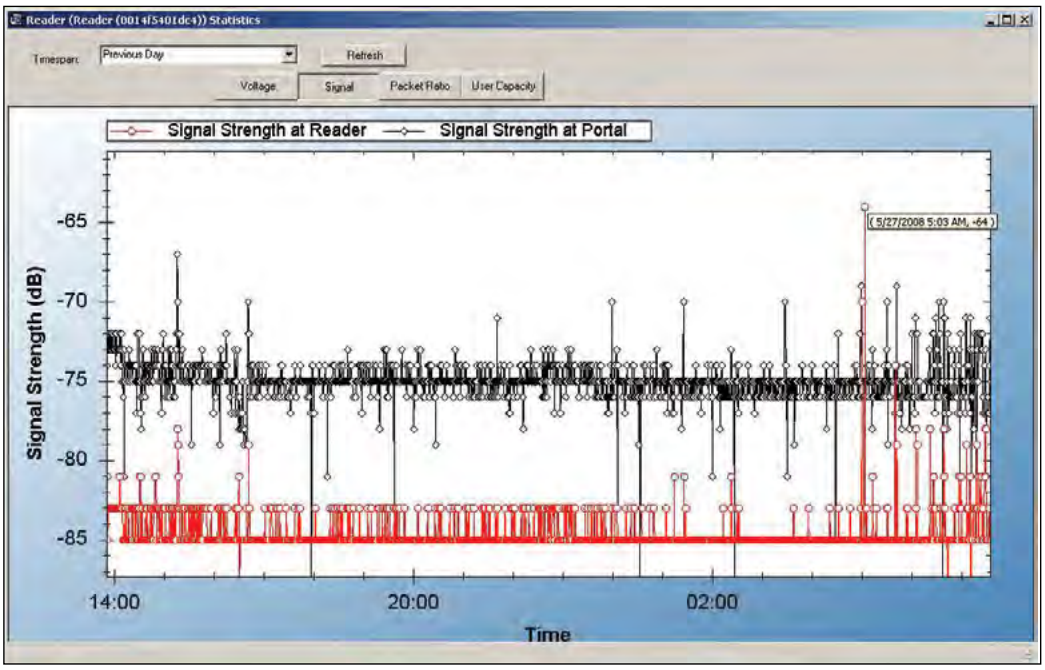
Signal Tab

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

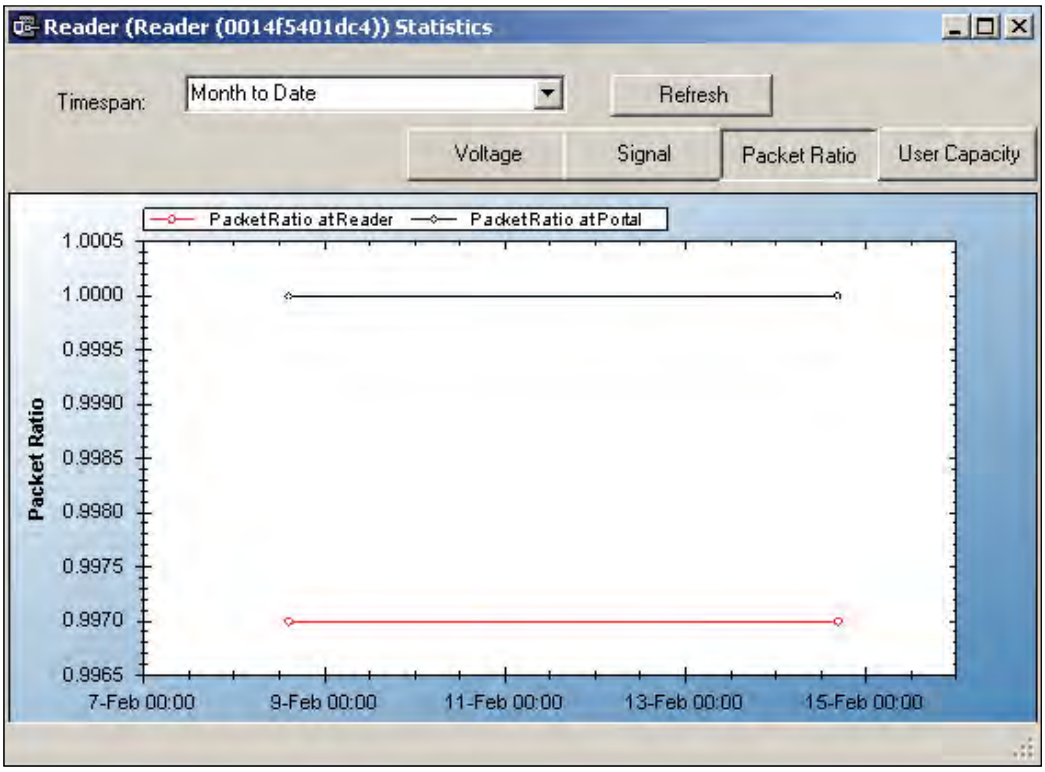
Figure 160 Reader Statistics Signal Tab



Packet Transfer Ratio Tab

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

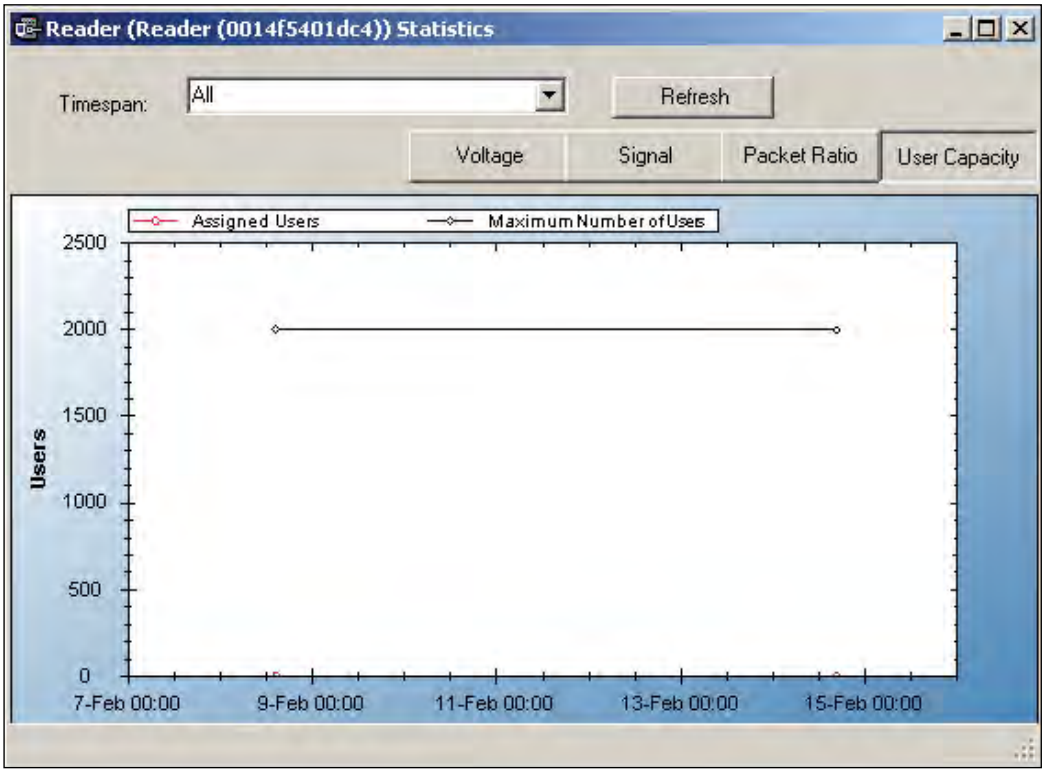
Figure 161 Reader Statistics Packet Radio Tab



User Capacity

This chart shows the Max allowable users for this reader and the current use. If you find that the use is nearing capacity, you may want to consider upgrading the reader capacity. See "Segment Item Upgrades" on page 179.

Figure 162 Reader Statistics User Capacity Tab

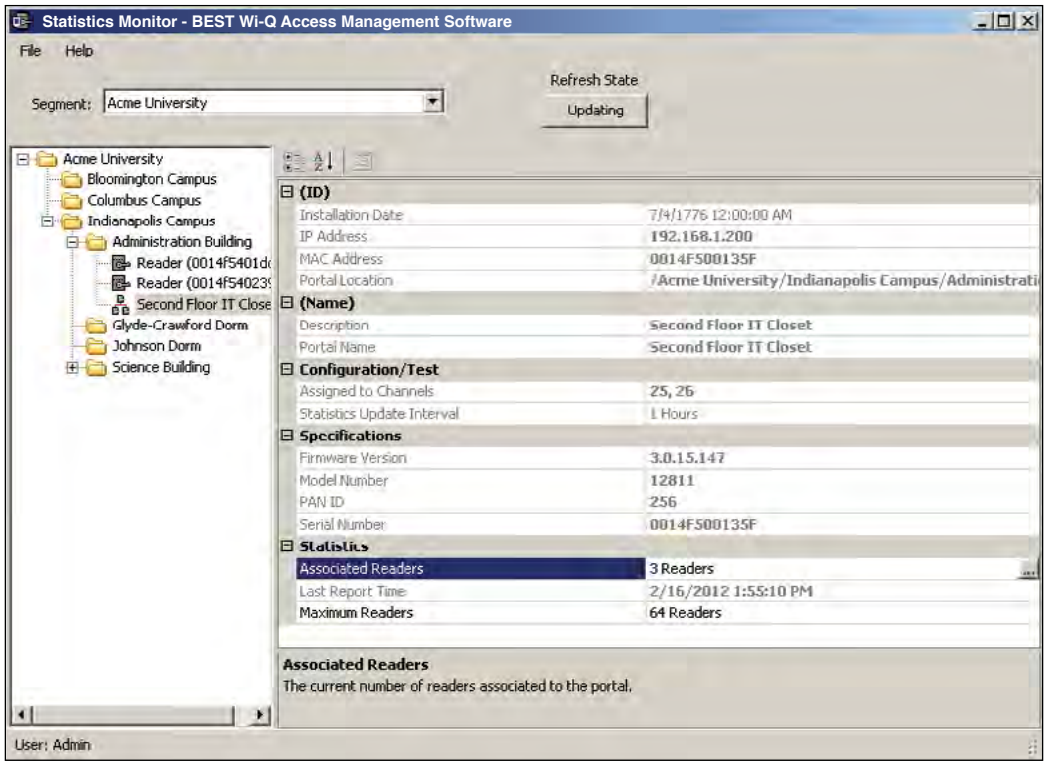


Portal Statistics

Portal Statistics display at the bottom of the Statistics Monitor. Select the top level in the Segment Tree to display all Portals in the system. See Figure 163.

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

Figure 163 Statistics Monitor Portal Properties



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

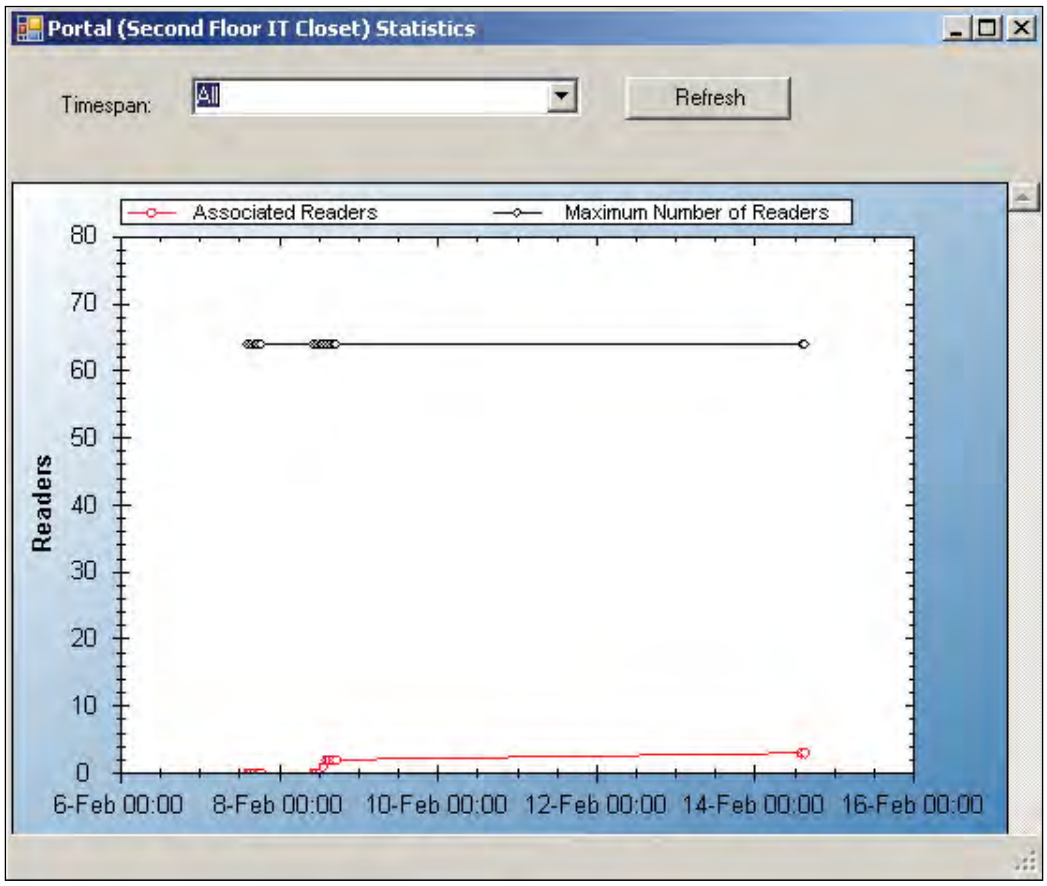
Portal Diagnostics

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

To review associated readers at Portals

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

Figure 164 Portal Statistics



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

Configuration/Test

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

Reports

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

To Launch Wi-Q AMS Reports

1 Select Start>All Programs>BEST Access>BEST Wi-Q AMS>Reports.

2 Enter your Login and Password. Reports opens.

Reports Overview

The software provides seven reports that you can modify:

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

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

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

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

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

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

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

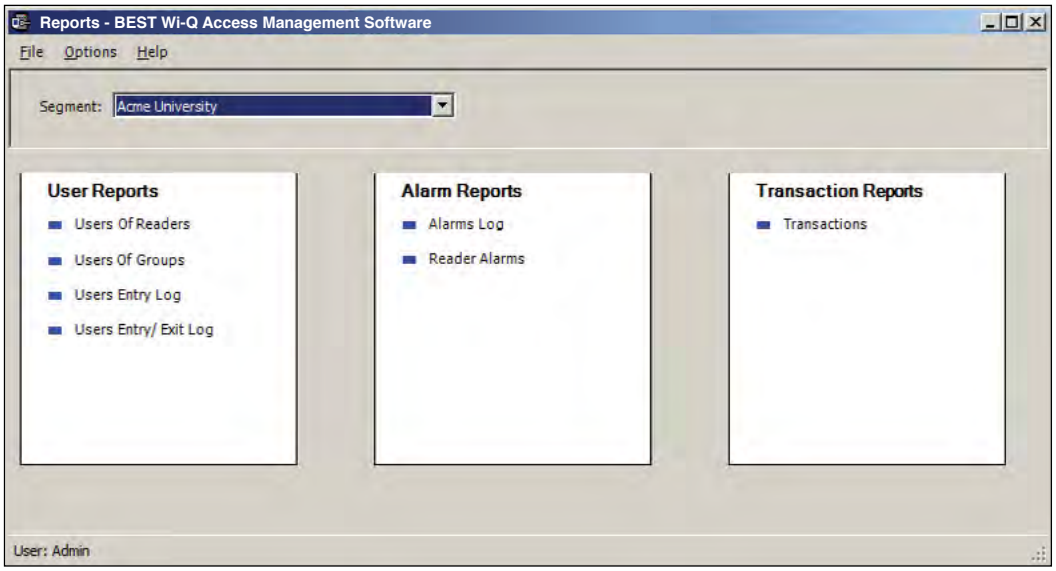
Creating Reports

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

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

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

Figure 165 Reports



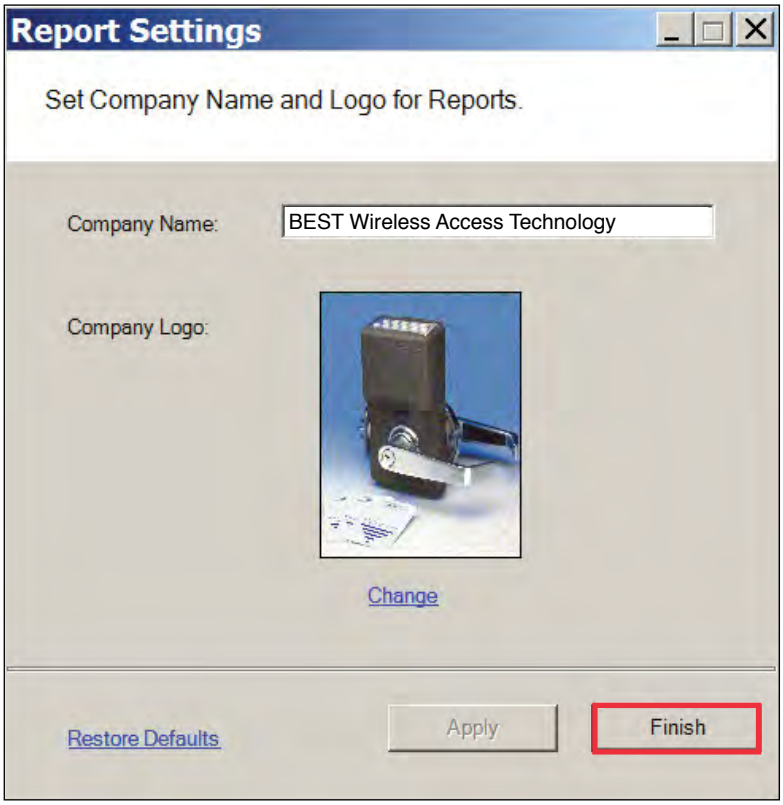
Configure Report Settings

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

1 In the Segment box, select the Segment for which you wish to create the setting.

2 Select Options>Report Settings. The Set Company Name and Logo for Reports dialog box opens.

Figure 166 Setting up a company name for a report



3 In the Company Name field, type in the company name you wish to appear on your reports.

4 Under Company logo, click the Change link. Use the Select Logo browser to navigate to the file you wish to include.

5 Click Open. The file is now uploaded to the Reports settings.

6 Click Finish to save your settings and begin working with Reports.

Generating a Report

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

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

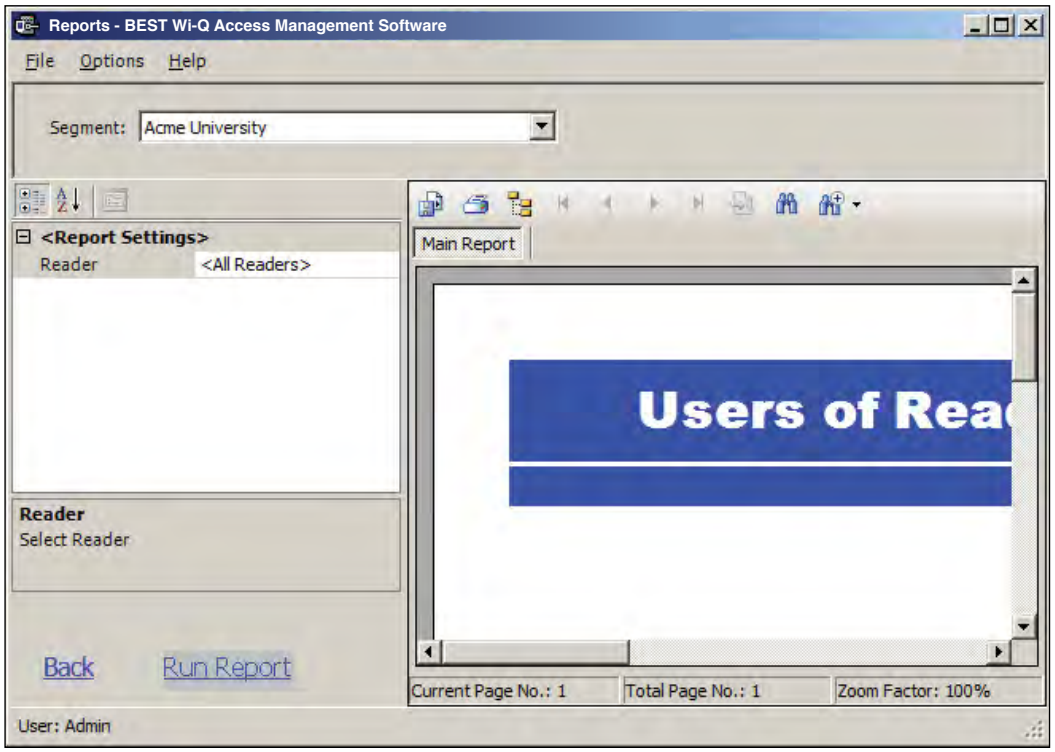
To Generate a Report

1 In the Reports main screen, under the User Reports box, click on Users of Readers. Reports opens at the basic users of Readers Reports generator.

2 In the Segment box, select the Segment you wish to report on.

3 Available report settings are listed on the left, and the results are shown on the right. For this particular report, the default will be <All Readers>.

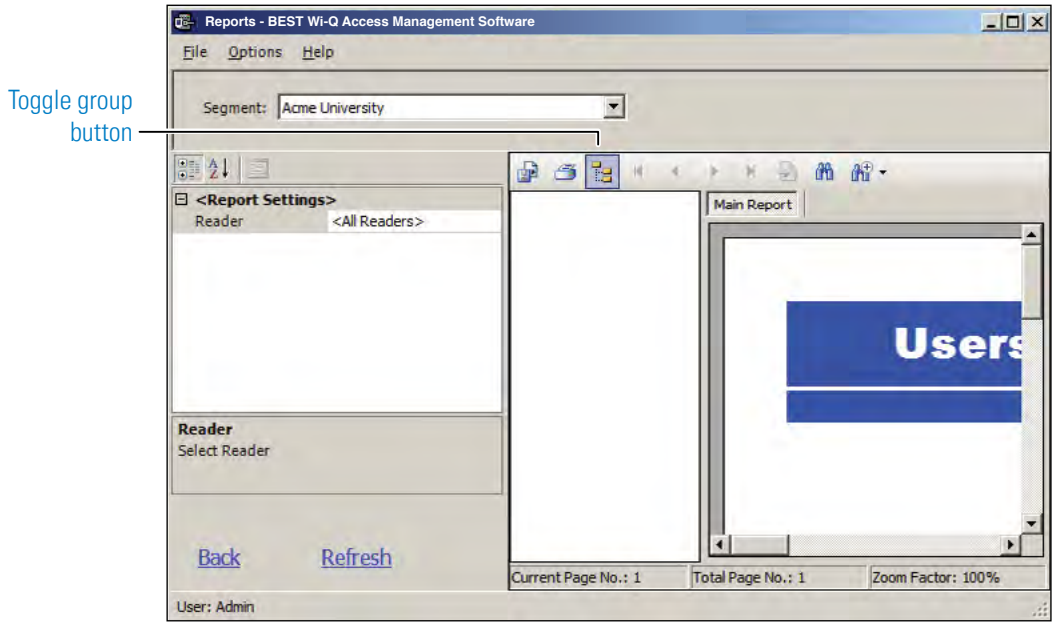
Figure 167 Viewing System Reports



4 Use the scroll bars to view the data, use menu icons to export, print, scroll through multi-paged reports, or use the Zoom tools to get a closer look.

5 If you have a large number of readers, Click the Toggle Group Tree icon and highlight a specific reader to jump to its section in the report.

Figure 168 Toggle Group



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

Generating Filtered Reports

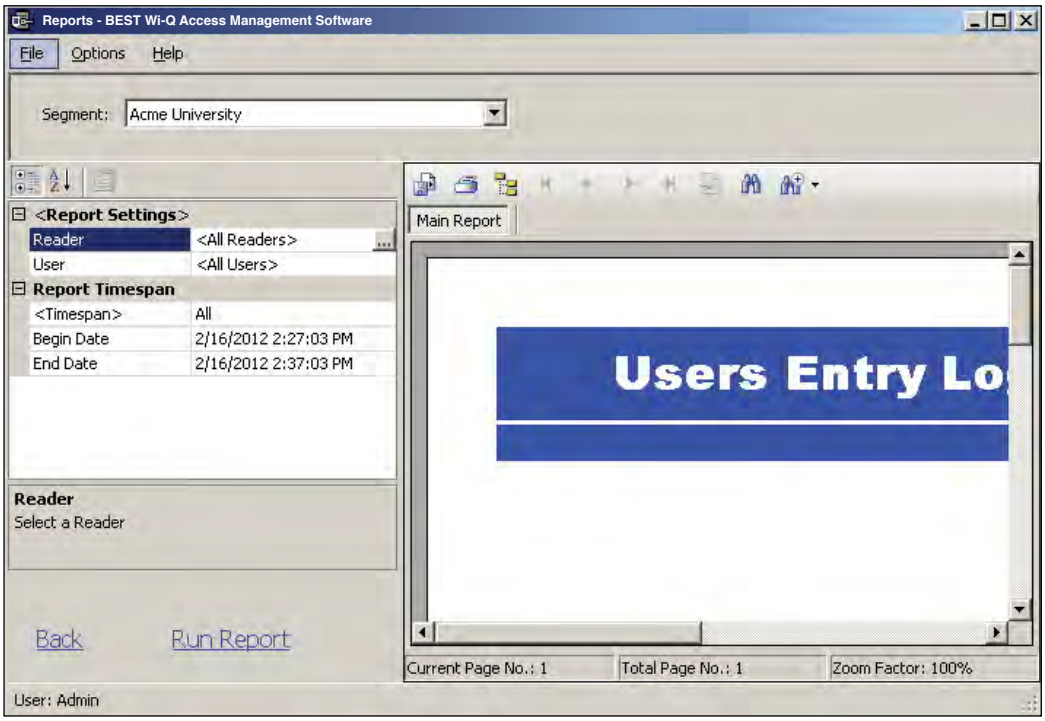
The report generator defaults to print all records. For example, when you select the Users of Readers report, report content displays users of all readers in the system. You can filter the report to display the users of only one specific reader, as in the following example.

To create filtered report

1 In the Reports main screen, select the Segment you wish to report on.

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

Figure 169 Users of Readers Report



3 To select a specific reader for this report, click on the Reader field's ellipsis button. The Select Reader dialog box opens.

4 Clear the All Readers box just below the drop-down list box.

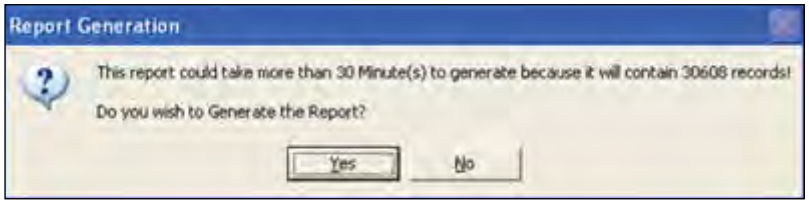
5 Select the reader to filter from the drop-down list.

6 Click Finish. The report results will display data for only the reader you selected.

Generating Larger Reports

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

Figure 170 Report Generation

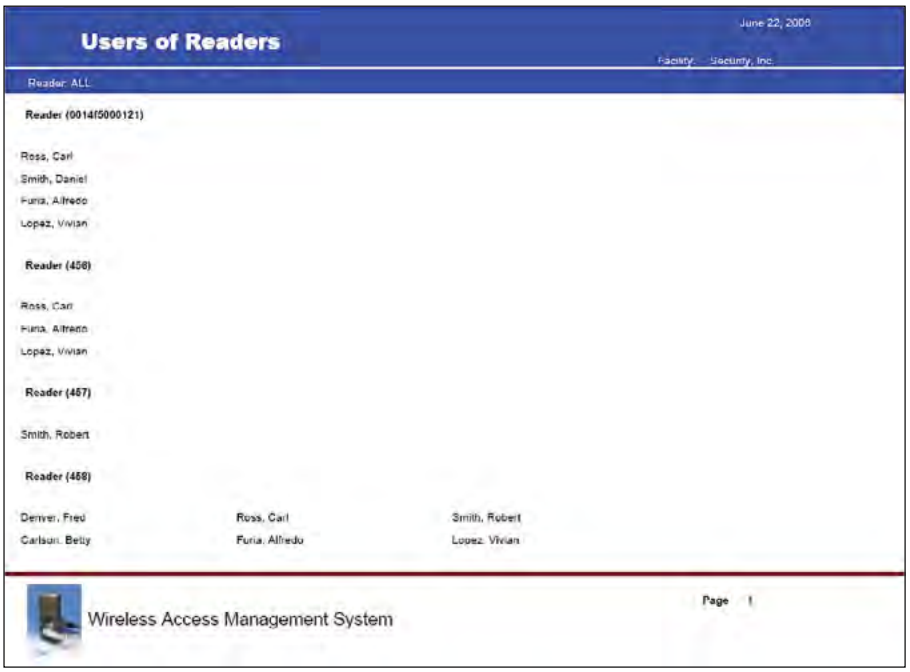


In the example, AMS detected that the defined report contains over 30,000 records and will take more than 30 minutes to generate. If this is acceptable, simply select Yes and the report will be generated. Select No if this is an inconvenient time to generate the report, or review your report definitions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

Printing and Exporting Reports

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

Figure 171 Sample report file



To print a report

1 Create the report using the features described in the previous sections.

2 Click the Printer icon in the menu bar.

3 Navigate to the printer you wish to use.

4 Print using the appropriate actions for the chosen printer.

To export a report

1 Create the report using the features described in the previous sections.

2 In the menu bar, click the Export Report option.

3 In the Export Report dialog box, select a format type from the drop-down list. The available types are:

- Crystal Reports (*.rpt)
- Adobe Acrobat (*.pdf)
- Microsoft Excel (*.xls)
- Microsoft Excel Data Only (*.xls)
- Microsoft Word (*.doc)
- Rich Test Format (*.rtf)

4 Navigate to the location you wish to export to.

5 Enter a filename for the file.

6 Click Save.

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

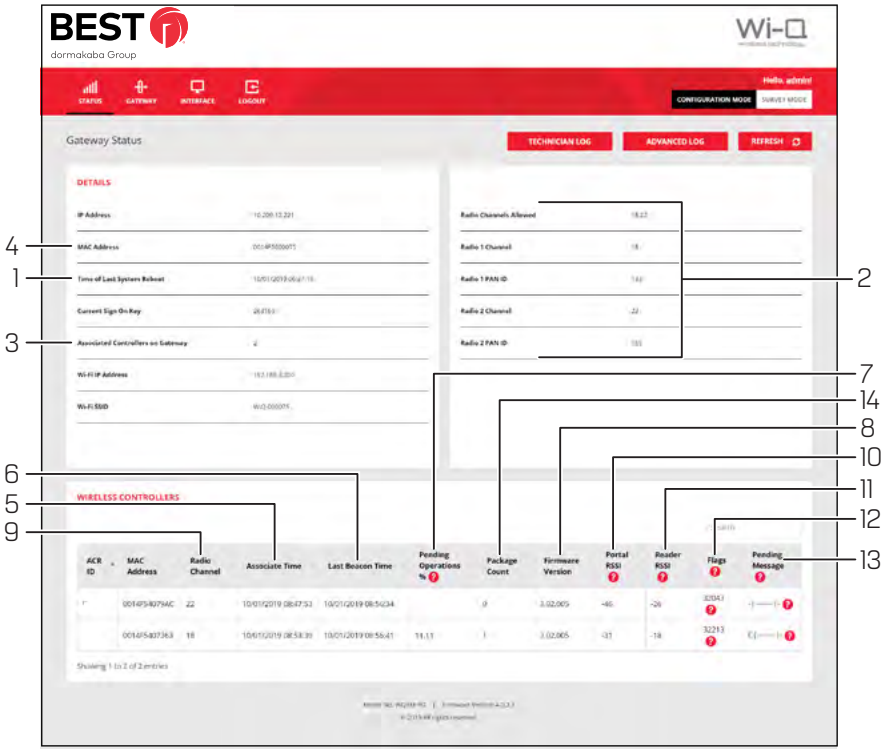
7 Wi-Q Gateway Web User Interface

This section provides an overview on the Wi-Q Gateway status webpage. You can access the status webpage for a specific Wi-Q Gateway by typing your desired Wi-Q gateway's IP address directly into your web browser. You will have to log into the Wi-Q gateway web page to get to the STATUS page.

- Inside the Portal Configuration Module, locate the desired Portal in the list and click on its hyperlink. See Figure 45.
- Type your desired Wi-Q Gateway's IP address directly into your internet browser.

Your browser will display the status of your Wi-Q Gateway and associated devices. See Figure 172.

Figure 172 Wi-Q Gateway Status Webpage



Clicking on Hyperlink will open the login page of the gateway webpage. You need login credentials to view the status page.

The Wi-Q Gateway Status webpage provides the following information:

1. **Time of Last System Reboot**
   Last time Wi-Q Gateway was reset or rebooted.

2. **Radio and Channel**
   Shows the channel associated with each radio in the Wi-Q Gateway.

3. **a) Associated Controllers on Gateway in the Details section**
   b) Wireless Controllers section will display the complete details of associated controllers
   Shows which devices are associated with the Wi-Q Gateway.

4. **MAC Address**
   Column shows the MAC Address of the Wi-Q Gateway.

5. **Associate Time**
   Column shows the time that the Controller last associated with the Wi-Q Gateway.

6. **Last Beacon Time**
   Column shows the time of the last Controller beacon.

7. **Pending Operations %**
   Column shows progress percentage of pending operations.

8. **Firmware Version**
   Column shows the firmware version number of associated Controller.

9. **Radio Channel**
   Column shows which radio the Controller is connecting to in the Wi-Q Gateway. Radio 18 is on the right side of the Wi-Q Gateway and Radio 22 is on the left side of the Wi-Q Gateway.

10. **Portal RSSI**
    Column shows the signal strength of the Controller as received at the Wi-Q Gateway. This signal strength ranges from -18 (highest) to -91 (lowest).

11. **Reader RSSI**
    Column shows the signal strength of the Wi-Q Gateway as received at the Controller. This signal strength ranges from -18 (highest) to -91 (lowest).

12. **FLAGS**
    Column shows the current operational status of the associated device.

13. **Pending Message**
    Column shows the abbreviation of the message currently in operation.

14. **Package Count**
    Displays the number of packets being sent to the controller.

Status Flags in the FLAGS Column

The following is a list of the bits in the FLAGS column and their corresponding Wi-Q Gateway status flags and definition.

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

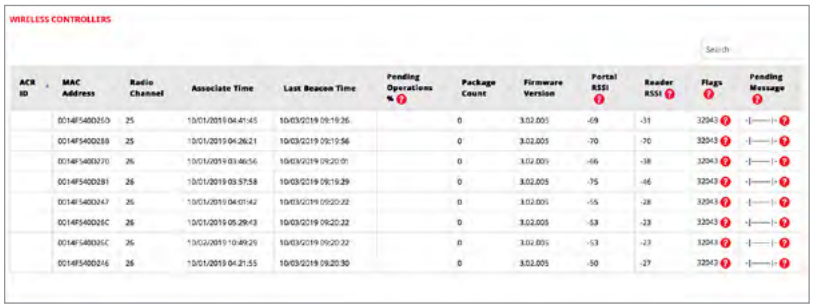
Table 1. Example Chart

Table 2. Bit			Table 3. Wi-Q Gateway Status Flag	Table 4. Definition
Right END	3	Bit 0	CONTROLLER_IS_ASSOCIATED	Set when the Controller is first associated with the Wi-Q Gateway.
		Bit 1	CONTROLLER_IS_VALID	Set during association, after the Wi-Q Gateway receives a beacon from the Controller.
		Bit 2	CONTROLLER_CONFIG_REQUIRED	Set during association, cleared by Wi-Q Gateway Communication Service after Controller configuration.
		Bit 3	CONTROLLER_ASSOC_PENDING_LIF	Set during association to indicate that Wi-Q Gateway requires LIF (Lock Information Frame) data.
	4	Bit 4	CONTROLLER_BEGIN_TRANSMISSION	Set when Wi-Q Gateway first transmits data to the Controller.
		Bit 5	CONTROLLER_DEEP_RESET_PENDING	Wi-Q Gateway must disassociate Controller when it receives the next beacon.
		Bit 6	CONTROLLER_VALID_INTERVALS	Set when Controller interval assignment has been received from the PC Communication Service.
		Bit 7	NOT USED	
	0	Bit 8	CONTROLLER_RETRY_LIMIT_EXCEEDED	Set when the retry limit on any command has been hit; used to limit downloads to firmware only.
		Bit 9	NOT USED	
		Bit 10	NOT USED	
		Bit 11	NOT USED	
	2	Bit 12	NOT USED	
		Bit 13	CONTROLLER_PREFERRED_PG_ENABLED	Set when Controller is locked to the Wi-Q Gateway.
		Bit 14	CONTROLLER_FIRMWARE_PENDING_DN	Set when the firmware commit has been sent to indicate that the disassociation is pending.
		Bit 15	CONTROLLER_FIRMWARE_PENDING	Set when firmware update is scheduled for the Controller, cleared when firmware commit is sent.
	3	Bit 16	CONTROLLER_REPORT_TIME _UPDATED	Set during association and when report time is updated.
		Bit 17	CONTROLLER_LIF_IS_VALID	Set when a LIF beacon is received.
Left END		Bit 18-31	NOT USED	

Update Flags in the PEND Column

At the bottom of the Gateway Status webpage will display the list of associated Wi-Q Controllers and their attributes.

Figure 173 Wi-Q Controllers



- **ACR ID** – The Reader ID when the Wi-Q Gateway is in Mercury Mode. This field will be blank when Mercury Mode is not in use.
- **MAC Address** – The Reader's unique Media Access Control address that uniquely addresses the device on the network.
- **Radio Channel** – The channel the door controller is communicating on with the Gateway.
- **Associate Time** – The date and time the Wi-Q Door Controller associated with the Gateway.
- **Last Beacon Time** – The last date and time the Wi-Q Door Controller beaconed information up to the Gateway.
- **Pending Operations** – Progress percentage of pending messages from the door controller to the Gateway.
- **Package Count** – The number of pending messages in the current queue that the Gateway has received from the Wi-Q Door Controller.
- **Firmware Version** – The current version of door controller firmware on the Wi-Q Device.
- **Portal RSSI** – Wi-Q Gateway RSSI is the how well the Gateway received a signal from the Wi-Q Door Controller. The signal strength ranges from -18 (highest/best) to -91 (lowest/worst). Ideally, this value should be -75dB or better.
- **Reader RSSI** – Reader RSSI is the how well the Wi-Q Door Controller receives a signal from the Gateway. The signal strength ranges from -18 (highest/best) to -91 (lowest/worst). Ideally, this should be -65dB or better.

- **Flags** – The Flags indicate the device status. Common device statuses for Wi-Q Con-

trollers when they are connected to a Gateway are below:

- **010001** – Controller initial connection to the Gateway.
- **30207** – Controller connected to the Gateway and is waiting for segment updates.
- **30063** – Controller has a deep reset command pending.
- **30017** – Controller waiting to be pulled into the segment and has not received segment updates.
- **30007** – Controller has received segment updates and is waiting in the "New Segment Items" folder in Wi-Q AMS Configuration software.
- **30043** – Controller is signed in to the ACS, connected, configured, and not locked to the Gateway.
- **30053** – Controller is taking configuration updates.
- **32043** – Controller is signed in to the ACS, connected, configured, and locked to the Gateway.
- **32243** – Controller is locked to Wi-Q Gateway but has not been added to an access level or a direct assignment to a User. No user credentials are assigned to the controller in the software.
- **38053** – Controller has a firmware update pending.
- **38043** – Controller is receiving a firmware update.
- **32207** – Controller completed the firmware update and is waiting for updates from the Wi-Q Gateway.

Pending Messages– The letters in the pending messages column are update messages that are being sent to the controller.

- **S** – Segment information (pin length, DST Times)
- **C** – Card formats
- **L** – Controller configuration (beacon time settings, channels, transaction masks, etc.)
- **U** – User credentials and properties
- **T** – Timezone intervals
- **I** – WAC I/O
- **F** – Firmware
- **P** – Ping (missing LIF data after association or updates)

A Glossary

100Base-T	The most common Ethernet wiring standard.
access level	An access control relationship made between a controller or controllers and a time zone or time zones. An access level is assigned to a badge ID for the purpose of granting access through a controller or controllers during a specified time.
access panel	A circuit board with on-board memory that is responsible for making most of the decisions in an access control system.
activation/deactivation date	The date that a credential becomes active or expires.
antipassback	A configuration limiting the ability of consecutive uses for a credential at a reader. Usually, configured with readers installed on both the secure and non-secure side of an opening. Once a credential has been used in a reader to gain access on one side of the opening, the credential cannot be used in the same reader until the credential is used to gain access to a reader from the opposite side of the opening.
APB exempt	Antipassback exempt. The cardholder with this privilege is exempt from antipassback rules.
badge	The credential or token that carries a cardholder's data.
badge ID	Part of the access control information that is encoded to a token. This information, usually numerical, is unique to a particular credential holder.
card format	The way that data is arranged and ordered on the card.
cardholder	An individual who is issued a particular credential.
chassis type	The designation that defines the physical lock type. Three types exist: cylindrical, mortise, or exit hardware. See those terms for more information.

common door	A configuration setting that allows for the allocation of duplicate badge ID ranges in separate offline locks.
communication port	The connector on the bottom of a Lock that allows the lock to be connected to a reader.
communication server	The server application designed to provide network services to access panels, controllers, PCs and PDAs.
credential	A physical token, usually a card or fob, encoded with access control information.
cylindrical	Lock chassis that installs into a circular bore in the door.
deadbolt override	The ability for an authorized credential to retract both the spring latch and the deadbolt when the deadbolt is engaged
directional antenna	An antenna type optimized to focus signal from point-to-point over longer distances and through obstacles.
dual access	The requirement for the presentation of two separate, authorized credentials in order to gain entry through an access controlled opening.
ethernet	The most common networking standard in the world, formally known as IEEE 802.3.
exit hardware	Lock chassis type that supports exit hardware trim lock.
extended unlock	The extra period of time the lock will unlock when an authorized credential with extended unlock privileges is presented.
guest	A feature that enables you to add and delete cardholders to and from a lock without having to go out to a lock to reprogram it.
Host	The computer on which Wi-Q AMS software is installed and set up to manage Wi-Q Gateways and readers on the network.
IP address	The numeric address (like 192.168.1.1) that identifies each device in a TCP/IP network.
input	A hardware connection point used for status reporting of a particular sensor.

intelligent system controller (ISC)	***See access panel.***
I/O device	A device, such as an alarm or parking gate that can be configured to operate on the network using a Wireless Access Controller.
issue code	Part of the access control information contained on a credential that allows reuse of the badge ID when a credential is lost, damaged, or stolen. Usually one or two digits in length, this code increments forward when creating a new credential. Access is granted only when the badge ID and the issue code match the current database information.
MAC address	The Media Access Control number (MAC). A unique, 12-digit number assigned by the manufacturer of a network device.
mortise	A lock chassis that installs into a mortised cavity in the edge of a door.
omni-directional antenna	An antenna type optimized to provide signal coverage in all directions.
packet	A discrete chunk of data, being transferred on a TCP/IP or other addressable network.
passage mode	The ability to double present an authorized credential within the strike time to unlock an opening. The lock is returned to its original status by a second, double presentation of an authorized credential.
Wi-Q gateway	The Wi-Q Gateway is a wireless device connected to the Host computer through a secure connection to transfer data signals from Wireless Controller locks to and from the Host computer.
request to exit	A sensor usually installed on the non-secure side of the door that will mask the door position switch upon activation.
segment code	Part of the access control information that can be encoded to a credential. This information, usually numerical, is unique to a group of credentials. Usually this feature is used to authenticate a credential to a particular organization.

sign-on key	Number generated within AMS to establish the connection between the readers and the Portals, and ultimately to a segment in the software.
site survey kit	The Wi-Q Technology Site Survey Kit tool used to determine optimum Wi-Q Gateway location to verify signal strength before permanently installing the hardware.
time interval	A specific range of time, which corresponds to a particular day or days of the week. A time zone can be comprised of several, individual intervals.
time zone	A defined range of time for assignment to various access control activities. A time zone may be applied to a reader or readers when creating an access level, to a reader to change the mode of operation, to a relay to activate and deactivate, to an input to mask and unmask, and a host of other operations.
unlock duration	The time that the lock momentarily unlocks.
use limit	A configuration limiting a credential to a defined number of uses.
Web Interface	The software program that allows setup and communication between the Wi-Q Gateway and the Host Computer.
Wi-Q Technology	Provides efficient, online access control decisions at the door.
Wireless Access Controller	Wireless Access Controller provides additional capability to connect stand-alone controllers and locks.
wireless reader lock	The wireless reader lock controls user access at the door and grants user requests according to how they are configured in the software.