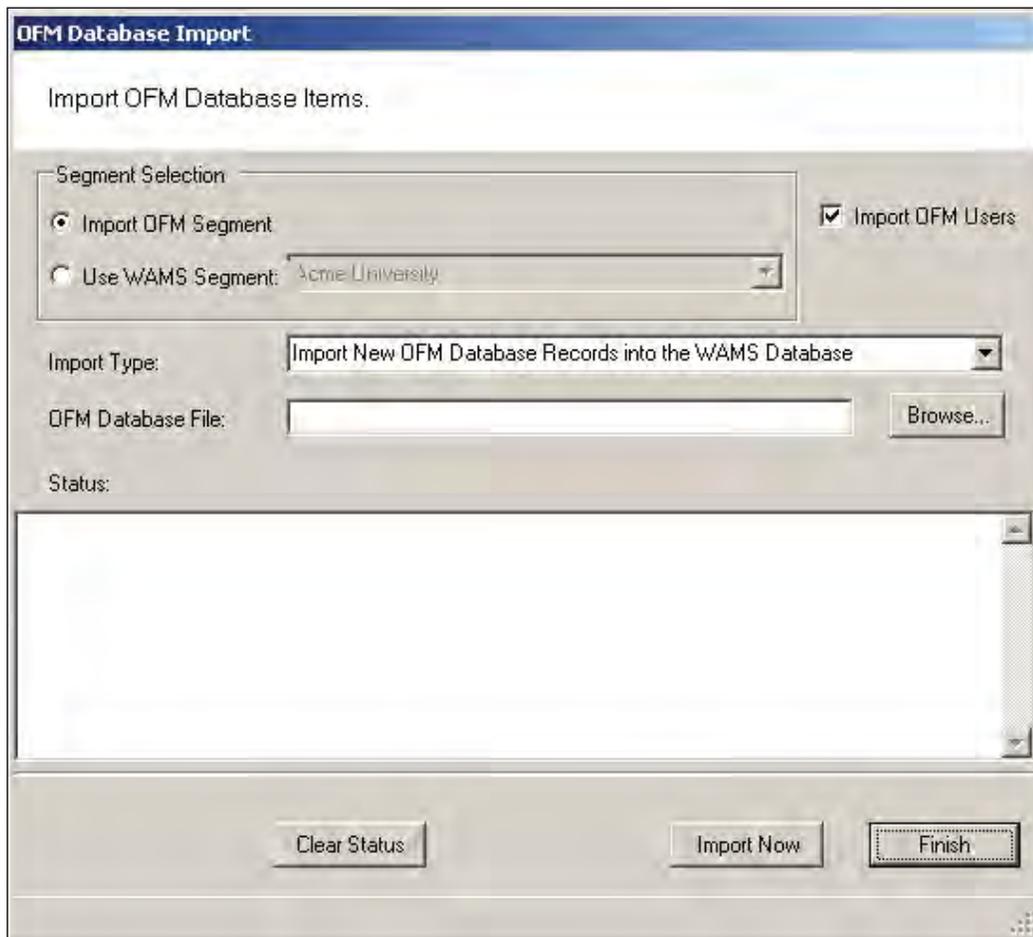
Importing Data from a Legacy OFM Database

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

To Import Data to AMS

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

Figure 141 OFM Database Import



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

Import Data from a Standard Comma-Delimited File

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

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

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

AMS Importer imports files in a few easy steps:

- Create the data file in the appropriate program, such as Microsoft Word, Excel, or other text-based program and save it as a .txt or .csv format.
- Prepare the Wi-Q AMS Import Utility to accept the file.
- Import the data.
- Send the Data to the database.

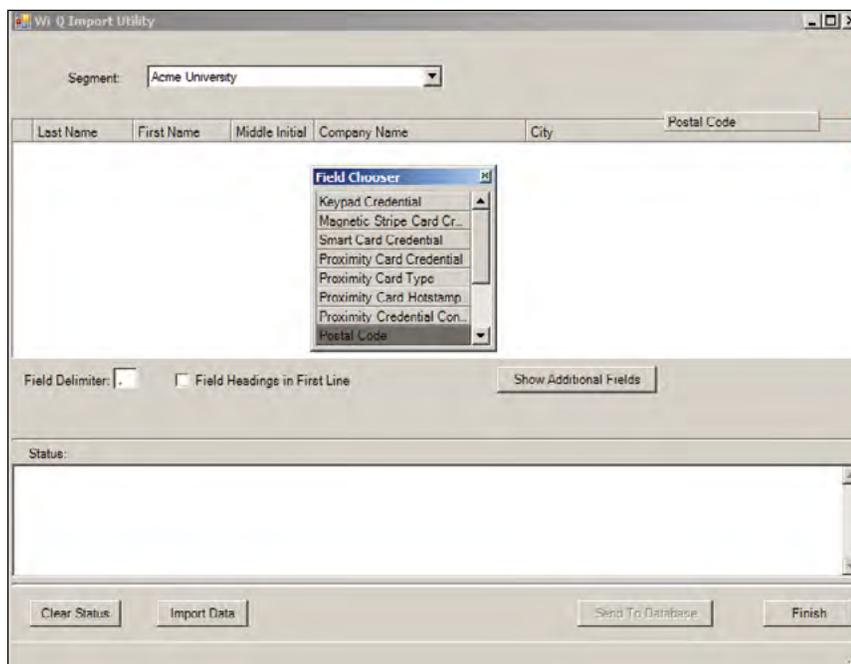
In the Import Utility, you can view the data as it imports into the window and make any corrections to the file or column headers until you are satisfied with the import before you actually send it to the database.

Detailed instructions are presented in the next few sections.

To prepare Wi-Q AMS Import Utility

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

Figure 142 Import Utility



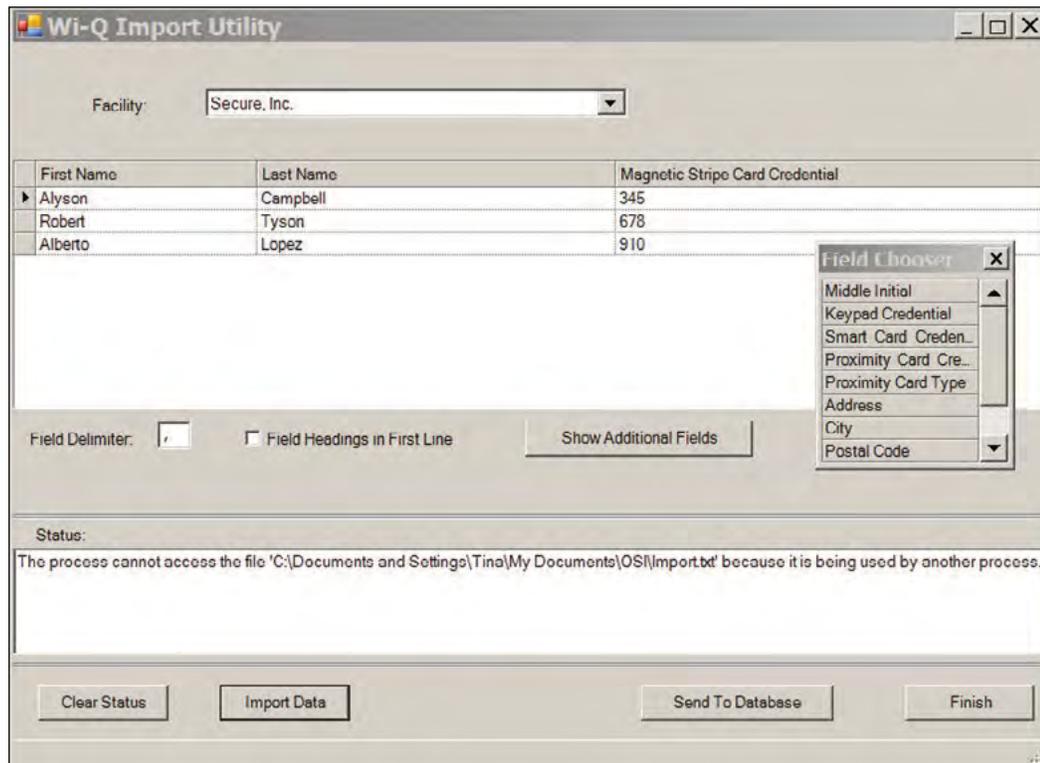
- 3 Use the cursor to drag the column headers into any order you wish.

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

To import the data

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

Figure 143 Using the Import Utility



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

Backing Up and Restoring Your AMS Database

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

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

Backing Up the Database

Perform the following steps to back up the database.

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

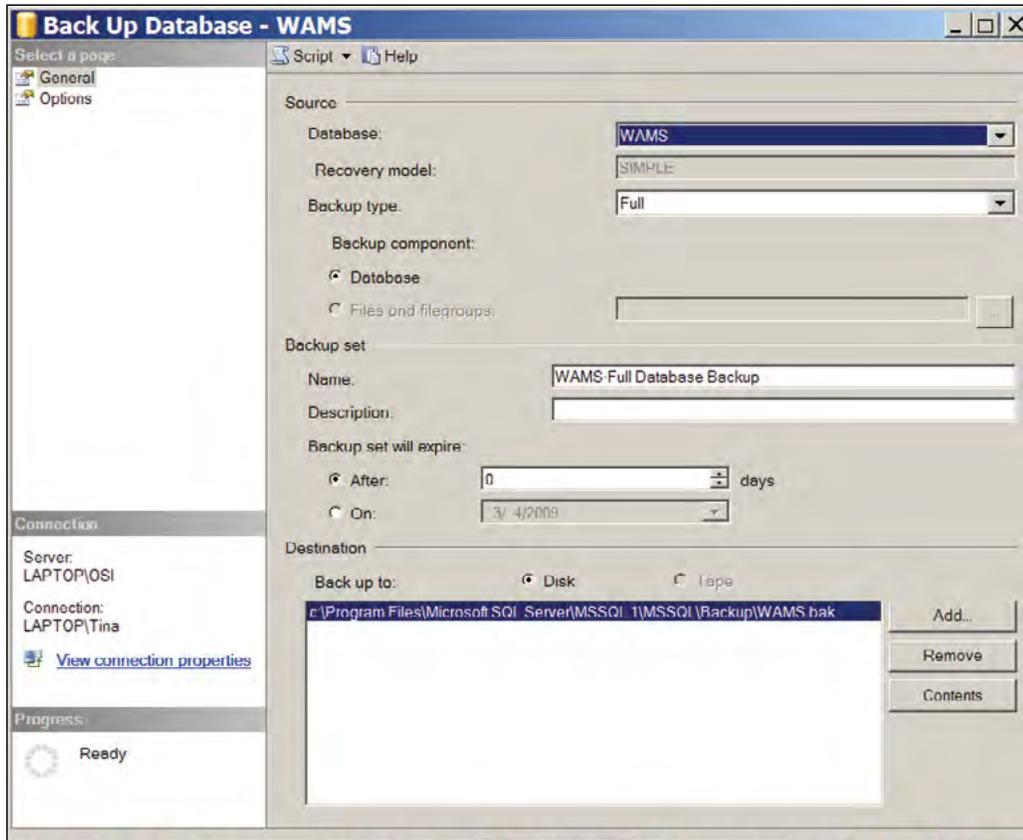
4 The program opens at the default database location.

Figure 144 Default database display in SQL Server



5 Double-click on databases, then right-click on the folder and select tasks>Backup. The backup database dialog box opens.

Figure 145 Backup Database



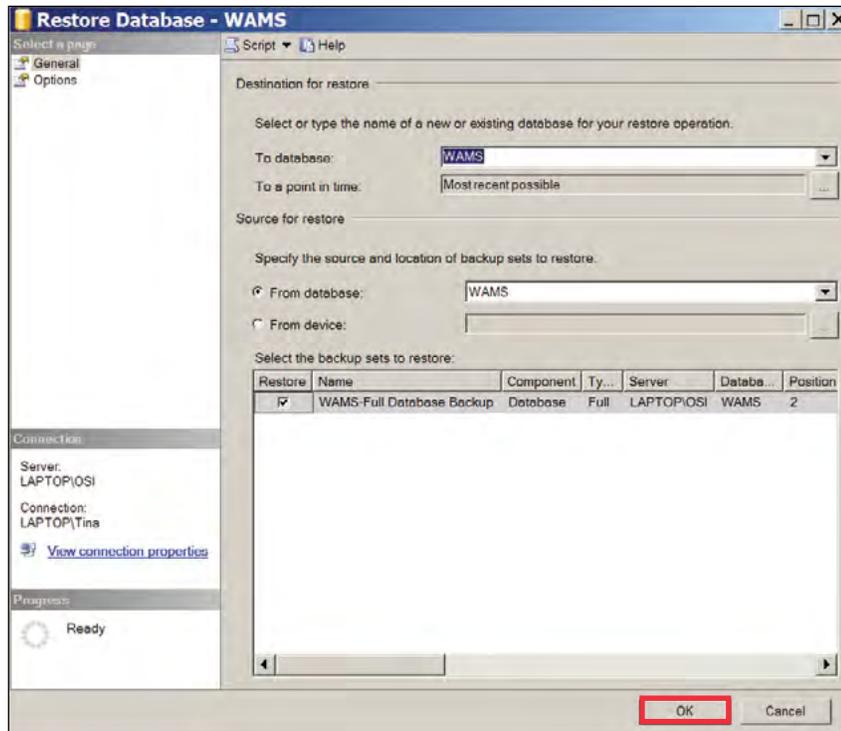
- 6 Define a Backup Type (full or differential) and add a description of the backup (optional).
- 7 The default destination displays. You can change the destination, if needed, for example if you wish to move the database to a new location on a different computer.
- 8 Click OK. The backup progresses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

To Restore the database

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

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

Figure 146 Restore Database



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

Firmware Updates

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

Firmware File Types

Every Controller has two firmware files:

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

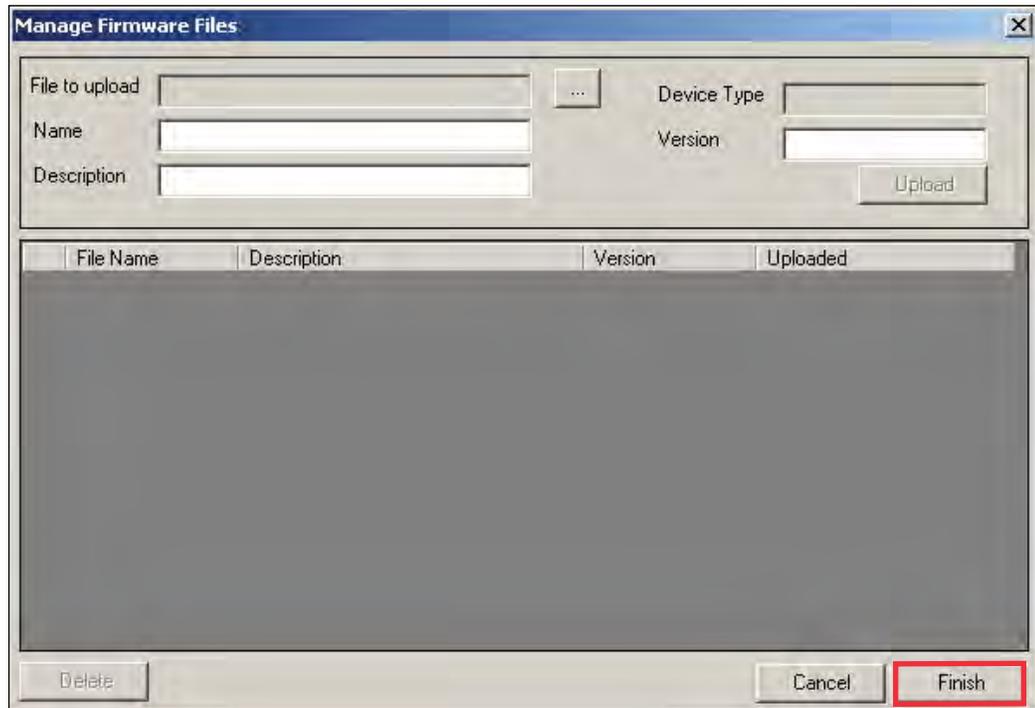
The application file is what is typically reprogrammed by the BEST Team, but it is possible that the bootloader file will require reprogramming as well. Controller firmware files will always have a ".bin" file extension.

For Wi-Q Gateways, only one file is required for reprogramming, and the file name begins with the version number and ends with ".image.bin.gz".

Uploading Firmware Files

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

Figure 147 Manage Firmware Files



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

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

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

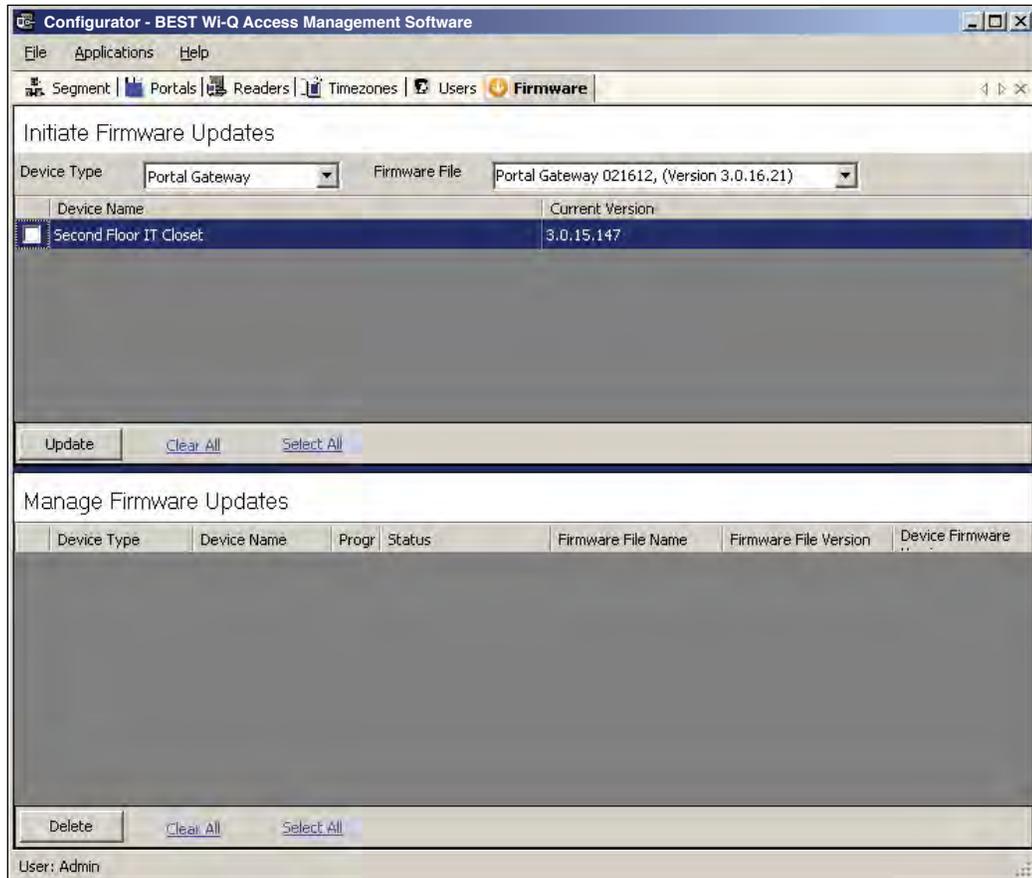
You are now ready to send the updates to your hardware.

Firmware Reprogram

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

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

Figure 148 Configurator Firmware Tab



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

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

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

Transactions Monitor

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

To Launch Transactions

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

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

Transactions Overview

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

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

Transactions Tab

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

Figure 149 Transactions

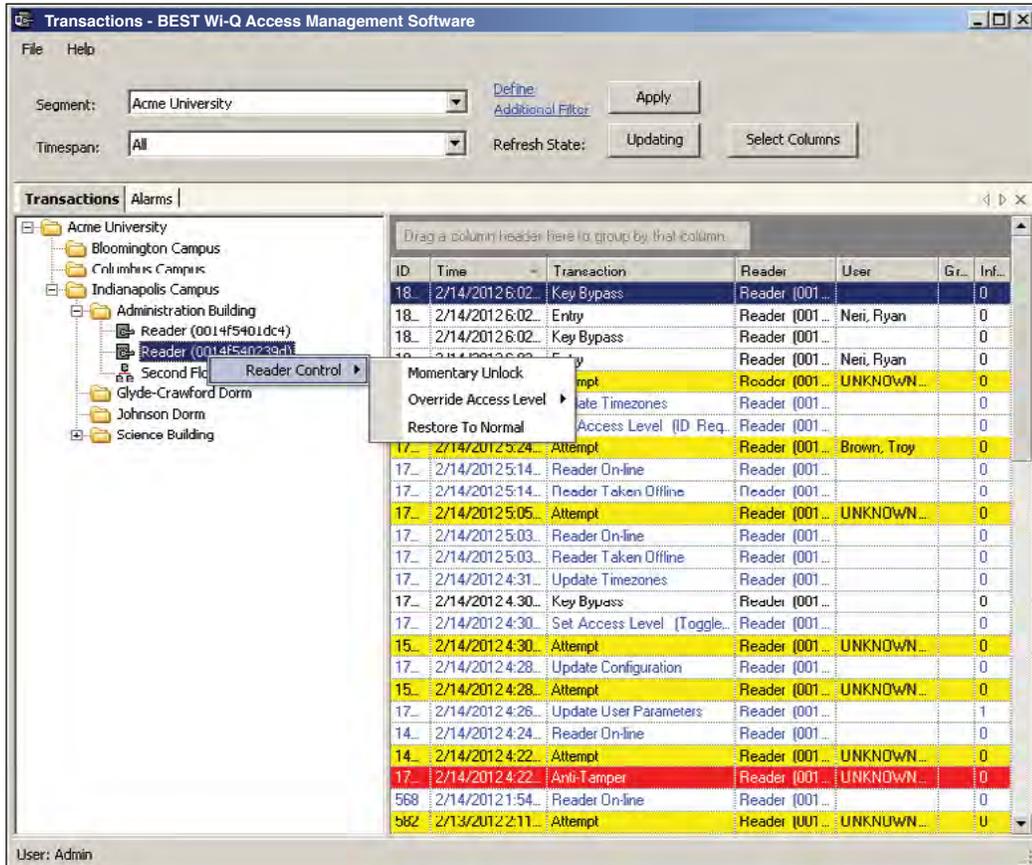
ID	Time	Transaction	Reader	User	Group	Info
18083	2/14/2012 6:02:25 PM	Key Bypass	Reader (0014f54023...			0
18080	2/14/2012 6:02:21 PM	Entry	Reader (0014f54023...	Neil, Ryan		0
18079	2/14/2012 6:02:10 PM	Key Bypass	Reader (0014f54023...			0
18078	2/14/2012 6:02:06 PM	Entry	Reader (0014f54023...	Neil, Ryan		0
18077	2/14/2012 6:02:04 PM	Attempt	Reader (0014f54023...	UNKNOWN <Keypad...		0
18060	2/14/2012 6:01:34 PM	Update Timezones	Reader (0014f54023...			0
18070	2/14/2012 6:01:34 PM	Set Access Level (ID Required)	Reader (0014f54023...			0
17956	2/14/2012 5:24:09 PM	Attempt	Reader (0014f54023...	Brown, Troy		0
17916	2/14/2012 5:14:39 PM	Reader On line	Reader (0014f54023...			0
17911	2/14/2012 5:14:22 PM	Reader Taken Offline	Reader (0014f54023...			0
17874	2/14/2012 5:05:38 PM	Attempt	Reader (0014f54023...	UNKNOWN <Keypad...		0
17869	2/14/2012 5:03:57 PM	Reader On line	Reader (0014f54023...			0
17854	2/14/2012 5:03:42 PM	Reader Taken Offline	Reader (0014f54023...			0
17786	2/14/2012 4:31:00 PM	Update Timezones	Reader (0014f54023...			0
17765	2/14/2012 4:30:59 PM	Key Bypass	Reader (0014f54023...			0
17767	2/14/2012 4:30:58 PM	Set Access Level (Toggle Entry (PIN Re...	Reader (0014f54023...			0
15306	2/14/2012 4:30:57 PM	Attempt	Reader (0014f54023...	UNKNOWN <Keypad...		0
17755	2/14/2012 4:28:11 PM	Update Configuration	Reader (0014f54023...			0
18026	2/14/2012 4:28:09 PM	Attempt	Reader (0014f54023...	UNKNOWN <Keypad...		0
17751	2/14/2012 4:26:40 PM	Update User Parameters	Reader (0014f54023...			1
14522	2/14/2012 4:24:38 PM	Reader On line	Reader (0014f54023...			0
14526	2/14/2012 4:22:34 PM	Attempt	Reader (0014f54023...	UNKNOWN <Keypad...		0
17742	2/14/2012 4:22:34 PM	Anti Tamper	Reader (0014f54023...	UNKNOWN <Keypad...		0
580	2/14/2012 1:54:21 PM	Reader On line	Reader (0014f54023...			0
582	2/13/2012 2:11:22 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
581	2/13/2012 2:11:14 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
580	2/13/2012 2:11:05 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
579	2/13/2012 2:10:38 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
578	2/13/2012 2:10:32 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
577	2/13/2012 2:06:08 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
14507	2/13/2012 2:06:01 PM	Anti Tamper	Reader (0014f54023...	UNKNOWN <Proxi...		0
576	2/13/2012 2:06:02 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
575	2/13/2012 2:05:55 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0
574	2/13/2012 2:05:42 PM	Attempt	Reader (0014f54023...	UNKNOWN <Proxi...		0

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

Reader and Portal Controls

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

Figure 150 Accessing Portals and Readers in the Transactions tab

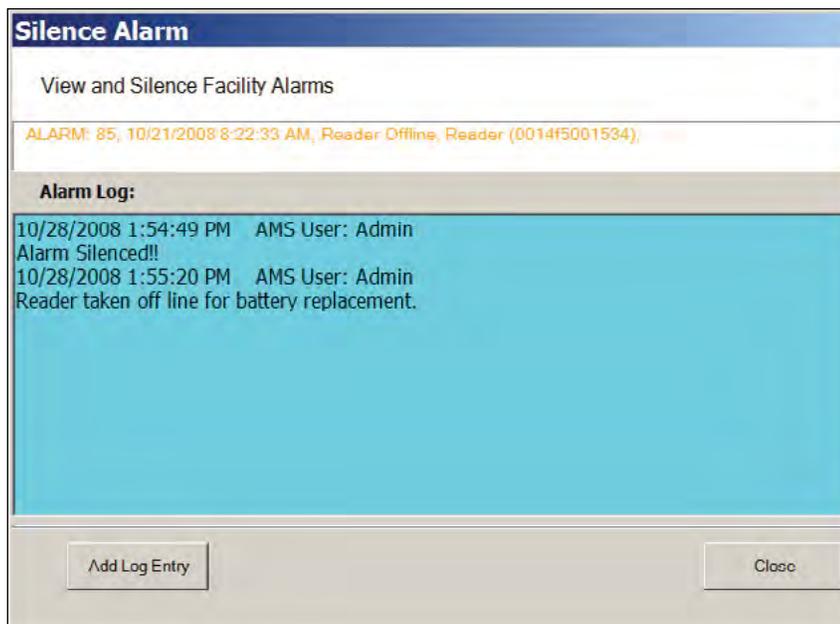


Alarms Tab

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

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

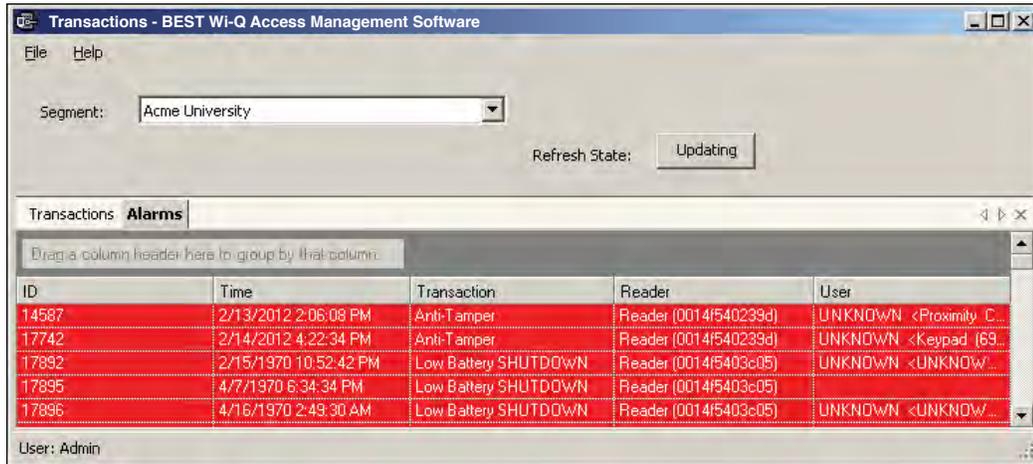
Figure 151 Silencing an alarm in the Alarms tab



Create an Alarm Response Protocol

Remember, when you “Silence” an alarm in Wi-Q AMS Transactions, you are only silencing a .wav file; you are not resolving the problem. It is important to establish Alarm Response protocols within your segment and follow up with action. [See “Responding to Alarms” on page 206.](#)

Figure 152 Alarms Tab



ID	Time	Transaction	Reader	User
14587	2/13/2012 2:06:08 PM	Anti-Tamper	Reader (0014f540239d)	UNKNOWN <Proximity C...
17742	2/14/2012 4:22:34 PM	Anti-Tamper	Reader (0014f540239d)	UNKNOWN <Keypad (69...
17892	2/15/1970 10:52:42 PM	Low Battery SHUTDOWN	Reader (0014f5403e05)	UNKNOWN <UNKNOWN...
17895	4/7/1970 6:34:34 PM	Low Battery SHUTDOWN	Reader (0014f5403e05)	
17896	4/16/1970 2:49:30 AM	Low Battery SHUTDOWN	Reader (0014f5403e05)	UNKNOWN <UNKNOWN...

Transaction Types

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

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

Organizing and Sorting Transactions

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

Display by Timespan

By default, Transactions displays all transactions in the order they occur. If you are monitor-

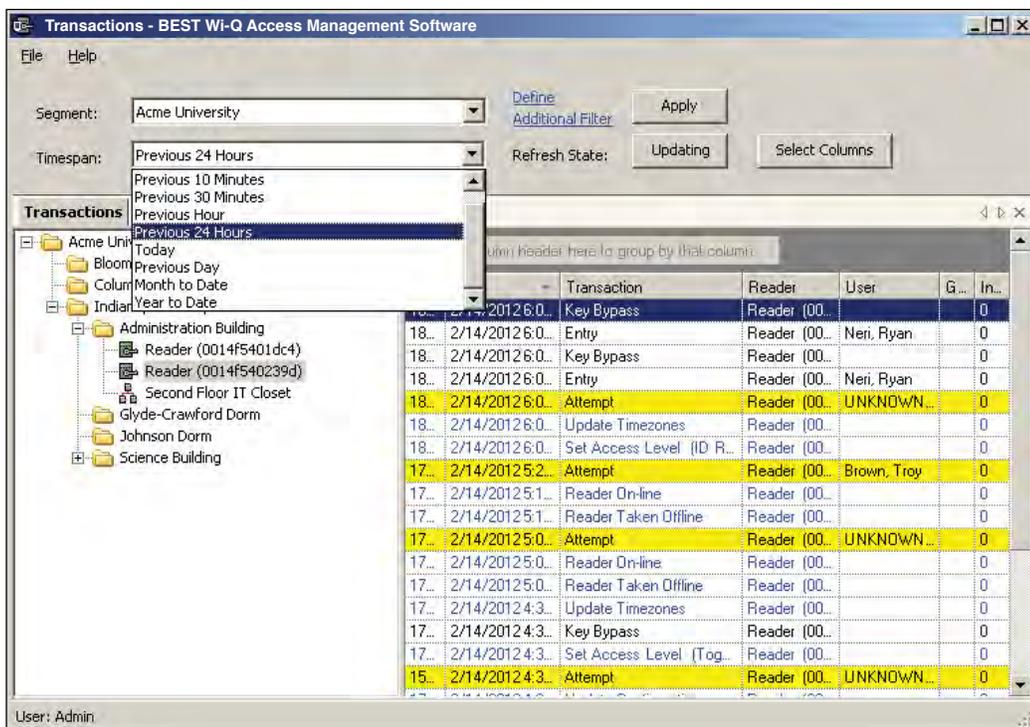
ing all transactions, you may want to simply watch them as they occur. However, in large systems, your effort may best be served by limiting transactions to only those that have occurred in the previous ten minutes, or previous hour. The software gives you a number of options from All to year to date.

To set the display timespan

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

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

Figure 153 Transactions Timespan



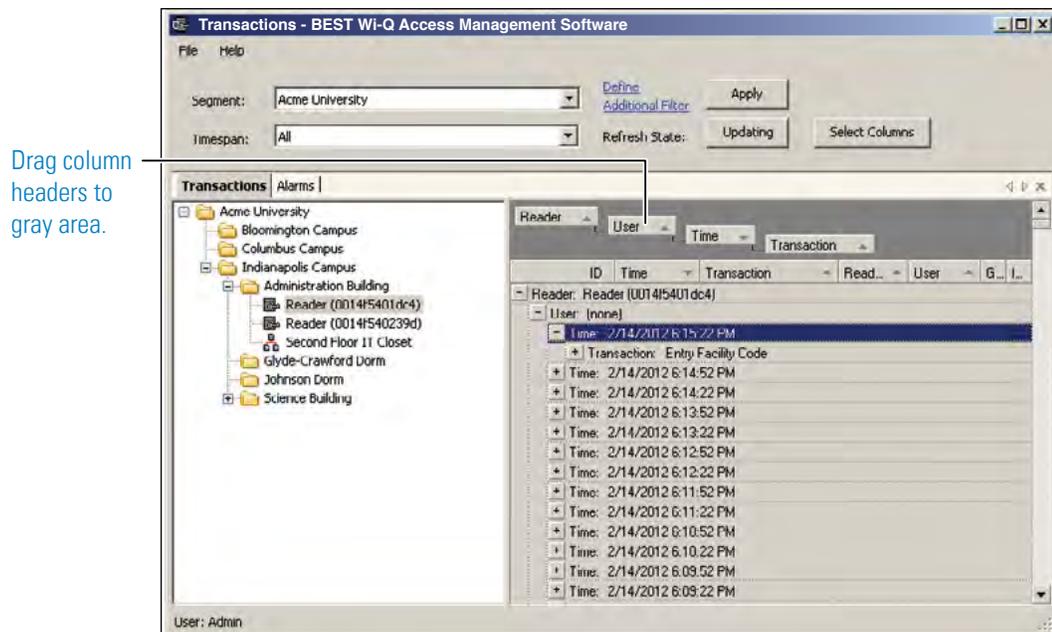
Sort by Column Header

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

View Transactions in Tree Levels

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

Figure 154 Transactions in Tree Levels

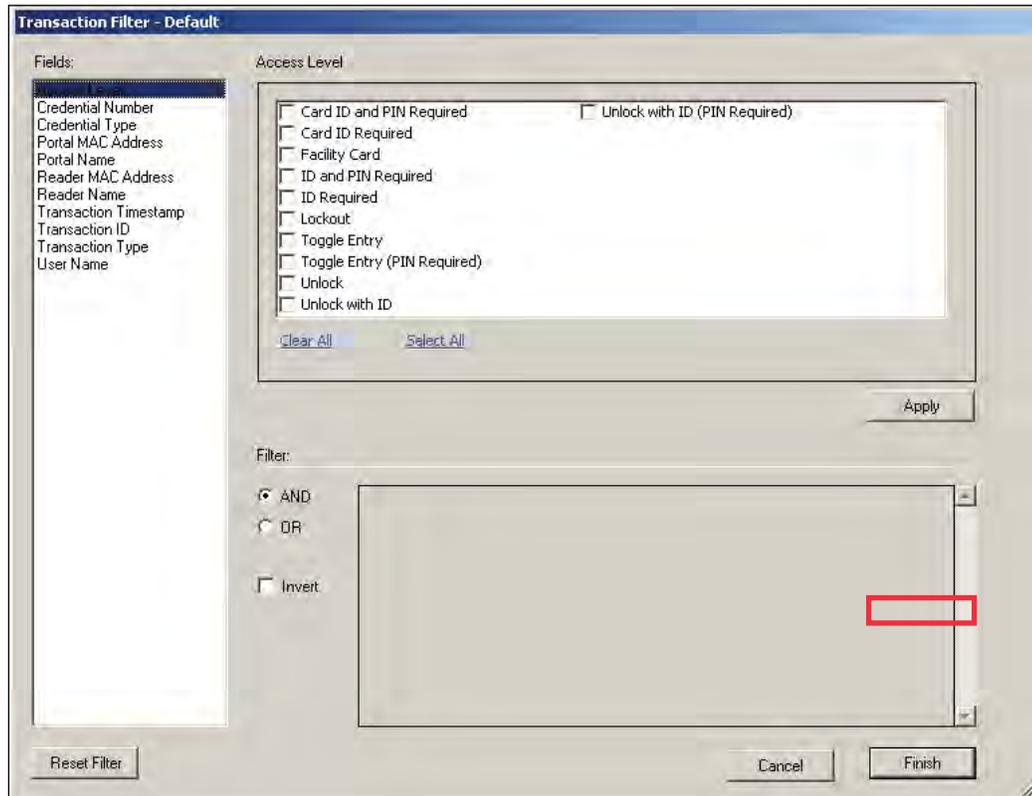


In this example, we placed Readers at the top of the tree; however, you can place them in any hierarchy you wish. When you select the plus sign next to the top level, the second and third level items expand to display. It's easy to create a Transactions Tree: simply drag and drop the column headers into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

Transaction Filters

If you want to search for a specific transaction by certain criteria (user name, reader name, etc.), click on Define Additional Filter at the top of the Transactions module. The Transaction Filter dialog box will open.

Figure 155 Transaction Filters



A list of fields is located on the left side of the dialog box. Clicking on a field will bring up checkbox or dropdown options specific to the selected field. In [Figure 155](#), the Access Level field is selected. Here, you can check multiple options. Once you've selected your options, click Apply. The Filter section at the bottom of the dialog box will reflect what filter you've applied.

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

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

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

Responding to Alarms

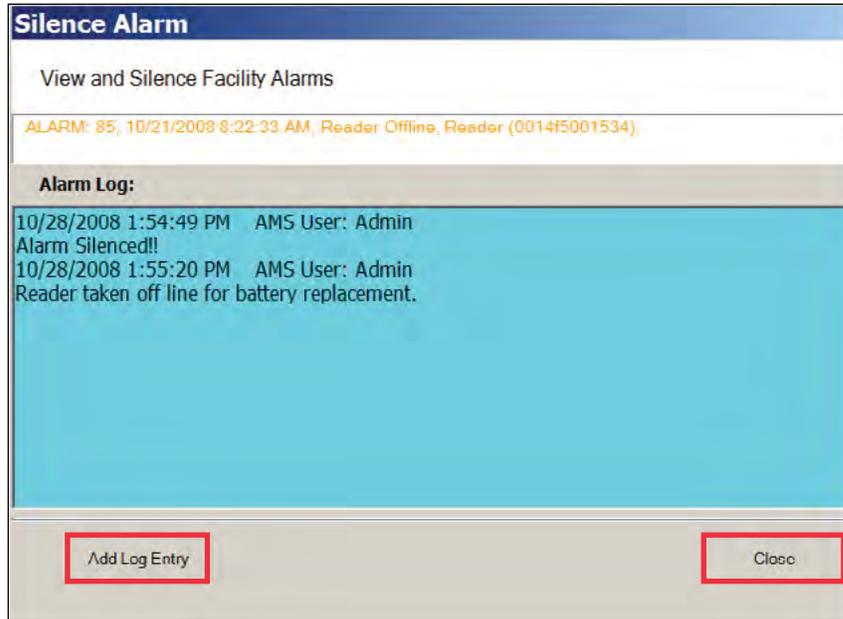
When an alarm occurs, the system immediately displays it in red in the Transactions Tab. The alarm will be categorized as either an Anti-Tamper or a Forced Entry type. At this point, you will take action according to your segment's security plan. In a small segment, you may simply dispatch a person to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

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

To respond to and silence an alarm

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

Figure 156 Log Entry Recorded



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

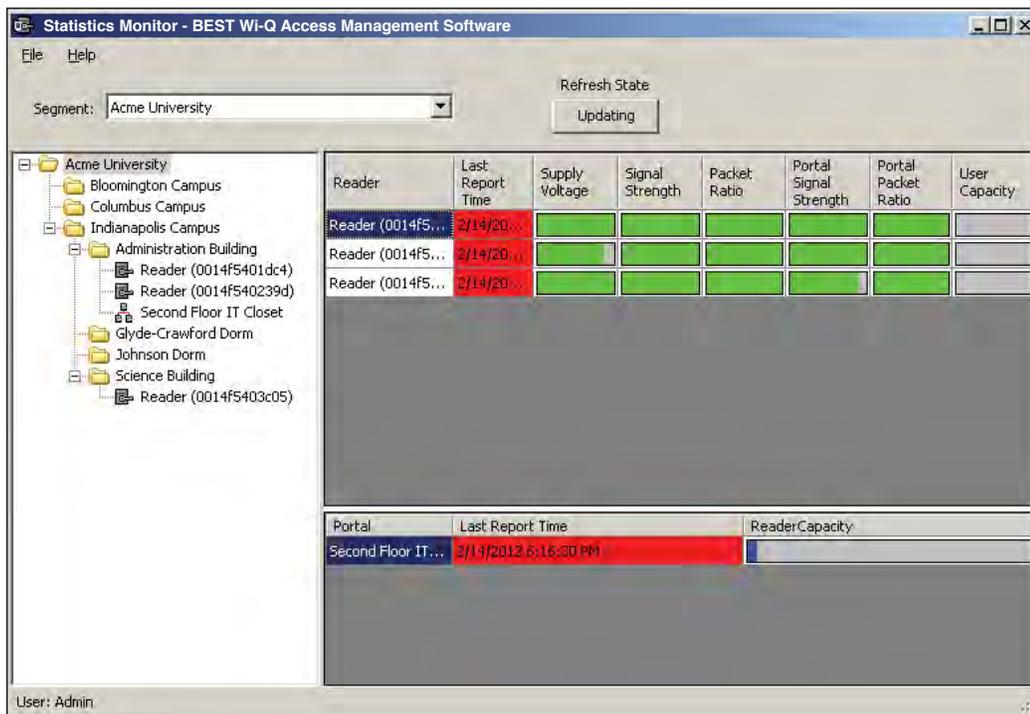
Statistics Monitor

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

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

Reader Statistics

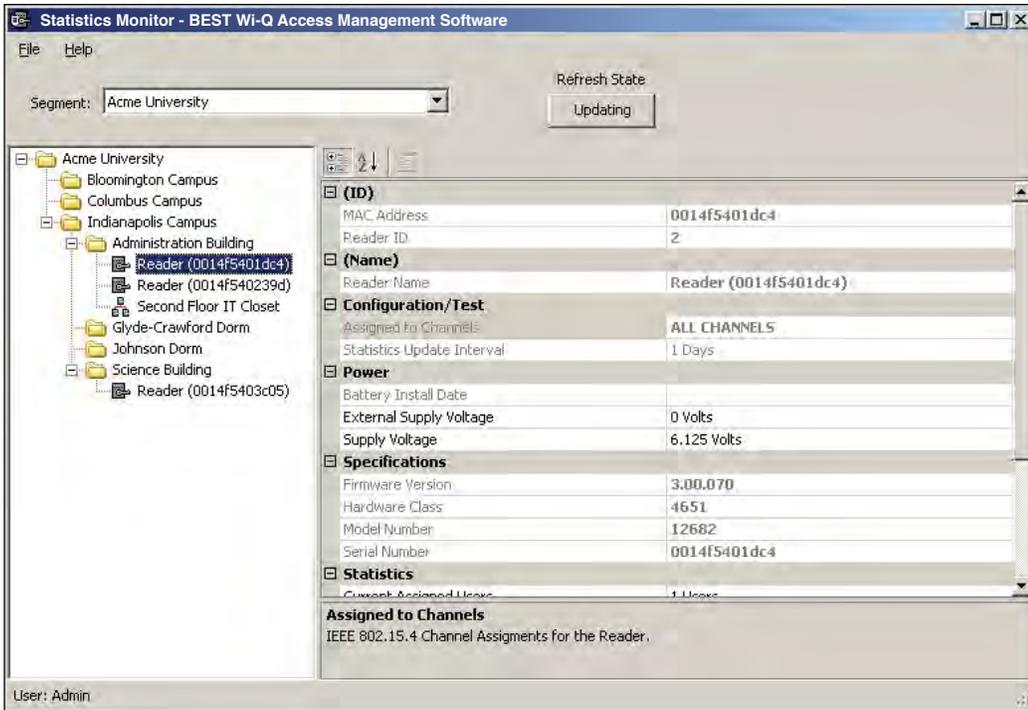
Figure 157 Viewing Reader Statistics



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

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

Figure 158 Display reader detail



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

Automatic Updates

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

Configuration/Test

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

Power

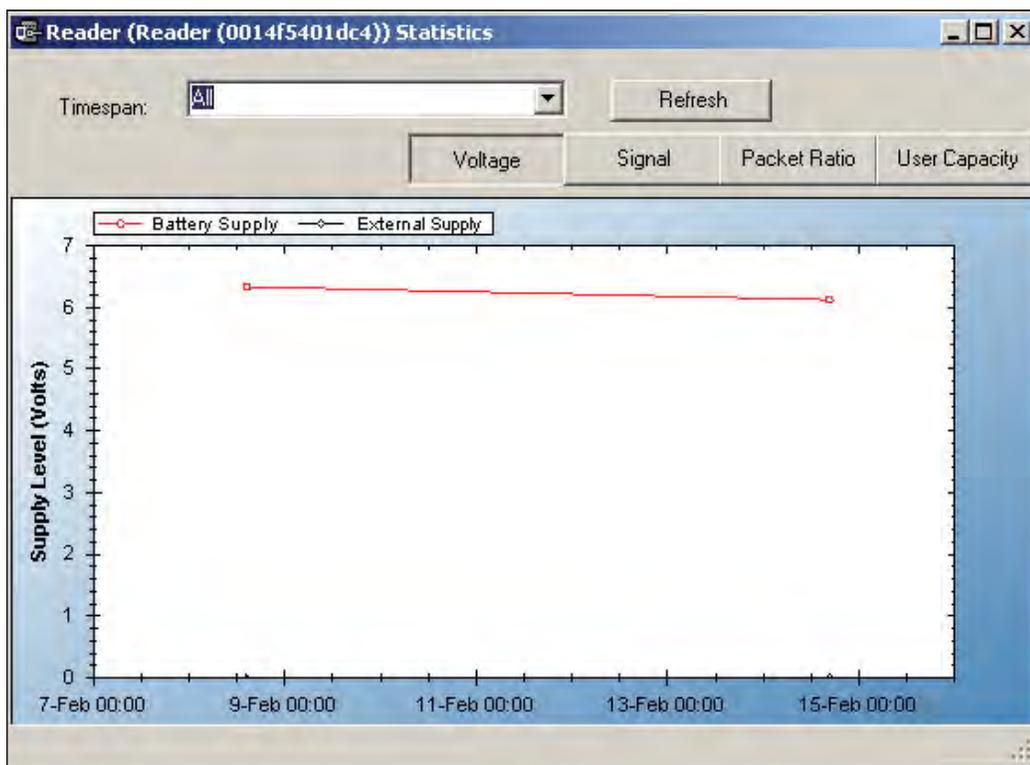
To view individual reader performance:

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

Voltage Tab

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

Figure 159 Reader Statistics Voltage Tab



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

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