

ACCESS IT! UNIVERSAL.NET USER MANUAL

VERSION 6.1

TABLE OF CONTENTS

Introduction	
Welcome	8
System Specifications	9
Getting Started	
Installing the Software	11
Setup and Configuration	13
Running the Software for the First Time	14
System Navigation	16
System Setup	
Software Parameters	
Card Formats	18
Reader Types	20
User Labels	22
Editing the Cardholder Database	26
Setup and Configuration	
Database Configuration Utility	29
Configuring the Network	34
Setting up Sites	35
Card Holders	
Managing Cardholders	37
Cardholder Detail	38
Finding Cardholders	46
Importing Cardholders	49
Exporting Cardholders	51
Bulk Cardholder Inserts	52
Batch Update/Delete Cardholders	60
Cards	
Managing Cards	61
Card Detail	63
Finding Cards	74
Previewing Cards	77

Printing Cards	78
Importing Cards	49
Exporting Cards	51
Bulk Card Inserts	52
Batch Update/Delete Card Data	60
Macros	
Managing Macros	79
Executing Macros	81
Macro Detail	82
Alarms	
View and Acknowledge Alarms	87
Set an Alarm Delay	90
Events	
View and Print Events	92
Tracking	
Tracking	94
Mustering	
Mustering	95
Maps	
Introduction to Maps	96
Map Designer	
Introduction to Map Designer	99
Setting the Map Properties	102
Map Designer Objects	
Map Device	103
Map Link	104
Map Macro	105
Map Text	106
Map Alarm Group	107
Hardware	
Using the Hardware Tree	108
Channels	
Managing Channels	109
Channel Detail	111

SCP's	
Managing SCPs	114
Sending Commands to SCPs	116
SCP Detail	119
Access Areas	
Managing Areas	134
Sending Commands to Areas	135
Area Detail	136
Alarm Zones	
Managing Alarm Zones	139
Sending Commands to Alarm Zones	140
Alarm Zone Detail	142
Tasks	
Managing Tasks	148
Manually Executing Tasks	149
Task Detail	150
SIO's	
Managing SIOs	161
Sending Commands to SIOs	163
SIO Detail	165
Readers	
Managing Readers	171
Sending Commands to Readers	173
Reader Detail	177
Inputs	
Managing Inputs	198
Sending Commands to Inputs	200
Input Detail	201
Outputs	
Managing Outputs	207
Sending Commands to Outputs	209
Output Detail	210
IP Locksets	
Managing IP Locksets	216

Sending Commands to IP Locksets	218
IP lockset Detail	219
Managing Card Groups	229
Card Group Detail	231
Salto Doors	
Managing Salto Doors	233
Salto Doors Detail	235
Card Groups	229
Managing Card Groups	229
Card Group Detail	231
Access Levels	
Managing Access Levels	242
Access Level Detail	244
Floor Codes	
Managing Floor Codes	248
Floor Code Detail	250
Intervals	
Managing Intervals	252
Interval Detail	253
Timezones	
Managing Timezones	255
Timezone Detail	257
Holidays	
Managing Holidays	259
Holiday Detail	261
Badge Types	
Add a Badge Type	263
Badge Designer	
Introduction to Badge Designer	264
Setting the Badge Properties	267
Badge Designer Objects	
Images	
Picture	270
Signature	273

Static Image	276
Shapes	
Horizontal Line	278
Vertical Line	280
Rectangle	282
Rounded Rectangle	284
Oval	286
Text	
Static Text	288
Badge Data	290
Badge Data Fields	292
Expression Builder	290
Badge Data Common Expressions	
Badge Data Common Expressions	296
User Groups	
Managing User Groups	300
User Group Detail	302
Users	
Managing Users	308
User Detail	310
Reports	
Run a Report	313
Recipients	
Managing Recipients	314
Recipient Detail	316
Data Exchange Packages	
Data Exchange Packages	319
Companies	
Managing Companies	326
Companies Detail	327
Alarm Event Filters	
Alarm Event Filters	328
Servers	
Managing Servers	329

Server Detail	331
Sites	
Managing Sites	35
Site Detail	333
Workstations	
Managing Workstations	339
Workstation Detail	341
Troubleshooting	
Diagnostics	345
System Maintenance	
Database Utility	29
IP Programmer	347
System Status	351

Welcome to Access It! Universal.NET

Thank you for choosing Access It! Universal.NET as your access control and photo id badging solution!

Access It! Universal.NET is a 32-bit software package that was developed with enterprise class functionality and ease of use in mind. Simple software installation, multi-server capabilities, fail-over cluster compatibility and the familiar single screen user interface make Access It! Universal.NET a powerful and easy to use solution.

This documentation is intended to be used as a step by step reference to be used while data is being entered into Access It! Universal.NET. This documentation will always stay on top of the desktop while it is open. This will allow it to be kept open while actual data entry is being performed. The first time the documentation opens, the table of contents will be hidden. To open the table of contents, simply click on the show button on the toolbar. This will display the table of contents and allow the documentation to be searched.

For additional product information and support, please visit our website at <http://www.rs2tech.com> or our knowledge base at <http://helpdesk.rs2tech.com>

System Specifications

Access It! Universal.NET has the following system specifications:

- Unlimited SCP Panels (1024 per regional server) (All Models with TCP/IP, RS-232, RS-485 and Dial-up support)
- Alternate (Backup) Communications Channel for SCP Panels
- 32 SIO Panels per SCP
- Hierarchical Device Tree with Active Status Icons
- Unlimited Readers (Determined by number of regional servers)
- Automatic Card Holder Enrollment Readers
- Unlimited Inputs and Alarm Monitoring with Graphical Maps
- Multiple Monitor Support
- Alarm Routing with Variable Annunciation Delay/Scheduling
- Unlimited Programmable Outputs
- User Definable Multi-Functional Tasks
- Macro and Report Scheduling
- Unlimited Workstations
- Database Partitioning
- Up to 255 Sites per Regional Server
- Hot Fail-Over using Microsoft Cluster Server
- Powerful SQL Server Database Engine
- Up to 32,767 Access Levels per site
- Up to 255 Elevator Floor Codes with support for up to 64 floors each per site
- Precision (Single Door) Access
- Up to 255 Timezones per site
- Up to 255 variable duration Holidays per site with support for up to 8 holiday groups each
- Multiple Cards per Card Holder
- Up to 128 Access Levels per Card
- Unlimited User Definable Text Fields per Cardholder
- Card Groups for Card Activation and Card Expiration
- Automatic Database Record Level Auditing
- TWAIN support for picture and signature capture devices
- WDM (Windows Driver Model) support for picture and signature capture devices
- Prints to any printer supported by the operating system
- Built in Badge Designer
- Built-in DVR Integration (Must be purchased separately)
- Built-in Intercom Integration (Must be purchased separately)
- Built-in CCTV Switcher integration (Must be purchased separately)
- Built-in Email and Pager notifications (Must be purchased separately)
- Built-in Terminal Server (thin client) (Must be purchased separately)

- Built-in Biometric Device Support (Must be purchased separately)
- Built-in Intrusion Panel Support (Must be purchased separately)

These specifications are subject to change without notice from the manufacturer.

Installing Access It! Universal.NET

To install Access It! Universal.NET follow the step by step instructions below for the type of system being installed.

Stand-Alone/Server Systems

A stand-alone system does not have a server or a client; rather it consists of only one computer facilitating all access control functions and is connected to one or more access control panels. This single computer hosts both the server service and the application database. The database requires SQL Server 2008 or higher to be loaded on the local machine prior to loading Access It! Universal.NET.

Installing Access It! Universal.NET

1. Do NOT install the Sentinel key (dongle) until the software is completely installed.
2. Disable any Anti-Virus software.
3. Insert the Access It! Universal.NET CD and the auto play menu will be displayed.
4. Follow the on-screen instructions.
5. Reboot the computer if prompted otherwise re-enable any Anti-Virus software.

Client / Server Systems

A client / server system is made up of two or more components, the server and the client(s). The main purpose of the server is to host both the server service and the application database while communicating to one or more access control panels. The main purpose of the client(s) is to facilitate all access control functions as needed. The database requires that SQL Server 2008 or higher be loaded on the server machine prior to loading Access It! Universal.NET. The database may optionally reside on a separate SQL Server.

To install your client / server system, follow the Server Installation instructions before following the Client Installation instructions below.

Installing Access It! Universal.NET on the Server

1. Do NOT install the Sentinel key (dongle) until the software is completely installed.
2. Disable any Anti-Virus software.
3. Insert the Access It! Universal.NET CD and the auto play menu will be displayed.
4. Follow the on-screen instructions.
5. Reboot the computer if prompted otherwise re-enable any Anti-Virus software.
6. Configure DCOM settings according to operating system and network environment. For more information on DCOM configuration, see the [Configuring the Network](#) help file topic.

Installing Access It! Universal.NET on the Client(s)

1. Disable any Anti-Virus software.
2. Do NOT install the Sentinel key (dongle) until the software is completely installed.
3. Disable any Anti-Virus software.
4. Insert the Access It! Universal.NET CD and the auto play menu will be displayed.
5. Follow the on-screen instructions.
6. Reboot the computer if prompted otherwise re-enable any Anti-Virus software.

Setting Up and Configuring Access It! Universal.NET

Before running Access It! Universal.NET for the first time, the system must be set up and configured before the application can be used.

During the installation of Access It! Universal.NET, the database configuration utility is automatically executed and will create the system database or upgrade an existing system database. Should an error occur during this phase, the Database Configuration Utility must be manually ran prior to opening the Access It! Universal.NET application. For more information on the database configuration utility, see the [Database Configuration Utility](#) help file topic.

SQL Server 2008 R2 or higher must be installed prior to installing the Access It! Universal.NET software on the server.

When using client workstations in a workgroup enviroment it is vital to have matching Windows usernames and passwords. See the [Configuring the Network](#) help file topic for more information.

The Access It! Universal.NET service must then be started on the server prior to clients being able to connect and to enable communication with the SCP panels. To start the service, click on the service manager utility from the Access It! Universal.NET | Server Utilities folder on the Windows start menu.

Running Access It! Universal.NET for the First Time

After performing the installation, setup and configuration of the software, several application parameters must be defined before the access control system can be brought on line.

Setting up Sites

Sites must then be created to host the system hardware. The default site "Main" is automatically created when the software is installed. Depending on the version of Access It! Universal.NET that has been installed the number of sites may be fixed at one. Sites are used to create new or maintain existing sites within a database and specify various site capacities and parameters. A site is used to segregate (partition) data in a database. For more information on sites, see the [Sites](#) help file topic.

Setting up User Groups

User groups must then be created to assign groups of user permissions. User groups are used to set up groups of users that will have the same access permissions to various areas of the software. User group permissions can be assigned which will allow no access, view only access or full access to all areas of the software. The default user group "Administrators" has access to all areas of the software. For more information on user groups, see the [User Groups](#) help file topic.

Setting up Users

After the installation of the Access It! Universal software, the default "Admin" user is assigned to the "Administrators" user group which has permission to run the application with access to all areas by default with no password assigned. If this installation was an upgrade from a version prior to 4.x then all of the users from the previous version will be imported also with no password assigned. Additional users will need to be given access to the application before anyone other than the "Admin" user can use the application. For more information about users, see the [Users](#) help file topic.

Setting up Timezones/Intervals

Timezones must then be set up as needed by using the timezones data entry screen. When creating new timezones, new intervals will also be created. The always timezone is predefined for 7 day a week, 24 hour a day access, including holidays. If time controlled access is not important, this timezone may be used instead of defining additional timezones. For more information about timezones, see the [Timezones](#) help file topic.

Configuring Hardware

System hardware must then be enabled and configured using the Hardware Tree. Hardware is used to define all panels, readers, inputs, outputs, intercoms, CCTV cameras and DVR cameras being used in the system. Using the Hardware Tree, the devices physically installed in the system must be enabled and configured for use in the system. For more information on setting up devices with the Hardware Tree, see the [Hardware Tree](#) help file topic.

Setting up Access Levels

Access levels must then be defined to determine who will have access to what doors and elevators, at what times. If no access levels are defined none of the card holders in the database will have access to any of the doors in the system. For more information about access levels, see the [Access Levels](#) help file topic.

Designing Badge Types

Badge types must then be designed as needed by using the badge type editor. Badge types determine the layout and content that will be printed on an id card or label. Badge types can be based on predefined system templates or created from scratch. For more information about badge types, see the [Badge Types](#) help file topic.

Adding Card Holders

Card holders and cards can then be added to set up card holders in the system and give them access to doors. For more information on adding Cardholders and Cards, see the [Cardholders](#) help file topic.

System Navigation

Access It! Universal.NET allows for customization of how screens are displayed and placement of windows. Control of the window functionality is determined by the options settings menu located off of the File menu:

Language

The language the application will be displayed in. In order to change from the default English setting, a custom language database must be provided. Contact your Authorized RS2 Dealer or RS2 Technologies for information on obtaining a language database.

Show advanced device commands

This option controls if a dialog box appears when sending a command to a device (for example, an unlock command to a reader). The dialog box allows for sending temporary commands to the device. When the option is not enabled, no dialog box will appear when a command is sent to a device.

Allow selection of only one site

This option only applies to the Enterprise editions of Access It! Universal.NET. When checked, the ribbon menu will contain a site drop list allowing for only one site to be selected. When that site is selected, only it's site-specific data will be displayed throughout the application. When the option is unchecked, the ribbon menu will have an advanced selector allowing for multiple different sites to be selected at once. The application will then display the site-specific data for all the selected sites.

Access to individual sites is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Advanced Window Control

This option controls how the windows in the software are displayed. When the option is not enabled, only one application screen is displayed at a time (with exceptions to Events and Alarms). The Events/Alarms/Maps screens can be undocked by selecting the respective option in the view menu of the ribbon. When the option is enabled, all screens open up as individual tabs in the application and can be "torn" away from the application into a new window. When torn away, there are additional right click menu options under the tab allowing for different placements of the detached window.

Allow non-modal dialogs

This option controls whether or not multiple forms can be opened at a single time. When the option is not enabled, only one form can be worked on at a time (with exceptions to Events and Alarms).

Column Chooser

With the exception of Events and Alarms, all screens can have additional columns added, or removed from their respective screens by selecting the Select Column icon located in the view menu of the ribbon. Within the column chooser window, drag and drop columns to/from the respective screens to add or remove columns.

Themes

This option allows for controlling the current theme. Themes will adjust the color schema throughout the application. Themes are selected from the view menu of the ribbon.

Preview Pane

The preview pane allows for a quick preview of the selected data without the need to edit first. The preview pane is toggled by selecting the Preview Pane icon in the view menu of the ribbon.

Reset

The reset option will revert all window settings and placements back to the factory default. This is useful in cases where the screens have been so customized navigation is difficult.

Card Formats

Card formats are used to specify the type of readers and cards being used in a system. The card format contains the number coded instructions that inform the SCP panel of the card format being used. Card formats are entered in the SCP's screen. For more information on SCP's, see the [SCP's](#) help file topic.

To set up a card format, go to the card formats tab on the SCP's screen and click on the edit card formats button. Card formats can be imported and exported by clicking the respective buttons. To add a new format, click on the new button and enter the required fields. The following card format parameters are supported:

Card Format Name

Enter the format name of the card format being specified. The name is used to identify the card format when it is being selected in the SCP's screen. It is recommended that a friendly name be assigned to all of the card formats being used. An example of a friendly name would be "Custom 37 Bit Wiegand". The format name can be up to 50 characters in length.

Card Type

Select the type of card being used.

Card Layout

Enter the card layout parameters for the card format being specified. This information will generally be provided by the reader or card manufacturer. The following parameters are supported in the format string:

Wiegand

- *Number of Bits* - This parameter is the total number of bits on the card.
- *Number of Bits to Sum for Even Parity* - This parameter is the number of bits to sum for even parity.
- *Address to Start From* - This parameter is the bit address to start summing for even parity.
- *Number of Bits to Sum for Odd Parity* - This parameter is number of bits to sum for odd parity.
- *Address to Start From* - This parameter is the bit address to start summing for odd parity.
- *Number of Facility Code Bits* - This parameter is the number of facility code bits.
- *Address to Start From* - This parameter is the bit address to start the facility code.

- *Number of Cardholder ID Bits* - This parameter is the number of card number bits.
- *Address to Start From* - This parameter is the bit address to start the card number.
- *Number of Issue Level Bits* - This parameter is the number of issue level bits.
- *Address to Start From* - This parameter is the bit address to start the issue level.

Mag Stripe

- *Minimum Number of Digits on Card* - This parameter is the total minimum number of digits on the card.
- *Maximum Number of Digits on Card* - This parameter is the total maximum number of digits on the card.
- *Number of Facility Code Digits* - This parameter is the number of facility code digits.
- *Address to Start From* - This parameter is for indexing to the most significant digit.
- *Number of Cardholder ID Digits* - This parameter is the number of card number digits.
- *Address to Start From* - This parameter is for indexing to the most significant digit.
- *Number of Issue Level Digits* - This parameter is the number of issue level digits.
- *Address to Start From* - This parameter is for indexing to the most significant digit.

Entering an invalid card format can compromise the security and functionality of the system.

Options

- Step parity calculations by 2 bits - Decodes a card with parity calculations made every 2 bits.
- Suppress Facility Code Checking
- 37 bit Parity Test with 4 Parity Bits
- 37 bit Parity Test with 2 Parity Bits
- Special 48 Bit Formatting (PIV) - Decode a card as a 48 PIV structured card and presented to the application software.
- Interpret card field as a Large Encoded ID (PIV-I) - Instead of Decoding a card, the actual encoded ID is presented to the application software.

Reader Types

Reader types are used to specify the type of readers and cards being used in a system. The reader type contains the number coded instructions that inform the SCP panel of the type of reader being attached to the SIO panel. Reader types are entered from the readers screen. For more information on readers, see the [Readers](#) help file topic.

To set up a reader type, go to the readers screen and click on the edit reader types button. To add a new reader type, click on the new button and enter the required fields. The following reader type parameters are supported:

Reader Type Name

Enter the reader type name of the reader type being specified. The name is used to identify the reader type when it is being selected in the readers screen. It is recommended that a friendly name be assigned to all of the reader types being used. An example of a friendly name would be "RS2 Proximity". The reader type name can be up to 50 characters in length.

Data Format

Select (check) the desired data options for the reader type. These parameters can be obtained from the reader manufacturer.

Keypad Mode

Select the keypad mode for the reader type. This determines the kind of keypad that this reader type will have.

LED Drive Mode

Select the LED drive mode for the reader type. This will control the display of the reader LED or LCD display for this reader type and enable or disable certain reader communication protocols.

OSDP Options

Open Supervised Device Protocol readers communicate through a secure bi-directional reader port. Currently only a single OSDP reader can be attached to a single reader port

Baud Rate - Select the baud rate for the OSDP readers. Typically, readers use a 9600 baud rate

Address - Select the address for the OSDP reader. Since currently a single reader is supported on a reader port, it is expected address 0 be used

Secure Channel - Select the secure channel option if the reader supports encrypted communications over OSDP. You additionally need to put the reader in link mode so that the default SCBK (Secure Channel Base Key) can be used to establish the unique SCBK between the reader port and the reader. The reader is placed in link mode by right clicking on the reader and selecting Start Link Mode from the commands list.

Enable diagnostic tracing - Select the enable diagnostic tracing to enable OSDP reader information to be logged within the SCP debug files.

Reader LED Function

Select the reader LED function mode for the reader type. Select the default option to use the default settings or choose custom to configure the LED display functions from the SCPs screen for various reader modes. For more information on SCPs, see the [SCPs](#) help file topic.

Reader types can be very complex and are only recommended to be entered by advanced users. Entering an invalid reader type can compromise the security and functionality of the system.

Cardholder User Fields

Cardholder user fields are used to customize the look and feel of the available user definable fields on the cardholders data entry screen. These user fields can be used for supplemental information, such as department, license plate number, hire dates, etc. Various data entry controls can also be used to define the type of data being entered into these fields. The number of available fields along their various properties are determined by the cardholder designer in the database configuration utility. For more information on the cardholder designer, see the [Database Configuration Utility](#) help file topic.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Editing Cardholder User Fields

To edit cardholder user fields, go to the user groups data entry screen by either clicking on the user groups toolbar button within the configuration group on the toolbar, or by selecting user groups from the go option on the system menu. Next, select the cardholder fields category in the permissions tree and click on the cardholder user field to be edited. Then click the edit field button to edit the properties for the selected cardholder user field.

Editing Cardholder Form Behavior

Cardholder form behavior can be edited from either of two locations, through the User Groups data entry screen or by clicking the Cardholder Fields button from within the Database Configuration Utility. Access the user groups data entry screen by clicking on the user groups toolbar button within the configuration group on the toolbar. Next, select the permissions tab and then the cardholder fields category within the tree and click on the edit cardholder form behavior button to edit the behavior properties for the cardholder form. Cardholder form behavior can be used to make certain fields required, perform calculations on fields and a wide variety of other behaviors. Cardholder form behavior uses the Visual Basic scripting language to control the behavior of the cardholder form. Discussion of the Visual Basic scripting language is beyond the scope of this documentation. All usertext fields, as well as first, last, and middle names can be controlled. Available properties are:

- SetFocus (All types of fields)
Example - Form.UserControls("UserText1").SetFocus
- Visible (All types of fields)
Example - Form.UserControls("UserText1").Visible = False
- Enabled (All types of fields)

Example - Form.UserControls.("UserText1").Enabled = False

- Text (Textbox fields only)

Example - Form.UserControls.("UserText1").Text = "Test"

- Value (Date/time or drop lists fields only)

Example - Form.UserControls.("UserText1").Value = "Test"

- Backcolor (Textbox fields only, value entered in HTML hex value)

Example - Form.UserControls.("UserText1").Backcolor = "#000000"

- Forecolor (Textbox fields only, value entered in HTML hex value)

Example - Form.UserControls.("UserText1").Forecolor = "#FFFFFF"

- Clear (Drop list fields only)

Example - Form.UserControls.("UserText1").Clear

- RemoveAll (Drop list fields only)

Example - Form.UserControls.("UserText1").RemoveAll

- AddItem (Drop list fields only)

Example - Form.UserControls.("UserText1").AddItem("Sales")

Editing the cardholder form behavior can render the cardholder form inoperable. This editor should only be used by persons that have extensive experience with the Visual Basic scripting language.

Display Order

To change the display order for cardholder user fields, go to the user groups data entry screen by either clicking on the user groups toolbar button within the configuration group on the toolbar, or by selecting user groups from the go option on the system menu. Next, select the cardholder fields category in the permissions tree and click on the cardholder user field to change the display order for. Then click the up or down arrow buttons to move the field up or down in the display order. Cardholder user fields will be displayed in the order that they are displayed here on the cardholder's form.

Display Name

Enter the display name for the cardholder user field. The display name is a "friendly" name that will be displayed on the card holders form and in all selection screens and reports. An example of a friendly name would be "Department". The display name can be up to 50 characters in length.

Edit Control

Select the type of edit control to be used for the cardholder user field. The edit control determines the look and functionality of the cardholder user field that is displayed on the card holders form for data entry. The following types of edit controls are available:

- *Text Box* - The text box edit control is used for the entry of free form alpha-numeric characters up to 50 characters in length. An input mask can also be defined to control the way that data is entered into the user field. For example, an input mask of "#####" would force numeric only data entry up to 6 digits in length. Several common predefined input masks are included.
- *Drop Down List* - The drop down list edit control is used to present a list of predefined items to choose from during data entry. This is useful when data consistency is desired for a certain user field. An example of this might be a "Department" user field with list items defined as "Sales", "Engineering", and "Management". This would ensure that instead of the operator typing in the word "Sales", it would be presented as a list item and would be entered the same way each time. An unlimited number of list items can be entered.
- *Date Combo* - The date combo edit control is used for the entry of dates. A calendar is also available when data entry is being performed to make entering dates easy.
- *Text Box with Required Entry* - The text box edit control is used for the entry of free form alpha-numeric characters up to 50 characters in length. An entry in this field will be required before a card holder can be saved. An input mask can also be defined to control the way that data is entered into the user field. For example, an input mask of "#####" would force numeric only data entry up to 6 digits in length. Several common predefined input masks are included.

List Items

Enter the list items for the drop down list control. List items can either be entered directly or can be entered as a keyed lookup list. Keyed lookup lists are entered in the following format:

1=Department 1
2=Department 2
3=Department 3
A=Apple
B=Banana
C=Cherry
P=Poodle

Entering keyed lookup lists in this manner will store the key in the database but display the equal to text or number in the card holders screen. For example, if the operator chose the A=Apple list item "A" would be stored in the database but "Apple"

would be displayed.

Default Value

Enter the default value for either the text box or the drop down list control. This value will be automatically displayed and entered in the card holders screen if no new value is entered. The default value is only used when adding a new card holder record.

OK/Cancel Buttons

Clicking on the OK button will save the changes made to the cardholder user fields. Clicking on the cancel button will not save the changes made to the cardholder user fields.

Edit the Cardholder Database

Editing the Cardholder database is used to change the structure of the Cardholder table in the system database. It is possible to change many attributes of the cardholder database fields; however, cardholder user fields present in the database upon installation cannot be deleted and these user fields also cannot have their data types changed. User-defined cardholder fields may be added, modified or deleted in the edit cardholder screen. Several different field types can be used along with several different data entry control types. Cardholder user field layouts can also be saved to and loaded from template files.

Database design can be very complex and is only recommended to be used by advanced users. It is recommended that a database backup be performed prior to saving any new fields or layouts to the system database. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

New Field

To add a new field to the Cardholder Database, click the New Field button. New fields added to the database will be inserted at the end of the database.

Edit Field

To edit an existing field in the Cardholder database, either double-click the row to be edited or click the Edit Field button while that row is highlighted. Note that fields which cannot be edited will appear grayed out.

Delete Field

To delete a cardholder field, select the row to be deleted and click the Delete Field button. Note that if the Delete Field button is grayed out, that field cannot be deleted from the Cardholder database.

Field Name

Enter the name of the new field.

Data Type

nvarchar - Variable-length Unicode character data can be a value from 1-4000 characters maximum.

bit - An integer data type that can take a value of 1, 0, or NULL.

datetime - Defines a date that is combined with a time of day with fractional seconds that is based on a 24-hour clock. Valid dates range from January 1, 1753 through

December 31, 9999. Valid times are 00:00:00 through 23:59:59.997.

int - Whole number data from -2,147,483,649 through 2,147,483,647.

ntext - Variable-length Unicode data with a maximum length of 1,073,741,823 characters.

Length

Use the up/down arrows to select the length of the new field.

Indexed

Use the drop down list to select whether indexing is to be used for the cardholder database field. Like databases in general, indexes must be designed carefully. Because they can take up significant disk space, it is inadvisable to implement more indexes than necessary. With this in mind, it is recommended that only cardholder database fields which will be used regularly as search criteria be indexed.

Yes - the field will be indexed, but not with a unique index.

No - the field will not be indexed.

Unique - the field will be index

Display Name

Enter the field display name.

Display Order

Use the up/down arrows to select the display order for the cardholder field. This is the order in which the user-defined/user-editable cardholder database fields will be display in Access It! Universal.NET.

Edit Control Type

Use the dropdown list to select the control type to be used for the field.

- *Text Box* - The text box edit control is used for the entry of free form alpha-numeric characters up to 50 characters in length.
 - *Input Mask* - An input mask can also be defined to control the way that data is entered into the user field. For example, an input mask of "#####" would force numeric only data entry up to 6 digits in length. Some common predefined input masks are included.
 - *Output Format* - An output format can be defined to control the way that entered data will appear when displayed. For example, an output format of (000)000-0000 would result in the input "8005551212" being formatted as (800)555-1212.
 - *Default Value* - If a value is entered, this will be the default value in the field for new

records added to the Cardholder database.

- *Drop Down List* - The drop down list edit control is used to present a list of predefined items to choose from during data entry. This is useful when data consistency is desired for a certain user field.
 - List Items - An example of this might be a "Department" user field with list items defined as "Sales", "Engineering", and "Management". This would ensure that instead of the operator typing in the word "Sales", it would be presented as a list item and would be entered the same way each time. An unlimited number of list items can be entered.
 - Default Value - If a value is entered, this will be the default value in the field for new records added to the Cardholder database
- *Date Combo* - The date combo edit control is used for the entry of dates. A calendar is also available when data entry is being performed to make entering dates easy.
- *Text Box with Required Entry* - The text box edit control is used for the entry of free form alpha-numeric characters up to 50 characters in length. An entry in this field will be required before a card holder can be saved. An input mask can also be defined to control the way that data is entered into the user field. For example, an input mask of "#####" would force numeric only data entry up to 6 digits in length. Several common predefined input masks are included.
 - Input Mask - An input mask can also be defined to control the way that data is entered into the user field. For example, an input mask of "#####" would force numeric only data entry up to 6 digits in length. Some common predefined input masks are included.
 - Output Format - An output format can be defined to control the way that entered data will appear when displayed. For example, an output format of (000)000-0000 would result in the input "8005551212" being formatted as (800)555-1212.
 - Default Value - If a value is entered, this will be the default value in the field for new records added to the Cardholder database

Save Field

Once the desired entries have been made for the new/updated cardholder field, click the Save button to commit the changes to the database. **Database design can be very complex and is only recommended to be used by advanced users. It is recommended that a database backup be performed prior to saving any new fields or layouts to the system database. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. The Access It! Universal.NET services must be restarted prior to having databases changes take effect.**

Database Configuration Utility

The Access It! Universal.NET database configuration utility is used to create, maintain and upgrade the system database. Transaction archives and backups are also performed with this utility as well as the server operating language selection. To run the database configuration utility, click on the windows start button, then choose the Database Configuration Utility from the Access It! Universal Utilities program folder.

Connect to Database

Enter the SQL Server connection information to connect to the system database server. Either Windows authentication or SQL Server authentication can be used depending upon how the SQL Server is configured. The server being connected to can either be on the same server as the application or on a remote SQL Server.

No other functions will be available until a successful database connection has been made.

Limited User

A limited user account can be created in cases when the system needs to be configured to run with the minimum SQL permissions. A limited user can be created by selecting Create Limited User from the File menu of the Database Configuration Utility.

Archive Events

Archiving is used to transfer events from the current events data file to an archive data file. Each time an archive is performed, a new archive event file is created. The archive data files are created and named with a date based file name assigned to them. The event and transaction history reports can then be used to run reports on any of the archive event files. For more information on printing event and history reports, see the [Reports](#) help file topic.

To initiate an immediate archive, click on the Archive button on the toolbar. Archive databases can also be taken offline and brought online with this utility to reduce the amount of time it takes to run an event or history report. To take an archive database online or offline, select the AIUEvents database and the Take Offline and Bring Online buttons on the toolbar will either be available or grayed out depending upon the current status of that events database. In addition, a database can be taken off-line permanently and moved to alternate storage media. Archives can also be set up to take place automatically by clicking on the archive settings tab. Archives can be set up to automatically archive when the event file reaches a certain number of events by selecting 'At a Predefined Event Count' in the Automatically Archive dropdown list. Selecting 'On a Schedule' from the Automatically Archive dropdown list enables the user to set up to archiving on a scheduled basis for whatever interval they choose. Changing the archive settings requires the AIUniversal

service be restarted for the changes to take effect.

Backup/Restore

Backup and restore are used to make backups of the system and event databases or to restore system and event databases. Backup files are stored in SQL Server .BAK file format. Backup files can be stored on any storage device locally attached to the SQL Server. Older backup files can be automatically removed if older than a specified number of days. Access It! Universal.NET is set up to perform a backup on a weekly basis by default if the SQL databases reside on the local computer; however, backups can also be scheduled to automatically occur on any other scheduled interval by adjusting the Backup Schedule parameters. An immediate backup can be performed by clicking the Backup button on the toolbar. Changing the Backup settings requires the AIUniversal service be restarted for the changes to take effect.

To restore a database, click the Restore button within the Utilities tab and then click the Restore button on the toolbar. Click the Select button to navigate to the folder containing the backup database file(s) to be restored. To restore multiple databases, check the boxes for all to be restored. By default, if more than one database is in the backup file, the utility will delete all existing Access It! Universal.NET databases. To retain an existing database, ensure that the Remove Existing Access It! Universal Database checkbox is unchecked. The Access It! Universal.NET services will be stopped prior to the restore executing.

When restoring databases from Access It! Universal.NET versions 1.x and 2.x, application data and event log backups will be in separate backup files and must be restored individually. The restore function MAY overwrite any existing databases if that option is selected!

Cardholder Fields

Edit Cardholder information is used to change the structure of the Cardholder table in the system database. It is possible to change many attributes of the cardholder database fields; however, cardholder user fields present in the database upon installation cannot be deleted and these user fields also cannot have their data types changed. User-defined cardholder fields may be added, modified or deleted in the edit cardholder screen. Several different field types can be used along with several different data entry control types. Cardholder user field layouts can also be saved to and loaded from template files. For more information modifying the structure of the Cardholder database, see the [Cardholder User Fields](#) help file topic.

Database design can be very complex and is only recommended to be used by advanced users. It is recommended that a database backup be performed prior to saving any new fields or layouts to the system database.

Replication

Replication is used to setup and maintain regional servers within the system. One regional server is designated as the publisher (master) and all other regional servers are designated

as subscribers (slaves). The system data is then replicated to and from the publisher and the subscribers to keep all of the databases in sync. Regional servers can be operated independently of each other in the event of a network failure and will re-synchronize when the network connection has been restored. The following replication functions are supported:

- *Create Publication* - This function is used to create a publication on the publishing server. A snapshot folder must be specified to store all of the publication files. This folder can either be a local folder or a network folder. All servers that are going to be subscribers to this publication must have read/write access to the snapshot folder. A publication must be created prior to creating any subscriptions.
- *Create Subscription* - This function is used to create a subscription to an existing publication. The publisher must be selected prior to creating the subscription. A new database must be created on each of the regional servers before the subscriptions can be initiated. Once the subscription has been created all of the data from the publisher will be downloaded to the new subscribing database. Data entered in either the publisher or subscriber will then be continuously synchronized as long as a network connection is available.
- *Drop Publication* - This function is used to drop a publication on the publishing server. Once the publication has been dropped all remaining subscriptions to the publication will also be dropped. No data will be removed from the system database when dropping a publication.
- *Drop Subscription* - This function is used to drop a subscription to an existing publication. Once the subscription has been dropped data will no longer be synchronized between the publisher and the subscriber. No data will be removed from the system database when dropping a subscription.

Regional server licenses must be purchased separately for each server. If the regional server option has not been licensed this section will not be available or displayed.

Load Reports

Load Reports will reload all stock reports into the Access It! Universal.NET database. Any custom created reports or stock reports with saved criteria will be retained. Load Reports can be accessed from the File menu of the Database Configuration Utility.

Data Manager

The Data Manager is used to execute SQL commands/queries on the SQL database that is currently selected from the dropdown list. Commands can be executed by typing them in the upper half of the right pane and then clicking the Execute button on the toolbar.

Database design can be very complex and is only recommended to be used by advanced users. It is recommended that a database backup be performed prior to performing any updates to any databases.

Database Utilities

Database Utilities can be accessed by clicking the Utilities button on the toolbar from within the Data Manager.

- *Set Security Mode*
 - *Integrated* - With integrated security, SQL Server leverages Windows NT authentication to validate SQL Server logon accounts. This allows the user to bypass the standard SQL Server logon process. With this approach, a network user can access a SQL Server database without supplying a separate logon identification or password because SQL Server obtains the user and password information from the Windows NT network security process.
 - *Mixed* - The mixed security mode allows validation by using either standard or integrated security modes. With mixed security mode, SQL Server uses integrated security for all trusted connections. For example, for a connection to a trusted ODBC source, authentication occurs via the Windows NT authentication process. If the integrated mode authentication fails, standard security mode is used requiring the entry of valid SQL Server logon information.
 - *SQL Server* - SQL Server uses its own validation process for checking all logon accounts. With standard security, each user provides an additional valid SQL Server logon ID and password. Each SQL Server logon specifies the allowed access to each database and its objects (tables, views, stored procedures, and rules). The logon accounts are considered valid if they appear in the encrypted syslogins table. Authentication consists of comparing the provided user name and password against similar information maintained in the SQL Server database.
Windows Authentication (Integrated) is much more secure than SQL Server Authentication. When possible, you should use Windows Authentication.
- *Change Password* - To change the password for the sa SQL Server account.
- *Check Database* - Performs a CHECKDB against the SQL database currently selected from the dropdown list. This checks only for allocation and consistency errors and does not correct any errors.
- *Repair Database* - Performs a CHECKDB against the SQL database currently selected from the dropdown list. This checks for and attempts to correct any errors encountered in the database. **Use the REPAIR option only as a last resort and only with the assistance of the Access It! Universal.NET technical support staff. To repair errors, restoring from a backup is preferred over repairing via the Repair Database option. Repair operations do not consider any of the constraints that may exist on or between tables.**
- *Single User Mode* - Only one user is permitted access to the SQL Server at a time.

Changing the security configuration requires a restart of the service.

Site Merge

The Site merge is used to import a separate Access It! Universal.NET system into another system as its own Site. The source and destination databases must both already be at the same revision. **The Enterprise edition of Access It! Universal.NET is required in order to use multiple sites.**

- Server Name
 - Enter the SQL Server name hosting the separate Access It! Universal.NET database
 - Authentication - Select either Windows Authentication or SQL Server Authentication
 - User Name - Enter a valid SQL username that has access to the SQL Server
 - Password - Enter a valid SQL password for the SQL username that has access to the SQL Server
- Database - Select the Access It! Universal.NET database

Configuring the Network

Firewall Settings

- Client - The firewall maybe turned on, no additional settings are required.
- Server - If the firewall is turned on, exceptions for TCP port 3030 and for the AIUniSvcNET.exe must be implemented.
- Other applications such as DVR interfaces, etc. will be application specific. Please reference the specific vendor's installation and configuration notes as needed.

General Notes

- You must be able to ping the server from the client.
- When in workgroup environments, the Windows username and password must match between the server and the client.
- If the service is running as local system account and the SQL Server is on another machine, the Database Configuration Utility needs to be setup for SQL authentication.

Troubleshooting

1. The server has rejected credentials for USER. Verify that the user name and password for this user are valid at the server.
 - Verify that the launching Windows user on the client workstation exists on the server as a local user.
2. Error 91: Object variable or with block variable not set
 - Check firewall settings.
 - Check Windows Application error log.
3. Couldn't connect to service - verify service is running on SERVER, the correct TCP port is specified and the firewall is properly configured.
 - Verify that the service is running on the server.
 - Verify that an exception has been made for either the Access It! Universal.NET service or TCP port 3030.

Sites

Sites Detail

Sites are used to create new or maintain existing sites within a database and specify various site capacities and parameters. A site is used to segregate (partition) data in a database. Only the hardware installed at a specific site will be available when connected to that site. To switch between the various sites select the desired site from the current site drop down located just under the system menu.

Any changes made at the site level will prompt for a reset all of the SCP panels in the site when changes are saved. If a reset is not performed a Macro can be scheduled to reset all the SCPs at a later point in time. Access to individual sites is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Site

To add a site, go to the sites entry screen by clicking on the Sites icon within the System group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu.

Editing a Site

To edit a site, go to the sites entry screen by clicking on the Sites icon within the System group of the Navigation pane. Select the site to be edited and click on the edit button on the toolbar, or double click the site to be edited. You can also select edit from the right click menu. When modifying a Site, all SCP's must be reset for any changes to take effect. Upon saving, the user is prompted to automatically reset all SCP's, or they can choose to manually reset the SCP's at a later point in time. If the user chooses to manually reset the SCP's, a [Macro](#) can be created and ran on a schedule to reset all SCPs at a designated time.

Deleting a Site

To delete a site, go to the sites entry screen by clicking on the Sites icon within the System group of the Navigation pane. All of the sites in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the site to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu.

Deleting a site will delete all associated site data along with the site itself. This deletion cannot be undone and the site will have to be manually re-entered or restored from a database backup! All event history for the deleted site will be retained in the event database but will not be accessible through the Access It! Universal.NET application.

Printing Site Reports

To print reports for a site, go to the sites entry screen by clicking on the Sites icon within the System group of the Navigation pane. All of the sites in the database will then be displayed in the right window pane of the Access It! Universal desktop. Select the sites to print reports for and click on the Reports button within the ribbon or from the right click menu select print reports. The following reports are available:

- *Site Listing* - This report provides a list of the selected sites and their various properties.

Cardholders

[Cardholders Detail](#)

Cardholders are used to maintain cardholders (people) and cards within the database. User fields are also available to store a variety of personnel information for each cardholder.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Cardholder

To add a cardholder, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Click on the new button on the toolbar or select new from the file option on the system menu or from the right click menu. A card and all associated information can also be added when adding a cardholder. If no card information is specified only a cardholder will be added.

Editing a Cardholder

To edit a cardholder, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Clicking on the search button with no criteria will display all cardholders in the database in the right window pane of the Access It! Universal.NET desktop. The list of cardholders can be sorted by clicking on any of the column titles in the display window. Cardholders can also be searched for by using the search function. For more information on finding specific cardholders, see the [Finding Cardholders](#) help file topic. Select the cardholder to be edited and click on the edit button on the toolbar, or double click the cardholder to be edited. You can also select edit from the right click menu.

Deleting a Cardholder

To delete a cardholder, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Clicking on the search button with no criteria will display all cardholders in the database in the right window pane of the Access It! Universal.NET desktop. The list of cardholders can be sorted by clicking on any of the column titles in the display window. Cardholders can also be searched for by using the search function. For more information on finding specific cardholders, see the [Finding Cardholders](#) help file topic. Select the cardholder to be deleted and click on the delete button on the toolbar. You can also select delete from the right click menu. You will then be asked to confirm the deletion, answer yes to delete the cardholder and all associated cards and no to cancel the deletion.

Cardholders Detail

Cardholders

Cardholders are used to maintain cardholders (people) and cards within the database. User fields are also available to store a variety of personnel information for each cardholder.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Last Name

Enter the last name for the card holder. This name can be up to 50 characters in length.

First Name

Enter the first name for the card holder. This name can be up to 50 characters in length.

Middle Initial

Enter the middle initial for the card holder. This name can be up to 1 character in length.

User Info

Enter user defined field information. These user fields can be used for supplemental information, such as department, license plate number, etc. These fields can be up to 50 characters in length. The labels for these user fields can be changed by using the cardholder user fields screen. For more information on editing cardholder user fields, see the [Cardholder User Fields](#) help file topic.

Access to the user fields is determined by the security settings for the currently logged on user. For more information on users, see the [Users](#) help file topic.

Capture

The capture button is used to activate the capture window and capture an image or signature for the card holder.

The style and functionality of the capture window will vary depending upon the type of capture device being used. See the manufacturer's documentation for the capture device for further information about the capture window.

▼ Capture Tools

The image capture tools button is used to bring up a tools menu for image or signature

capturing. The following tools are available:

- *Cut* - The cut option is used to delete the current image and copy it to the clipboard. This option is useful for either deleting an unwanted image from a card holder, or for moving an image to the clipboard.
- *Copy* - The copy option is used to copy the current image to the clipboard. This option is useful for copying a card holder image to the clipboard and pasting into an imaging application such as windows paintbrush.
- *Paste* - The paste option is used to paste the contents of the clipboard into the image capture window. This option is useful for capturing images created with a windows paintbrush application, or from another imaging application that does not have TWAIN or VFW software drivers.
- *Import* - The import option is used to capture an image from a physical disk file. This option is useful for capturing images from capture devices that have the capability of storing images to a file. The supported image file formats are JPEG (.JPG) and Windows Bitmap (.BMP).
- *Export* - The export option is used to export a captured image to a physical disk file. This option is useful for exporting images for use with imaging applications that can use disk based image files. The supported image file formats are JPEG (.JPG) and Windows Bitmap (.BMP).
- *Twain* - The Twain option is used to select the TWAIN device source and to acquire (capture) an image from the selected TWAIN source. This option is useful if an image is being captured using a TWAIN device that is not set as the default capture device. **The TWAIN sources will vary according to the third-party device drivers that are installed on the local workstation.**
- *Adjust* - The adjust option is used to adjust the brightness or contrast (lightness or darkness) of a captured image. Images can also be cropped using this option. To adjust the brightness and or contrast, click on the sliders to increase or decrease the brightness or contrast of the image. Click on apply to save the changes to the image or click on cancel to cancel the changes.

Cardholder Status

- *Inactive* - Cards for this cardholder will be inactive and will not work at any of the doors in the system regardless of the access levels assigned to the card.
- *Active* - Cards for this cardholder will be active and will work at any of the doors in the system that the access levels assigned to the card allow.
- *Date Based* - Cards for this cardholder card will become active on the date and time entered in the active date and time fields and will become inactive on the date and time entered in the expire date and time fields. **The option selected here will override whatever option is selected for the Card Status.**

Access Levels

A maximum of one hundred twenty-eight access levels may be assigned to a cardholder and each of their cards. For instance, if the cardholder is assigned one hundred access levels, any card assigned to that cardholder may be assigned up to an additional twenty-eight access levels. To assign access levels to a cardholder, select the access levels, then "move" the access levels that you wish to be assigned to the cardholder from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected access levels from the available window to the assigned window. The "<<" button will move all selected access levels from the assigned window to the available window. Multiple access levels can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired access levels. For more information on access levels, see the [Access Levels](#) help file topic.

Access to a cardholder's access levels is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. The maximum number of access levels that can be assigned to a cardholder/card can be set within the site property window. For more information on sites, see the [Sites](#) help file topic.

Sites

To assign sites to a cardholder, "move" the sites that you wish to be assigned to the cardholder from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected sites from the available window to the assigned window. The "<<" button will move all selected sites from the assigned window to the available window. Multiple sites can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired sites. For more information on sites, see the [Sites](#) help file topic.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Company

Select the company that this cardholder will be assigned to. If a company is selected only users with permissions to the selected company will have access to this cardholder. This cardholder can also be assigned to all companies which is useful for a shared cardholder.

Companies are used to partition cardholders within a site. For more information on companies, see the [Companies](#) help file topic. For more information on users, see the [Users](#) help file topic.

The available companies are determined based on a User's UserGroup permissions. If a User has full access to the companies feature, the User will have access to all companies, as well as the <None> company.

Biometrics

To capture a biometric template, click on the capture template button and follow the biometric device manufacturers instructions to complete the capture. To clear a template, click on the clear template button.

Biometric licenses must be purchased separately and a biometric reader type must be specified for the site.

The following fields will only be presented when adding a new cardholder:

Card Number

Enter the encoded card number to be added to the database. The encoded card number is the number that has been programmed into the card by the card manufacturer. The card number can range from 1 to 2147483647.

In certain card formats, the encoded card number and the printed card number may be different. If this field is left blank while adding a cardholder a cardholder will still be added with no cards associated to them.

Facility Code

Enter the facility code for the card being added to the database. The facility code is the number that has been programmed into the card by the card manufacturer. The facility code range depends upon the card formats being used.

In certain card formats, the facility code number may not be used. In these cases, enter a "-1" for the facility code number.

Embossed Number

Enter the Embossed Number on the Card. This field is an informational field used for selection/viewing/ reporting purposes.

PIN Number

Enter the PIN number for the card. The PIN number will be required at any doors that have a keypad reader and the reader mode is set to card and pin. The PIN number can range from 4 to 9 digits in length depending upon the number of PIN digits setting in each site. A random,

automatically generated PIN number can be assigned by clicking the auto button. For more information on reader modes, see the [Readers](#) help file topic. For more information on sites, see the [Sites](#) help file topic.

Issue Level

Select or enter the issue level. The issue level is one of the numbers that has been programmed into the card by the card manufacturer. The issue level can range from 1 to 255. Issue levels are generally used only with magnetic stripe cards.

In certain card formats, the issue level number may not be used. In these cases, use the default of "0" for the issue level number.

Use Limit

Select or enter the use limit for the card. Use limits will limit the number of times that the card can be used at any reader that has the non-zero use limit option set. Each time the card is granted access at any of these readers the number of uses remaining will be decremented by one. For more information on readers requiring non-zero use limits, see the [Readers](#) help file topic.

A use limit of 255 means the card will have unlimited uses and be exempt from use limit restrictions. Use limits are specific to each of the SCP panels in the system. If a card has a use limit of 20 and has access to readers set up to for use limits that are attached to two different SCP's, the card will have 20 uses at each of the SCP's. In addition, if an SCP panel is reset, the use limit will be reset to the value entered in this field. Use limits must be enabled for the site in order for this field to be available. For more information on sites, see the [Sites](#) help file topic.

Card Group

Select the card group for the card. The card group will group together cards with the same card group assigned to them. The card group can then be used to have a single card or a group of cards perform tasks when a card number from a certain card group is presented at a reader. The card group can also be used to set up mandatory or default card activation and expiration dates. The task to be performed by the card group and the conditions under which to perform the task are defined in the tasks screen. For more information on tasks, see the [Tasks](#) help file topic. For more information on card groups, see the [Card Groups](#) help file topic.

The card group is defaulted to "Main Card Group" for all cards being entered if card groups are not being used. A card group can contain anywhere from a single card, to all of the cards in the system.

Badge Type

Select the badge type to be used for this card. Only the badge type(s) that exist in the database will be available. For more information on badge types see the [Badge Types](#) help file topic.

Classification

Select the classification for this card. The classification can be used to group cards together for selection/viewing purposes and for reporting purposes.

PIN Exempt

Select (check) this option if this card is to be exempt from entering a PIN number at any of the doors that have a keypad reader and the reader mode is set to card and pin. When this option is checked, the pin number will be ignored and the cardholder will be granted or denied access strictly based on the card settings. For more information on reader modes, see the [Readers](#) help file topic.

Extended Access Times

Select (check) this option if this card is to have extended door access times. The door will remain unlocked and allowed to stay open longer than cards without this option selected. For more information on extended access, see the [Readers](#) help file topic.

Anti-passback Exempt

Select (check) this option if this card is to be exempt from anti-passback violations at any of the readers that are set up to use anti-passback and areas. When this option is checked, the anti-passback area will be ignored and the cardholder will be granted or denied access strictly based on the card settings. For more information on anti-passback and areas, see the [Readers](#) help file topic.

Unused Card Expiration Exempt

Select (check) this option if this card is to be exempt from being automatically deactivated if this card has not been used for a set number of days. When this option is checked, the card will not be automatically deactivated regardless of how long it had been since the card has been used. For more information on automatic card deactivation, see the [Servers](#) help file topic.

Card Status

- *Inactive* - The card will be inactive and will not work at any of the doors in the system regardless of the access levels assigned to the card.

- *Active* - The card will be active and will work at any of the doors in the system that the access levels assigned to the card allow.
- *Date Based* - The card will become active at midnight on the date entered in the active date field and will become inactive at midnight on the date entered in the expire date field.

Temporary Deactivate

Enter the temporary deactivate date and the temporary reactivate date for the card. Temporary card deactivation will temporarily deactivate a card at midnight on the date entered in the deactivate date field and reactivate the card at midnight on the date entered in the reactivate date field. While the card is temporarily deactivated it will not work at any of the doors in the system regardless of the access levels assigned to the card. This feature is useful for vacations, leaves of absence, etc.

Temporary card deactivation must be enabled for the site in order for these fields to be available. For more information on sites, see the [Sites](#) help file topic.

Available/Assigned Access Levels

To assign access levels to a card, select the access levels and "move" the access levels that you wish to be assigned to the card from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected access levels from the available window to the assigned window. The "<<" button will move all selected access levels from the assigned window to the available window. Multiple access levels can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired access levels. Up to 128 access levels can be assigned to a card.

Access to a cards access levels is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Temporary Access

Select the site, access level, activate date and deactivate date for temporary access for the card. Temporary access will assign the specified access level to the card during the time period specified. This is useful is a card needs temporary access to an area that it would not normally have access to.

Temporary access will only be displayed if it has been enabled for the site.

Precision Timezone

Select the timezone to be used for all of the selected readers being assigned for precision access. Only one timezone can be selected at a time, so when readers are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned reader it must be moved back to the

available window, then re-assigned with the new timezone.

This step will be skipped if precision access has not been enabled for the site. For more information on precision access, see the [Sites](#) help file topic.

Precision Available/Assigned Readers/Timezones

To assign readers for precision access, select the timezone and the desired reader(s), then "move" the readers that you wish to be assigned to the card from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window. The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired readers.

This step will be skipped if precision access has not been enabled for the site. For more information on precision access, see the [Sites](#) help file topic.

Save Only

This option will save the card to the database, but will not preview or print the card.

Save/Preview Badge

This option will save the cardholder/card to the database and also display (preview) the card on the screen. The card can also be printed from the preview window.

Save/Print Badge

This option will save the cardholder/card to the database and also print the card to the assigned printer. The printer that the card will be sent to is assigned when the badge type is designed. For more information on the Badge Designer, see the [Badge Designer](#) help file topic.

[Cardholders](#)

Finding Cardholders

Cardholders are used to maintain cardholders (people) within the database. User fields are also available to store a variety of personnel information for each cardholder.

Look For

Expanding the drop list under Look For allows the ability to change the default search criteria when searching cards. The default search criteria is Last name or Card Number.

Find Now

To find a specific cardholder, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Clicking on the search button without any criteria will display all cardholders in the database in the right window pane of the Access It! Universal.NET desktop. The list of cardholders can be sorted by clicking on any of the column titles in the display window. The list can then be manually searched to find the desired cardholder. A specific cardholder can also be located by entering the last name or part of a last name and clicking the find now button. To change the default search criteria from last name or cardholder, select the specified field from the Search for drop list.

Additional card holder data fields can be displayed in the card holders screen by right clicking anywhere inside the card holders grid and choosing select display fields from the right click menu. Any or all additional fields can then be displayed and the display order can be adjusted.

Advanced Find

The advanced find option is used to find cardholders by fields other than last name and is selectable by clicking the binocular icon within the Cardholders screen. The advanced find option is also used to build more advanced queries that can contain more than one search parameter. These advanced queries can also be saved to disk and loaded later for re-use.

Field

Select the field to be searched.

Condition

Select the condition that the data must meet to be included in the search results. The following conditions are available:

- *Is Equal To* - The value stored in the data field must be exactly the same as the value being searched for to be included in the search results. This is the equivalent of "=" in most query languages.
- *Is Not Equal To* - The value stored in the data field must not be exactly the same as the value being searched for to be included in the search results. This is the equivalent of "<>" in most query languages.
- *Is One Of* - The value stored in the data field must be the same as one of the values being searched for to be included in the search results. This is the equivalent of "OR" in most query languages.
- *Is Not One Of* - The value stored in the data field must not be the same as any of the values being searched for to be included in the search results. This is the equivalent of "<>" and "OR" in most query languages.
- *Is Less Than* - The value stored in the data field must be less than the value being searched for to be included in the search results. This is the equivalent of "<" or "LESS THAN" in most query languages.
- *Is Less Than Or Equal To* - The value stored in the data field must be less than or exactly the same as the value being searched for to be included in the search results. This is the equivalent of "<=" or "LESS THAN OR EQUAL TO" in most query languages.
- *Is Greater Than* - The value stored in the data field must be greater than the value being searched for to be included in the search results. This is the equivalent of ">" or "GREATER THAN" in most query languages.
- *Is Greater Than Or Equal To* - The value stored in the data field must be greater than or exactly the same as the value being searched for to be included in the search results. This is the equivalent of ">=" or "GREATER THAN OR EQUAL TO" in most query languages.
- *Is Between* - The value stored in the data field must be greater than or the same as the first value being searched for and less than or the same as the second value being searched for to be included in the search results. This is the equivalent of ">= AND <=" in most query languages.
- *Is Not Between* - The value stored in the data field must not be greater than or the same as the first value being searched for and not less than or the same as the second value being searched for to be included in the search results. This is the equivalent of "< AND >" in most query languages.
- *Is Like* - The value stored in the data field must be similar to the value being searched for to be included in the search results. This is the equivalent of "*abc*" or "LIKE" in most query languages.
- *Is Not Like* - The value stored in the data field must not be similar to the value being searched for to be included in the search results. This is the equivalent of "*abc*" or "NOT LIKE" in most query languages.
- *Is Empty* - The value stored in the data field must be empty or null to be included in the search results. This is the equivalent of "" or "NULL" in most query languages.
- *Is Not Empty* - The value stored in the data field must not be empty or null to be included in the search results. This is the equivalent of "" or "NOT NULL" in most query languages.

languages.

Value

Select or enter the value to be searched for. This field will vary based upon the condition that is selected. For some conditions, one value may be required and for other conditions multiple values may be required.

Add to List

After specifying the search field, condition and value(s), click on the add to list button to add the search criteria item to the list of search parameters. Multiple search criteria items can be added to refine the search parameters. All search criteria items are added together during the search.

Remove

Search criteria items can be removed by selecting (clicking) on an item in the list of search parameters and clicking the remove button.

Load Search

Search parameters can be loaded from previously saved queries by clicking on the load search button and selecting a saved query. All of the previously saved search criteria items will be loaded into the search parameter list. This option is useful for frequently run complex searches.

Save Search

Search parameters can be saved to disk by clicking on the save search button and assigning a name to the saved query. All of the search criteria items will be saved for later use. This option is useful for frequently run complex searches.

Import Data

Import card data is used to import cardholder and card data from external sources in to the Access It! Universal.NET database. Import card data can import data, images and signatures from a wide variety of sources. To import data, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Next, select import data from the Data drop list within the ribbon.

The ability to do Batch Updates/Imports/Exports is an optional feature and will not be available to select unless purchased. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Data Source Type

Select the data source type for the card data import. The data source type identifies the type of source data to be used for the import. The following data source types are supported:

- *Microsoft Access* - The data source is a Microsoft Access database.
- *Microsoft Excel* - The data source is a Microsoft Excel spreadsheet.
- *Microsoft SQL Server* - The data source is a Microsoft SQL Server database.
- *Text File* - The data source is a comma or tab delimited plain text file.

File Location/Connection Parameters

Enter or select the file or database to import data from. The parameters necessary will depend upon the data source type selected.

Select/Preview Data to be Imported

Select the data to be imported. Once selected a sample preview of the data to be imported will be displayed. The parameters necessary or the data being displayed will depend upon the data source type selected.

Drag and Drop the Source Fields to the Destination Fields

To assign source fields to destination fields, select the desired source field, then drag and drop the source field on to the destination field. To assign a static value to a destination field drag and drop the "<Static Value>" item on to the desired destination field and enter the static value when prompted. Field maps can then be saved and loaded for reuse.

The list of destination fields is dependent upon the options set for the current site. For example, if the number of access levels per card is set to six per card for the current site only six access level destination fields will be displayed. For more information on sites, see the

[Sites help file topic.](#)

Ready to Import

Click on the finish button to begin the import. A progress bar will display the percentage of completion as the import progresses. After the import completes a text file will be created listing all error messages if any errors have occurred.

Export Data

Export data is used to export cardholder and card data from the Access It! Universal database for use by an external source. Export card data can export data, images and signatures from the Access It! Universal.NET database. To export card data, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Next, select export card data from the Data drop list within the ribbon. **The ability to do Batch Updates/Imports/Exports is an optional feature and will not be available to select unless purchased. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.**

Select Records to Export

Select all records to export all of the cardholder and card data in the Access It! Universal database or choose selected records to export only specified data. For more information on finding specific records to export, see the [Finding Cardholders](#) help file topic.

Select Fields to Export

Select the cardholder and card fields to export. To assign fields to export, select the fields, then "move" the fields that you wish to export from the available window to the selected window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected fields from the available window to the selected window. The "<<" button will move all selected fields from the selected window to the available window. Multiple fields can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired fields.

Select Folder Location for Export.txt

Enter or select the destination folder in which the exported data (Export.txt), pictures and signatures are to be stored. Clicking on the change button will bring up a browse window for searching for and selecting the destination directory.

Two separate folders will be created under the destination folder specified. The pictures will be stored in a sub folder named "Pictures" and the signatures will be stored in a sub folder named "Signatures". Both of these folders will be created automatically.

Ready to Export

Click on the finish button to begin the export. A progress bar will display the percentage of completion as the export progresses. After the export completes a message will be displayed showing the number of records exported.

Bulk Card Insert

Bulk card insert is used to add specified cardholder and card data in bulk or batches to the Access It! Universal.NET database. Multiple cards can be added to a single cardholder or to multiple cardholders. To perform a bulk card insert, go to the cardholders data entry screen by either clicking on the cardholders toolbar button within the main group on the toolbar, or by selecting cardholders from the go option on the system menu. Next, select bulk card insert from the file option on the system menu.

The ability to do Batch Updates/Imports/Exports is an optional feature and will not be available to select unless purchased. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

The following parameters can be specified during a bulk card insert:

Last Name

Enter the last name for the card holder. This name can be up to 50 characters in length.

First Name

Enter the first name for the card holder. This name can be up to 50 characters in length.

Middle Initial

Enter the middle initial for the card holder. This name can be up to 1 character in length.

User Info

Enter user defined field information. These user fields can be used for supplemental information, such as department, license plate number, etc. These fields can be up to 50 characters in length. The labels for these user fields can be changed by using the cardholder user fields screen. For more information on editing cardholder user fields, see the [Cardholder User Fields](#) help file topic.

Access to the user fields is determined by the security settings for the currently logged on user. For more information on users, see the [Users](#) help file topic.

Capture

The capture button is used to activate the capture window and capture an image or signature for the card holder.

The style and functionality of the capture window will vary depending upon the type of

capture device being used. See the manufacturer's documentation for the capture device for further information about the capture window.

▼ Capture Tools

The image capture tools button is used to bring up a tools menu for image or signature capturing. The following tools are available:

- *Cut* - The cut option is used to delete the current image and copy it to the clipboard. This option is useful for either deleting an unwanted image from a card holder, or for moving an image to the clipboard.
- *Copy* - The copy option is used to copy the current image to the clipboard. This option is useful for copying a card holder image to the clipboard and pasting into an imaging application such as windows paintbrush.
- *Paste* - The paste option is used to paste the contents of the clipboard into the image capture window. This option is useful for capturing images created with a windows paintbrush application, or from another imaging application that does not have TWAIN or VFW software drivers.
- *Import* - The import option is used to capture an image from a physical disk file. This option is useful for capturing images from capture devices that have the capability of storing images to a file. The supported image file formats are JPEG (.JPG) and Windows Bitmap (.BMP).
- *Export* - The export option is used to export a captured image to a physical disk file. This option is useful for exporting images for use with imaging applications that can use disk based image files. The supported image file formats are JPEG (.JPG) and Windows Bitmap (.BMP).
- *Twain* - The Twain option is used to select the TWAIN device source and to acquire (capture) an image from the selected TWAIN source. This option is useful if an image is being captured using a TWAIN device that is not set as the default capture device. **The TWAIN sources will vary according to the third-party device drivers that are installed on the local workstation.**
- *Adjust* - The adjust option is used to adjust the brightness or contrast (lightness or darkness) of a captured image. Images can also be cropped using this option. To adjust the brightness and or contrast, click on the sliders to increase or decrease the brightness or contrast of the image. Click on apply to save the changes to the image or click on cancel to cancel the changes.

Cardholder Status

The cardholder status will override the status of any individual card.

- *Inactive* - The cardholder's cards will be inactive, all cards added for this cardholder will be inactive and will not work at any of the doors in the system regardless of the access levels assigned to the card.

- *Active* - The cardholder's cards will be active and will work at any of the doors in the system that the access levels assigned to the card allow.
- *Date Based* - The cardholder's cards will become active at midnight on the date entered in the active date field and will become inactive at midnight on the date entered in the expire date field.

Cardholder Access Levels

To assign access levels to a cardholder, select the access levels and "move" the access levels that you wish to be assigned to the cardholder from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected access levels from the available window to the assigned window. The "<<" button will move all selected access levels from the assigned window to the available window. Multiple access levels can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired access levels. Up to 128 access levels can be assigned to a cardholder.

Access to a cardholder's access levels is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Sites

To assign sites to a cardholder, "move" the sites that you wish to be assigned to the cardholder from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected sites from the available window to the assigned window. The "<<" button will move all selected sites from the assigned window to the available window. Multiple sites can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired sites. For more information on sites, see the [Sites](#) help file topic.

Company

Select the company that this cardholder will be assigned to. If a company is selected only users with permissions to the selected company will have access to this cardholder. This cardholder can also be assigned to all companies which is useful for a shared cardholder. Companies are used to partition cardholders within a site. For more information on companies, see the [Companies](#) help file topic. For more information on users, see the [Users](#) help file topic.

Biometrics

To capture a biometric template, click on the capture template button and follow the biometric device manufacturers instructions to complete the capture. To clear a template, click on the clear template button.

Biometric licenses must be purchased separately and a biometric reader type must be specified for the site.

Number of Cards to Add

Select or enter the number of cards to be added. The cards being added can either be added to a single cardholder or a cardholder can be created for each card being added.

First Card Number

Enter the first encoded card number to be added to the database. The first card number will be added and then incremented by one for each card being bulk inserted. The encoded card number is the number that has been programmed into the card by the card manufacturer. The card number can range from 1 to 2147483647.

In certain card formats, the encoded card number and the printed card number may be different. If this field is left blank while adding a cardholder a cardholder will still be added with no cards associated to them.

Facility Code

Enter the facility code for the card being added to the database. The facility code is the number that has been programmed into the card by the card manufacturer. The facility code range depends upon the card formats being used.

In certain card formats, the facility code number may not be used. In these cases, enter a "-1" for the facility code number.

PIN Number

Enter the PIN number for the card. The PIN number will be required at any doors that have a keypad reader and the reader mode is set to card and pin. The PIN number can range from 4 to 9 digits in length depending upon the number of PIN digits setting in each site. A random, automatically generated PIN number can be assigned by clicking the auto button. For more information on reader modes, see the [Readers](#) help file topic. For more information on sites, see the [Sites](#) help file topic.

Issue Level

Select or enter the issue level. The issue level is one of the numbers that has been programmed into the card by the card manufacturer. The issue level can range from 1 to 255. Issue levels are generally used only with magnetic stripe cards.

In certain card formats, the issue level number may not be used. In these cases, use the default of "0" for the issue level number.

Use Limit

Select or enter the use limit for the card. Use limits will limit the number of times that the card can be used at any reader that has the non-zero use limit option set. Each time the card is granted access at any of these readers the number of uses remaining will be decremented by one. For more information on readers requiring non-zero use limits, see the [Readers](#) help file topic.

A use limit of 255 means the card will have unlimited uses and be exempt from use limit restrictions. Use limits are specific to each of the SCP panels in the system. If a card has a use limit of 20 and has access to readers set up to for use limits that are attached to two different SCP's, the card will have 20 uses at each of the SCP's. In addition, if an SCP panel is reset, the use limit will be reset to the value entered in this field. Use limits must be enabled for the site in order for this field to be available. For more information on sites, see the [Sites](#) help file topic.

Card Group

Select the card group for the card. The card group will group together cards with the same card group assigned to them. The card group can then be used to have a single card or a group of cards perform tasks when a card number from a certain card group is presented at a reader. The card group can also be used to set up mandatory or default card activation and expiration dates. The task to be performed by the card group and the conditions under which to perform the task are defined in the tasks screen. For more information on tasks, see the [Tasks](#) help file topic. For more information on card groups, see the [Card Groups](#) help file topic.

The card group is defaulted to "Main Card Group" for all cards being entered if card groups are not being used. A card group can contain anywhere from a single card, to all of the cards in the system.

Badge Type

Select the badge type to be used for this card. Only the badge type(s) that exist in the database will be available. For more information on badge types see the [Badge Types](#) help file topic.

Classification

Select the classification for this card. The classification can be used to group cards together for selection/viewing purposes and for reporting purposes.

PIN Exempt

Select (check) this option if this card is to be exempt from entering a PIN number at any of

the doors that have a keypad reader and the reader mode is set to card and pin. When this option is checked, the pin number will be ignored and the cardholder will be granted or denied access strictly based on the card settings. For more information on reader modes, see the [Readers](#) help file topic.

Extended Access Times

Select (check) this option if this card is to have extended door access times. The door will remain unlocked and allowed to stay open longer than cards without this option selected. For more information on extended access, see the [Readers](#) help file topic.

Anti-passback Exempt

Select (check) this option if this card is to be exempt from anti-passback violations at any of the readers that are set up to use anti-passback and areas. When this option is checked, the anti-passback area will be ignored and the cardholder will be granted or denied access strictly based on the card settings. For more information on anti-passback and areas, see the [Readers](#) help file topic.

Unused Card Expiration Exempt

Select (check) this option if this card is to be exempt from being automatically deactivated if this card has not been used for a set number of days. When this option is checked, the card will not be automatically deactivated regardless of how long it had been since the card has been used. For more information on automatic card deactivation, see the [Servers](#) help file topic.

Card Status

- *Inactive* - The card will be inactive and will not work at any of the doors in the system regardless of the access levels assigned to the card.
- *Active* - The card will be active and will work at any of the doors in the system that the access levels assigned to the card allow.
- *Date Based* - The card will become active at midnight on the date entered in the active date field and will become inactive at midnight on the date entered in the expire date field.

Temporary Deactivate

Enter the temporary deactivate date and the temporary reactivate date for the card. Temporary card deactivation will temporarily deactivate a card at midnight on the date entered in the deactivate date field and reactivate the card at midnight on the date entered in the reactivate date field. While the card is temporarily deactivated it will not work at any of the

doors in the system regardless of the access levels assigned to the card. This feature is useful for vacations, leaves of absence, etc.

Temporary card deactivation must be enabled for the site in order for these fields to be available. For more information on sites, see the [Sites](#) help file topic.

Assign Access Levels

To assign access levels to a card, select the access levels and "move" the access levels that you wish to be assigned to the card from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected access levels from the available window to the assigned window. The "<<" button will move all selected access levels from the assigned window to the available window. Multiple access levels can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired access levels. Up to 128 access levels can be assigned to a card.

Access to a cards access levels is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Temporary Access

Select the site, access level, activate date and deactivate date for temporary access for the card. Temporary access will assign the specified access level to the card during the time period specified. This is useful is a card needs temporary access to an area that it would not normally have access to.

Temporary access will only be displayed if it has been enabled for the site.

Precision Timezone

Select the timezone to be used for all of the selected readers being assigned for precision access. Only one timezone can be selected at a time, so when readers are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned reader it must be moved back to the available window, then re-assigned with the new timezone.

This step will be skipped if precision access has not been enabled for the site. For more information on precision access, see the [Sites](#) help file topic.

Precision Available/Assigned Readers/Timezones

To assign readers for precision access, select the timezone and the desired reader(s), then "move" the readers that you wish to be assigned to the card from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window. The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding down the <Ctrl> key on the keyboard while

selecting (clicking) the desired readers.

This step will be skipped if precision access has not been enabled for the site. For more information on precision access, see the [Sites](#) help file topic.

Save Only

This option will save the card to the database, but will not preview or print the card.

Save/Preview Badge

This option will save the cardholder/card to the database and also display (preview) the card on the screen. The card can also be printed from the preview window.

Save/Print Badge

This option will save the cardholder/card to the database and also print the card to the assigned printer. The printer that the card will be sent to is assigned when the badge type is designed. For more information on the Badge Designer, see the [Badge Designer](#) help file topic.

Batch Update/Delete Data

Batch update/delete data is used to perform batch data updates or deletions to cardholder and card data in the Access It! Universal.NET database. To perform a batch update/delete, go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Next, select batch update/delete card data from the data pick list on the ribbon.

The ability to do Batch Updates/Imports/Exports is an optional feature and will not be available to select unless purchased. Also note that batch updates and deletes cannot be undone, so be sure to perform a database backup prior to any major changes. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

The following parameters can be specified during a batch update/delete:

Select Records to Update/Delete

Select all records to update or delete all of the cardholder and card data in the Access It! Universal.NET database or choose selected records to update or delete only specified data. For more information on finding specific records to update or delete, see the [Finding Cardholders](#) help file topic.

Select the Operation to Perform

Select either batch update or batch delete. If batch update is selected specify the field to be updated for the selected records and the new value to be inserted in to the field. If batch delete is selected choose whether to delete cards only or both cardholders and cards for the selected records.

Batch updates and deletes cannot be undone! It is highly recommended that a database backup be performed prior to batch updates or deletes. For more information on performing database backups see the Database Configuration Utility help file topic.

Ready to Perform Batch

The amount of records that will be updated will be displayed. Click on the finish button to begin the batch update or delete. A progress bar will display the percentage of completion as the update or delete progresses. After the update or delete completes a message will be displayed showing the number of records processed.

Cards

[Cards Detail](#)

Cards are used to maintain cards within the database. A card format that corresponds to the type of card being entered must be set up in the SCP panel properties for the card to function correctly.

The maximum number of supported cards is dependent upon the amount of memory installed in the SCP panels being used. The total number of supported cards is displayed in the SCP panel screen after the SCP model has been selected. For more information on card capacities, see the [SCP's](#) help file topic.

Adding a Card

There are two methods for adding cards. To add a card to a new cardholder go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Click on the new cardholder button on the ribbon or select new cardholder from the right click menu. To add a card to an existing cardholder go to the cardholders entry screen by clicking on the Cardholders icon within the Main group of the Navigation pane. Find or choose the cardholder to add a card to, then click on the drop list within the New button in the ribbon and select card or select new card from the right click menu within the cards section. For more information on cardholders, see the [Cardholders](#) help file topic.

Editing a Card

To edit a card, go to the cards entry screen by clicking on the Cards icon within the Main group of the Navigation pane. Clicking on the search button with no criteria defined will display all cards in the database in the right window pane of the Access It! Universal.NET desktop. The list of cards can be sorted by clicking on any of the column titles in the display window. Cards can also be searched for by using the search function. For more information on finding specific cards, see the [Finding Cards](#) help file topic. Select the card to be edited and click on the edit button on the toolbar, or double click the card to be edited. You can also select edit card from the right click menu. The cards will either have green, red or yellow icons. A green card icon indicates an active card. A red card icon indicates an inactive, expired or not yet active card. A yellow icon indicates a card with date based activation that is currently active for its specified date range.

 *Active Card*

 *Inactive Card*

 *Date Based Card*

Deleting a Card

To delete a card, go to the cards entry screen by clicking on the Cards icon within the Main group of the Navigation pane. Clicking on the search button with no criteria defined will display all cards in the database in the right window pane of the Access It! Universal.NET desktop. The list of cards can be sorted by clicking on any of the column titles in the display window. Cards can also be searched for by using the search function. For more information on finding specific cards, see the [Finding Cards](#) help file topic. Select the card to be deleted and click on the delete button on the toolbar. You can also select delete card from the right click menu. You will then be asked to confirm the deletion, answer yes to delete the card and no to cancel the deletion.

Cards Detail

Cards

Cards are used to maintain cards within the database. A card format that corresponds to the type of card being entered must be set up in the SCP panel properties for the card to function correctly.

The maximum number of supported cards is dependent upon the amount of memory installed in the SCP panels being used. The total number of supported cards is displayed in the SCP panel screen after the SCP model has been selected. For more information on card capacities, see the [SCP's](#) help file topic.

Card Number

Enter the encoded card number. The encoded card number is the number that has been programmed into the card by the card manufacturer. The card number can range from 1 to 2147483647 for small card number support or 1 to 9223372036854775807 for large card number support. Clicking on the auto button will automatically generate the next highest available card number by adding one to the largest card number in the database.

In certain card formats, the encoded card number and the printed card number may be different. For more information on large card number support, see the [Sites](#) help file topic.

Facility Code

Enter the facility code number. The facility code is the number that has been programmed into the card by the card manufacturer. The facility code range depends upon the card formats being used. This field will default to the last entry that was made.

In certain card formats, the facility code number may not be used. In these cases, enter a "-1" for the facility code number.

Embossed Number

Enter the Embossed Number on the Card. This field is an informational field used for selection/viewing/ reporting purposes.

PIN Number

Enter the PIN number for the card. The PIN number will be required at any doors that have a keypad reader and the reader mode is set to card and pin. The PIN number can range from 4 to 9 digits in length depending upon the number of PIN digits setting in each site. A random, automatically generated PIN number can be assigned by clicking the auto button. For more information on reader modes, see the [Readers](#) help file topic. For more information on sites,

see the [Sites](#) help file topic.

Issue Level

Select or enter the issue level. The issue level is one of the numbers that has been programmed into the card by the card manufacturer. The issue level can range from 1 to 255. Issue levels are generally used only with magnetic stripe cards.

In certain card formats, the issue level number may not be used. In these cases, use the default of "0" for the issue level number.

Use Limit

Select or enter the use limit for the card. Use limits will limit the number of times that the card can be used at any reader that has the non-zero use limit option set. Each time the card is granted access at any of these readers the number of uses remaining will be decremented by one. For more information on readers requiring non-zero use limits, see the [Readers](#) help file topic.

A use limit of 255 means the card will have unlimited uses and be exempt from use limit restrictions. Use limits are specific to each of the SCP panels in the system. If a card has a use limit of 20 and has access to readers set up to for use limits that are attached to two different SCP's, the card will have 20 uses at each of the SCP's. In addition, if an SCP panel is reset, the use limit will be reset to the value entered in this field. Use limits must be enabled for the site in order for this field to be available. For more information on sites, see the [Sites](#) help file topic.

Card Group

Select the card group for the card. The card group will group together cards with the same card group assigned to them. The card group can then be used to have a single card or a group of cards perform tasks when a card number from a certain card group is presented at a reader. The card group can also be used to set up mandatory or default card activation and expiration dates. The task to be performed by the card group and the conditions under which to perform the task are defined in the tasks screen. For more information on tasks, see the [Tasks](#) help file topic. For more information on card groups, see the [Card Groups](#) help file topic.

The card group is defaulted to "Main Card Group" for all cards being entered if card groups are not being used. A card group can contain anywhere from a single card, to all of the cards in the system.

Classification

Select the classification for this card. The classification can be used to group cards together for selection/viewing purposes and for reporting purposes.

Large Encoded ID

The Large Encoded ID is a representation of the GUID on a PIV-I card. It is recommended this field is automatically entered using an enrollment reader. For more information on enrollment readers see the [Workstations](#) help file topic.

Large Encoded ID must be enabled for the site in order for this field to be available. For more information on sites, see the [Sites](#) help file topic.

PIN Exempt

Select (check) this option if this card is to be exempt from entering a PIN number at any of the doors that have a keypad reader and the reader mode is set to card and pin. When this option is checked, the pin number will be ignored and the cardholder will be granted or denied access strictly based on the card settings. For more information on reader modes, see the [Readers](#) help file topic.

Anti-passback Exempt

Select (check) this option if this card is to be exempt from anti-passback violations at any of the readers that are set up to use anti-passback and areas. When this option is checked, the anti-passback area will be ignored and the cardholder will be granted or denied access strictly based on the card settings. For more information on anti-passback and areas, see the [Readers](#) help file topic.

Extended Access Times

Select (check) this option if this card is to have extended door access times. The door will remain unlocked and allowed to stay open longer than cards without this option selected. For more information on extended access, see the [Readers](#) help file topic.

Unused Card Expiration Exempt

Select (check) this option if this card is to be exempt from being automatically deactivated if this card has not been used for a set number of days. When this option is checked, the card will not be automatically deactivated regardless of how long it had been since the card has been used. For more information on automatic card deactivation, see the [Servers](#) help file topic.

Card Status

- *Inactive*- The card will be inactive and will not work at any of the doors in the system regardless of the access levels assigned to the card.
- *Active* - The card will be active and will work at any of the doors in the system that the

access levels assigned to the card allow.

- *Date Based* - The card will become active at midnight on the date entered in the active date field and will become inactive at midnight on the date entered in the expire date field.

Cardholder status overrides Card status. For example, if the Card status is Active, but the Cardholder status is Inactive, the card will be inactive.

Temporary Deactivate

Enter the temporary deactivate date and the temporary reactivate date for the card. Temporary card deactivation will temporarily deactivate a card at midnight on the date entered in the deactivate date field and reactivate the card at midnight on the date entered in the reactivate date field. While the card is temporarily deactivated it will not work at any of the doors in the system regardless of the access levels assigned to the card. This feature is useful for vacations, leaves of absence, etc.

Temporary card deactivation must be enabled for the site in order for these fields to be available. For more information on sites, see the [Sites](#) help file topic.

Cardholder Status

- *Inactive* - The card will be inactive and will not work at any of the doors in the system regardless of the access levels assigned to the card.
- *Active* - The card will be active and will work at any of the doors in the system that the access levels assigned to the card allow.
- *Date Based* - The card will become active at midnight on the date entered in the active date field and will become inactive at midnight on the date entered in the expire date field. **This is informational only and cannot be changed from this screen. Go to the Edit Cardholder screen to make changes to this option.**

Site

Use the dropdown list to select the Site for which access levels will be added to the card. **Access to a Site is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. For more information on sites, see the [Sites](#) help file topic.**

Access Levels

A maximum of one hundred twenty-eight access levels may be assigned to a cardholder and each of their cards. For instance, if the cardholder is assigned one hundred access levels, any card assigned to that cardholder may be assigned up to an additional twenty-eight access levels. To assign access levels to a card, select the access levels, then "move" the access levels that you wish to be assigned to the card from the available window to the

assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected access levels from the available window to the assigned window. The "<<" button will move all selected access levels from the assigned window to the available window. Multiple access levels can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired access levels. For more information on access levels, see the [Access Levels](#) help file topic. **Access to a card's access levels is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. The maximum number of access levels(6, 32, or 128) that can be assigned to a cardholder/card can be set for the site. For more information on sites, see the [Sites](#) help file topic.**

Cardholder Access Level

This area cannot be edited from this screen and is informational only. Cardholder access levels are access levels that apply in addition to access levels defined for the card.

Access to a cardholder's access levels is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. For more information on setting Cardholder Access Levels, see the [Cardholders](#) help file topic.

Temporary Access

Select the site, access level, activate date and deactivate date for temporary access for the card. Temporary access will assign the specified access level to the card during the time period specified. This is useful is a card needs temporary access to an area that it would not normally have access to. **Temporary access will only be displayed if it has been enabled for the site.**

Precision Timezone

Select the timezone to be used for all of the selected readers being assigned for precision access. Only one timezone can be selected at a time, so when readers are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned reader it must be moved back to the available window, then re-assigned with the new timezone. For more information on precision access, see the [Sites](#) help file topic. **The precision access tab will only be displayed if precision access has been enabled for the site.**

Precision Available/Assigned Readers/Timezones

To assign readers for precision access, select the timezone and the desired reader(s), then "move" the readers that you wish to be assigned to the card from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window. The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding

down the <Ctrl> key on the keyboard while selecting (clicking) the desired readers. For more information on precision access, see the [Sites](#) help file topic. **The precision access tab will only be displayed if precision access has been enabled for the site.**

User Type

Select the IP lockset user type for the card. More information on the user types can be found in the [User Types](#) help file.

Access Mode

- *Card Only* - Only a valid card will need to be presented at the IP lockset to gain access to the door.
- *Card Or PIN* - A valid card or a valid PIN will need to be presented at the IP lockset to gain access to the door.
Persona locksets do not support Card Or PIN
- *Card And PIN* - A valid card and a valid PIN will need to be presented at the IP lockset to gain access to the door.
- *Card Then PIN* - A valid card then a valid PIN will need to be presented at the IP lockset to gain access to the door.

Depending upon the type of IP lockset being used some of these access modes may not be supported. IP lockset licenses must be purchased separately. This tab will only be visible if one or more IP lockset licenses have been purchased.

Credential Format

Select the credential format to be used for this card. The credential format is used to select the type of cards being used with the IP locksets. Credential formats can be added, edited and deleted using the edit button to go to the credential format editor. The parameter information will generally be provided by the lockset or card manufacturer. For more information on credential formats, see the [Credential Formats](#) help file topic.

IP lockset licenses must be purchased separately. This tab will only be visible if one or more IP lockset licenses have been purchased.

IP Lockset Timezone

Select the timezone to be used for all of the selected IP locksets being assigned for access. Only one timezone can be selected at a time, so when locksets are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned lockset it must be moved back to the available window, then re-assigned with the new timezone.

IP lockset licenses must be purchased separately. This tab will only be visible if one or more IP lockset licenses have been purchased.

IP Lockset Available/Assigned Locksets/Timezones

To assign IP locksets for access, select the timezone and the desired lockset(s), then "move" the locksets that you wish to be assigned to the card from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected locksets from the available window to the assigned window. The "<<" button will move all selected locksets from the assigned window to the available window. Multiple locksets can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired locksets.

IP lockset licenses must be purchased separately. This tab will only be visible if one or more IP lockset licenses have been purchased.

SALTO Key Options

- *Override Privacy* - Allows the user access to a door that has been locked from the inside.
- *Override Lockdown* - Allows the user to open a door closed by lockdown.
Applies to both online doors and offline doors that have AMOK locks.
- *Set Lockdown* - Allows the user to enable or disable the lockdown mode on a door. This is done by presenting a valid key to the door's inside reader.
Applies to both online doors and offline doors that have AMOK locks.
- *Office* - Allows the user to set doors to Office mode.
- *Use Antipassback* - Ensures that a user cannot enter through the same door multiple times until they have first exited the door (or until a specified time period has passed). This is to prevent a key being used by a number of different users.
- *Audit Openings in the Key* - Ensures that a user cannot enter through the same door multiple times until they have first exited the door (or until a specified time period has passed). This is to prevent a key being used by a number of different users.
- *PIN Code Enabled* - This allows a user entry to access points that require card and PIN code. SALTO Door integrated reader licenses must be purchased separately. This tab will only be visible if the SALTO integration is enabled.

SALTO Key Expiration

Timezones must be configured within Salto ProAccess SPACE.

- *Calendar* - Select Calendar to be applied to the key. Calendar must be created within Salto ProAccess SPACE.
- *Enable Revalidation of Key Expiration* - Allows for automatic renewal of keys when presented at an online lock. The key will be renewed for the specified update period.
- *Update Period* - The amount of time the key will be renewed for when presented at an

online lock. Salto Door integrated reader licenses must be purchased separately. This tab will only be visible if the SALTO integration is enabled.

Salto Key Status

- **Assign Key** - Initializes selected encoder. To encode a new key, present it to the Salto encoder.
- **Update Key** - Initializes selected encoder. To update an existing key, present it to the Salto encoder.
- **Cancel Key** - Initializes selected encoder. Deactivates current key. Key will continue to work at offline locks until presented at an online reader.

Salto Door integrated reader licenses must be purchased separately. This tab will only be visible if the Salto integration is enabled.

Timezones must be configured within Salto ProAccess SPACE.

Salto Door/Timezone Access

To assign Salto Doors to an access level, select the timezone and the desired Salto Door(s), then "move" the Salto Doors that you wish to be assigned to the access level from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected Salto Doors from the available window to the assigned window. The "<<" button will move all selected Salto Doors from the assigned window to the available window. Multiple Salto Doors can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired Salto Doors.

Salto Door integrated reader licenses must be purchased separately. This tab will only be visible if the SALTO integration is enabled.

Timezones must be configured within SALTO ProAccess SPACE.

Elevator

The Elevator tab is used in conjunction with advanced elevator control. Currently the only supported integration is with Otis Destination Dispatching.

The Advanced Elevator integrated license must be purchased separately. This tab will only be visible if the Advanced Elevator integration is enabled.

Default Floor

- *Default Floor* - Used with Otis elevator modes 2 and 4. This is the default floor access will be given to.
- *Door* - When using elevator cabs with front and rear entry this is used by Otis elevator modes 2 and 4. This is the default door access will be given to when arriving to the

default floor.

User Types

- *VIP* - When this user is granted access to the elevator reader, a VIP call is made to the elevator
- *Vertigo* - When this user is granted access to the elevator reader, a Vertigo call is made to the elevator
- *Split Group Operation* - When this user is granted access to the elevator reader, a split group operation call is made to the elevator.
- *Vertigo2* - When this user is granted access to the elevator reader, a Vertigo 2 call is made to the elevator
- *Cart Service* - When this user is granted access to the elevator reader, a Cart Service call is made to the elevator
- *CIM Override* - When this user is granted access to the elevator reader, a CIM Override call is made to the elevator

Badge Type

Select the badge type for the card. The badge type will determine the graphical appearance and layout of the card when it is printed or previewed to the screen. For more information on badge types, see the [Badge Types](#) help file topic. **Only badge types that have been designed and saved using the badge type designer will be available for selection. For more information on the badge designer, see the [Badge Designer](#) help file topic.**

Issued By

This field stores the user name of the logged in user whenever the card is printed. This field is only updated when the card is printed and not when the card is previewed to the screen. This field cannot be updated by any other means than printing the card.

Date Issued

This field stores the current date and time whenever the card is printed. This field is only updated when the card is printed and not when the card is previewed to the screen. This field cannot be updated by any other means than printing the card.

Number of Times Printed

This field stores the number of times that the card has been printed. Each time the card is printed, this field will be automatically incremented by one. This field is only updated when the card is printed and not when the card is previewed to the screen. This field cannot be updated by any other means than

printing the card.

Event Type

[Card Event Types](#)

Annunciation Type

- *Disregard*: Card events (transactions) for this event type will not be recorded in the event file and will not be displayed in either the events window or in the alarms window.
- *Log Only*: Card events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display*: Card events (transactions) for this event type will be recorded in the event file and displayed in the events window.
- *Alarm*: Card events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic. **The alarm priority is only used for event types that have the annunciation type set to "Alarm".**

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on alarms, see the [Alarms](#) help file topic. **The alarm message is only used for event types that have the annunciation type set to "Alarm".**

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the alarms

window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic. **The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.**

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Usage

These fields will display the last place used, last time used and the last activity for the current card. These fields are for display purposes only and cannot be edited.

Save/Close Buttons

Clicking on the save button will save the changes made to the card. Clicking on the close button will not save the changes made to the card.

[Cards](#)

Finding Cards

Cards are used to maintain cards within the database. A card format that corresponds to the type of card being entered must be set up in the SCP panel properties for the card to function correctly.

The maximum number of supported cards is dependent upon the amount of memory installed in the SCP panels being used. The total number of supported cards is displayed in the SCP panel screen after the SCP model has been selected. For more information on card capacities, see the [SCP's help file](#) topic.

Find Now

To find a specific card, go to the card groups entry screen by clicking on the Card Groups icon within the Main group of the Navigation pane. Clicking on the search button with no criteria specified will display all cards in the database in the right window pane of the Access It! Universal.NET desktop. The list of cards can be sorted by clicking on any of the column titles in the display window. The list can then be manually searched to find the desired card. A specific card can also be located by entering the card number and clicking the search button. To change the default search criteria from last name or cardholder, select the specified field from the Search for drop list. Cards can be located by the cardholder that they belong to using the search button from the cardholders screen. For more information on finding cardholders, see the [Finding Cardholders](#) help file topic.

Additional card data fields can be displayed in the cards screen by right clicking anywhere inside the cards grid and choosing select display fields from the right click menu. Any or all additional fields can then be displayed and the display order can be adjusted.

Advanced Find

The advanced find option is used to find cards by fields other than card number and is selectable by clicking the binocular icon within the Cards screen. The advanced find option is also used to build more advanced queries that can contain more than one search parameter. These advanced queries can also be saved to disk and loaded later for re-use.

Field

Select the field to be searched.

Condition

Select the condition that the data must meet to be included in the search results. The following conditions are available:

- *Is Equal To* - The value stored in the data field must be exactly the same as the value being searched for to be included in the search results. This is the equivalent of "=" in most query languages.
- *Is Not Equal To* - The value stored in the data field must not be exactly the same as the value being searched for to be included in the search results. This is the equivalent of "<>" in most query languages.
- *Is One Of* - The value stored in the data field must be the same as one of the values being searched for to be included in the search results. This is the equivalent of "OR" in most query languages.
- *Is Not One Of* - The value stored in the data field must not be the same as any of the values being searched for to be included in the search results. This is the equivalent of "<>" and "OR" in most query languages.
- *Is Less Than* - The value stored in the data field must be less than the value being searched for to be included in the search results. This is the equivalent of "<" or "LESS THAN" in most query languages.
- *Is Less Than Or Equal To* - The value stored in the data field must be less than or exactly the same as the value being searched for to be included in the search results. This is the equivalent of "<=" or "LESS THAN OR EQUAL TO" in most query languages.
- *Is Greater Than* - The value stored in the data field must be greater than the value being searched for to be included in the search results. This is the equivalent of ">" or "GREATER THAN" in most query languages.
- *Is Greater Than Or Equal To* - The value stored in the data field must be greater than or exactly the same as the value being searched for to be included in the search results. This is the equivalent of ">=" or "GREATER THAN OR EQUAL TO" in most query languages.
- *Is Between* - The value stored in the data field must be greater than or the same as the first value being searched for and less than or the same as the second value being searched for to be included in the search results. This is the equivalent of ">= AND <=" in most query languages.
- *Is Not Between* - The value stored in the data field must not be greater than or the same as the first value being searched for and not less than or the same as the second value being searched for to be included in the search results. This is the equivalent of "< AND >" in most query languages.
- *Is Like* - The value stored in the data field must be similar to the value being searched for to be included in the search results. This is the equivalent of "*abc*" or "LIKE" in most query languages.
- *Is Not Like* - The value stored in the data field must not be similar to the value being searched for to be included in the search results. This is the equivalent of "*abc*" or "NOT LIKE" in most query languages.
- *Is Empty* - The value stored in the data field must be empty or null to be included in the search results. This is the equivalent of "" or "NULL" in most query languages.
- *Is Not Empty* - The value stored in the data field must not be empty or null to be included in the search results. This is the equivalent of "" or "NOT NULL" in most query

languages.

Value

Select or enter the value to be searched for. This field will vary based upon the condition that is selected. For some conditions, one value may be required and for other conditions multiple values may be required.

Add to List

After specifying the search field, condition and value(s), click on the add to list button to add the search criteria item to the list of search parameters. Multiple search criteria items can be added to refine the search parameters. All search criteria items are added together during the search.

Remove

Search criteria items can be removed by selecting (clicking) on an item in the list of search parameters and clicking the remove button.

Load Search

Search parameters can be loaded from previously saved queries by clicking on the load search button and selecting a saved query. All of the previously saved search criteria items will be loaded into the search parameter list. This option is useful for frequently run complex searches.

Save Search

Search parameters can be saved to disk by clicking on the save search button and assigning a name to the saved query. All of the search criteria items will be saved for later use. This option is useful for frequently run complex searches.

Previewing Cards

Cards are used to maintain cards within the database. A card format that corresponds to the type of card being entered must be set up in the SCP panel properties for the card to function correctly.

The maximum number of supported cards is dependent upon the amount of memory installed in the SCP panels being used. The total number of supported cards is displayed in the SCP panel screen after the SCP model has been selected. For more information on card capacities, see the [SCP's help file topic](#).

Previewing a Card

Cards can be previewed by going to the card entry screen by clicking on the Cards icon within the Main group of the Navigation pane. Clicking on the search button without criteria will display all cards in the database in the right window pane of the Access It! Universal.NET desktop. The list of cards can be sorted by clicking on any of the column titles in the display window. Cards can also be searched for by using the search function. For more information on finding specific cards, see the [Finding Cards](#) help file topic. Select the card to be previewed and click on the print button on the toolbar. You can also select print from the right click menu. Cards can also be previewed from the cardholders screen. For more information on cardholders, see the [Cardholders](#) help file topic.

Printing Cards

Cards are used to maintain cards within the database. A card format that corresponds to the type of card being entered must be set up in the SCP panel properties for the card to function correctly.

The maximum number of supported cards is dependent upon the amount of memory installed in the SCP panels being used. The total number of supported cards is displayed in the SCP panel screen after the SCP model has been selected. For more information on card capacities, see the [SCP's help file topic](#).

Printing a Card

Cards can be printed by going to the card entry screen by clicking on the Card icon within the Main group of the Navigation pane. Clicking on the search button without criteria will display all cards in the database in the right window pane of the Access It! Universal.NET desktop. The list of cards can be sorted by clicking on any of the column titles in the display window. Cards can also be searched for by using the search function. For more information on finding specific cards, see the [Finding Cards](#) help file topic. Select the card to be printed and click on the print button on the toolbar. You can also select print from the right click menu. A print dialog will be presented and the card will be sent to the printer selected. For more information on the Badge Designer, see the [Badge Designer](#) help file topic. Cards can also be printed from the cardholders screen. For more information on cardholders, see the [Cardholders](#) help file topic.

Batch Print Cards

Cards can be printed in batches by going to the card entry screen by clicking on the Card icon within the Main group of the Navigation pane. Clicking on the search button without criteria will display all cards in the database in the right window pane of the Access It! Universal.NET desktop. The list of cards can be sorted by clicking on any of the column titles in the display window. Cards can also be searched for by using the search function. For more information on finding specific cards, see the [Finding Cards](#) help file topic. Select the Batch Print Badges button on the toolbar. A print dialog will be presented allowing for entering the criteria of the card(s) to be printed as well as the sort order. For more information on the Badge Designer, see the [Badge Designer](#) help file topic. Cards can also be printed from the cardholders screen. For more information on cardholders, see the [Cardholders](#) help file topic.

Macros

[Macros Detail](#)

Macros are used to execute tasks, send email and paging notifications, print/email reports and run external programs from within the system. Macros can execute multiple tasks at the same time and execute tasks from different SCP panels, providing a way to execute tasks globally across all of the SCP panels within the system. Macros can also execute any command line program or utility that can be run from the operating system command prompt. **Macros are stored in the server computer's database and will only execute while the SCP panel(s) is being communicated to with the Access It! Universal.NET software. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.**

Adding a Basic Macro

To add a basic macro, go to the macros entry screen by clicking on the Macros icon within the Main group of the Navigation pane. All of the macros in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the New | Basic Macro button within the ribbon or select New Basic Macro from the right click menu.

Adding a Macro

To add a macro, go to the macros entry screen by clicking on the Macros icon within the Main group of the Navigation pane. All of the macros in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the New | Macro button within the ribbon or select New Macro from the right click menu.

Editing a Macro

To edit a macro, go to the macros data entry screen by either clicking on the macros toolbar button within the main group on the toolbar, or by selecting macros from the go option on the system menu. All of the macros in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the macro to be edited and click on the edit button on the toolbar, or double click the macro to be edited. You can also select edit from the file option on the system menu or from the right click menu.

Deleting a Macro

To delete a macro, go to the macros entry screen by clicking on the Macros icon within the Main group of the Navigation pane. All of the macros in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the macro to be

deleted and click on the delete button within the ribbon. You can also select delete from the right click menu.

Printing Macro Reports

To print reports for a macro, go to the macros entry screen by clicking on the Macros icon within the Main group of the Navigation pane. All of the macros in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the macros to print reports for and click on the print button on the toolbar or select print from the file option on the system menu or from the right click menu. The following reports are available:

- *Macro History* - This report provides a list of all database updates to the selected macros as well as macro execution history.
- *Macro Listing* - This report provides a list of the selected macros and their various properties.
- *Macro Scheduled for Execution* - This report provides a list of the selected macros and their schedules, as well as the next scheduled execution time.

Schedule / Calendar Tab

The Schedule tab displays a calendar listing all the Macros scheduled. Existing Macro's can be edited by double clicking, or right clicking on a scheduled Macro. To create a new macro for a specific day, double click or right click on the day and select New Basic Macro.

- *Import Schedule* - To create a new Macro based off an iCal file, right click within the scheduler and select Import. Upon import the new Basic Macro wizard will run with the schedule tab populated with the dates from the iCal file.
- *Export Schedule* - To export a scheduled Macro to a iCal file, right click on the scheduled event and select Export. The iCal file will contain the Macro's name, and scheduled date/time information.

Macro Execution

To manually execute a macro, go to the macros entry screen by clicking on the Macro icon within the Hardware group of the Navigation pane. All of the macros in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the macro to execute and click on the execute macro drop down next to the refresh button on the toolbar. You can also manually execute a macro by selecting execute macro from the right click menu.

To automatically execute a macro, select the macro to be executed for any of the event types in the following screens: cards, SCP's, SIO's, readers, inputs or outputs. For more information on executing macros from any of these screens, see the associated help file topic.

Macros Detail

Macros

Macros are used to execute tasks, send email and paging notifications, print/email reports and run external programs from within the system. Macros can execute multiple tasks at the same time and execute tasks from different SCP panels, providing a way to execute tasks globally across all of the SCP panels within the system. Macros can also execute any command line program or utility that can be run from the operating system command prompt. **Macros are stored in the server computer's database and will only execute while the SCP panel(s) is being communicated to with the Access It! Universal.NET software. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.**

Macro Type

- Basic Macro - A Basic Macro is a single operation Macro that can be scheduled. Additional operations can be added to the Basic Macro after it has been saved.
- Standard Macro (Legacy) - The legacy New Macro form. Multiple operations can be added and the Macro can be scheduled.

Macro Name

Enter the name to be used for this macro. All of the macros have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the macros being used. An example of a friendly name would be "Emergency Evacuation - Unlock ALL Doors". The macro name can be up to 50 characters in length.

Macro Enabled

Select (check) this option if this macro is to be enabled. If the macro enabled option is checked, the macro is enabled and can be executed either manually or automatically. If the macro enabled option is not checked, the macro cannot be executed either manually or automatically. This is useful for temporarily disabling a macro from being executed without having to delete the macro.

Global Macro

Select (check) this option if this macro is to be available to other Macro's located in separate sites.

Continue On Error

Select (check) this option if this macro contains multiple steps and the Macro should not stop if one of the steps does not complete successfully.

Macro Actions/Steps

Enter the actions/steps to be performed by this macro. Macros can perform as many steps as desired. Click on the add button and choose the step to be performed. The following macro steps are supported:

- Reader/Door Actions
 - *Grant Access* - Grant Access to the selected reader(s).
 - *Disable Reader* - Disable the selected reader(s).
 - *Unlock Reader/Door* - Unlock the selected reader(s).
 - *Lock Reader/Door* - Lock the selected reader(s).
 - *Set Mode to Facility Code Only* - Set the selected reader(s) to Facility Code Only Mode.
 - *Set Mode to Card Only* - Set the selected reader(s) to Card Only Mode.
 - *Set Mode to PIN Only* - Set the selected reader(s) to PIN Only Mode.
 - *Set Mode to Card And PIN Only* - Set the selected reader(s) to Card And PIN Mode.
 - *Set Mode to Card Or PIN Only* - Set the selected reader(s) to Card Or PIN Mode.
 - *Cancel Temporary Reader Mode* - Cancel the temporary mode for the selected reader(s).
- Task Actions
 - *Execute Task* - The selected task will be executed.
 - *Enable Task* - The selected task will be enabled.
 - *Disable Task* - The selected task will be disabled.
- Recipient Actions
 - *Email Recipient* - The selected recipient will be sent an email when executed.
 - *Email Report* - The selected report will be sent via email to the selected recipient in the selected format when executed.
- Macro Actions
 - *Execute Macro* - The selected Macro will be executed. Used in conjunction with the global macro option, this can be used to execute Macro's across sites.
- Report Actions
 - *Print Report* - The selected report will be sent to the selected printer when executed.
- Card Actions
 - *Activate Card* - The card presented will be activated when executed.
 - *Deactivate Card* - The card being presented will be deactivated after the specified number of access denied attempts when executed.
 - *Delete Card* - The card being presented will be deleted after the specified number

of access denied attempts when executed.

- *Delete Card and Cardholder* - The card being presented will be deleted along with its associated cardholder after the specified number of access denied attempts when executed.
- *Assign Access Level* - The card being presented will have the specified access level assigned to it when executed.
- *Revoke Access Level* - The card being presented will have the specified access level removed from it when executed.
- IP Lockset Actions
 - *Lock IP Lockset* - The selected IP Lockset will lock.
 - *Unlock IP Lockset* - The selected IP Lockset will unlock.
 - *Enable IP Lockset Panic Mode* - The selected IP lockset will go into panic mode. Panic mode results in the door being locked and only master and emergency user types will be granted access.
 - *Disable IP Lockset Panic Mode* - The selected IP lockset will reset from panic mode.
- Panel Actions
 - *Send Direct Command to SCP Hardware* - The entered command will be sent to the destined SCP hardware when executed.
 - *Send Direct Command to 2g Hardware* - The entered command will be sent to the destined 2g hardware when executed.
 - *Reset All Panels* - All SCP panels will be reset. SCP's will be reset 5 at a time in no specific order.
- Program Actions
 - *Execute Program Hidden* - The entered command line will be executed with all specified arguments and hidden (not displayed) when executed.
 - *Execute Program and Activate* - The entered command line will be executed with all specified arguments and will be made the active program when executed.
 - *Execute Program Minimized and Activate* - The entered command line will be executed with all specified arguments and will be made the active program in a minimized window when executed.
 - *Execute Program Maximized and Activate* - The entered command line will be executed with all specified arguments and will be made the active program in a maximized window when executed.
 - *Execute Program* - The entered command line will be executed with all specified arguments when executed.
 - *Execute Program Minimized* - The entered command line will be executed with all specified arguments in a minimized window when executed.
- Intrusion Processing Actions
 - *Arm Intrusion Area* - The selected intrusion area will be armed when executed.
 - *Disarm Intrusion Area* - The selected intrusion area will be disarmed when executed.
 - *Bypass Intrusion Point* - The selected intrusion area will be bypassed when

executed.

- *Reset Intrusion Point* - The selected intrusion area will be reset when executed.
- *De-energize Intrusion Output* - The selected intrusion output will be de-energized when executed.
- *Energize Intrusion Output* - The selected intrusion output will be energized when executed.
- CCTV Switcher Actions
 - *Send String to Video Switcher (feature deprecated)* - The entered command string will be sent to the attached video switcher when executed.

● Event Type

Macro events (transactions) are recorded in the event file every time a Macro is executed. Macro events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Macro succeeded* - The Macro executed successfully.
- *Macro failed* - The Macro failed to executed.
- *Macro succeeded with errors* - The Macro executed and one or more of the steps failed.

Schedule

Select the schedule type and options for this macro. The macro will automatically be executed each time the schedule occurs. Scheduled Macro's can also be viewed, created, and modified in an calendar within the Macro's screen by clicking the Schedule tab.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database. The last time a Macro executed and its result are also displayed.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the macro. Clicking on the close button will not save the changes made to the macro.

Alarms

Alarms are events (transactions) that are recorded in the event database and displayed in the alarms window every time an event occurs for a card or hardware device that has event types defined as an alarm. Alarm notification is also displayed by flashing the Access It! Universal.NET alarm workstation taskbar icon if the application is minimized or another application is being used on the local workstation. Alarms are generally used to monitor inputs that have devices such as smoke detectors attached to them. Alarms are also used to monitor doors being forced open, etc. For more information on setting up event types, see the [Hardware](#) help file topic.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Viewing Alarms

To view alarms, go to the alarms screen by clicking on the Alarms icon within the Main group of the Navigation pane. Pending alarms can be viewed by clicking on the red flashing alarms bar located at the bottom of the application. All of the alarms for sites that the currently logged in user has access to will then be displayed in the right window pane of the Access It! Universal.NET desktop or in the alarms window. The alarms window can either be docked within the main application window or displayed in a separate window using the view option on the Ribbon. Displaying the alarms in a separate window is useful on systems that use multiple monitors.

The alarms that are displayed can be filtered by either the event type or the location that the alarm occurred. Event/Alarm filters are configured for each user group. The filter can be selected within the current filter drop list within the alarms toolbar. For more information on user groups, see the [User Groups](#) help file topic.

Pending Alarms

Pending alarms are active alarms that have not been acknowledged by any user. Pending alarms are identified by the red alarm icon in the alarms window. If a sound file has been associated with the alarm, it will be played at this time if the local workstation has sound support. Pending alarms are sorted first by alarm priority, then by the date and time that they occurred. If the device that produced the alarm has a camera associated with it a camera icon will be displayed indicating that there may be a video clip for this alarm.

Acknowledging Alarms

To acknowledge alarms, select the alarms to be acknowledged and click on the acknowledge button on the toolbar or select acknowledge from the right click menu. Once the alarm has

been acknowledged, its icon will change from red to yellow and the status will become acknowledged.

Clearing Alarms

To clear alarms, select the alarms to be cleared and click the clear on the toolbar or select clear from the right click menu. All pending and current alarms can also be cleared from the alarms window by selecting purge all alarms from the file option on the alarms toolbar or from the right click menu. If the device that produced the alarm has the require comments check box checked for this event type, a screen will be displayed to enter text information about the alarm(s). If not, required text can also be entered by clicking on the comments button and the toolbar and entering the information. Comments can be viewed when running a report that includes the alarm event.

If a hardware device has it's require secure condition before alarm clear option checked, the alarm cannot be cleared until the device that produced the alarm has been returned to a secure (normal) state.

Sending Commands

To send commands to a device select the alarm associated with the device and click the command drop down on the toolbar or select commands from the right click menu.

Current Filter

Select a predefined filter to be applied within the Alarms screen. Filters are defined in the filters section located in the configuration menu of the software.

Group By Device

Select this option to group all alarms by the source of the alarm. This is a useful option when multiple alarms all occur from the same device. When grouped, alarms can be viewed by expanding the specified device and all alarms for that device can be selected by clicking the group header.

Editing Alarm Responses

Frequently used alarm responses can be saved and re-used by adding them to the alarm responses in the database. This is accomplished by selecting the edit alarm responses from the right click menu and entering the alarm response name and the alarm response text to be saved. The alarm response name(s) will be displayed in the acknowledgment screen and the alarm response text will be filled in automatically once the alarm response name has been selected. This feature is useful if there are alarm response messages that are commonly re-used.

Alarm Annunciation

By default, Access It! Universal.NET relies on the operating systems 'Default Beep' sound when a new alarm occurs. To change or disable the alarm annunciation, select the annunciation sound option from the right click menu in the alarms screen.

Alarm Delay

Alarm delays are used to "route" or "bump" alarms from one workstation to another based upon a time schedule. Alarm delays are useful when one or more sites are unmanned during a certain time of day and it is necessary to send the alarms to a different workstation for operator handling. For more information on alarms, see the [Alarms](#) help file topic.

To set up an alarm delay, go to the user groups entry screen by clicking on the User Groups icon within the Configuration group of the Navigation pane. All of the user groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the user group to be edited and click on the edit button on the toolbar, or double click the user group to be edited. You can also select edit from the right click menu. Select the desired site in the permissions tree and expand the tree using the ">" sign. Next click on the alarms branch in the tree to display the alarms permission and alarm delay settings.

Intervals

Select the days of the week to be used for each of the 4 alarm delay intervals. Only 1 interval needs to be set up to enable an alarm delay, but all 4 can be used if desired. Enter the appropriate start time and end time for any of the intervals being used. The start time is when the alarm delay interval will become active and the end time is when the alarm delay interval will become inactive.

Delay When any Interval is Active

Select or enter the alarm delay time in seconds when any of the 4 intervals are active. This entry determines the amount of time in seconds that an alarm will be delayed before being announced at the specified site during the active interval. The alarm delay can range from 1 to 9999 seconds.

Delay When all Intervals are Inactive

Select or enter the alarm delay time in seconds when all 4 of the intervals are inactive. This entry determines the amount of time in seconds that an alarm will be delayed before being announced at the specified site when all intervals are inactive. The alarm delay can range from 1 to 9999 seconds.

As an example, if a site named "Child Care" was only monitoring alarms during business hours 5 days a week and the "Command Center" site is responsible for the child care site alarms during the evening and weekends the following settings would be made for the command center site:

Interval	Su	Mo	Tu	We	Th	Fr	Sa	Start Time	End Time
1:			X	X	X	X	X	09:00 AM	05:00PM
Delay when any interval is active								90	
Delay when all intervals are inactive								0	

This would annunciate all alarms immediately at the child care site during business hours and then 90 seconds later annunciate them at the command center site if the alarm remained unacknowledged at the child care site during business hours. Then during non-business hours, the alarms for the child care site would immediately be annunciated at the command center site for processing.

Events

Events are recorded in the event file every time something happens within the system. Card transactions, data being edited, commands being issued to doors are all events that are displayed in the Access It! Universal events window and recorded in the system event file. The system event file will retain all of the current events until an archive is performed. For more information on archiving events, refer to the [Database Configuration Utility](#) help file topic.

Viewing and Filtering Events

To view events, go to the events screen by either clicking on the events toolbar button within the main group on the toolbar, or by selecting events from the go option on the system menu. All of the events for sites that the currently logged in user has access to will then be displayed in the lower window pane of the Access It! Universal.NET desktop or in the events window. The events window can either be docked within the main application window or displayed in a separate window using the view option on the system menu. Displaying the alarms in a separate window is useful on systems that use multiple monitors.

The events window can be paused to view previous events and prevent the viewer from jumping to the bottom of the list every time a new event is displayed. This is accomplished by clicking on the pause button on the events window toolbar or from the right click menu. The scroll bar can then be used to scroll backwards and forwards through all of the events in the current event file. Click on the resume button on the events window toolbar or from the right click menu to resume normal event viewing. Cardholder and card information can be viewed for card related events by right clicking on the event and choosing the appropriate option.

Access It! Universal.NET will retain the past 1,000 events that occur. If the events screen is paused, up to 5,000 events will be queued in the event window. By default, the past 100 events are automatically displayed in the event screen upon the workstation starting. This value can be modified by selecting the options menu from the file menu and adjusting the Events to load at startup setting.

The events that are displayed in the events windows can be filtered by either the event type or the location that the event occurred. Event filters are configured in the Alarm/Event Filters screen. Filters can be enabled by selecting them in the Current Filter pick list. An example of event filtering would be if this workstation is used as a photo id verification workstation for positive identification purposes, it may be desirable to filter the event locations for this workstation to only the readers that are being used for verification purposes. For more information on Filters, see the [Alarm/Event Filters](#) help file topic.

Photo ID Verification

Photo ID verification is the process by which a card holder presents a card at a specified reader and their stored image from the cards data file is then displayed in the events window. This is useful to make sure that the person using the card is indeed the person that the card was issued to. To turn on photo id verification, right click on the cardholders button in the events window. A photo window will be displayed on the right-hand side of the events window. If there is an image on file when a card holder presents their card at a reader, the associated image will then be displayed in the photo window.

Operator Journal

Operator journal entries are used to record miscellaneous text information into the system event log file. This is useful when an operator wants to make a text entry in to the log file that will be permanently stored along with the operator name and the workstation that was used to make the entry. To make a journal entry, click on the journal button on the events window toolbar or from the right click menu.

Printing Events

Events are printed using the Event Listing Report. For more information on using the Reports, refer to the [Reports](#) help file topic.

Tracking

The Tracking window is used to isolate and monitor select Cardholders, Cards, and Readers. Items selected to be tracked will display in this screen. There is no limit to the number of items that can be tracked.

Tracked events to load at startup

The number of tracked items to display upon startup is defined in the options screen accessed from the File menu.

Tracking a Cardholder

To track a cardholder, navigate to the Cardholders screen and locate the cardholder to be monitored. Right click on the cardholder and select the option Track Cardholder. To stop tracking a cardholder, highlight the record in the tracking screen and select Stop Tracking.

Tracking a Card

To track a card, navigate to the Cards screen and locate the card to be monitored. Right click on the card and select the option Track Card. To stop tracking a card, highlight the record in the tracking screen and select Stop Tracking.

Tracking a Reader

To track a reader, navigate to the Readers screen and locate the reader to be monitored. Right click on the reader and select the option Track Reader. To stop tracking a reader, highlight the record in the tracking screen and select Stop Tracking.

Mustering

The Mustering window allows for a near real-time view of configured Areas and which cardholders are within them. In order to make use of Mustering, 2 or more readers must already be configured for Anti-passback (APB). See the [Readers Detail](#) and the [Access Areas Detail](#) for more information on APB setup.

Select Areas

Select the access areas to be monitored in the Mustering window by moving the area from the Available areas list to the Monitored areas list. Only areas configured to be used in conjunction with anti-passback (APB) will be displayed. See the [Readers Detail](#) and the [Access Areas Detail](#) for more information on APB setup.

Refresh Interval

The refresh interval is how often the mustering window will update the areas occupancy detail. Values range between 5 and 120 seconds.

Omit cards not used in

If a card's last activity is greater than the value set, it will not appear within the Mustering window. Values range between 1 and 100 seconds. Setting the value to 0 will never omit any cards from the Mustering window.

Maps

Maps are used to display a graphical interface to the access control system. In some cases, this may be a graphical representation of the facility being controlled by the system including floors, offices, parking lots, etc. In other cases, it may just be a colored background with all of the often-used hardware devices placed upon it for easy access and system control. Maps can be linked to other maps to create a "virtual tour" of the facility being controlled. Real-time hardware device status and single button hardware device control are also provided. Maps are designed with the map designer, for more information on the map designer, see the [Map Designer](#) help file topic.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Viewing Maps

To view maps, go to the maps entry screen by clicking on the Maps icon within the Main group of the Navigation pane. All of the maps in the database will then be displayed in the map tree of the Access It! Universal.NET maps window. The maps window can either be docked within the main application window or displayed in a separate window using the view option on the ribbon. Displaying the maps in a separate window is useful on systems that use multiple monitors.

Expand the map tree if necessary and select (click) on the map to be displayed. The zoom level can be adjusted by either clicking on the zoom in or zoom out buttons on the maps toolbar or from the right click menu. A certain area of a map can be enlarged by clicking on the zoom to toolbar button or the right click menu and dragging the area to be viewed. If the map being displayed is larger than the display window, use the maps window scroll bars to move left, right, up or down. The entire map can be viewed by clicking on the fit in window button on the maps toolbar or from the right click menu.

Maps can also be displayed from the alarms screen by selecting a pending alarm from the pending alarms window and clicking on the maps button within the main group on the toolbar. The default map for the hardware device associated with the selected alarm will then be displayed in the maps window. The default map for a hardware device is selected on the events tab for each of the hardware devices. Maps can also be set up to be automatically displayed when an alarm is selected in the alarms window from within the associated hardware device. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The hierarchy in which the maps are displayed in the map tree is determined by each map's parent map setting. For more information on setting a map's parent map property, see the [Map Properties](#) help file topic.

Map Hardware Devices

Map hardware devices are used to display the alarm state of a hardware device, to display current status information for a device and to issue commands to a hardware device. Alarms can also be acknowledged and cleared from map hardware devices. When a hardware device is in an alarm state, the hardware device icon will "flash" with a red color indicating an alarm state. When the alarm has been acknowledged, the device icon will stop flashing and display a solid red color. When the alarm has been cleared, the device icon will return to a normal state with no red color. Current status information is displayed when the mouse cursor is positioned anywhere over the hardware device icon. The current status dialog will appear and follow the mouse cursor as long as the mouse is not moved outside of the hardware device's icon border. The status information is provided "real time" and will change regardless of whether or not the mouse is being moved. To issue commands to a hardware device, simply select (click) the desired hardware device and select the appropriate command from the maps toolbar to issue the command. The icon border for a device will animate when selected to identify the currently selected hardware device. For more information on adding hardware devices to a map, see the [Map Devices](#) help file topic.

Map Links

Map links are used to link maps together for easy navigation from map to map. Map links are generally used to "zoom in" on a location when viewing a map that covers a large area such as a floor in a building. A map link might be used in this situation for each of the reader locations located on the floor. A map link might also be used to "return" to the overall map of the entire floor from the reader location map. Map links are identified with a picture and with the name of the map being linked to and are activated by clicking on them. For more information on adding map links to a map, see the [Map Links](#) help file topic.

Map Macros

Map macros are used to execute system macros to perform various functions. Map macros are identified with a picture and with the name of the macro being executed and are activated by clicking on them. For more information on adding map macros to a map, see the [Map Macros](#) help file topic.

Map Text

The map text object is used to add static text or labels to the map design. For more information on adding map text to a map, see the [Map Text](#) help file topic.

Map Alarm Zone

The map alarm zone object is used to add an alarm zone to the map design. Alarm zones

are used to group devices together in a zone so that any of the devices that fall within the borders of the alarm zone will cause the entire zone to flash when any of the devices are in an alarm state. For more information on adding alarm zones to a map, see the [Map Alarm Zone](#) help file topic.

Map Designer

The map designer is used to create new or modify existing graphical map designs. Maps can be designed with many different styles and functions. Objects and hardware devices are added to the map and properties are set to determine the functionality of these objects. For more information on maps, see the [Maps](#) help file topic.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Map

To add a map, go to the map designer entry screen by clicking on the Map Designer icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu. All of the maps in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the toolbar or select new from the right click menu.

Editing a Map

To edit a map, go to the map designer entry screen by clicking on the Map Designer icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu. All of the maps in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the map to be edited and click on the edit button on the toolbar, or double click the map to be edited. You can also select edit from the right click menu.

Deleting a Map

To delete a map, go to the map designer entry screen by clicking on the Map Designer icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu. All of the maps in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the map to be deleted and click on the delete button on the toolbar or select delete from the right click menu.

Steps

The first step when designing a map is to set the overall map properties. These properties control the way the map is linked to other maps in the system and displayed in the map tree. For more information on map properties, see the [Map Properties](#) help file topic.

The second step when designing a map is to set the background picture or color. These

options determine whether the map will use a picture or a solid color as a background. Normally, this option would be set to a drawing of the area that the map is being designed to display. For more information on map backgrounds, see the [Map Background](#) help file topic.

The third step when designing a map is to add objects to the map design and set their properties if necessary. For more information on map designer objects see any of the map designer object help file topic.

The following design and formatting functions are supported in the map designer:

Font

These options set the font and any special formatting characters for the map text object. Choose the desired font, size and any special effects for the text. For more information on map text objects, see the [Map Text Object](#) help file topic.

The fonts available are based upon the fonts installed on the local computer.

Picture

The picture function is used to change the picture that is displayed on the map for either the selected map device object or the selected map link object. For more information on the map device object, see the [Map Device Object](#) help file topic. For more information on the map link object, see the [Map Link Object](#) help file topic.

Visible

The visible at runtime checkbox is used to determine whether or not the selected map device object or the selected map link object will be visible when the map is displayed in the maps window. This option is useful when you want to put an "invisible" hot spot on a map that links to either a device or a map link.

Bring to Front/Back

The bring to front/back functions are used to set the front to back (top to bottom) order of a single object or multiple objects.

Grid

The grid functions are used to control the display and sizing of the formatting grid. To access the grid functions, select grid from the format option on the system menu. The following grid functions are supported:

- *Show Grid*

This function turns on and off the display of the formatting grid.

- *Snap to Grid*

This function turns on and off the snap to grid option of the formatting grid. It is recommended that this option be left on to make it easier to line up objects within the map design.

- *Grid Size*

This function sets the horizontal and vertical size of the grid.

Map Properties

The map properties control the way a map is linked to other maps in the system and displayed in the map tree. To access the map properties, select map settings from the file option on the system menu.

The following map properties are supported:

Map Name

Enter the map name for the map design. The map name will be displayed in the map tree and should be something to identify the location or purpose of the map. The map name can be up to 128 characters in length.

Parent Map

Select the parent map for the map design. The parent map option is used to organize the maps in the map tree. If a parent map is specified for a map, it will be displayed under the map specified as the parent map. This option is useful for grouping maps that refer to the same location or area together. If a parent map is not specified, the map will be displayed as a master branch (folder) in the map tree.

Map Device Object

The map device object is used to add system hardware devices to the map design. To add a map device object to the map design, expand the devices branch by clicking on the plus sign, then expand the desired device type and click on the device that is to be added and drag it to the desired location on the map design. A map device object will then be placed on the map design at the default size with the default single state (static) picture. The map device object should then be moved to the correct location on the map design by clicking anywhere inside the map device object and dragging it to the desired location. The map device object should then be resized by clicking on any of the handles on the map device object and dragging it to the desired size. The map device object's picture can then be changed if desired by clicking on the picture button within the ribbon.

The following device object picture types are supported:

- *Default Icon* - This option will display the default single state (static) device icon.
- *Default Multi-state Icons* - This option will display the default multi-state icons which reflect the state of the device object being placed on the map design in real time.
- *Custom Multi-state icons* - This option will display the custom icons specified for each of the available states for the device object being placed on the map design in real time. Supported image types are BMP, JPEG, and PNG.

Only installed hardware devices will be displayed in the devices tree. For more information on installing hardware devices, see the [Hardware](#) help file topic. If the map device object's picture is changed to a custom icon, note that only the areas that are colored red on the selected picture will "flash" when the hardware device is in alarm.

Map Link Object

The map link object is used to link maps together for easy navigation from map to map. Map links are generally used to "zoom in" on a location when viewing a map that covers a large area such as a floor in a building. A map link might be used in this situation for each of the reader locations located on the floor. A map link might also be used to "return" to the overall map of the entire floor from the reader location map. To add a map link object to the map design, expand the map links branch by clicking on the plus sign, then expand the desired parent map and click on the map that is to be added and drag it to the desired location on the map design. A map link object will then be placed on the map design at the default size with the default picture. The map link object should then be moved to the correct location on the map design by clicking anywhere inside the map link object and dragging it to the desired location. The map link object should then be resized by clicking on any of the handles on the map link object and dragging it to the desired size. The map link object's picture can then be changed if desired by clicking on the change picture button on the toolbar or by selecting change picture from the format system menu.

Map Macro Object

The map macro object is used to add system macros to the map design. To add a map macro object to the map design, expand the macros branch by clicking on the plus sign and click on the macro that is to be added and drag it to the desired location on the map design. A map macro object will then be placed on the map design at the default size with the default picture. The map macro object should then be moved to the correct location on the map design by clicking anywhere inside the map macro object and dragging it to the desired location. The map macro object should then be resized by clicking on any of the handles on the map macro object and dragging it to the desired size. The map macro object's picture can then be changed if desired by clicking on the picture button on the toolbar or by selecting picture from the format system menu.

Only macros that have steps will displayed in the macros tree. For more information on adding steps to macros, see the [Macros](#) help file topic.

Map Text Object

The map text object is used to add static text or labels to the map design. To add a map text object to the map design, click on the text object on the map design tree and drag it to the desired location on the map design. A window will then be displayed to enter the text to be added to the map design. The text can be up to 255 characters in length. A map text object will then be placed on the map design at the default size. The map text object should then be moved to the correct location on the map design by clicking anywhere inside the map text object and dragging it to the desired location. The map text object should then be resized by clicking on any of the handles on the map text object and dragging it to the desired size. The map text object format properties can then be changed if desired. The map text object format properties can be set by clicking on the appropriate toolbar button or by selecting the appropriate option from the format system menu.

The following format properties are supported for the map text object:

Font

These options set the font and any special formatting characters for the map text object. Choose the desired font, size and any special effects for the text.

The fonts available are based upon the fonts installed on the local computer.

Bring to Front/Back

The bring to front/back functions are used to set the front to back (top to bottom) order of the map text object.

Visible at Runtime

The visible at runtime function is used to determine whether or not the map text object will be visible when the map is displayed in the maps window. This option is useful when you want to put an "invisible" identifier on a map that would only be displayed when the map is being designed.

Map Alarm Group Object

The map alarm zone object is used to add an alarm group to the map design. Alarm groups are used to group devices together in a zone so that any of the devices that fall within the borders of the alarm group will cause the entire group to flash when any of the devices are in an alarm state. To add an alarm group object to the map design, click on the alarm group branch on the map design tree and drag it to the desired location on the map design. A map alarm group object will then be placed on the map design at the default size. The map alarm group object should then be moved to the correct location on the map design by clicking anywhere inside the map alarm group object and dragging it to the desired location. The map alarm group object should then be resized by clicking on any of the handles on the map alarm group object and dragging it to the desired size. Finally, the map alarm group object should be sent to the back of any devices that are in the map alarm group area.

Hardware

Hardware is used to define all panels, readers, inputs, outputs, intercoms, intrusion panels, IP Locksets, CCTV cameras and DVR cameras being used in the system. Hardware is displayed in a tree style format for ease of use and is organized in the same fashion that the hardware is physically installed in the system. The hardware tree is also used to display real time status information for various system hardware devices. Click on the arrow sign next to any of the items to expand the tree and display the items contained within that item. Clicking on one of the items in the tree will display all of the related items in the right window pane of the Access It! Universal desktop. The item can then be selected and edited by clicking on the edit button on the toolbar, or be double clicking on the item to be edited.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

For additional information, select any of the following hardware categories.

[Channels](#)

[SCPs](#)

[SIOs](#)

[Readers](#)

[Inputs](#)

[Outputs](#)

[Tasks](#)

[DVRs](#)

[CCTV Switchers](#)

[Intercom Switches](#)

[Intrusion Panels](#)

[IP Locksets](#)

Channels

[Channels Detail](#)

Channels are used to define the communication method from the comm server computer to each of the SCP panels. Channels can be either RS232, TCP/IP (network) or Dial-up using a modem.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Channel

To add a channel, go to the Channels entry screen by clicking on the Channel icon within the Hardware group of the Navigation pane. All of the channels will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button within the ribbon or select new from the file option on the system menu or from the right click menu.

Editing a Channel

To edit a channel, go to the Channels entry screen by clicking on the Channel icon within the Hardware group of the Navigation pane. All of the channels will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the channel to be edited and click on the edit button on the toolbar, or double click the channel to be edited. You can also select edit from the right click menu.

Deleting a Channel

To delete a channel, go to the Channels entry screen by clicking on the Channel icon within the Hardware group of the Navigation pane. All of the channels will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the channel to be deleted and click on the delete button on the toolbar or select delete from the right click menu.

Printing Channel Reports

To print reports for a channel, go to the Channels entry screen by clicking on the Channel icon within the Hardware group of the Navigation pane. All of the channels will then be displayed in the right window pane of the Access It! Universal desktop. Select the channels to print reports for and click on the print button on the toolbar or select print from the file option on the system menu or from the right click menu. The following reports are available:

- *Channel History* - This report provides a list of all database updates for the selected channels.

- *Channel Listing* - This report provides a list of the selected channels and their various properties.

Channels Detail

Channels

Channels are used to define the communication method from the comm server computer to each of the SCP panels. Channels can be either RS232, TCP/IP (network) or Dial-up using a modem.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Channel Name

Enter the name to be used for this channel. All of the channels have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the channels being used. An example of a friendly name would be "COM1". The channel name can be up to 50 characters in length.

Channel Enabled

Select (check) this option if this channel is to be enabled (activated). If the channel is enabled, communication with the SCP panel(s) attached to this channel will be initiated. If the channel is disabled (unchecked), no communication will occur with the SCP panel(s) attached to this channel.

During system installation, it may be helpful to leave the channel disabled until all of the hardware has been set up for the channel. That way, the system can be "predefined" without receiving various communications and status alarms while panels, readers and associated hardware is being installed in the system.

Protocol Type

Select the protocol type for this channel. Select the SCP protocol type for the SCP and/or EP-series family of access control hardware or choose the 2g protocol type for the second generation of the SCP hardware family.

It is very important that the protocol selected matches the hardware type being used on the channel. Choosing the wrong protocol type will result in system malfunctions

Channel Type

- *Hardwired* - The SCP panel(s) are directly attached to one of the serial communications ports on the comm server computer. The SCP panel(s) can either be directly connected to the serial port on the computer, or connected using an RS485 converter or some other serial conversion device.

- *Dial-up* - The SCP panel(s) are being communicated to via a modem or other Dial-up device on the comm server computer.
- *IP Server* - The SCP panel(s) are being communicated to over a network connection from the comm server computer to the SCP panel(s). This is the most common TCP/IP configuration.
- *IP Client* - The SCP panel(s) are communicating over a network connection from the SCP panel(s) to the comm server computer. This configuration is useful if panel side firewalls are involved. Only the firewall at the comm server computer would need multiple ports opened up for network communications as most firewalls are configured to allow all outgoing traffic. This Channel uses a unique TCP port for each SCP.
- *IP Client (single port)* - The SCP panel(s) are communicating over a network connection from the SCP panel(s) to the comm server computer. This configuration is useful if panel side firewalls are involved. Only the firewall at the comm server computer would need a single port opened up for network communications as most firewalls are configured to allow all outgoing traffic. This Channel uses a single shared TCP port for all SCPs.
EP Series only.

Channel Settings

- *Comm Port Number (Hardwired Only)* - Enter the physical serial communications port number that the SCP panel(s) are attached to on the comm server computer.
- *Baud Rate (Hardwired Only)* - Select the serial communications baud rate to communicate with the SCP panel(s).
The baud rate must match the DIP switch settings on the SCP panel(s). For more information on setting the SCP panel DIP switches, see the Access It! Universal.NET Hardware Reference Manual.
- *Modem Name (Dial-up Only)* - Select the modem to use to call (dial) the SCP panel(s).
The modem must first be installed using the operating system control panel applet. For more information on setting up a modem with the operating system, refer to the operating system documentation.
- *IP Client Settings (IP Client Only)* - Enter the TCP port that the comm server will listen on for incoming panel connections. When used in this manner, each SCP must use a unique IP Client channel and TCP port.
If a firewall is in place this port will need to be configured for incoming TCP traffic.
- *IP Client (single port)* - Enter the TCP port that the comm server will listen on for incoming panel connections. When used in this manner, each SCP must share the IP Client channel and use a single inbound TCP port. In Enterprise systems, this Channel is available within every site.
If a firewall is in place this port will need to be configured for incoming TCP traffic. Only one IP Client (single port) channel may be used per regional server.

Transport Layer Security (TLS)

Select (check) this option if Transport Layer Security (TLS) encryption is required between the EP controller and host.

The EP controller must have the Data Security option TLS Required set within its internal Web browser prior to communicating using TLS encryption.

Advanced Comm Settings

- *Use Default Settings* - The channel will use default communication settings
- *Specify Settings* - The channel will use the specified communication settings
 - Response Timeout (ms)
 - The timeout in milliseconds the server will wait for a response from a TCP/IP SCP before a retry is initiated
 - TCP Retry Time (ms)
 - The time in milliseconds the server will wait before trying to reopen a connection with a TCP/IP SCP. The server will close a connection when the max retry count is exceeded. The max retry count is set in the SCP properties screen.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the channel. Clicking on the close button will not save the changes made to the channel.

[Channels](#)

SCP's

[SCP's Detail](#)

SCP's are used to define the model and operational parameters for each of the SCP panels in the system. If the main SCP item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the SCP panels. The SCP icon will also display the current alarm state for each of the SCP panels.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Searching SCPs

To search for a SCP, type in the search box located in the upper right hand corner. Results will be dynamically displayed as search criteria is entered. To include a wildcard in the search use the asterisk (*) symbol.

Custom filtered views can be selected for the SCPs screen. When applied, SCPs will dynamically populate based on their changing states. Newly added devices will not appear in the filtered list until the grid is refreshed by clicking the green refresh icon. Filtered views include:

- *(No Filter)* - No filter will be applied to the SCPs grid.
- *Installed* - Only SCPs installed will display within the SCPs grid.
- *Online* - Only SCPs in an online state will display within the SCPs grid.
- *Offline* - Only SCPs in an offline state will display within the SCPs grid.

Adding an SCP

To add an SCP, go to the SCP entry screen by clicking on the SCP icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu.

Editing an SCP

To edit a SCP, go to the SCP entry screen by clicking on the SCP icon within the Configuration group of the Navigation pane. Select the SCP to be edited and click on the edit button on the toolbar, or double click the SCP to be edited. You can also select edit from the right click menu.

Deleting an SCP

To delete a SCP, go to the SCP entry screen by clicking on the SCP icon within the Configuration group of the Navigation pane. All of the SCPs in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SCP to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu.

Printing SCP Reports

To print reports for a SCP, go to the SCP entry screen by clicking on the SCP icon within the Configuration group of the Navigation pane. All of the SCPs in the database will then be displayed in the right window pane of the Access It! Universal desktop. Select the SCP to print reports for and click on the Reports button within the ribbon or from the right click menu select print reports. The following reports are available:

- *Hardware Map* - This report provides a hierarchical listing of all hardware attached to the selected SCPs. This report includes SCPs, SIOs, readers, inputs and outputs.
- *SCP History* - This report provides a list of all history for the selected SCPs. This report includes all database updates as well as all hardware activity.
- *SCP Listing* - This report provides a list of the selected SCPs and their various properties.

SCP Commands

To send a command to an SCP, go to the SCP entry screen by clicking on the SCP icon within the Configuration group of the Navigation pane. All of the SCP's will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SCP to send a command to and click on the SCP commands drop down next to the edit button in the ribbon or select commands from the right click menu. Select the command to be issued from the list and click on the command to be sent to the SCP panel.

The following SCP commands are supported:

Request SCP Status

The request SCP status command is used to view current status information for the SCP panel. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *SCP Name* - Display the name of the SCP panel.
- *Device ID* - Displays the device ID or SCP number of the SCP panel.
- *Device Version* - Displays the hardware version of the SCP panel.
- *Software Revision* - Displays the current firmware revision number of the SCP panel.
- *Serial #* - Displays the serial number of the SCP panel.
- *MAC Address* - Displays the MAC address of the SCP panel.
- *RAM Size* - Displays the total amount of on-board memory for the SCP panel.
- *RAM Free* - Displays the amount of available on board memory for the SCP panel.
- *SCP Time* - Displays the current date and time stored in the SCP panel's internal clock.
- *Max Cards* - Displays the maximum card capacity of the SCP panel.
- *Cards Active* - Displays the current number of cards stored in the SCP panel.
- *DIP Switch at Powerup* - Displays the DIP switch settings when power was applied to the SCP panel.
- *DIP Switch Current* - Displays the current DIP switch settings for the SCP panel.
- *Power State* - Displays the current state of the power failure input.
- *Tamper State* - Displays the current state of the tamper input.
- *OEM Code* - Displays the current OEM code number of the SCP panel.

Transaction Buffer Status Request

The transaction buffer status request command is used to view current transaction (event) buffer status information for the SCP panel. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *SCP Name* - Display the name of the SCP panel.
- *Capacity* - Displays the total number of transactions the SCP panel can store when the panel is off-line (not being communicated to by the comm server computer).
- *Oldest* - Displays the transaction number of the oldest transaction in the SCP panel buffer. This number should always be one when the SCP panel transaction buffer is empty.
- *Last Reported* - Displays the transaction number of the last transaction that was sent to the comm server computer from the SCP panel.
- *Last Logged* - Displays the transaction number of the last transaction that was logged in the SCP panel. The last reported and last logged numbers will be equal when the SCP panel transaction buffer is empty.

Request Biometric Database Status

The request biometric database status command is used to view current biometric database status information for the SCP panel. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *Biometric Reader Type* - Displays the currently selected biometric reader type for the system.
- *Max Records* - Displays the maximum number of biometric templates that can be stored in the SCP panel.
- *Record Size* - Displays the memory size in bytes that each biometric template requires in the SCP panel.
- *Active Records* - Displays the number of biometric templates currently stored in the SCP panel.

Download All Files

The download all files command is used to download all of the data files from the comm server computer to the SCP panel.

Download Firmware

The download firmware command is used to download firmware to the selected SCP panel.

Downloading firmware can be very complex and is only recommended to be used by advanced users with the assistance of the Access It! Universal.NET technical support staff. Sending an invalid firmware file can compromise the security and functionality of the system.

Reset SCP

The reset SCP command will cause the SCP panel to reset and will re-initialize the SCP panel's on-board database. All of the data files will then automatically be downloaded from the comm server computer to the SCP panel. During a reset, cards will stop being granted access for up to 10 minutes.

Load AES Keys

Sends 128 bit and 256 bit AES keys to the SCP in order to encrypt the communication between SCP and host.

SCP's Detail

SCP's

SCP's are used to define the model and operational parameters for each of the SCP panels in the system. If the main SCP item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the SCP panels. The SCP icon will also display the current alarm state for each of the SCP panels.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

SCP Name

Enter the name to be used for this SCP. All of the SCP's have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the SCP's being used. An example of a friendly name would be "Main Building SCP". The SCP name can be up to 50 characters in length.

Model

Select the model for this SCP panel.

It is very important that the model selected matches the model of the panel being installed. Choosing the wrong SCP model could result in system malfunctions.

Card Capacity

This field displays the total number of cards that can be stored in the SCP panel. This number is calculated based on the SCP model, which determines the amount of physical memory that the SCP panel has on board, and the number specified for the number of transactions to store in the SCP. This card capacity is for informational purposes only and cannot be changed.

Device Installed

Select (check) this option if this SCP has been physically installed in the system. If the device installed option is checked, communication with the SCP panel will be initiated. If the device installed option is unchecked, no communication will occur with the SCP panel.

SCP Time Zone

Select the local time zone for the location that the SCP panel is being installed.

The time zone that the server computer is located in and the time zone that the SCP panel is installed at may be different. Be sure and select the time zone for the location that the SCP panel is being physically installed and not the time zone that the server computer is located in.

Number of Transactions to Store

Displayed for Legacy panels only. Enter the number of transactions to store in the SCP panel when the panel is off-line (not being communicated to by the server computer). The SCP panel will store all card transactions, door transactions, etc. and download them to the server computer when Access It! Universal.NET is started. Each of the SCP panels can have the number of transactions to store set individually to accommodate different transactions volumes at different locations.

Increasing this number reduces the total card capacity in the SCP panel. Depending on the panel model selected this field may not be displayed and the number of transactions to store will be fixed at 50,000.

Store Device Names

Displayed for Legacy panels only. Select (check) this option to store device names in the SCP panel when using the MR-DT LCD display keypad. This will allow the MR-DT to display friendly device names for readers and inputs instead of the default names.

This option is only displayed for SCPe controllers. Selecting this option reduces the total card capacity in the SCP panel.

Initialization String

Enter the initialization string to be sent to the SCP panel. The initialization string is used to enable special functionality within the SCP panel. Further discussion of initialization strings is beyond the scope of this documentation. The initialization string will be sent to the SCP panel each time the SCP panel is reset.

Initialization strings can be very complex and are only recommended to be used by advanced users with the assistance of the Access It! Universal.NET technical support staff. Sending an invalid initialization string can compromise the security and functionality of the system.

Address

Select or enter the physical hardware address of the SCP panel.

The address must match the DIP switch settings on the 2g/SCP panel or the web configuration of the EP series. For more information on setting the SCP addresses, see the Access It! Universal.NET SCP Quick Reference document.

SIO Port Speed

Select the SIO port speed for the SIO panels that are being attached to this SCP. Depending upon the SCP model being used, SIO port two may or may not be available. This setting controls the baud rate on the "downstream" side of the SCP panel. This is the baud rate at which the SCP panel will communicate with the SIO panels. It is generally recommended that this baud rate be left at the default (38400), unless there is a problem with the data wiring or a device such as a short haul modem is being used for a remotely installed SIO panel.

The baud rate must match the DIP switch settings on the SIO panel(s). For more information on setting the SIO panel DIP switches, see the [Access It! Universal.NET SCP Quick Reference document](#).

• SIO Port Protocol

The SIO Protocol defines the communication protocol used to communicate downstream to sub-panels. Available options are:

- *MSPI (Standard)* - Used to communicate to traditional Mercury-Security hardware
- Schlage PIM - Used to communicate to Schlage PIM modules or Allegion NDE gateways
- Salto SALLIS - Used to communicate to Salto SALLIS routers
- Vanderbilt - Used to communicate to Vanderbilt hardware
- Virtual SIO - Used to define virtual panels to be used in conjunction with the BACNet integration
- Inovonics - Used to communicate via TCP/IP to an Inovonics ACG
- SimonsVoss - Used to communicate via TCP/IP to a SimonVoss router

Comm Channel

Select the primary communications channel that this SCP panel is being attached to. The channel must first be defined in the channels screen. For more information on channels, see the [Channels](#) help file topic. The following parameters need to be specified:

- *Hardwired* - No additional parameters are required.
- *Dial-up* - Enter the phone number for the SCP panel and the phone number for the host modem. Optionally a password may be entered for security purposes. Enter or select the connect retry count which is the number of times a call will be attempted if there is no answer, a busy signal or communication problems. Select the call times that a call will be placed automatically to the SCP panel to download any available transactions and send any pending updates.
- *IP Server* - Enter the TCP/IP address that has been programmed in to the SCP panel. A host name can also be entered here if the SCP panel is using DHCP for automatic TCP/IP addressing. Enter the TCP port number that has been programmed in to the SCP panel for communications.

- *IP Client* - Leave the TCP/IP address blank

Alternate (Backup) Comm Channel

Select the alternate (backup) communications channel that this SCP panel is being attached to. The alternate comm channel will be used if the primary comm channel to the SCP panel fails. Switch over to the alternate comm channel is performed automatically after the primary comm channel fails. The channel must first be defined in the channels screen. For more information on channels, see the [Channels](#) help file topic.

The alternate comm channel is only available on the SCPe, EP-1502, and EP-2500 series of SCP panels.

Advanced

- *Use Default Settings* - The channel will use default communication settings
- *Specify Settings* - The channel will use the specified communication settings
 - Max Errors Before Offline
 - The max retry count before an SCP is flagged as being offline
 - Poll Delay - Primary Comm (ms)
 - Time in milliseconds that the server will wait between inactive polls while polling a TCP/IP SCP. An inactive poll is defined as a poll by the server in which the SCP has only an acknowledge (no data/information) to return.
 - Poll Delay - Alternate Comm (ms)
 - Time in milliseconds that the server will wait between inactive polls while polling a TCP/IP SCP using the alternate channel. An inactive poll is defined as a poll by the server in which the SCP has only an acknowledge (no data/information) to return.
 - Offline Timeout
 - Time in milliseconds that the SCP will wait between polls before declaring itself offline from the server.

Card Format Name

Select the card format(s) to be used with this SCP panel. The card format(s) are used to select the type of cards being used with the system. The card format will be determined by the type of readers and cards being used with the system. Custom card formats can also be added using the edit card formats button. This information will generally be provided by the reader or card manufacturer. Up to eight card formats can be entered for each SCP panel. For more information on card formats, see the [Card Formats](#) help file topic.

Facility Code

Enter the facility code(s) to be used with this SCP panel. This option can be set to -1 to

instruct the system to ignore the facility code for card formats that do not utilize one. This information will generally be provided by the card manufacturer.

Supervised Inputs

Custom Supervised Input Resistance Tables allow for customized resistor values used in reader/input supervised circuits. 4 custom tables can be created and applied to each SCP. The default resistor values are 2K closed and 1K open.

- Creating a custom Supervised Input Table requires the input reporting status to be mapped to thresholds of low/high resistance values. The values are entered in Ohms. While not all 8 fields are required, there must be a threshold set for active and inactive.

Reader LED Display

Enter the parameters to control the reader LED display properties for the various reader modes. These settings will apply to all readers that are attached to the selected SCP panel that have a reader mode configured to use the SCP LED table.

Reader LCD Display

Enter the custom text to be displayed on the MR-DT LCD keypad display for the desired events. This text will be displayed in place of the default message for each event that custom text has been entered for here.

Event Type

SCP events (transactions) are recorded in the event file every time there is a communication, tamper or power change of state for the SCP. SCP events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Comm Fail* - Communication between the server computer and the SCP panel has been lost. This can be caused when the SCP panel has been reset.
- *Comm Normal* - Communication between the server computer and the SCP panel has been restored.
- *Tamper Alarm* - The tamper device for the SCP panel is reporting that the panel has been tampered with.
- *Tamper Normal* - The tamper device for the SCP panel is reporting that it has been restored to a normal condition.
- *Power Loss* - The SCP panel is reporting that it has lost power.

- *Power Restored* - The SCP panel is reporting that power has been restored to a normal condition.
- *Comm Disconnected* - Communication between the server computer and the SCP panel has been successfully terminated. This state occurs when a channel or an SCP is disabled, or when a Dial up communication session has completed successfully.
- *Timezone Activated* - A timezone has become activated by either reaching it's start time or by being sent a command.
- *Timezone Deactivated* - A timezone has become deactivated by either reaching it's stop time or by being sent a command.
- *Login Service Offline* - EP-4502 event - The connection to a web login such as Over-Watch is offline.
- *Login Service Online* - EP-4502 event - The connection to a web login such as Over-Watch is online.

Annunciation Type

- *Disregard*: SCP events (transactions) for this event type will not be recorded in the event file and will not be displayed in either the events window or in the alarms window.
- *Log Only* - SCP events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display* - SCP events (transactions) for this event type will be recorded in the event file and displayed in the events window.
- *Alarm* - SCP events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic.

The alarm priority is only used for event types that have the annunciation type set to "Alarm".

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on alarms, see the [Alarms](#) help file topic.

The alarm message is only used for event types that have the annunciation type set to "Alarm".

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the alarms window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic.

The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Message

Enter the event message for this event type. The event messages will be displayed in the events window each time this event type is generated. The event message is generally used to provide friendly text identification to the person monitoring events to identify the input point. This field can be up to 256 characters in length. For more information on events, see the [Events](#) help file topic.

Alarm Expiration Threshold

Select or enter the alarm expiration threshold for this SCP panel. The alarm expiration threshold is the amount of time in hours that an SCP panel can be off line with the comm server computer before the alarms stored in the panel "expire". When communication is restored to the SCP panel all of the expired alarms will be written to the system event log but not displayed in the alarms window. The alarm expiration threshold can range from 0 to 999 hours.

Default Map when SCP in Alarm

Select the default map to be associated with this device. The default map will be displayed whenever the show map toolbar button is clicked from the alarms window while any pending alarm for this device is selected. The map must be defined in the maps screen prior to selecting a default map for a device. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Require Secure Condition Before Alarm Clear

Select (check) this option to require that an alarm be secured before it can be cleared from the alarms screen for this event type. This option is used to make sure that an alarm cannot be ignored by simply acknowledging and clearing it without any action being taken. For example, if a door has been forced open, if this option is checked, the door would have to be closed before the alarm could be cleared from the alarms window. For more information on alarms, see the [Alarms](#) help file topic.

The require secure condition before alarm clear option is only used for event types that have the annunciation type set to "Alarm".

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Biometrics

Multiple Biometric Types can be added to a SCP. Each Biometric Type has its own unique parameters that must be configured. To add a new Biometric Type select the Edit Biometric Types... button. To assign a Biometric Type to the SCP select the Assign Biometric Type to SCP... and enter the number of biometrics templates to be allocated. To adjust a currently assigned Biometric Type, select Edit Biometric Type Assignment.... To remove an assigned Biometric Type, select Remove Biometric Type Assignment(s).

Default Security Threshold (Bioscrypt/Morpho Fingerprint)

Select the default security level to be used for all of the Bioscrypt biometric devices attached to this SCP. The default security level determines the ratio of false rejects to false accepts during biometric verification. The following security thresholds are supported:

- *Highest* - This option will provide the highest level of false rejections and the lowest level of false acceptances. This is the most secure setting.
- *High* - This option will provide a high level of false rejections and a low level of false acceptances.
- *Medium* - This option will provide an even balance between false rejections and false acceptances. This is the default and recommended setting for most applications.
- *Low* - This option will provide a low level of false rejections and a high level of false acceptances.
- *Lowest* - This option will provide the lowest level of false rejections and the highest level of false acceptances. This is the least secure setting.

Store Security Threshold per User (Bioscrypt/Morpho Fingerprint)

Select (check) this option to store the security threshold setting on a per user basis. When this option is checked, the default security threshold for the SCP can be overridden on a per card holder (user) basis. This option is useful when environmental conditions may require certain card holders to have a less secure security threshold to allow biometric verification when dealing with dirty or harsh environments.

Default Maximum Score (Schlage Handkey)

Enter the default maximum read score to be used for all of the RSI Handkey devices attached to this SCP. The default maximum score determines how accurately the card holders hand must be placed in the reader during biometric verification. The higher the value that is set here the less accurately the hand needs to be placed in the reader. A higher value entered here also allows a greater possibility for a false acceptance during verification.

Store Maximum Score per User (Schlage Handkey)

Select (check) this option to store the maximum score setting on a per user basis. When this option is checked, the default maximum score for the SCP can be overridden on a per card holder (user) basis. This option is useful when certain card holders may have difficulty placing their hands in the reader consistently yielding and unusually high read score and thus many false rejections for the card holder.

SCP database template type (Suprema Fingerprint)

Each SCP can have up to 4 OSDP related biometric types assigned. Each biometric type must have a unique OSDP number type assigned.

Minimum Default Score (Suprema Fingerprint)

Enter the minimum default accept score to be used for all of the Suprema devices attached

to this SCP. The default score determines how accurately the card holders finger must be placed on the reader during biometric verification. The higher the value that is set here the less accurately the finger needs to be placed in the reader. A higher value entered here also allows a greater possibility for a false acceptance during verification.

Store Minimum Score per User (Suprema Fingerprint)

Select (check) this option to store the minimum score setting on a per user basis. When this option is checked, the default maximum score for the SCP can be overridden on a per card holder (user) basis. This option is useful when certain card holders may have difficulty placing their fingers on the reader consistently yielding and unusually high read score and thus many false rejections for the card holder.

Extended Door Time

Enter the extended door time parameters. This option will set up the MR-DT or OSDP LCD display keypad to extend the door held open time to a value entered by the card holder. To activate the extended door held open function a valid credential or pin must be presented at the reader or keypad. Next press the <--- (*) button followed by the user command code followed by the three-digit time in minutes that the door held open is to be extended by. Finally press the command (#) key to complete the sequence. The LCD keypad display will then count down the time until the door held open event or alarm will be generated.

- *Command Code* - Enter the command code for extended door times. The command code is the code that must be entered at the MR-DT or OSDP LCD display keypad in order to extend door open times. The command code can be used at any valid MR-DT or OSDP LCD keypad display attached to the SCP panel. This field can be up to 6 digits in length.
- *Access Delay* - Select or enter the access delay for extended door times. The access delay is the amount of time in seconds that will be allowed between the presentation of a valid credential and the entering of the command code at a MR-DT or OSDP LCD keypad display. If the access delay has been exceeded the command code will be invalid.
- *Allowed Card Group* - Select the allowed card group for extended door times. The allowed card group is the only card group that will be allowed to perform extended door time functions at any of the valid MR-DT or OSDP LCD keypad displays attached to the SCP panel. If the card holder does not belong to this card group the command code will be invalid.
- *Command is Valid at All Readers* - Select (check) this option to allow command codes to be entered at any of the readers attached to the SCP panel. Uncheck this option to specify the valid readers for command code entry for the SCP panel. To assign valid readers, "move" the readers that you wish to be valid from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window.

The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired readers.

Extended User Commands

Enter the extended user command parameters. This option will set up the MR-DT or OSDP LCD display keypad or a standard keypad reader to execute specified tasks when extended keypad commands are entered. To enter extended keypad commands a valid credential or pin must be presented at the reader or keypad. Next press the <--- (*) button followed by the extended keypad command. Finally press the command (#) key to execute the specified task. Extended keypad commands are defined in the readers screen. For more information on readers, see the [Readers](#) help file topic.

- *Command Code* - Enter the command code for extended user commands. The command code is the code that must be entered at the MR-DT or OSDP LCD display keypad in order to execute extended user commands. The command code can be used at any valid MR-DT or OSDP LCD keypad display attached to the SCP panel. This field can be up to 6 digits in length.
- *Access Delay* - Select or enter the access delay for extended user commands. The access delay is the amount of time in seconds that will be allowed between the presentation of a valid credential and the entering of the command code at a MR-DT or OSDP LCD keypad display. If the access delay has been exceeded the command code will be invalid.
- *Allowed Card Group* - Select the allowed card group for extended user commands. The allowed card group is the only card group that will be allowed to execute extended user command functions at any of the valid MR-DT or OSDP LCD keypad displays attached to the SCP panel. If the card holder does not belong to this card group the command code will be invalid.
- *Command is Valid at All Readers* - Select (check) this option to allow command codes to be entered at any of the readers attached to the SCP panel. Uncheck this option to specify the valid readers for command code entry for the SCP panel. To assign valid readers, "move" the readers that you wish to be valid from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window. The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired readers.

Intrusion Processing

Enter the intrusion processing parameters. This option will set up the MR-DT or OSDP LCD display keypad for intrusion processing when command codes are entered.

- *Intrusion Processing Mode* - Select the intrusion processing mode for the SCP or EP panel. **NOTE: Enhanced intrusion processing is only available on the EP series of SCP panels.**
 - *Alarm Zone Arm/Disarm* - This option will set up the MR-DT or OSDP LCD display keypad to arm and disarm alarm zones. To arm or disarm an alarm zone a valid credential or pin must be presented at the reader or keypad. Next press the <--- (*) button followed by the command code followed by the two-digit alarm zone number. Finally press the command (#) key and follow the instructions on the MR-DT or OSDP LCD keypad display to arm or disarm the alarm zone. Alarm zones are defined in the alarm zones screen. For more information on alarm zones, see the [Alarm Zones](#) help file topic.
 - *Alarm Zone Arm/Disarm By Reader* - This option will set up the MR-DT or OSDP LCD display keypad to arm and disarm alarm zones associated with a specific reader. To arm or disarm an alarm zone a valid credential or pin must be presented at the reader or keypad. Next press the <--- (*) button followed by the command code. Next enter the command number to be executed (0 = View Zone Status, 1 = Disarm Zone, 2 = Arm Zone, 3 = Arm Zone in Stay Mode, 4 = Force Arm Zone). Finally press the command (#) key and follow the instructions on the MR-DT or OSDP LCD keypad display. No two-digit alarm zone needs to be entered in this mode. All functions performed will be performed on the alarm zone that is associated with the reader used. The associated alarm zone is defined in the readers screen. For more information on readers, see the [Readers](#) help file topic.
 - *Enhanced Intrusion Processing* - This option will set up the MR-DT or OSDP LCD display keypad to arm and disarm alarm zones with enhanced processing. To arm or disarm an alarm zone a valid credential or pin must be presented at the reader or keypad. Next press the <--- (*) button followed by the command code followed by the two-digit alarm zone number. Next enter the command number to be executed (0 = View Zone Status, 1 = Disarm Zone, 2 = Arm Zone in Away Mode, 3 = Arm Zone in Stay Mode, 4 = Arm Zone in Instant Mode, 5 = Toggle Keypad Chime, 6 = Bypass Points). Finally press the command (#) key and follow the instructions on the MR-DT or OSDP LCD keypad display to arm or disarm the alarm zone. Alarm zones are defined in the alarm zones screen. For more information on alarm zones, see the [Alarm Zones](#) help file topic.
 - *Enhanced Intrusion Processing By Reader* - This option will set up the MR-DT or OSDP LCD display keypad to arm and disarm alarm zones associated with a specific reader or group of readers with enhanced processing. To arm or disarm an alarm zone a valid credential or pin must be presented at the reader or keypad. Next press the <--- (*) button followed by the command code. Next enter the command number to be executed (0 = View Zone Status, 1 = Disarm Zone, 2 = Arm Zone in Away Mode, 3 = Arm Zone in Stay Mode, 4 = Arm Zone in Instant Mode, 5 = Toggle Keypad Chime, 6 = Bypass Points). Finally press the command (#) key and follow the instructions on the MR-DT or OSDP LCD keypad display. No two-digit alarm zone needs to be entered in this mode. All functions performed will

be performed on the alarm zone that is associated with the reader used. The associated alarm zone is defined in the readers screen. For more information on readers, see the [Readers](#) help file topic.

- *Command Code* - Enter the command code for intrusion processing. The command code is the code that must be entered at the MR-DT or OSDP LCD display keypad in order to execute intrusion processing commands. The command code can be used at any valid MR-DT or OSDP LCD keypad display attached to the SCP or EP panel. This field can be up to 6 digits in length.
- *Access Delay* - Select or enter the access delay for intrusion processing. The access delay is the amount of time in seconds that will be allowed between the presentation of a valid credential and the entering of the command code at a MR-DT or OSDP LCD keypad display. If the access delay has been exceeded the command code will be invalid.
- *Allowed Card Group* - Select the allowed card group for intrusion processing. The allowed card group is the only card group that will be allowed to execute intrusion processing command functions at any of the valid MR-DT or OSDP LCD keypad displays attached to the SCP or EP panel. If the card holder does not belong to this card group the command code will be invalid.
- *Command is Valid at All Readers* - Select (check) this option to allow command codes to be entered at any of the readers attached to the SCP or EP panel. Uncheck this option to specify the valid readers for command code entry for the SCP or EP panel. To assign valid readers, "move" the readers that you wish to be valid from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window. The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired readers.

Web Logins

Web Logins are used to manage logins used by the SCP. These credentials include the EP web browser login (currently not supported), PSIA client logins, and BACnet logins. In order for a SCP to make use of any web logins, it must be communicating over an encrypted channel.

- *Standard Web Login* - This login is used in conjunction with the web browser of the EP and LP series controllers.
- *PSIA/REST Server* - This login is used in conjunction with the option Access It! Universal.NET PSIA service
- *PSIA Client Login* - This login is used by PSIA client such as the Inovonics ACG or KONE Elevators
- *BACnet Server Login* - This login is used in conjunction with the BACnet integration. Read/Write permissions can be applied to all BACnet devices

- *Over-Watch Login* - This login is used in conjunction with global SCP communications. This currently is only supported on the EP-4502 and is used only by the Otis Elevator solution

Elevator

Elevator setup is required for advanced elevator control. Currently the only supported integrations are the Otis Destination Dispatching and KONE KCG solutions.

This tab is only visible if the Advanced Elevator control in the license is enabled.

Elevator Control Type

- *Otis*- Select when using an Otis destination dispatching (DDS) system.
 - *Number of destinations* - Enter the total number of destination used by the elevator. A front and rear entry door would be considered as separate destinations.
 - *Number of destinations below ground level* - Enter the number of destinations located below ground level. A front and rear entry door would be considered as separate destinations.
 - *Elevator cabs have rear floors* - Select (check) this option if the elevator solution has a front and rear entry door.
When using a front and rear entry elevator cab, each side is considered a unique floor.
 - *Primary Otis DDS controller* - Select (check) this option if this is the primary OTIS-EP4502 controller.
- *KONE* - Select when using a KONE controller group (KCG) system.
 - *Number of destinations* - Enter the total number of destination used by the elevator. A front and rear entry door would be considered as separate destinations.
 - *Elevator cabs have rear floors* - Select (check) this option if the elevator solution has a front and rear entry door.
When using a front and rear entry elevator cab, each side is considered a unique floor.
 - Enter the maximum number of cab access configurations. Values can range from 1-32767. Cab configurations are applied to each card and can be defined by clicking the Edit Configuration... button.
 - *Primary KONE DCS controller* - Select (check) this option if this EP-4502 if the primary KONE-EP4502 controller that will be defining the global access configurations.
Only one Primary EP-4502-KONE can be used per site.
 - *Global Access Configuration (only visible for Primary KONE-EP4502)* - Configure the GFC for each floor as needed. The GFC is a floor code override that applies to all readers within the KONE system.

Save/Close Buttons

Clicking on the save button will save the changes made to the SCP. Clicking on the close button will not save the changes made to the SCP.

[SCP's](#)

Access Areas

[Access Areas Detail](#)

Access areas are physical or virtual areas used to control the number of cardholders within an area. Access areas can be used to control the minimum number of cardholders required in an area, the maximum number of cardholders allowed in an area or to disable access to an area all together. Access It! Universal.NET supports up to 32 access areas for each SCP panel.

Access areas must be used in conjunction with anti-passback. For more information about anti-passback readers, see the [Readers](#) help file topic. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Editing an Access Area

To edit an access area, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the access area to be edited. Next, click on the access areas item within the SCP. All of the access areas associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the access area to be edited and click on the edit button on the toolbar, or double click the access area to be edited. You can also select edit from the right click menu.

Access Area Commands

To send a command to an Area, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the area(s). Next, select areas. All of the areas associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the access area to send a command to and click on the access areas command drop down next to the edit button on the toolbar or select commands from the right click menu. Select the command to be issued from the list and click on the command to be sent. You can also send a command by selecting commands from the file option on the system menu and selecting the command to be sent.

The following access area commands are supported:

Disable

The access area will be disabled and access will not be allowed to any cardholders.

Enable

The access area will be enabled and access will be granted to authorized cardholders as long as the area is not full.

Set Occupancy Count

The occupancy count will be set to the value entered.

Request Area Status

The request area status command is used to view current status information for the access area. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *Area Name* - Displays the name of the access area.
- *Area State* - Displays whether or not the area is enabled.
- *Multiple Occupancy Required* - Displays whether or not two or more cardholders are required to be in the area.
- *Occupancy Count* - Displays the current occupancy count of the area.

Access Areas Detail

Access Areas

Access areas are physical or virtual areas used to control the number of cardholders within an area. Access areas can be used to control the minimum number of cardholders required in an area, the maximum number of cardholders allowed in an area or to disable access to an area all together. Access It! Universal.NET supports up to 32 access areas for each SCP panel.

Access areas must be used in conjunction with anti-passback. For more information about anti-passback readers, see the [Readers](#) help file topic. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Area Name

Enter the name to be used for this access area. All of the access areas have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the access areas being used. An example of a friendly name would be "Parking Garage". The access area name can be up to 50 characters in length.

SCP Name

This field displays the name of the SCP panel to which this access area is associated. This field is displayed for informational purposes only and cannot be changed.

Require 2 or More Cards in Area

Select (check) this option to enable the require two or more cards in this area option. This option will require two or more cards to be presented at the reader in order for access to be granted to the area if no cardholders are currently in the area. This option is used when it is desirable to have more than one person in an area at a time (multiple occupancy). The last two cardholders in the area will need to present both cards at the reader in order to leave the area and decrement the occupancy count to zero.

Area Enabled

Select (check) this option to enable this access area. When an access area is disabled (not checked) no cardholders will be allowed access to the area regardless of their assigned access levels. This option is useful to quickly disable access to a group of readers in the event of an emergency or accident.

Maximum Occupancy

Select or enter the maximum occupancy count for this area. The maximum occupancy count is the maximum number of cardholders that will be allowed in to the area. Once the maximum occupancy count has been reached no additional cardholder will be allowed in to the area regardless of their assigned access levels until another cardholder leaves the area.

Occupancy Threshold Going Up

Select or enter the occupancy threshold going up for this area. The occupancy threshold going up will generate an event or alarm when this threshold has been reached when a cardholder is entering the area. This could be used to turn on a "Lot Full" sign in a parking lot when the last allowed car enters a parking garage.

Occupancy Threshold Going Down

Select or enter the occupancy threshold going down for this area. The occupancy threshold going down will generate an event or alarm when this threshold has been reached when a cardholder is leaving the area. This could be used to turn off a "Lot Full" sign in a parking lot when a car leaves a parking garage.

Enable mantrap/airlock

Select (check) this option to configure this area in mantrap/airlock mode. When enabled, only one area can grant access to another area at a time. This mode supports multiple doors granting access to the same area at the same time.

One open door only mode

Used in conjunction with the mantrap/airlock mode. When enabled, only one door can be opened between areas at a given time.

Event Type

Access area events (transactions) are recorded in the event file every time there is a change of state for the access area. Access area events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Area Disabled* - The access area has been disabled and access will not be allowed to any cardholders.
- *Area Enabled* - The access area has been enabled and access will be granted to

authorized cardholders as long as the area is not full.

- *Area Empty* - The last cardholder in an area has left and the access area is empty.
- *Area at Downward Limit* - The access area has reached the value set for the occupancy threshold going down.
- *Area at Upward Limit* - The access area has reached the value set for the occupancy threshold going up.
- *Area Full* - The access area is full and access will not be allowed to any cardholders.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the access area. Clicking on the cancel button will not save the changes made to the access area.

[Access Areas](#)

Alarm Zones

[Alarm Zones Detail](#)

Alarm zones are groups of input and reader alarm events (conditions) which can be armed and disarmed producing various events. These events can then be acted upon by tasks and macros. Access It! Universal.NET supports up to 64 alarm zones for each SCP panel. All of the default alarm zones have no devices assigned to them.

Alarm zones cannot be deleted from the database. To "delete" or disable an alarm zone, simply remove all of the assigned conditions within the alarm zone. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Editing an Alarm Zone

To edit an alarm zone, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the alarm zone to be edited. Next, click on the alarm zone within the SCP.. All of the alarm zones associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the alarm zone to be edited and click on the edit button on the toolbar, or double click the alarm zone to be edited. You can also select edit from the right click menu.

Alarm Zone Commands

To send a command to an alarm zone, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the alarm zone(s). Next, select alarm zones.. All of the alarm zones associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the alarm zone to send a command to and click on the alarm zones command drop down next to the edit button on the toolbar or select commands from the right click menu. Select the command to be issued from the list to send the command. You can also send a command by selecting commands from the file option on the system menu and selecting the command to be sent.

The following alarm zone commands are supported:

Disarm

The disarm alarm zone command is used to disarm the currently selected alarm zone or to increment the disarm count if the alarm zone is already disarmed.

Override

The override alarm zone command is used to set the disarm count to the value entered for the currently selected alarm zone.

Force Arm

The force arm alarm zone command is used to arm the alarm zone or to decrement the disarm count while there are active alarm conditions for the currently selected alarm zone.

Arm

The arm alarm zone command is used to arm the alarm zone or to decrement the disarm count while there are no active alarm conditions for the currently selected alarm zone.

Override Arm

The override arm alarm zone command is used to arm the alarm zone or to decrement the disarm count while there are active alarm conditions for the currently selected alarm zone.

Request Alarm Zone Status

The request alarm zone status command is used to view current status information for the

alarm zone. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *Alarm Zone Name* - Displays the name of the alarm zone.
- *Disarm Count* - Displays the disarm count of the alarm zone.
- *Active Alarm Conditions* - Displays the number of active alarm conditions in the alarm zone.

Alarm Zones Detail

Alarm Zones

Alarm zones are groups of input and reader alarm events (conditions) which can be armed and disarmed producing various events. These events can then be acted upon by tasks and macros. Access It! Universal.NET supports up to 64 alarm zones for each SCP panel. All of the default alarm zones have no devices assigned to them.

Alarm zones cannot be deleted from the database. To "delete" or disable an alarm zone, simply remove all of the assigned conditions within the alarm zone. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Alarm Zone Name

Enter the name to be used for this alarm zone. All of the alarm zones have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the alarm zones being used. An example of a friendly name would be "Front Office". The alarm zone name can be up to 50 characters in length.

SCP Name

This field displays the name of the SCP panel to which this alarm zone is associated. This field is displayed for informational purposes only and cannot be changed.

Alarm Zone Number

This field displays the alarm zone number associated with this alarm zone. Based on how the SCP is configured, the alarm zone number may be required when alarm zones are armed and disarmed from the MR-DT reader. This field is displayed for informational purposes only and cannot be changed.

Default State

Select the default state for this alarm zone. The default state determines the mode that the alarm zone will default to when the alarm zone is first set up or when the SCP panel is reset or a download is performed. The following default states are supported:

Disarmed - The alarm zone will default to a disarmed state.

Fault - The alarm zone will default to a fault state.

Armed-Away - The alarm zone will default to an armed-away state.

Armed-Stay - The alarm zone will default to an armed-stay state.

Armed-Instant - The alarm zone will default to an armed-instant state.

Entry Delay in Progress - The alarm zone will default to an armed state with an entry delay in progress.

Exit Delay in Progress - The alarm zone will default to a disarmed state with an exit delay in progress.

Alarm-New - The alarm zone will default to an armed state with new alarms in progress.

Silenced Alarm - The alarm zone will default to an armed state with cancelled alarms pending.

This option is only available for enhanced intrusion processing modes. For more information on intrusion processing modes, see the [SCPs](#) help file topic.

Entry Delay

Enter or select the entry delay for this alarm zone. The entry delay is the amount of time that a card holder will be allowed when a perimeter point has changed to an alarm state to present a valid credential, enter a command code and disarm the system prior to an alarm being generated. This value can range from 1 to 32767 seconds.

This option is only available for enhanced intrusion processing modes. For more information on intrusion processing modes, see the [SCPs](#) help file topic.

Exit Delay

Enter or select the exit delay for this alarm zone. The exit delay is the amount of time that the system will wait to arm once a valid credential has been presented, a command code has been entered and an arm command has been issued to allow a card holder to exit. This value can range from 1 to 32767 seconds.

This option is only available for enhanced intrusion processing modes. For more information on intrusion processing modes, see the [SCPs](#) help file topic.

Auto Disarm on Valid Access

Select (check) this option to enable auto disarm on valid access mode for this alarm zone. When auto disarm on valid access mode is enabled the alarm zone will be disarmed when a card is presented and valid access is granted at any of the readers associated with this alarm zone.

This option is only available for enhanced intrusion processing modes. For more information on readers see the [Readers](#) help file topic.

Skip "Alarm Cancelled" (Go Straight to "Disarmed")

Select (check) this option to enable skip alarm cancelled mode. When skip alarm cancelled mode is enabled and an alarm is cancelled the alarm zone will go to a disarmed state instead of an alarm cancelled state.

This option is only available for enhanced intrusion processing modes.

Point Name/Details

Select the points to be used in this alarm zone. Add all of the input or door points to be used in this alarm zone and set the point type and parameters. Any points added to this alarm zone will result in an alarm condition upon change of state to an alarm condition. Click on the add button and choose the point to be added and set the point parameters and options. The following point parameters are supported:

Point Type - Select either an input point or a reader/door point then select the name of the point to add to the alarm zone.

Point Mode - Select the point mode for the point being added to the alarm zone. The point type can be either 24 hour (instant), perimeter (entry and exit delays will apply) or interior (arm-stay mode applies). The point mode selected, along with the alarm zone state, defines the way in which alarm reporting is processed. For additional information, see the [Alarm Reporting](#) help file topic. Select (check) chime to produce a chime at the keypad whenever the point state changes.

Default Monitoring Mode - Select the default monitoring mode for the point being added to the alarm zone. Select normal monitoring to process change of states and produce alarms, bypassed to bypass the point for alarm processing but still produce change of state events or disabled to ignore the point by default.

Entry Delay - Select the entry delay for the point being added to the alarm zone. Select instant for no delay, start entry delay to begin an entry delay when the point changes to an alarm state before producing an alarm or follow entry delay if this point is to be part of an entry delay group of points.

This option is only available for enhanced intrusion processing modes. For more information on intrusion processing modes, see the [SCPs](#) help file topic.

SIA Zone Number

Enter the SIA zone number for this alarm zone point. The SIA zone number will be the zone number that gets reported to the central station when this alarm zone point goes in to an alarm condition.

This option is only available for enhanced intrusion processing modes. The tab will only be available when central station reporting has been enabled for the alarm zone.

SIA Point Type

Select the SIA point type for this alarm zone point. The SIA point type will determine the SIA alarm code that gets sent to the central station when this alarm zone point goes in to an alarm condition. For example, if the point type is set to burglary a "BA" would be sent to the central station for identification of the type of alarm being reported.

This option is only available for enhanced intrusion processing modes. The tab will only be

available when central station reporting has been enabled for the alarm zone.

Tasks

Select the task to execute for each of the alarm zone states. The select task will be executed each time any of the points in the alarm zone change to the indicated state.

This option is only available for enhanced intrusion processing modes. For more information on intrusion processing modes, see the [SCPs](#) help file topic. A Task configured to execute a Macro must have an additional step in it in order to properly execute.

Central Station Reporting

Select (check) this option to enable central station reporting for this alarm zone. If central station reporting is enabled for this alarm zone enter the account ID, alternate account ID, group number and comm timeout. This information can be obtained from the central station provider. Some of these fields may be optional depending upon the service provider.

This option is only available for enhanced intrusion processing modes.

Available/Assigned Alarm Conditions

To assign conditions to an alarm zone, select the condition(s), then "move" the conditions that you wish to be assigned to the alarm zone from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected conditions from the available window to the assigned window. The "<<" button will move all selected conditions from the assigned window to the available window. Multiple conditions can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired conditions.

This option is only available for standard intrusion processing modes. For more information on intrusion processing modes, see the [SCPs](#) help file topic.

Event Type

Alarm zone events (transactions) are recorded in the event file every time there is a change of state for the alarm zone. Alarm zone events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported for standard intrusion processing modes:

- *Alarm Zone Disarmed* - The alarm zone has been disarmed and no devices were in alarm condition.
- *Alarm Zone Disarmed Already Disarmed* - The alarm zone has been disarmed again while already in a disarmed state.
- *Alarm Zone Override Armed* - The alarm zone has been override armed with one or

more devices in alarm condition and the disarm count has been set to zero.

- *Alarm Zone Override Disarm Count Set* - The alarm zone has been override disarmed and the disarm count has been set to a non-zero value.
- *Alarm Zone Force Arm Zone Armed* - The alarm zone has been force armed with one or more devices in alarm condition.
- *Alarm Zone Force Arm Disarm Count* - The alarm zone has been attempted to be armed with one or more devices in alarm condition and the disarm count has been decremented.
- *Alarm Zone Armed* - The alarm zone has been armed and no devices were in alarm condition.
- *Alarm Zone Not Armed Zone Active* - The alarm zone has been attempted to be armed with one or more devices in alarm condition and the zone was not armed.
- *Alarm Zone Arm Still Disarmed* - The alarm zone disarm count has been decremented but is still greater than zero and the alarm zone is still disarmed.
- *Alarm Zone Override Arm* - The alarm zone has been override armed with one or more devices in alarm condition and the disarm count has been set to zero.
- *Alarm Zone Override Arm Still Disarmed* - The alarm zone disarm count has been decremented but is still greater than zero and the alarm zone is still disarmed.

The following event types are supported for enhanced intrusion processing modes:

- *Alarm Zone Disarmed* - The alarm zone has been disarmed and no devices were in alarm condition.
- *Alarm Zone Fault* - The alarm zone is in a fault state. One or more of the points in the alarm zone are in a fault condition
- *Alarm Zone Armed Away* - The alarm zone has been armed and an exit delay will begin at any perimeter points.
- *Alarm Zone Armed Stay* - The alarm zone has been armed and all perimeter point will be armed and all interior points will not be armed.
- *Alarm Zone Armed Instant* - The alarm zone has been armed and no exit delay will begin at any perimeter points.
- *Alarm Zone Entry Delay* - A perimeter point has changed to an alarm state and an entry delay has begun.
- *Alarm Zone Exit Delay* - The alarm zone has been armed and an exit delay has begun.
- *Alarm Zone In Alarm* - One or more of the points in the alarm zone has changed to an alarm state.
- *Alarm Zone Alarm Canceled* - An alarm has been acknowledged and the system has been disarmed.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each

time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the alarm zone. Clicking on the close button will not save the changes made to the alarm zone.

[Alarm Zones](#)

Tasks

[Tasks Detail](#)

Tasks are used to perform automated actions within the system. Tasks can perform a wide variety of actions, such as, disabling a point during a timezone, changing a reader mode during a timezone and pulsing an output when an input is activated. Tasks can contain multiple steps and perform more than one action at a time. Task execution can either be automatically or manually executed.

Tasks are stored in the SCP panel and will execute regardless of whether or not the SCP panel is being communicated to with the Access It! Universal.NET software. Tasks can only perform actions on devices installed within the selected SCP panel. Tasks cannot perform actions on devices located on other SCP panels in the system. To perform global actions across multiple SCP panels use a Macro to perform the action. For more information on macros, see the [Macros](#) help file topic. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Editing a Task

To edit a task, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the task(s) to be edited and select Tasks. All of the tasks associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the task to be edited and click on the edit button on the toolbar, or double click the task to be edited. You can also select edit from the right click menu.

Tasks cannot be deleted from the system database. To disable or "delete" a task, either uncheck task enabled, or select revert to default.

Printing Task Reports

To print reports for a task, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the task(s) to be printed and select Tasks. All of the tasks associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the tasks to print reports for and click on the report button within the ribbon. You can also select print reports from the right click menu. The following reports are available:

- *Task History* - This report provides a list of all history for the selected Tasks, as well as task executions.
- *Task Listing* - This report provides a list of all tasks for the selected SCPs. This report includes execute conditions as well as task steps.

Manual Task Execution

To manually execute a task, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the task(s) to be edited. Next, click on the tasks item within the SCP. All of the tasks associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the task to execute and click on the execute task command within the ribbon. You can also manually execute a task by selecting execute task from the right click menu.

Tasks Detail

Tasks

Tasks are used to perform automated actions within the system. Tasks can perform a wide variety of actions, such as, disabling a point during a timezone, changing a reader mode during a timezone and pulsing an output when an input is activated. Tasks can contain multiple steps and perform more than one action at a time. Task execution can either be automatically or manually executed.

Tasks are stored in the SCP panel and will execute regardless of whether or not the SCP panel is being communicated to with the Access It! Universal.NET software. Tasks can only perform actions on devices installed within the selected SCP panel. Tasks cannot perform actions on devices located on other SCP panels in the system. To perform global actions across multiple SCP panels, use a Macro to perform the action. For more information on macros, see the [Macros](#) help file topic. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Task Name

Enter the name to be used for this task. All of the tasks have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the tasks being used. An example of a friendly name would be "Unlock All Doors". The task name can be up to 50 characters in length.

Task Enabled

Select (check) this option to enable the task. When disabled the task will not function.

SCP Name

This field displays the name of the SCP panel to which this task is associated. This field is displayed for informational purposes only and cannot be changed.

Conditionally Execute

Select the execute conditions for this task. The execute conditions are the conditions under which this task will be executed. The following execute conditions are supported:

- *Manual Only* - The task can only be executed manually with a command or by a macro.
- *When an Input Changes State* - The task will execute each time the selected input changes to the selected state during the selected timezone.
- *When an Output Changes State* - The task will execute each time the selected output

changes to the selected state during the selected timezone.

- *When a Reader Mode Changes* - The task will execute when the reader mode for the selected reader(s) changes to the selected reader mode(s) during the selected timezone.
- *When a Door Opens or Closes* - The task will execute each time the selected reader changes to the selected state during the selected timezone.
- *When a Cardholder Presents a Valid Card* - The task will execute each time the selected card transaction is generated at the selected reader during the selected timezone. A specific card group can also be specified so that the task will only execute for a certain group of cards that generate the selected card transaction.
- *When a Cardholder Presents an Invalid Card* - The task will execute each time the selected card transaction is generated at the selected reader during the selected timezone. A specific card group can also be specified so that the task will only execute for a certain group of cards that generate the selected card transaction.
- *When a Request to Exit is Granted* - The task will execute each time the selected reader is granted a request to exit either by the request to exit device at the door or by a reader command during the selected timezone.
- *When a Timezone Begins or Ends* - The task will execute each time the selected timezone begins or ends, during the selected timezone.
- *When a User Enters a Keypad Command* - The task will execute when a card holder enters the specified numeric command at the specified reader during the timezone specified. The keypad command must include the "*" character at the beginning of the command and the "#" character at the end of the command when being entered at the specified keypad reader.
- *When a User Enters a User Command* - The task will execute when a card holder enters the specified user command at the specified reader during the timezone specified. A user command must be preceded by a valid card holder authentication (card swipe, pin entry, etc.) prior to successful execution.
- *When an Alarm Zone Changes State* - The task will execute each time the selected alarm zone changes to the selected state during the selected timezone.
- *When an Area Changes State* - The task will execute each time the selected area changes to the selected state during the selected timezone.
- *When an SIO comm state changes* - The task will execute each time the selected SIO changes its communication state during the selected timezone.
- *When an SIO tamper state changes* - The task will execute each time the selected SIO changes its tamper state during the selected timezone.
- *When an SIO power state changes* - The task will execute each time the selected SIO changes its power state during the selected timezone.
- *When an SCP comm state changes* - The task will execute each time the selected SCP changes its communication state during the selected timezone.
- *When an SCP power/tamper state changes* - The task will execute each time the selected SCP changes its tamper or power state during the selected timezone.

Task Steps

Enter the steps (actions) to be performed by this task. Tasks can perform as many steps as desired. Click on the add button and choose the step to be performed and the device on which to perform the step. The following task steps are supported:

- *Enable Input* - The selected input will be enabled and reporting of events (transactions) will occur from the device attached to the input.
- *Disable Input* - The selected input will be disabled and no reporting of events (transactions) will occur from the device attached to the input.
- *Deactivate Output* - The selected output will be deactivated (de-energized).
- *Activate Output* - The selected output will be activated (energized).
- *Pulse Output* - The selected output will be pulsed (activated, then deactivated) for the amount of time specified in the pulse time setting for the task step.
- *Disable Reader* - The selected door will be locked and the reader will not grant access to any cards, even if they have a valid access level or facility code for the selected door.
- *Unlock Reader/Door* - The selected door will be unlocked.
- *Lock Reader/Door* - The selected door will be locked. No cards presented will be able to obtain access to the reader. Request to exit functionality will continue to function.
- *Set Reader to Facility Code Only* - The selected door will be locked and any card with a valid facility code will be granted access to the selected door at any time. The card does not require a valid access level to be granted access in this mode.
- *Set Reader to Card Only* - The selected door will be locked and only cards with valid facility codes and access levels will be granted access in this mode.
- *Set Reader to PIN Only* - The door will be locked and any valid PIN number entered will be granted access in this mode.
- *Set Reader to Card and PIN* - The selected door will be locked and only cards with valid facility codes and access levels will be granted access in this mode. A pin number entry that matches the card number's PIN number field will also be required at the selected reader's keypad. This option is supported for readers with keypads only.
- *Set Reader to Card Or PIN* - The door will be locked and only cards with valid facility codes and access levels or valid PIN numbers will be granted access in this mode.
- *Enable 2 Card Mode* - The door will be locked and will require two valid cards to be presented at this reader in order for access to be granted to the door.
- *Disable 2 Card Mode* - The door will be locked and will require a single card to be presented at this reader in order for access to be granted to the door.
- *Enable Biometric Verify* - The door will be locked and biometric verification will be required in addition to either a valid card or PIN (depending on reader mode) for access to be granted to the door.
- *Disable Biometric Verify* - The door will be locked and biometric verification will not be required in addition to either a valid card or PIN (depending on reader mode) for access to be granted to the door.
- *Disable Cipher Mode* - The door will be locked and the ability to enter a facility code and

card number instead of presenting a card at this reader for access to be granted to the door will be disabled.

- *Enable Cipher Mode* - The door will be locked and the ability to enter a facility code and card number instead of presenting a card at this reader for access to be granted to the door will be enabled.
- *Otis DEC Mode 1 - default floors* - Used in conjunction with OTIS destination dispatch solutions. Configure the selected DEC to grant access upon a card presentation and allow access to the default floor assigned to the card.
- *Otis DEC Mode 2 - authorized floors* - Used in conjunction with OTIS destination dispatch solutions. Configure the selected DEC to grant access upon a card presentation and allow access to any floor the card has access to.
- *Otis DEC Mode 3 - user entry of floor* - Used in conjunction with OTIS destination dispatch solutions. Configure the selected DEC to grant access upon a card presentation and allow access to any floor selected.
- *Otis DEC Mode 4 - default floors or user entry* - Used in conjunction with OTIS destination dispatch solutions. Configure the selected DEC to grant access upon a card presentation and allow user to enter desired floor. If no floor selected the DEC will grant access to the default floor assigned to the card.
- *Disable Reader Temporary* - The selected door will be locked and the reader will not grant access to any cards, even if they have a valid access level or facility code for the selected door for the specified amount of time.
- *Unlock Reader/Door Temporary* - The selected door will be unlocked for the specified amount of time.
- *Lock Reader/Door Temporary* - The selected door will be locked for the specified amount of time.
- *Set Reader to Facility Code Only Temporary* - The selected door will be locked and any card with a valid facility code will be granted access to the selected door at any time for the specified amount of time. The card does not require a valid access level to be granted access in this mode.
- *Set Reader to Card Only Temporary* - The selected door will be locked and only cards with valid facility codes and access levels will be granted access in this mode for the specified amount of time.
- *Set Reader to PIN Only Temporary* - The door will be locked and any valid PIN number entered will be granted access in this mode for the specified amount of time.
- *Set Reader to Card And PIN Temporary* - The selected door will be locked and only cards with valid facility codes and access levels will be granted access in this mode for the specified amount of time. A pin number entry that matches the card number's PIN number field will also be required at the selected reader's keypad. This option is supported for readers with keypads only.
- *Set Reader to Card Or PIN Temporary* - The door will be locked and only cards with valid facility codes and access levels or valid PIN numbers will be granted access in this mode for the specified amount of time.
- *Enable Door Forced Open* - The selected doors forced open event (transaction) WILL

be reported while the door forced open is enabled.

- *Disable Door Forced Open* - The selected doors forced open event (transaction) WILL NOT be reported while the door forced open is disabled.
- *Enable Door Held Open* - The selected doors held open event (transaction) WILL be reported while the door held open is enabled.
- *Disable Door Held Open* - The selected doors held open event (transaction) WILL NOT be reported while the door held open is disabled.
- *Grant Access* - The selected door will be unlocked for the amount of time specified in the standard unlock time field for the selected reader.
- *Dial Host* - The SCP panel associated with this task will dial the host phone number that has been stored in the SCP when this step executes. This is generally used to set up immediate dial back notification for important alarms when using a SCP panel in a Dial-up configuration.
- *Execute Macro* - The selected macro will be executed.
- *Temporary Timezone Deactivate* - The selected timezone(s) will be temporarily deactivated until the next valid timezone interval reactivates the timezone(s).
- *Temporary Timezone Activate* - The selected timezone(s) will be temporarily activated until the next valid timezone interval deactivates the timezone(s).
- *Timezone Deactivate* - The selected timezone(s) will be deactivated until a task is performed to reactivate the timezone or until the timezone is reset to the default timezone mode.
- *Timezone Activate* - The selected timezone(s) will be activated until a task is performed to deactivate the timezone or until the timezone is reset to the default timezone mode.
- *Return Timezone to Normal* - The selected timezone(s) will be set to normal mode until the next valid timezone interval changes the timezone mode or until the timezone is reset to the default timezone mode.
- *Refresh Timezone* - The selected timezone(s) will be refreshed to the correct state Based on the time of day. This is useful when it is desirable to set a timezone to a correct state when it's state has been changed by a command or by an SCP panel reset. If a door was unlocked during a timezone and the SCP panel had been reset refreshing the timezone would then unlock the door again without having to wait for the next timezone interval to take place.
- *Delay (Seconds)* - The task will be delayed for the number of seconds entered in this step. This is useful when it is desirable to have a "pause" in between task steps (see example below).
- *Abort a Delayed Task* - The execution of the selected delayed task will be canceled (see example below).
- *Execute a Task* - The selected task will be executed from within the task step. This is useful for "nesting" task execution (see example below).
- *Resume a Delayed Task* - The execution of the selected delayed task will be resumed (see example below).
- *Issue Free Pass to All Cards* - This task step will issue a free pass to all cards in the system. This will reset all cards for anti-passback use at any of the readers in the

system and then set the cards area to the area that the first reader used grants access to.

- *Temporary Reader LED Control* - This task step will allow temporary control of the selected readers LED and Beeper. This is useful to send a sequence of beeps to a reader when a door has been forced or held open (see example below).
- *LCD Text Output* - This task step will output the specified text to the selected readers with the options specified. This is useful for sending text to the MR-DT or OSDP LCD display keypad when various functions are performed for visual feedback of operations.
- *Disarm Alarm Zone* - The selected alarm zones will be disarmed.
- *Override Alarm Zone* - The selected alarm zones will be overridden and the disarm count will be set to the new value specified.
- *Force Arm Alarm Zone* - The selected alarm zones will be armed regardless of whether or not they are in a secure state.
- *Arm Alarm Zone* - The selected alarm zones will be armed as long as they are in a secure state.
- *Override Arm Alarm Zone* - The selected alarm zones will be overridden and armed and the disarm count will be set to zero.
- *Send Data Out RS-485 Port* - This task step will output the specified data to the selected downstream port on the SCP panel. This is useful for controlling external devices such as fuel dispensers.
- *Disable Access Area* - The selected access areas will be disabled.
- *Enable Access Area* - The selected access areas will be enabled.
- *Set Access Area Occupancy Count* - The selected access areas occupancy count will be set to the value specified.

Some examples of common tasks are:

Sounding an audible alarm when a door has been forced or held open:

This is a common task set which will sound an audible alarm using the readers beeper when a door has been propped or forced open. This task can be accomplished by setting up the following task entries:

Task 1:

Task Name = Sound Beeper on Forced or Held

Execute Mode = Automatic

Execute this Task When = A Door Opens or Closes

Reader Name = Select the desired reader name

Only During Timezone = Always

Door Conditions = Door has been Forced or Held Open

Task Step 1 = Temporary Reader LED Control, select the desired reader name and set repeat count and beep count to 5

Task Step 2 = Delay (Seconds), set the delay time to 1

Task Step 3 = Execute a Task, "Sound Beeper on Forced or Held" (this will restart the

current task performing a loop while the door is not secure)

Task 2:

Task Name = Cancel Forced or Held Beeper

Execute Mode = Automatic

Execute this Task When = A Door Opens or Closes

Reader Name = Select the desired reader name

Only During Timezone = Always

Door Conditions = Any Door Secure Condition

Task Step 1 = Abort a Delayed Task, "Sound Beeper on Forced or Held" (this will cancel the looping task when the door has been secured)

In order for this example to work, the reader must have a beeper and it must be wired correctly to the SIO panel.

Unlocking a door when a when a teacher enters the classroom and re-locking the door when the teacher leaves the room.

This is a common task set which is generally used when it is desirable to have a specific person or persons in an area and then unlock the door so that other people may enter without having to use a card. This task can be accomplished by setting up the following task entries:

Task 1:

Task Name = Unlock Wood Shop Door

Execute Mode = Automatic

Execute this Task When = A Cardholder Presents a Valid Card

Reader Name = Select the desired reader name

Only During Timezone = Always

Card Transaction Types = Access Granted

Specify Card Group = The card group of the card or cards allowed to execute the task. This task requires that a special card group be set up, otherwise ALL cards will be capable of unlocking the door.

Task Steps = Unlock Reader/Door, select the desired reader name

Task 2:

Task Name = Lock Wood Shop Door

Execute Mode = Automatic

Execute this Task When = A Cardholder Presents an Invalid Card

Reader Name = Select the desired reader name

Only During Timezone = Always

Card Transaction Types = Access Granted Access Point Unlocked

Specify Card Group = The card group of the card or cards allowed to execute the task

Task Steps = Set Reader to Card Only, select the desired reader name

Setting up a door alarm bypass relay (output).

This is a common task which is generally used when there is a crash bar or other door alarm device attached to a door and it is necessary to shunt or bypass this device during normal business hours, when a motion detector produces a request to exit for the door.

Task 1:

Task Name = Shunt Door Alarm

Execute Mode = Automatic

Execute this Task When = A Request to Exit is Granted

Reader Name = Select the desired reader name

Only During Timezone = Office Hours

Request to Exit Conditions = Normal Exit Cycle

Task Steps = Pulse Output, select the desired output name

Changing the mode of a reader to require a supervisor to enter an area before non-supervisors can use the reader. (Supervisor Card Feature)

This is a common task used to ensure that a supervisor or a member of a certain group of employees is the first to enter the facility at the start of a business day. This is useful if only certain employees are allowed to disarm the alarm system. This functionality can be used to ensure that the supervisor is the first person to be granted access to the facility even if other employees have arrived first and tried to use their cards to enter the facility. This task can be accomplished by setting up the following task entries:

Task 1:

Task Name = Temporary Timezone Activate upon Supervisor Entry

Execute Mode = Automatic

Execute this Task When = A Cardholder presents a Valid Card

Reader Name = Select the desired reader name

Only During Timezone = Always

Card Transaction Types = Access Granted, Specify Supervisor Card Group

Task Steps = Temporary Timezone Activate, select the desired timezone name

In order for this example to work, the supervisor card or cards will need to have their card group set to non-zero. In addition, the desired timezone will need to have the default timezone mode set to always inactive so that the timezone does not activate until a supervisor with the proper card group uses the selected reader.

Setting up a "man trap" that will disable a secondary entrance reader until the primary entrance door has been closed.

This is a common task used to ensure that an outside door has been closed before the card holder can gain access to an inner door such as a clean room. This task can be accomplished by setting up the following task entries::

Task 1:

Task Name = Enable Inner Lab Entrance Reader

Execute Mode = Automatic
Execute this Task When = A Door Opens or Closes
Reader Name = Select the desired reader name
Only During Timezone = Always
Door Conditions = Door Opens Then Closes

Task Step 1 = Set Reader to Card Only, select the desired inner (clean room) reader name
Task Step 2 = Disable Reader, select the desired outer (outer lab entrance) reader name

The Outer Lab reader would need to be disabled by another task when either a request to exit is granted into the holding area from the clean room or when access is granted at the clean room reader. This will prevent both doors from being open at the same time.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Event Type

Task events (transactions) are recorded in the event file every time there is a change of state for the task. Task events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Task Activated* - The task has been activated using an execute condition and not manually.
- *Task Executed* - The task has been executed.
- *Task Canceled* - The task has been canceled.
- *Task Resumed* - The task has been resumed after being delayed.

Annunciation Type

- *Disregard* - Task events (transactions) for this event type will not be recorded in the event file and will not be displayed in either the events window or in the alarms window.

- *Log Only* - Task events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display* - Task events (transactions) for this event type will be recorded in the event file and displayed in the events window.
- *Alarm* - Task events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic.

The alarm priority is only used for event types that have the annunciation type set to "Alarm".

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on alarms, see the [Alarms](#) help file topic.

The alarm message is only used for event types that have the annunciation type set to "Alarm".

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the alarms window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic.

The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Message

Enter the event message for this event type. The event messages will be displayed in the events window each time this event type is generated. The event message is generally used to provide friendly text identification to the person monitoring events to identify the input point. This field can be up to 256 characters in length. For more information on events, see the [Events](#) help file topic.

Save/Cancel Buttons

Clicking on the save button will save the changes made to the task. Clicking on the cancel button will not save the changes made to the task.

Tasks

SIO's

[SIO's Detail](#)

SIO's are used to define the model and operational parameters for each of the SIO panels in the system. If the main SIO item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the SIO panels. The SIO icon will also display the current alarm state for each of the SIO panels. **Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.**

Searching SIOs

To search for an SIO, type in the search box located in the upper right hand corner. Results will be dynamically displayed as search criteria is entered. To include a wildcard in the search use the asterisk (*) symbol.

Custom filtered views can be selected for the SIOs screen. When applied, SIOs will dynamically populate based on their changing states. Newly added devices will not appear in the filtered list until the grid is refreshed by clicking the green refresh icon. Filtered views include:

- *(No Filter)* - No filter will be applied to the IP Locksets grid.
- *Online* - Only SIOs in the online state will display within the SIOs grid.
- *Offline* - Only SIOs in the online state will display within the SIOs grid.

Adding a SIO

To add a SIO expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the SIO(s) to be added and select SIOs. Select the SIO to be added and click on the edit button on the toolbar, or double click the SIO to be edited. You can also select edit from the file option on the system menu or from the right click menu. Select (check) the box Device Installed to add the SIO. All Inputs/Outputs/Readers will automatically then be created.

When an EP-series SCP is created, a SIO at address 0 is automatically installed.

Editing an SIO

To edit a SIO expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the SIO(s) to be edited and select SIOs. All of the SIOs associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SIO to be edited and click on the edit button on

the toolbar, or double click the SIO to be edited. You can also select edit from the file option on the system menu or from the right click menu.

Deleting an SIO

To delete a SIO expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the SIO(s) to be deleted and select SIOs. All of the SIOs associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SIO to be deleted and click on the edit button on the toolbar, or double click the SIO to be edited. You can also select edit from the file option on the system menu or from the right click menu. Uncheck the option Device Installed to remove this SIO.

All Inputs/Outputs/Readers will be removed from the system. If any peripheral devices are used within Tasks, the SIO will not be removed.

Printing SIO Reports

To print reports for an SIO, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the SIO(s) to be edited and select SIOs. All of the SIOs associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SIO's to print reports for and click on the Reports button within the ribbon or select print reports from the right click menu. The following reports are available:

- *SIO History* - This report provides a list of all history for the selected SIOs. This report includes all database updates as well as all hardware activity.
- *SIO Listing* - This report provides a list of the selected SIOs and their various properties.

SIO Commands

To send a command to an SIO, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the SIO and select SIOs. All of the SIO's associated with the selected SCP will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SIO to send a command to and click on the SIO commands drop down next to the edit button in the ribbon or select commands from the right click menu. Select the command to be issued from the list and click on the command to be sent to the SIO panel.

The following SIO commands are supported:

Request SIO Status

The request SIO status command is used to view current status information for the SIO panel. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *SIO Name* - Displays the name of the SIO Panel.
- *Comm Status* - Displays the communication status of the SIO panel. This is the status of the communication between the SCP and the SIO panel.
- *Retry Count* - Displays the communication retry count. A high number here could indicate a wiring problem between the SCP and the SIO panel.
- *Tamper Status* - Displays the status of the tamper device for the SIO panel.
- *Power Status* - Displays the status of the power monitoring device for the SIO panel.
- *Model* - Displays the model number of the SIO panel.
- *Firmware* - Displays the current firmware revision number of the SIO panel (x.x.x.).
- *Serial #* - Displays the serial number of the SIO panel.
- *Device Status* - Displays the current status of all of the devices attached to the SIO panel. These fields will vary based on the type of SIO panel installed.
- *OEM Code* - Displays the current OEM code number of the SIO panel.

Download Firmware

The download firmware command is used to download firmware to the selected SIO panel. **Downloading firmware can be very complex and is only recommended to be used by advanced users with the assistance of the Access It! Universal.NET technical support staff. Sending an invalid firmware file can compromise the security and functionality of the system.**

Load AES Keys

Sends 128-bit AES keys to the SIO in order to encrypt the communication between SCP and SIO.

SIO's Detail

SIO's

SIO's are used to define the model and operational parameters for each of the SIO panels in the system. If the main SIO item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the SIO panels. The SIO icon will also display the current alarm state for each of the SIO panels. **Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.**

SIO Name

Enter the name to be used for this SIO. All of the SIO's have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the SIO's being used. An example of a friendly name would be "Main Building SCP - MR52 01 - Gate Readers". The SIO name can be up to 50 characters in length.

Attached to SCP

This field displays the name of the SCP panel to which this SIO panel is attached. This field is displayed for informational purposes only and cannot be changed.

Model

Select the model for this SIO panel.

It is very important that the model selected matches the model of the panel being installed. Choosing the wrong SIO model could result in system malfunctions.

Device Installed

Select (check) this option if this SIO has been physically installed in the system. If the device installed option is checked, communication with the SIO panel will be initiated. If the device installed option is unchecked, no communication will occur with the SIO panel.

During system installation, it may be helpful to leave the device installed option unchecked until all of the hardware has been set up for the SIO. That way, the system can be "predefined" without receiving various communications and status alarms while panels, readers and associated hardware is being installed in the system.

Address

This field displays the physical hardware address of the SIO panel. The address can be

determined by the default name assigned to the SIO panel. This field is displayed for informational purposes only and cannot be changed.

The address must match the DIP switch settings on the SIO panel. For more information on setting the SIO panel DIP switches, see the [Access It! Universal.NET Quick Reference document](#).

Encrypt Communications

Select (check) this option if this SIO will be using 128 bit AES encryption to communicate to the SCP. Prior to selecting this option, the AES keys must first be loaded into the SIO see [SIO Commands](#) for more information.

IP Address Mode (MR-51E)

- *Use Panel DHCP Server* - If this option is selected, an IP address and the MAC address from the MR51E must be entered and the panel will reserve the IP address for the MR51E.
- *Use Public DHCP Server* - If this option is selected, the MAC address from the MR51E must be entered and the public DHCP server will assign and associate an IP address to the MAC address.
- *Static IP Address* - If this option is selected, enter the IP address and MAC address that were programmed into the MR51E utilizing the MSC MR51E Address Configuration Tool.

IP Address (MR-51E)

Enter the IP address that you want this SIO panel to use. This address will be downloaded to the EP-1502 or EP-2500 and then automatically assigned to the SIO panel when power is applied to it.

MAC Address (MR-51E)

Enter the MAC address of this SIO panel. The MAC address is printed on the SIO board next to the Ethernet connector. This address will be used to assign the IP address to the SIO panel.

Channel (IN)

Select the downstream input channel that this SIO panel is being attached to on the SCP. For more information on SCP downstream channels, see the [SCP's](#) help file topic.

Channel (OUT)

Select the downstream output channel that this SIO panel is being attached to on the SCP. For more information on SCP downstream channels, see the [SCP's](#) help file topic.

The channel in and channel out settings are set to the same channel when using 2-wire RS485 communications. When using 4-wire RS485 communications, set the transmit pair to a separate channel from the receive pair.

SIO for continuation of Inputs

Select the SIO panel that will be used as the next SIO panel to chain floor selection inputs for elevator control. This option allows the inputs from multiple SIO panels located anywhere on the same SCP and at any address to be used as a virtual single SIO panel with many floor selection inputs. This facilitates the control of up to 64 elevator floors even though a single SIO panel has a maximum of 16 inputs. The first SIO is selected in the readers screen and each of the next SIO panels with inputs to be used for floor selection is selected in this field.

This field is only used when one or more readers are defined as elevator with floor select readers. For more information on readers, see the [Readers](#) help file topic.

SIO for continuation of Outputs

Select the SIO panel that will be used as the next SIO panel to chain outputs for elevator control. This option allows the outputs from multiple SIO panels located anywhere on the same SCP and at any address to be used as a virtual single SIO panel with many floor control outputs. This facilitates the control of up to 64 elevator floors even though a single SIO panel has a maximum of 16 outputs. The first SIO is selected in the readers screen and each of the next SIO panels with outputs to be used for floor control is selected in this field.

This field is only used when one or more readers are defined as elevator readers. For more information on readers, see the [Readers](#) help file topic.

Event Type

SIO events (transactions) are recorded in the event file every time there is a communication, tamper or power change of state for the SIO. SIO events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Comm Fail*: Communication between the SCP and the SIO panel has been lost.
- *Comm Normal*: Communication between the SCP and the SIO panel has been restored.
- *Tamper Alarm*: The tamper device for the SIO panel is reporting that the panel has been tampered with.
- *Tamper Normal*: The tamper device for the SIO panel is reporting that it has been restored to a normal condition.
- *Power Loss*: The SIO panel is reporting that it has lost power.

- *Power Restored*: The SIO panel is reporting that power has been restored to a normal condition.

Annunciation Type

- *Disregard*: SIO events (transactions) for this event type will not be recorded in the event file and will not be displayed in either the events window or in the alarms window.
- *Log Only*: SIO events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display*: SIO events (transactions) for this event type will be recorded in the event file and displayed in the events window.
- *Alarm*: SIO events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic.

The alarm priority is only used for event types that have the annunciation type set to "Alarm".

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on alarms, see the [Alarms](#) help file topic.

The alarm message is only used for event types that have the annunciation type set to "Alarm".

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the

alarms window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic.

The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Message

Enter the event message for this event type. The event messages will be displayed in the events window each time this event type is generated. The event message is generally used to provide friendly text identification to the person monitoring events to identify the input point. This field can be up to 256 characters in length. For more information on events, see the [Events](#) help file topic.

Default Map when SIO in Alarm

Select the default map to be associated with this device. The default map will be displayed whenever the show map toolbar button is clicked from the alarms window while any pending alarm for this device is selected. The map must be defined in the maps screen prior to selecting a default map for a device. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Require Secure Condition Before Alarm Clear

Select (check) this option to require that an alarm be secured before it can be cleared from the alarms screen for this event type. This option is used to make sure that an alarm cannot be ignored by simply acknowledging and clearing it without any action being taken. For example, if a door has been forced open, if this option is checked, the door would have to be closed before the alarm could be cleared from the alarms window. For more information on alarms, see the [Alarms](#) help file topic.

The require secure condition before alarm clear option is only used for event types that have the annunciation type set to "Alarm".

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the SIO. Clicking on the close button will not save the changes made to the SIO.

[SIO's](#)

Readers

[Readers Detail](#)

Readers are used to define the model, type and operational parameters for the readers attached to each of the SIO panels in the system. If the main reader item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal desktop for each of the attached readers. The reader icon will also display the current alarm state for each of the readers.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Searching Readers

To search for a reader, type in the search box located in the upper right hand corner. Results will be dynamically displayed as search criteria is entered. To include a wildcard in the search use the asterisk (*) symbol.

Custom filtered views can be selected for the readers screen. When applied, readers will dynamically populate based on their changing states. Newly added devices will not appear in the filtered list until the grid is refreshed by clicking the green refresh icon. Filtered views include:

- *(No Filter)* - No filter will be applied to the readers grid.
- *Closed Doors* - Only doors in a closed state will display within the readers grid.
- *Opened Doors* - Only doors in an opened state will display within the readers grid.
- *Unsecured Doors* - Only doors in an unsecured state will display within the readers grid.
- *Unlocked Doors* - Only doors in an unlocked state will display within the readers grid.

Editing a Reader

To edit a reader, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the reader(s) to be edited. Next, expand the SIO's list and locate the SIO containing the output(s). All of the readers associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the reader to be edited and click on the edit button on the toolbar, or double click the reader to be edited. You can also select edit from the file option on the system menu or from the right click menu.

You can also view all of the enabled (installed) readers, sorted by name, by clicking on the installed readers item in the hardware tree. This view is the quickest and easiest way to interact with the readers in the system once the installation of the system hardware has been completed. Readers can be edited and commands can be sent to readers from this view as

well.

Printing Reader Reports

To print reports for a reader, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the reader(s) to be printed. Next, expand the SIO's list and locate the SIO containing the reader(s). All of the readers associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the readers to print reports for and click on the print button on the toolbar or select print from the file option on the system menu or from the right click menu. The following reports are available:

- *Access By Reader* - This report provides a list of cardholders and cards that have access to the selected readers. This report includes the timezone/floor code that corresponds to the selected readers.
- *Access Levels By Reader* - This report provides a list of all access levels that contain the selected readers. This report includes the timezone/floor code that corresponds to the selected reader.
- *Reader Access Denied Events* - This report provides a list of all access denied card usage events for the selected readers.
- *Reader Access Events* - This report provides a list of all access card usage events for the selected readers.
- *Reader Access Granted Events* - This report provides a list of all access granted card usage events for the selected readers.
- *Reader Activity* - This report provides a list of all reader activity for the selected readers.
- *Reader Antipassback Events* - This report provides a list of all antipassback events for the selected readers. The report includes both access grants and access denials.
- *Reader Audit History* - This report provides a list of all database updates and user issued commands for the selected readers.
- *Reader History* - This report provides a list of all database updates, user issued commands and reader activity for the selected readers.
- *Reader Listing* - This report provides a list of the selected readers and their various properties.
- *Reader Listing with Event Information* - This report provides a list of the selected readers and their various properties along with a listing of event information.

Reader Commands

To send commands to a reader, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the reader(s) to be edited. Next, expand the SIO's list and locate the SIO containing the reader(s). All of the readers associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the reader to send a command to and click on the reader commands drop down next to the refresh button on the toolbar. Select the command to be issued from the list and click on the command text button on the toolbar to send the command. You can also send a command by selecting commands from the file option on the system menu or from the right click menu and selecting the command to be sent.

The following reader commands are supported:

Temporary commands are only supported when the reader is installed under an EP series controller and will not work if using a legacy SCP controller.

Grant Access

The door will be unlocked for the amount of time specified in the standard unlock time field for this reader.

Disable Reader

The door will be locked and the reader will not grant access to any cards, even if they have a valid access level or facility code for this door. This mode is generally used when access to an area is not desired due to construction hazards, etc.

Unlock Reader/Door

The door will be unlocked.

Lock Reader/Door

The door will be locked. When locked no cards presented will be able to obtain access to the reader. Request to exit functionality will continue to function.

Set Mode to Facility Code Only

The door will be locked and any card with a valid facility code will be granted access to the door at any time. The card does not require a valid access level to be granted access in this mode.

Set Mode to Card Only

The door will be locked and only cards with valid facility codes and access levels will be granted access in this mode.

Set Mode to PIN Only

The door will be locked and any valid PIN number entered will be granted access in this mode.

Set Mode to Card And Pin

The door will be locked and only cards with valid facility codes and access levels will be granted access in this mode. A pin number entry that matches the card number's PIN number field will also be required at the reader's keypad. This option is supported for readers with keypads only.

Set Mode to Card Or PIN

The door will be locked and only cards with valid facility codes and access levels or valid PIN numbers will be granted access in this mode.

Enable 2 Card Mode

The door will be locked and will require two valid cards to be presented at this reader in order for access to be granted to the door.

Disable 2 Card Mode

The door will be locked and will require a single card to be presented at this reader in order for access to be granted to the door.

Enable Biometric Verify Mode

The door will be locked and biometric verification will be required in addition to either a valid card or PIN (depending on reader mode) for access to be granted to the door.

Disable Biometric Verify Mode

The door will be locked and biometric verification will not be required in addition to either a valid card or PIN (depending on reader mode) for access to be granted to the door.

Enable Cipher Mode

The door will be locked and the ability to enter a facility code and card number instead of presenting a card at this reader for access to be granted to the door will be enabled.

Disable Cipher Mode

The door will be locked and the ability to enter a facility code and card number instead of presenting a card at this reader for access to be granted to the door will be disabled.

Start Link Mode

Used by Schlage/Allegion locksets. Link Mode will place the gateway into link mode for the specified reader number. Once started, the lock itself needs to be manually linked to the gateway.

Abort Link Mode

Used by Schlage/Allegion locksets. Abort Link Mode will cancel the current active link mode.

Disable Forced Open

The door forced open event (transaction) WILL NOT be reported while the door forced open is disabled.

This differs greatly from setting the annunciation type in the reader properties events screen. Disabling the forced open event with this command will cause the SCP panel to NOT report the event at all. This means that not only will the forced open event not be reported, it will also not be logged as an event in the system event log.

Enable Forced Open

The door forced open event (transaction) WILL be reported while the door forced open is enabled.

Disable Held Open

The door held open event (transaction) WILL NOT be reported while the door held open is disabled.

This differs greatly from setting the annunciation type in the reader properties events screen. Disabling the held open event with this command will cause the SCP panel to NOT report the event at all. This means that not only will the held open event not be reported, it will also not be logged as an event in the system event log.

Enable Held Open

The door held open event (transaction) WILL be reported while the door held open is enabled.

Request Reader Status

The request reader status command is used to view current status information for the reader/door. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *Reader Name* - Displays the name for this reader.
- *Reader Mode* - Displays the current reader mode for this reader.
- *Reader Status* - Displays the current state of the tamper input for this reader.
- *Strike Status* - Displays the current state of the door strike output for this reader.
- *Door Status* - Displays the current state of the door contact input for this reader.
- *Request to Exit Status* - Displays the current state of the door request to exit input for this reader.
- *Forced Open Status* - Displays the current state of the door and whether or not door forced open is enabled or disabled for reporting.
- *Forced Open Reporting Status* - Displays the current reporting state for the door forced open status. If this is disabled no door forced open events will be processed or displayed for this reader.
- *Held Open Status* - Displays the current state of the door and whether or not door held open is enabled or disabled for reporting.
- *Held Open Reporting Status* - Displays the current reporting state for the door held open status. If this is disabled no door held open events will be processed or displayed for this reader.

Readers Detail

Readers

Readers are used to define the model, type and operational parameters for the readers attached to each of the SIO panels in the system. If the main reader item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal desktop for each of the attached readers. The reader icon will also display the current alarm state for each of the readers.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Reader Name

Enter the name to be used for this reader. All of the readers have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the readers being used. An example of a friendly name would be "Main Building - Front Door". The reader name can be up to 50 characters in length.

Attached to SIO

This field displays the name of the SIO panel to which this reader is attached. This field is displayed for informational purposes only and cannot be changed.

Reader Number

This field displays the physical location that this reader is attached to on the SIO panel. The reader number can be determined by the default name assigned to the reader. This field is displayed for informational purposes only and cannot be changed.

The available number of readers will be based on the model number of the SIO panel.

Device Installed

Select (check) this option if this reader has been physically installed in the system. If the device installed option is checked, the reader will be displayed in the installed readers branch of the hardware tree. If the device installed option is not checked, the reader will not be displayed in the installed readers branch of the hardware tree. This is useful for hiding extra readers that SIO panels support but that are not in use and makes viewing and sorting installed readers easier. Uninstalling this device has no impact to the functionality of the reader.

Access Configuration

Select the reader access configuration for this reader. The reader access configuration determines whether this reader will be used stand-alone at a door, or paired with another reader for in/out use at the same door. The following access configurations are supported:

- *Standard* - This reader will be used as a stand-alone (single reader per door) reader. This is the most common reader access configuration.
- *Paired (IN)* - This reader will be used as the IN reader with another paired OUT reader. The corresponding door strike output for this reader will be the one used for both this reader and the paired OUT reader.
- *Paired (OUT)* - This reader will be used as the OUT reader with another paired IN reader. The corresponding door strike output for this reader will be the one associated with this reader's paired IN reader, not the corresponding door strike output normally used for this reader.
- *Elevator* - This reader will be used as an elevator reader. Select the number of floors (outputs) to control, the floor code override (optional), the output SIO panel and the starting output number on the selected SIO panel. The output SIO panel and starting output number will determine the beginning output that gets activated for each of the floors defined within a floor code. The floor code override, if selected, will activate all of the outputs defined in the selected floor code when the timezone defined in the selected floor code becomes active or starts. This functionality is similar to unlocking a door during a timezone. Additional floors can be controlled by defining more SIO panels to chain to for additional outputs. For more information on SIO's, see the [SIO's](#) help file topic.
- *Elevator with Floor Select* - This reader will be used as an elevator reader with floor selection control. Select the number of floors (outputs) to control, the floor code override (optional), the output SIO panel, the starting output number on the selected SIO panel, the input SIO panel and the starting input number on the selected SIO panel. The output SIO panel and starting output number will determine the beginning output that gets activated for each of the floors defined within a floor code. The input SIO panel and starting input number will determine the beginning input used for floor selection control for each of the floors defined within a floor code. These inputs define the floor (output) that is being selected to activate the corresponding output. When the reader is in this mode, none of the outputs are activated until a floor selection is made at one of the floor selection inputs. The floor code override, if selected, will activate all of the outputs defined in the selected floor code when the timezone defined in the selected floor code becomes active or starts. This functionality is similar to unlocking a door during a timezone. Additional floors can be controlled by defining more SIO panels to chain to for additional outputs and inputs. For more information on SIO's, see the [SIO's](#) help file topic.
- *Enrollment Reader* - This reader will be used as a card holder enrollment reader. Card holder enrollment readers are used to automatically fill in the encoded card number and facility code when a new card is presented at an enrollment reader and look up and display existing cards when presented. Enrollment reader options are set using

options... from the tools option on the system menu. Check (select) any of the available enrollment readers for which options are to be defined. Next, select whether to display the cards screen or the card wizard when a new card is presented and whether to display the cards screen when an existing card is presented. **Only readers defined as enrollment readers will be displayed in the enrollment options dialog on the tools menu.**

- *Turnstile* - This reader will be used as a turnstile reader. Door pulse times and door contact configuration will be set to allow rapid entry through the door.

Reader Type

Select the reader type for this reader. The reader type is the type of reader (Wiegand, magstripe), as opposed to the model number, for this reader. Several standard reader types are included with the system. Custom reader types can also be added using the edit reader types button. This information will generally be provided by the reader manufacturer. For more information on reader types, see the [Reader Types](#) help file topic.

Default Reader Mode

Select the default reader mode for this door. The default reader mode sets the manner in which a reader will respond to a card being presented during normal system operations. The following default reader modes are supported:

- *Disabled* - The door will be locked and the reader will not grant access to any cards, even if they have a valid access level or facility code for this door. This mode is generally used when access to an area is not desired due to construction hazards, etc.
- *Unlocked* - The door will be unlocked.
- *Locked* - The door will be locked and no cards presented will be able to obtain access to the reader. Request to exit functionality will continue to function.
- *Facility Code Only* - The door will be locked and any card with a valid facility code will be granted access to the door at any time. The card does not require a valid access level to be granted access in this mode.
- *Card Only* - The door will be locked and only cards with valid facility codes and access levels will be granted access in this mode. This is the most commonly used default reader mode.
- *Pin Only* - The door will be locked and any valid PIN number entered will be granted access in this mode. No card needs to be presented in order to gain access when the reader is in this mode. NOTE: The enforce unique PIN number option must be set in the configuration utility in order to ensure that no duplicate PIN numbers exist in the system in order for this mode to function properly. This option is supported for readers with keypads only.
- *Card And PIN* - The door will be locked and only cards with valid facility codes and access levels will be granted access in this mode. A pin number entry that matches the card number's PIN number field will also be required at the reader's keypad. This option

is supported for readers with keypads only.

- *Card or PIN* - The door will be locked and only cards with valid facility codes and access levels or valid PIN numbers will be granted access in this mode. NOTE: The enforce unique PIN number option must be set in the Server configuration in order to ensure that no duplicate PIN numbers exist in the system in order for this mode to function properly. This option is supported for readers with keypads only.

The default reader mode will take effect whenever a change is made to any reader's settings, or when the SCP panel has been reset or lost power. Any reader commands sent to a door will only result in a temporary reader mode change. For more information about reader commands, see the [Reader Commands](#) help file topic.

Off-line Reader Mode

Select the off-line reader mode for this door. The off-line reader mode sets the manner in which a reader will respond to a card being presented when "downstream" communications have been lost between the SCP panel and the SIO panel to which this reader is attached. The following off-line reader modes are supported:

- *Disabled* - The door will be locked and the reader will not grant access to any cards, even if they have a valid access level or facility code for this door.
- *Unlocked* - The door will be unlocked.
- *Facility Code Only* - The door will be locked and any card with a valid facility code will be granted access to the door at any time. The card does not require a valid access level to be granted access in this mode. This is the most commonly used off-line reader mode.

Time and Attendance Mode

Select the time and attendance mode for this door. The time and attendance mode sets up a reader as either an entrance or exit reader for time and attendance reporting purposes. The following time and attendance modes are available:

- *None* - The door will not be enabled for time and attendance reporting.
- *Entrance Reader* - The door will be used as an entrance reader to "clock in" cardholders when granted access at the door.
- *Exit Reader* - The door will be used as an exit reader to "clock out" cardholders when granted access at the door.

Require 2 Cards at this Reader

Select (check) this option to enable the require two cards at this reader option. This option will require two valid cards to be presented at this reader in order for access to be granted to the door. This option is generally used when it is desirable to have more than one person in an area at a time.

Do NOT Pulse Door Strike on Request To Exit

Select (check) this option to enable the do not pulse door strike on request to exit option for this reader. If this option is selected (checked), the door strike will not be activated when a request to exit device has been activated. If this option is not selected (unchecked), the door strike will be activated when a request to exit device has been activated.

Decrement Use Limit/Require Non Zero Use Limit

Select (check) this option to enable use limits for this reader. Use limits will limit the number of times that a card can be used at this reader. Each time a card is granted access at this reader the number of uses remaining for that card will be decremented by one. Cards that have a use limit of zero or have no uses remaining will always be denied access at this reader regardless of their assigned access levels.

Use limits are specific to each of the SCP panels in the system. If a card has a use limit of 20 and has access to readers set up to for use limits that are attached to two different SCP's, the card will have 20 uses at each of the SCP's. In addition, if an SCP panel is reset, the use limit will be reset to the value entered in this field. The use limits option must be enabled for the site in order for this option to work. For more information on configuring use limits, see the [Sites](#) help file topic.

Enable Cipher Mode

Select (check) this option to enable cipher mode for this reader. Cipher mode provides the ability to enter a facility code and card number in to this readers keypad instead of presenting a card for access requests. The facility code and card number must be preceded by a "*" and followed by a "#" e.g. *536467#. This option is useful when a card holder has lost his card or the card is temporarily unavailable.

This option is supported for readers with keypads only. A Magnetic Stripe card format must be defined that matches the card and facility code data being entered.

Log all Access Granted events as Door Used

Select (check) this option to log all access granted events as door used. When checked, this option will assume that the door attached to this reader has been cycled regardless of whether or not the door was actually opened and then closed. When unchecked, an access granted event will be generated when a valid card is presented at this reader but no door activity will be assumed unless the door is actually opened or closed. This option is useful in anti-passback situations when a cardholder presents a valid card but does not go through the door. If this option is checked the cardholder's area would be changed to the new area regardless of whether or not the cardholder actually went through the door.

Deny Access on Duress Entry

Select (check) this option to deny access during a duress entry. When checked, this option will not grant access to this reader when a duress entry is attempted. A duress event will still be generated but access will be denied.

Filter False Door Forced Open Events

Select (check) this option to ignore any door forced open events that occur within three seconds after the door closes on a valid access.

Require PIN Number after Card in Card + PIN Mode

Select (check) this option to require that the PIN code be entered after the card is presented. This option only applies when the reader is in Card + PIN mode.

Enable Double-Card Event

Select (check) this option to allow for double presentations of card swipes to be able to used in extended features as well as task execute conditions.

Scheduled Reader Mode Changes

Select the timezone, starting and ending reader modes for this reader. The reader mode will change to the selected mode when the timezone starts at the start time of the selected timezone and change to the selected mode when the timezone ends at the end time of the selected timezone, during any of the days specified in any of the intervals within the selected timezone. This option is most commonly used to unlock a door during a specified timezone.

First Card Unlock

Select the timezone, and card group for the first card unlock mode. A first card unlock will unlock the door upon the first valid card presented during the specified timezone. In order to relock the door, the schedule reader mode change mode must be used with the relock timezone and Mode when timezone starts set to (No Mode Change) and Mode when timezone ends set to the preferred reader mode.

Door Contact Configuration

Select the door contact configuration for this door. This option will depend upon the type of hardware being installed for the door contact input. The following options are supported:

- *Normally Closed* - This option should be used when the door contact is wired in a normally closed configuration.
- *Normally Open* - This option should be used when the door contact is wired in a

normally open configuration.

- *Normally Closed Supervised* - This option should be used when the door contact is wired in a normally closed configuration and uses a 2K resistor network for contact state supervision.
- *Normally Open Supervised* - This option should be used when the door contact is wired in a normally open configuration and uses a 2K resistor network for contact state supervision.

Custom defined supervision can be defined in the SCPs screen.

Door Contact Response

Select the door contact response for this door. This option will depend upon the physical location characteristics of the door contact. The following options are supported:

- *Fast* - This option should be selected for a door that has absolutely no bounce upon closure.
- *Normal* - This option should be selected for a door that has very minimal to no bounce upon closure. This is the default and recommended setting for a typical door.
- *Slow* - This option should be selected for a door which may experience bounce/vibration upon closure.
- *Very Slow* - This option should be selected for a door which regularly experiences bounce/vibration upon closure to accommodate slow-responding door hardware and avoid false door forced open alarms/events.

Door Contact SIO

Specify the SIO and input number containing the door contact input. This is used when using a reader board that does not have any on-board inputs.

Request To Exit Configuration

Select the request to exit (egress) configuration for this door. This option will depend upon the type of hardware being installed for the request to exit input. The following options are supported:

- *Normally Closed* - This option should be used when the request to exit is wired in a normally closed configuration.
- *Normally Open* - This option should be used when the request to exit is wired in a normally open configuration.
- *Normally Closed Supervised* - This option should be used when the request to exit is wired in a normally closed configuration and uses a 2K resistor network for request to exit state supervision.
- *Normally Open Supervised* - This option should be used when the request to exit is

wired in a normally open configuration and uses a 2K resistor network for request to exit state supervision.

Custom defined supervision can be defined in the SCPs screen.

Request to Exit SIO

Specify the SIO and input number containing the request to exit input. This is used when using a reader board that does not have any on-board inputs.

Relock Mode

Select the door strike relock mode for this door. The following options are supported:

- *When Door Opens* - The door strike will be re-locked as soon as the door has opened or after the unlock time passes, whichever occurs first.
- *When Door Closes* - The door strike will be re-locked as soon as the door has closed or after the unlock time passes, whichever occurs first.

Strike Drive Mode

Select the strike drive mode for this door. This option will depend upon the type of hardware being installed for the door strike output. The following options are supported:

- *De-energized when Locked* - This option should be used when the door strike is wired in a normally open configuration.
- *Energized when Locked* - This option should be used when the door strike is wired in a normally closed configuration.

Strike SIO

Specify the SIO and output number containing the door relay. This is used when using a reader board that does not have any on-board outputs.

Standard Door Times

Select or enter the unlock time and the allowed open time fields for this door. The unlock time is the amount of time that the door will remain unlocked after a valid card has been presented, or an access granted command has been issued. The open time is the amount of time that the door can be open after a valid card has been presented, or an access granted command has been issued. Both of these times can range from 1 to 99 seconds.

Extended Door Times

Select or enter the extended unlock time and the extended allowed open time fields for this

door. The extended unlock time is the extended amount of time that the door will remain unlocked after a valid card has been presented. This time will be added on to the standard unlock time for all cards that have the extended access times option checked. The extended open time is the extended amount of time that the door can be open after a valid card has been presented. This time will be added on to the standard open time for all cards that have the extended access times option checked. Both of these times can range from 1 to 999 seconds.

Pre-Alarm Time

Select or enter the pre-alarm time for this door. The pre-alarm time is the amount of time before the door open time expires, that a pre-alarm door event (transaction) will be reported. This is generally used to activate a sounder or other device to warn the card holder to close the door before a door held open event is reported. If the door open time was set to thirty seconds and the door pre-alarm time was set to five seconds, the pre-alarm event would occur at twenty-five seconds. The pre-alarm time can range from 0 to 99 seconds.

Strike Follow (This functionality is available on EP-series boards only.)

These options will pulse an output following the door strike. The output that will be pulsed is an internal function of the board type as follows:

EP-1501, Door 1 will be followed by Auxiliary Output 2;

EP-1502, Door 1 will be followed by Auxiliary Output 2, Door 2 will be followed by Auxiliary Output 4;

MR-50, Door 1 will be followed by Auxiliary Output 2;

MR-51e, Door 1 will be followed by Auxiliary Output 2;

MR-52, Door 1 will be followed by Auxiliary Output 2, Door 2 will be followed by Auxiliary Output 4

Select the duration for the pulsing of the output to follow the door strike for the reader. If a delay prior to the pulsing of the output is required, select the appropriate amount of time for the delay.

- *Duration* - Use the dropdown list to select the amount of time for the output to be activated.
- *Delay* - Use the dropdown list to select the amount of time to delay prior to activating the selected output.

This functionality is available on EP-series boards only.

Anti-passback Mode

Select the anti-passback mode for this reader. The anti-passback mode will determine whether or not this reader will operate as an anti-passback reader and the how it will handle

anti-passback functions. Anti-passback is used to prevent the "passing back" of a card from card holder to card holder when entering or leaving a designated area. If the card is used more than once, the card holder may or may not be granted access to the area and an anti-passback event (transaction) will be generated. The following options are supported:

- *None* - This reader will not function as an anti-passback reader.
- *Soft* - Anti-passback will be enabled for this reader in soft mode. Soft mode anti-passback will generate an anti-passback violation event (transaction) when an anti-passback violation occurs but will still grant the card holder access to the area. Select the area that this reader is located in and the area to which this reader will be granting access. Areas can be defined using the edit areas button. Enter the area name for each of the areas being defined.
- *Hard* - Anti-passback will be enabled for this reader in hard mode. Hard mode anti-passback will generate an anti-passback violation event (transaction) when an anti-passback violation occurs and will deny the card holder access to the area. Select the area that this reader is located in and the area to which this reader will be granting access.
- *Timed By Reader* - Anti-passback will be enabled for this reader in timed reader mode. Timed reader mode anti-passback will generate an anti-passback violation event (transaction) when an anti-passback violation occurs and will deny the card holder access to this reader for the amount of time specified in the anti-passback delay field. Select the area that this reader is located in and the area to which this reader will be granting access.
- *Timed By User no location change* - Anti-passback will be enabled for this reader in timed user mode. Timed user mode anti-passback will generate an anti-passback violation event (transaction) when an anti-passback violation occurs and will deny the card holder access to the entire area for the amount of time specified in the anti-passback delay field. Select the area that this reader is located in and the area to which this reader will be granting access. When this anti-passback mode is used, the users location (area) WILL NOT be changed to the area that the reader is granting access to.
- *Timed By User location change* - Anti-passback will be enabled for this reader in timed user mode. Timed user mode anti-passback will generate an anti-passback violation event (transaction) when an anti-passback violation occurs and will deny the card holder access to the entire area for the amount of time specified in the anti-passback delay field. Select the area that this reader is located in and the area to which this reader will be granting access. When this anti-passback mode is used, the users location (area) WILL be changed to the area that the reader is granting access to.

Anti-passback functionality must be enabled in for the site for any of the anti-passback modes to work. For more information on configuring anti-passback, see the [Sites help file topic](#).

Event Type

Reader events (transactions) are recorded in the event file every time there is a card presented at the reader. Reader events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Device Online* - The on-board reader is online
- *Device Offline* - The on-board reader port is offline
- *Access Granted* - A card has been presented at the reader and access has been granted to the door.
- *Access Granted Anti-passback Violation* - A card has been presented at the reader and has produced an anti-passback violation. Access has been granted to the door due to the fact that the reader is operating in soft anti-passback mode.
- *Access Granted Under Duress* - A card has been presented at the reader and access has been granted because a special PIN entry has been made to indicate a duress entry. A duress entry occurs when a card holder enters their PIN number and adds one to the number. For example, if a card has a PIN number of 1111 in the card file and the PIN number is entered as 1112 when the card is presented at a card plus PIN reader, this will produce a duress event.
- *Access Granted Door Not Used* - A card has been presented at the reader and access has been granted but the door was not used (no door contact cycle).
- *Access Granted APB Violation Door Not Used* - A card has been presented at the reader and has produced an anti-passback violation. Access has been granted to the door due to the fact that the reader is operating in soft anti-passback mode. The door was not used (no door contact cycle).
- *Access Granted Under Duress Door Not Used* - A card has been presented at the reader and access has been granted because a special PIN entry has been made to indicate a duress entry. A duress entry occurs when a card holder enters their PIN number and adds one to the number. For example, if a card has a PIN number of 1111 in the card file and the PIN number is entered as 1112 when the card is presented at a card plus PIN reader, this will produce a duress event. The door was not used (no door contact cycle).
- *Access Granted Door Unlocked* - A valid card has been presented while the reader is in the unlocked state.
- *Double Card Event* - A valid card has been presented twice while the enable double card event option is enabled.
- *Double Card Event (door locked/unlocked)* - A valid card has been presented twice while the enable double card event option is enabled and the door is unlocked or locked.
- *Access Denied No Access* - A card has been presented at the reader and access has been denied because the card presented is not allowed access to this door at any time. This is determined by the access levels assigned to the card in the cards data file.
- *Access Denied Invalid Facility Code* - A card has been presented at the reader and

access has been denied because the facility code on the card presented is not one of the correct facility codes for the system.

- *Access Denied Unknown Card* - A card has been presented at the reader and access has been denied because the card presented is not in the cards data file.
- *Access Denied Card Inactive* - A card has been presented at the reader and access has been denied because the card presented is inactive in the cards data file.
- *Access Denied Card Not Yet Active* - A card has been presented at the reader and access has been denied because the card presented is using date based activation and has not reached the active date specified in the cards data file.
- *Access Denied Card Expired* - A card has been presented at the reader and access has been denied because the card presented is using date based activation and has passed the expiration date specified in the cards data file.
- *Access Denied Wrong Time* - A card has been presented at the reader and access has been denied because the card presented is not allowed access to this door at this time. This is determined by the access levels assigned to the card in the cards data file.
- *Access Denied Wrong PIN Number* - A card has been presented at the reader and access has been denied because the PIN number entered for the card presented does not match the PIN number assigned to the card in the cards data file.
- *Access Denied Anti-passback Violation* - A valid card has been presented at the reader and has produced an anti-passback violation. Access has been denied due to the fact that the reader is operating in hard or timed anti-passback mode.
- *Access Denied Under Duress* - A card has been presented at the reader and access has been denied because a special PIN entry has been made to indicate a duress entry. A duress entry occurs when a card holder enters their PIN number and adds one to the number. For example, if a card has a PIN number of 1111 in the card file and the PIN number is entered as 1112 when the card is presented at a card plus PIN reader, this will produce a duress event.
- *Access Denied No 2nd Card Presented* - A single card has been presented at the reader and access has been denied because the reader is set up to require two cards for valid access.
- *Access Denied Area Full* - A card has been presented at the reader and access has been denied because the area that the reader is granting access to has reached the maximum occupancy count.
- *Access Denied Area Disabled* - A card has been presented at the reader and access has been denied because the area that the reader is granting access to has been disabled.
- *Access Denied Invalid Issue Level* - A card has been presented at the reader and access has been denied because the issue level of the card presented does not match the card's issue level in the cards data file.
- *Access Denied Use Limit Exceeded* - A card has been presented at the reader and access has been denied because the card has exceeded the number of allowed uses specified in the cards data file.
- *Access Denied Biometric Verify Error* - A card has been presented and a biometric

verification has been attempted and access has been denied because the biometric data presented does not match the biometric template in the cards data file.

- *Access Denied No Biometric Record* - A card has been presented and a biometric verification has been attempted and access has been denied because there is no biometric template in the cards data file.
- *Access Denied No Biometric Device* - A card has been presented and a biometric verification has been attempted and access has been denied because the biometric device is missing or malfunctioning.
- *Access Denied - No Escort Card Presented* - A card requiring an escort has been presented and the escort did not swipe their card prior.
- *Access Denied - Door Locked* - A card has been presented at the reader and access has been denied to the door because the door mode has been overridden to the Locked mode.
- *Access Denied - Floor Not Served* - Advanced Elevator event - A card has been presented at the elevator and access to a non-existing floor was requested.
- *Access Denied - Floor Not Authorized* - Advanced Elevator event - A card has been presented at the elevator and access to a floor a user has no access to was requested.
- *Access Denied - Elevator Timeout* - Advanced Elevator event - A card has been presented at the reader and access was requested to the elevator but there was no response
- *Access Denied - Elevator Unknown Error* - Advanced Elevator event - A card has been presented at the reader and access has been denied for an unknown reason.
- *Access Denied - Mantrap Busy* - A card has been presented at the reader configured to transition to an area configured as a mantrap/airlock and the area has an opening transitioning to another area.
- *Access Denied - Authentication Timeout* - Axillary Authentication event - The SCP timed out while externally authenticating the credential.
- *Access Denied - Authentication Failure* - Axillary Authentication event - The SCP verified the credential but the authentication request failed.
- *Door Open* - The door has been opened.
- *Door Forced Open* - The door has been forced open without either a valid card being presented or an access granted command being sent to the reader.
- *Door Held Open* - The door has been open longer than the allowed open time setting for this reader.
- *Door Closed* - The door has been closed.
- *Door Supervisory Fault* - The door contact input has reported a fault. This can be either a short or an open circuit when a 2K resistor network is installed.
- *Request to Exit* - A request to exit has been initiated for this reader by the associated request to exit device.
- *Request to Exit Host Initiated* - A request to exit command has been sent to the reader by the host computer.
- *User Command Executed* - A user command has been entered and executed at the reader.

- *User Command Not Allowed at Reader* - A user command has been entered and not allowed at the reader where it was entered.
- *User Command Not Authorized for User* - A user command has been entered and not allowed at the reader for the user that entered the command.
- *Invalid User Command Parameter* - An invalid user command has been entered at the reader for the user that entered the command.
- *Interior Push Button Activated* - The defined interior push button has changed state to unsecure.
- *Interior Push Button Deactivated* - The defined interior push button has changed state to secure.
- *Interior Push Button Fault* - The defined interior push button is in a fault state.
- *Deadbolt Activated* - Schlage AD lockset event - The deadbolt was thrown.
- *Deadbolt Deactivated* - Schlage AD lockset event - The deadbolt was retracted.
- *Request To Enter Activated* - Schlage AD lockset event - A request to exit has been initiated for this reader.
- *Request To Enter Deactivated* - Schlage AD lockset event - A request to exit has been initiated for this reader.
- *Motor Stall Activated* - Schlage AD lockset event - The lockset motor has stalled.
- *Motor Stall Deactivated* - Schlage AD lockset event - The lockset motor has recovered from a stalled condition.
- *Lock Clutch Activated* - Schlage AD lockset event - The lockset clutch has engaged.
- *Lock Clutch Deactivated* - Schlage AD lockset event - The lockset clutch has disengaged.
- *Low Battery Activated* - Schlage AD lockset event - The lockset power has reached a low battery level.
- *Low Battery Deactivated* - Schlage AD lockset event - The lockset power has recovered from a low battery level.
- *Critical Battery Activated* - Schlage AD lockset event - The lockset power has reached a critical battery level.
- *Critical Battery Deactivated* - Schlage AD lockset event - The lockset power has recovered from a critical battery level.
- *Bezel Tamper Activated* - Schlage AD lockset event - The lockset bezel tamper has engaged.
- *Bezel Tamper Deactivated* - Schlage AD lockset event - The lockset bezel tamper has disengaged.
- *Keyswitch Activated* - Schlage AD lockset event - A physical hard key was entered into the lockset.
- *Keyswitch Deactivated* - Schlage AD lockset event - A physical hard key was removed from the lockset.
- *RF Loss Activated* - Schlage AD lockset event - The lockset lost communication to the PIM unit.
- *RF Loss Deactivated* - Schlage AD lockset event - The lockset restored communication

to the PIM unit

- *Lock Not Paired Activated* - Schlage AD lockset event - The lockset is not paired to a PIM unit
- *Lock Not Paired Deactivated* - Schlage AD lockset event - The lockset became paired to a PIM unit.
- *Elevator DEC Online* - Advanced Elevator event - The associated Advanced Elevator destination elevator computer is online.
- *Elevator DEC Offline* - Advanced Elevator event - The associated Advanced Elevator destination elevator computer is offline.

Annunciation Type

- *Disregard* - Reader events (transactions) for this event type will not be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log Only* - Reader events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display* - Reader events (transactions) for this event type will be recorded in the event file and displayed in the events window.
- *Alarm* - Reader events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic.

The alarm priority is only used for event types that have the annunciation type set to "Alarm".

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on

alarms, see the [Alarms](#) help file topic.

The alarm message is only used for event types that have the annunciation type set to "Alarm".

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the alarms window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic.

The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Message

Enter the event message for this event type. The event messages will be displayed in the events window each time this event type is generated. The event message is generally used to provide friendly text identification to the person monitoring events to identify the input point. This field can be up to 256 characters in length. For more information on events, see the [Events](#) help file topic.

Default Map when Reader in Alarm

Select the default map to be associated with this device. The default map will be displayed whenever the show map toolbar button is clicked from the alarms window while any pending alarm for this device is selected. The map must be defined in the maps screen prior to selecting a default map for a device. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Automatically Show Map

Select (check) this option to have the map specified as the default map automatically displayed in the alarms window when an alarm for this device is acknowledged. If no default map is specified then selecting this option will have no effect. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Require Secure Condition Before Alarm Clear

Select (check) this option to require that an alarm be secured before it can be cleared from the alarms screen for this event type. This option is used to make sure that an alarm cannot be ignored by simply acknowledging and clearing it without any action being taken. For example, if a door has been forced open, if this option is checked, the door would have to be closed before the alarm could be cleared from the alarms window. For more information on alarms, see the [Alarms](#) help file topic.

The require secure condition before alarm clear option is only used for event types that have the annunciation type set to "Alarm".

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information etc. There is no limit as to how long a notes field can be.

Associated Intercom Station

Select the intercom station to be associated with this device. The associated intercom station will be automatically connected when an alarm for this device is acknowledged in the alarms window. Automatic connection will also occur when this device is selected on a map or when any of the other associated devices are selected. The intercom must be defined in the hardware screen prior to selecting an associated intercom for a device. In addition, each of the workstations that will be using the intercom integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

Intercom integration licenses must be purchased separately for each workstation.

Associated Camera

Select the CCTV or DVR camera to be associated with this device. The associated CCTV camera will be automatically selected when an alarm for this device is acknowledged in the alarms window. Automatic selection will also occur when the CCTV device is selected on a map or when any of the other associated devices are selected. The CCTV or DVR camera

must be defined in the hardware screen prior to selecting an associated CCTV or DVR camera for a device. In addition, each of the workstations that will be using the CCTV or DVR integration must have that option setup for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

CCTV and DVR integration licenses must be purchased separately for each workstation.

Camera Preset Number

Enter the preset number for the associated CCTV camera for this device. The associated CCTV camera will be automatically selected and stationed at the preset number entered when an alarm for this device is acknowledged in the alarms window. Automatic preset selection will also occur when this device is selected on a map or when any of the other associated devices are selected. If no associated CCTV camera is specified then this entry will have no effect. The CCTV camera must be defined in the hardware screen prior to selecting an associated CCTV camera for a device. In addition, each of the workstations that will be using the CCTV integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

CCTV integration licenses must be purchased separately for each workstation.

Associated DVR Cameras

Displays any DVR cameras that have been associated with this reader.

Associated Biometric Reader

Select the biometric gateway and reader number on the gateway to be associated with this reader. When a card is presented at the primary reader and the require biometric verification option is checked, biometric verification will be required in order for access to be granted.

Biometric licenses must be purchased separately and a biometric reader type must be specified for the site. For more information on biometric configuration, see the [Sites](#) help file topic.

Floor Descriptions

Edit the floor descriptions for this reader. The floor descriptions will be displayed in the floor codes screen during floor code setup. The floor description makes it easier to identify which floors are physically connected to what outputs on the elevator controller SIO panel. This tab is only available when the reader access configuration is set to elevator or elevator with floor select.

Keypad Commands

Edit the keypad commands for this reader. Up to eight keypad commands can be defined for each of the readers attached to the SCP panel. Click on the edit button and enter the task information to be associated with the keypad sequence. Keypad commands can be executed by pressing the <--- (*) key followed by the command number and then the command (#) key. If the reader is valid and the user is authorized the associated task will be executed. The SCP panel that the reader is attached to must be set up for the correct user command type and the reader and card group must be valid. For more information on user command options, see the [SCP's](#) help file topic. For more information on setting up tasks, see the [Tasks](#) help file topic.

Timezone

Select the timezone to be used for all of the selected access levels being assigned to the reader. Only one timezone can be selected at a time, so when access levels are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned access level it must be moved back to the available window, then re-assigned with the new timezone.

Available/Assigned Access Levels/Timezones

To assign access levels to a reader, select the timezone and the desired access level(s), then "move" the access levels that you wish to be assigned to the reader from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected access levels from the available window to the assigned window. The "<<" button will move all selected access levels from the assigned window to the available window. Multiple access levels can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired access levels.

Default Alarm Zone

Select the alarm zone to be associated with this reader. Once a reader has been associated with an alarm zone the reader will control all points within that alarm zone for alarm processing functions.

Access Delay

Select or enter the access delay for the associated alarm zone. The access delay will specify the amount of time allowed between a valid credential being presented at the reader and a command code being entered for alarm processing functions.

Authorization Groups

Select the permissions to be assigned to the reader for the available authorization groups. Only the selected functions will be available at the reader for the three authorization groups.

Display

Select the display parameters for the reader. Only the selected information will be displayed at the MR-DT or OSDP LCD keypad display during alarm processing or normal operation.

Extended Feature

Extended Features allow for quick setup of common reader scenarios. In order to use Extended Features, an EP controller with 1.18.x firmware or higher is required. In all Extended features throwing the deadbolt (Schlage Ad Series) will lock the door and override any extended feature in use.

- Classroom - The reader is normally secure and the inside lever/REX always allow for free egress. Allows for a double swipe of any valid card to toggle the reader between Unlocked/Locked. In order to use this feature, the Enable Double-Card Event option within the Reader Settings tab must be selected (checked)
- Office - The reader is normally secure and the inside lever/REX always allow for free egress. Allows for a double swipe of any valid card, or pressing the specified Interior Push Button SIO/Input to toggle the reader between Unlocked/Locked. In order to use this feature, the Enable Double-Card Event option within the Reader Settings tab must be selected (checked).
- Privacy - The reader is normally secure and the inside lever/REX always allow for free egress. Pressing the specified Interior Push Button SIO/Input will lock the door. Opening the door, or pressing the specified Interior Push Button SIO/Input again will deactivate the privacy feature.
- Apartment - The reader is normally secure and the inside lever/REX always allow for free egress. Allows for a single swipe of any valid card to toggle the reader between Unlocked/Locked. Pressing the specified Interior Push Button SIO/Input will relock the door.
- Classroom - Schlage - This functionality only applies to Schlage AD series locksets. The reader is normally secure and the inside lever/REX always allow for free egress. Allows for a double swipe of any valid card to toggle the reader between Unlocked/Locked. In order to use this feature, the Enable Double-Card Event option within the Reader Settings tab must be selected (checked)
- Office - Schlage - This functionality only applies to Schlage AD series locksets. The reader is normally secure and the inside lever/REX always allow for free egress. Allows

for a double swipe of any valid card, or pressing the Interior Push Button to toggle the reader between Unlocked/Locked. In order to use this feature, the Enable Double-Card Event option within the Reader Settings tab must be selected (checked).

- Privacy - Schlage - This functionality only applies to Schlage AD series locksets. The reader is normally secure and the inside lever/REX always allow for free egress. Pressing the Interior Push Button will lock the door. Opening the door, or pressing the the Interior Push Button again will deactivate the privacy feature.
- Apartment - Schlage - This functionality only applies to Schlage AD series locksets. Schlage. The reader is normally secure and the inside lever/REX always allow for free egress. Allows for a single swipe of any valid card to toggle the reader between Unlocked/Locked. Pressing the Interior Push Button will relock the door.

Save/Close Buttons

Clicking on the save button will save the changes made to the reader. Clicking on the close button will not save the changes made to the reader.

[Readers](#)

Inputs

[Inputs Detail](#)

Inputs are used to define the type and operational parameters for the inputs attached to each of the SIO panels in the system. If the main input item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the attached inputs. The input icon will also display the current alarm state for each of the inputs.

Only inputs which are available for general use are displayed. Some of the inputs on the SIO panels are preprogrammed for the door contact, request to exit button, etc. These inputs will not be displayed as they cannot be used for any other purpose. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users help file topic](#).

Searching Inputs

To search for an input, type in the search box located in the upper right hand corner. Results will be dynamically displayed as search criteria is entered. To include a wildcard in the search use the asterisk (*) symbol.

Custom filtered views can be selected for the inputs screen. When applied, inputs will dynamically populate based on their changing states. Newly added devices will not appear in the filtered list until the grid is refreshed by clicking the green refresh icon. Filtered views include:

- *(No Filter)* - No filter will be applied to the inputs grid.
- *Secured Inputs* - Only inputs in a secured state will display within the inputs grid.
- *Unsecured Inputs* - Only inputs in an unsecured state will display within the inputs grid.

Editing an Input

To edit an input, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the input(s) to be edited. Next, expand the SIO's list and locate the SIO containing the input(s). All of the inputs associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the input to be edited and click on the edit button on the toolbar, or double click the input to be edited. You can also select edit from the right click menu.

You can also view all of the enabled (installed) inputs, sorted by name, by clicking on the installed inputs item within the hardware section of the Navigation Pane. This view is the quickest and easiest way to interact with the inputs in the system once the installation of the system hardware has been completed. Inputs can be edited and commands can be sent to

inputs from this view as well.

Printing Input Reports

To print reports for an input, go to the hardware tree by either clicking on the hardware toolbar button within the main group on the toolbar, or by selecting hardware from the go option on the system menu. Then, expand the SCP panel that contains the SIO with the attached input by clicking on the plus sign next to the desired SCP. Next, expand the SIO panel that contains the input to print reports for by clicking on the plus sign next to the desired SIO. Next, click on the inputs item within the SIO. All of the inputs associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the input to print reports for and click on the print button on the toolbar. You can also select print from the file option on the system menu or from the right click menu. The following reports are available:

- *Input Activity* - This report provides a list of all input activity for the selected inputs.
- *Input Audit History* - This report provides a list of all database updates and user issued commands for the selected inputs.
- *Input History* - This report provides a list of all database updates, user issued commands and input activity for the selected inputs.
- *Input Listing* - This report provides a list of the selected inputs and their various properties.

Input Commands

To send commands to an input, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the input(s) to be edited. Next, expand the SIO's list and locate the SIO containing the input(s). All of the inputs associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the input to send a command to and click on the input commands drop down next to the refresh button on the toolbar. Select the command to be issued from the list and click on the command text button on the toolbar to send the command. You can also send a command by selecting commands from the file option on the system menu or from the right click menu and selecting the command to be sent.

The following input commands are supported:

Temporary commands are only supported when the input is installed under an EP series controller and will not work if using a legacy SCP controller.

Enable Input

The input will be enabled and reporting of events (transactions) will occur from the device attached to the input.

Disable Input

The input will be disabled and no reporting of events (transactions) will occur from the device attached to the input.

Request Input Status

The request input status command is used to view current status information for the input. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *Input Name* - Displays the name of the input.
- *Input State* - Displays whether the input is in an alarm (unsecured) or secured state.
- *Input Reporting Status* - Displays the current reporting state for the input. If this is disabled no input events will be processed or displayed for this input.

Inputs Detail

Inputs

Inputs are used to define the type and operational parameters for the inputs attached to each of the SIO panels in the system. If the main input item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the attached inputs. The input icon will also display the current alarm state for each of the inputs.

Only inputs which are available for general use are displayed. Some of the inputs on the SIO panels are preprogrammed for the door contact, request to exit button, etc. These inputs will not be displayed as they cannot be used for any other purpose. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Input Name

Enter the name to be used for this input. All of the inputs have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the inputs being used. An example of a friendly name would be "Main Building - Lobby Smoke Detector". The input name can be up to 50 characters in length.

Attached to SIO

This field displays the name of the SIO panel on which this input is located. This field is displayed for informational purposes only and cannot be changed.

Input Number

This field displays the physical location that this input is located on the SIO panel. The input number can be determined by the default name assigned to the input. This field is displayed for informational purposes only and cannot be changed.

The available number of inputs will be based on the model number of the SIO panel.

Device Installed

Select (check) this option if this input has been physically installed in the system. If the device installed option is checked, the input will be displayed in the installed inputs branch of the hardware tree. If the device installed option is not checked, the input will not be displayed in the installed inputs branch of the hardware tree. This is useful for hiding extra inputs that SIO panels support but that are not in use and makes viewing and sorting installed inputs easier. Uninstalling this device has no impact to the functionality of the input.

Input Configuration

Select the input configuration for this input. This option will depend upon the type of hardware being installed for use with the input. The following options are supported:

- *Normally Closed* - This option should be used when the device attached to this input operates in a normally closed configuration.
- *Normally Open* - This option should be used when the device attached to this input operates in a normally open configuration.
- *Normally Closed Supervised* - This option should be used when the device attached to this input operates in a normally closed configuration and uses a 2K resistor network for input state supervision.
- *Normally Open Supervised* - This option should be used when the device attached to this input operates in a normally open configuration and uses a 2K resistor network for input state supervision.

Custom defined supervision can be defined in the SCPs screen.

Response

Select the response time for this input. The response time is the amount of time in between the opening and closing of the device attached to this input. The following response times are supported:

- *Fast* - This option should be used when a device with a fast open/closed cycle is attached to this input. This option will set the input sensitivity to high.
- *Normal* - This option should be used when a device with a normal open/closed cycle is attached to this input. This option will set the input sensitivity to medium. This is the most commonly used setting.
- *Slow* - This option should be used when a device with a slow open/closed cycle is attached to this input. This option will set the input sensitivity to low.

Disable Input During Timezone

Select the timezone that this input should be disabled during. The input will be disabled at the start time of the selected timezone and re-enabled at the end time of the selected timezone, during any of the days specified in any of the intervals within the selected timezone. When the input is disabled, no reporting of events (transactions) will occur from the device attached to the input.

Input Mode

Select the input mode for this input. The input mode determines when a change of state at an input will be reported as an event or alarm.

The following event input modes are supported:

- *Normal* - Input changes of state will be reported immediately with no delay.
- *Delayed Action* - Input changes of state will be reported after the amount of time entered in the delay time field has passed. The delay time can range from 0 to 9999 seconds.

Event Type

Input events (transactions) are recorded in the event file every time there is a change of state for the input. Input events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Input Secure* - The input has returned to a secure state. The secure state is determined by the input configuration setting.
- *Input Alarm* - The input has reported an alarm. The alarm state is determined by the input configuration setting.
- *Input Supervisory Fault* - The input has reported a fault. This can be either a short or an open circuit when a 2K resistor network is installed.
- *Input Delay In Progress* - The input has changed state and the specified input delay has been started.

Annunciation Type

- *Disregard*: Input events (transactions) for this event type will not be recorded in the event file and will not be displayed in either the events window or in the alarms window.
- *Log Only*: Input events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display*: Input events (transactions) for this event type will be recorded in the event file and displayed in the events window.
- *Alarm*: Input events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic.

The alarm priority is only used for event types that have the annunciation type set to "Alarm".

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on alarms, see the [Alarms](#) help file topic.

The alarm message is only used for event types that have the annunciation type set to "Alarm".

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the alarms window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic.

The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Message

Enter the event message for this event type. The event messages will be displayed in the events window each time this event type is generated. The event message is generally used to provide friendly text identification to the person monitoring events to identify the input point. This field can be up to 256 characters in length. For more information on events, see the [Events](#) help file topic.

Default Map when Input in Alarm

Select the default map to be associated with this device. The default map will be displayed whenever the show map toolbar button is clicked from the alarms window while any pending alarm for this device is selected. The map must be defined in the maps screen prior to selecting a default map for a device. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Automatically Show Map

Select (check) this option to have the map specified as the default map automatically displayed in the alarms window when an alarm for this device is acknowledged. If no default map is specified then selecting this option will have no effect. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Require Secure Condition Before Alarm Clear

Select (check) this option to require that an alarm be secured before it can be cleared from the alarms screen for this event type. This option is used to make sure that an alarm cannot be ignored by simply acknowledging and clearing it without any action being taken. For example, if a door has been forced open, if this option is checked, the door would have to be closed before the alarm could be cleared from the alarms window. For more information on alarms, see the [Alarms](#) help file topic.

The require secure condition before alarm clear option is only used for event types that have the annunciation type set to "Alarm".

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Associated Intercom Station

Select the intercom station to be associated with this device. The associated intercom station will be automatically connected when an alarm for this device is acknowledged in the alarms window. Automatic connection will also occur when this device is selected on a map or when any of the other associated devices are selected. The intercom must be defined in the hardware screen prior to selecting an associated intercom for a device. In addition, each of

the workstations that will be using the intercom integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

Intercom integration licenses must be purchased separately for each workstation.

Associated Camera

Select the camera to be associated with this device. The associated camera will be automatically selected when an alarm for this device is acknowledged in the alarms window. Automatic selection will also occur when this device is selected on a map or when any of the other associated devices are selected. The camera must be defined in the hardware screen prior to selecting an associated camera for a device. In addition, each of the workstations that will be using the integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

Integration licenses must be purchased separately for each workstation.

Camera Preset Number

Enter the preset number for the associated camera for this device. The associated camera will be automatically selected and stationed at the preset number entered when an alarm for this device is acknowledged in the alarms window. Automatic preset selection will also occur when this device is selected on a map or when any of the other associated devices are selected. If no associated camera is specified then this entry will have no effect. The camera must be defined in the hardware screen prior to selecting an associated camera for a device. In addition, each of the workstations that will be using the integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

Integration licenses must be purchased separately for each workstation.

Save/Close Buttons

Clicking on the save button will save the changes made to the input. Clicking on the close button will not save the changes made to the input.

[Inputs](#)

Outputs

[Outputs Detail](#)

Outputs are used to define the type and operational parameters for the outputs attached to each of the SIO panels in the system. If the main output item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the attached outputs. The output icon will also display the current alarm state for each of the outputs.

Only outputs which are available for general use are displayed. Some of the outputs on the SIO panels are preprogrammed for the door strike, etc. These outputs will not be displayed as they cannot be used for any other purpose. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Searching Outputs

To search for an output, type in the search box located in the upper right hand corner. Results will be dynamically displayed as search criteria is entered. To include a wildcard in the search use the asterisk (*) symbol.

Custom filtered views can be selected for the outputs screen. When applied, outputs will dynamically populate based on their changing states. Newly added devices will not appear in the filtered list until the grid is refreshed by clicking the green refresh icon. Filtered views include:

- *(No Filter)* - No filter will be applied to the outputs grid.
- *Active Outputs* - Only outputs in an activated state will display within the outputs grid.
- *Inactive Outputs* - Only outputs in an inactive state will display within the outputs grid.

Editing an Output

To edit an output, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the output(s) to be edited. Next, expand the SIO's list and locate the SIO containing the output(s). All of the outputs associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the output to be edited and click on the edit button on the toolbar, or double click the output to be edited. You can also select edit from the file option on the system menu or from the right click menu.

You can also view all of the enabled (installed) outputs, sorted by name, by clicking on the installed outputs item in the hardware tree. This view is the quickest and easiest way to interact with the outputs in the system once the installation of the system hardware has been

completed. Outputs can be edited and commands can be sent to outputs from this view as well.

Printing Output Reports

To print reports for an output, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the output(s) to print reports for. Next, expand the SIO's list and locate the SIO containing the output(s). All of the outputs associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the output to print reports for and click on the print button on the toolbar. You can also select print from the file option on the system menu or from the right click menu. The following reports are available:

- *Output Activity* - This report provides a list of all output activity for the selected outputs.
- *Output Audit History* - This report provides a list of all database updates and user issued commands for the selected outputs.
- *Output History* - This report provides a list of all database updates, user issued commands and output activity for the selected outputs.
- *Output Listing* - This report provides a list of the selected outputs and their various properties.

Output Commands

To send commands to an output, expand the SCP node within the Hardware group of the Navigation pane and then expand the SCP panel that contains the output(s) to be edited. Next, expand the SIO's list and locate the SIO containing the output(s). All of the outputs associated with the selected SIO will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the output to send a command to and click on the output commands drop down next to the refresh button on the toolbar. Select the command to be issued from the list and click on the command text button on the toolbar to send the command. You can also send a command by selecting commands from the right click menu and selecting the command to be sent.

The following output commands are supported:

Temporary commands are only supported when the output is installed under an EP series controller and will not work if using a legacy SCP controller.

Activate Output

The output will be activated (energized).

Deactivate Output

The output will be deactivated (de-energized).

Pulse Output

The output will be pulsed (activated, then deactivated) for the amount of time specified in the pulse time setting for this output.

Request Output Status

The request output status command is used to view current status information for the output. This tool can be useful in troubleshooting system problems and is also used for informational purposes. The following information is displayed:

- *Output Name* - Displays the name of the output.
- *Output State* - Displays whether the output is in an active or inactive state.

Outputs Detail

Outputs

Outputs are used to define the type and operational parameters for the outputs attached to each of the SIO panels in the system. If the main output item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the attached outputs. The output icon will also display the current alarm state for each of the outputs.

Only outputs which are available for general use are displayed. Some of the outputs on the SIO panels are preprogrammed for the door strike, etc. These outputs will not be displayed as they cannot be used for any other purpose. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Output Name

Enter the name to be used for this output. All of the outputs have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the outputs being used. An example of a friendly name would be "Main Building - Disaster Siren". The output name can be up to 50 characters in length.

Attached to SIO

This field displays the name of the SIO panel on which this output is located. This field is displayed for informational purposes only and cannot be changed.

Output Number

This field displays the physical location that this output is located on the SIO panel. The output number can be determined by the default name assigned to the output. This field is displayed for informational purposes only and cannot be changed.

The available number of outputs will be based on the model number of the SIO panel.

Device Installed

Select (check) this option if this output has been physically installed in the system. If the device installed option is checked, the output will be displayed in the installed outputs branch of the hardware tree. If the device installed option is not checked, the output will not be displayed in the installed outputs branch of the hardware tree. This is useful for hiding extra outputs that SIO panels support but that are not in use and makes viewing and sorting installed outputs easier. Uninstalling this device has no impact to the functionality of the

output.

Output Drive Mode

Select the output drive mode for this output. This option will depend upon the type of hardware being installed for use with the output. The following options are supported:

- *De-energized when Inactive* - This option should be used when the device attached to this output operates in a normally open configuration.
- *Energized when Inactive* - This option should be used when the device attached to this output operates in a normally closed configuration.

Select or enter the amount of time that this output will remain activated when it has been pulsed. The pulse time can range from 1 to 99 seconds.

Activate Output During Timezone

Select the timezone that this output should be activated during. The output will be activated at the start time of the selected timezone and deactivated at the end time of the selected timezone, during any of the days specified in any of the intervals within the selected timezone.

Event Type

Output events (transactions) are recorded in the event file every time there is a change of state for the output. Output events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Output Activated* - The output has been activated (energized).
- *Output Deactivated* - The output has been deactivated (de-energized).

Annunciation Type

- *Disregard*: Output events (transactions) for this event type will not be recorded in the event file and will not be displayed in either the events window or in the alarms window.
- *Log Only* - Output events (transactions) for this event type will only be recorded in the event file and not displayed in either the events window or in the alarms window.
- *Log And Display* - Output events (transactions) for this event type will be recorded in the event file and displayed in the events window.

- *Alarm* - Output events (transactions) for this event type will be recorded in the event file and displayed in the alarms window.

Priority

Enter the alarm priority for this event type. The alarm priority determines the order that this event type will display in the alarms window. An event type with an alarm priority of 1 will display first in the alarms window and an event type with an alarm priority of 9999 will display last in the alarms window. The alarm priority can range from 1 to 9999. For more information on alarms, see the [Alarms](#) help file topic.

The alarm priority is only used for event types that have the annunciation type set to "Alarm".

Macro

Select the macro to be executed for this event type. The selected macro will be executed each time this event type is generated. The actions to be performed by the macro must be defined in the macros screen. For more information on macros, see the [Macros](#) help file topic.

Alarm Message

Enter the alarm message for this event type. The alarm messages will be displayed in the alarms window each time this event type is generated. The alarm message is generally used to provide text instructions to the person monitoring alarms as to what actions to take when the alarm occurs. This field can be up to 256 characters in length. For more information on alarms, see the [Alarms](#) help file topic.

The alarm message is only used for event types that have the annunciation type set to "Alarm".

Sound File

Choose the sound (.WAV) file for this event type. The sound file will be played from the alarms window each time this event type is generated. The sound file is generally used to provide verbal instructions to the person monitoring alarms as to what actions to take when the alarm occurs. For more information on alarms, see the [Alarms](#) help file topic.

The sound is only used for event types that have the annunciation type set to "Alarm". The sound file must be accessible either on the local machine or over the network to be played.

Require Comments

Select (check) this option to require the user to make a text entry or choose one of the predefined alarm responses in the acknowledge alarms window in order to acknowledge an alarm for this event type. This is useful when it is desirable to have some sort of explanation

recorded in the events file along with the alarm acknowledgment event. For more information on alarms, see the [Alarms](#) help file topic.

Message

Enter the event message for this event type. The event messages will be displayed in the events window each time this event type is generated. The event message is generally used to provide friendly text identification to the person monitoring events to identify the input point. This field can be up to 256 characters in length. For more information on events, see the [Events](#) help file topic.

Default Map when Output in Alarm

Select the default map to be associated with this device. The default map will be displayed whenever the show map toolbar button is clicked from the alarms window while any pending alarm for this device is selected. The map must be defined in the maps screen prior to selecting a default map for a device. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Automatically Show Map

Select (check) this option to have the map specified as the default map automatically displayed in the alarms window when an alarm for this device is acknowledged. If no default map is specified then selecting this option will have no effect. For more information on maps, see the [Maps](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

Require Secure Condition Before Alarm Clear

Select (check) this option to require that an alarm be secured before it can be cleared from the alarms screen for this event type. This option is used to make sure that an alarm cannot be ignored by simply acknowledging and clearing it without any action being taken. For example, if a door has been forced open, if this option is checked, the door would have to be closed before the alarm could be cleared from the alarms window. For more information on alarms, see the [Alarms](#) help file topic.

The require secure condition before alarm clear option is only used for event types that have the annunciation type set to "Alarm".

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Associated Intercom Station

Select the intercom station to be associated with this device. The associated intercom station will be automatically connected when an alarm for this device is acknowledged in the alarms window. Automatic connection will also occur when this device is selected on a map or when any of the other associated devices are selected. The intercom must be defined in the hardware screen prior to selecting an associated intercom for a device. In addition, each of the workstations that will be using the intercom integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

Intercom integration licenses must be purchased separately for each workstation.

Associated CCTV Camera

Select the CCTV camera to be associated with this device. The associated CCTV camera will be automatically selected when an alarm for this device is acknowledged in the alarms window. Automatic selection will also occur when this device is selected on a map or when any of the other associated devices are selected. The CCTV camera must be defined in the hardware screen prior to selecting an associated CCTV camera for a device. In addition, each of the workstations that will be using the CCTV integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.

CCTV integration licenses must be purchased separately for each workstation.

Camera Preset Number

Enter the preset number for the associated CCTV camera for this device. The associated CCTV camera will be automatically selected and stationed at the preset number entered when an alarm for this device is acknowledged in the alarms window. Automatic preset selection will also occur when this device is selected on a map or when any of the other associated devices are selected. If no associated CCTV camera is specified then this entry will have no effect. The CCTV camera must be defined in the hardware screen prior to selecting an associated CCTV camera for a device. In addition, each of the workstations that

will be using the CCTV integration must have that option selected for the workstation. For more information on hardware, see the [Hardware](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic. For more information on maps, see the [Maps](#) help file topic. For more information on workstations, see the [Workstations](#) help file topic.
CCTV integration licenses must be purchased separately for each workstation.

Save/Cancel Buttons

Clicking on the save button will save the changes made to the output. Clicking on the cancel button will not save the changes made to the output.

Outputs

IP Locksets

[IP Locksets Detail](#)

IP locksets are used to define the serial number and operational parameters for each of the IP locksets in the system. If the main IP lockset item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the IP locksets. The IP lockset icon will also display the current alarm state for each of the IP locksets.

Access to this screen is determined by the settings for the currently logged in user. IP lockset permissions inherit their settings from the reader settings for the user group. For more information on users, see the [Users](#) help file topic.

Searching IP Locksets

To search for an IP Lockset, type in the search box located in the upper right hand corner. Results will be dynamically displayed as search criteria is entered. To include a wildcard in the search use the asterisk (*) symbol.

Custom filtered views can be selected for the IP Locksets screen. When applied, IP locksets will dynamically populate based on their changing states. Newly added devices will not appear in the filtered list until the grid is refreshed by clicking the green refresh icon. Filtered views include:

- *(No filter)* - No filter will be applied to the IP Locksets grid.
- *Online* - Only IP Locksets in the online state will display within the IP Locksets grid.
- *Offline* - Only IP Locksets in the offline state will display within the IP Locksets grid.
- *Exception* - Only IP Locksets in the exception state will display within the IP Locksets grid.

Adding an IP Lockset

To add an IP lockset, go to the IP locksets entry screen by clicking on the IP Lockset icon within the Hardware group of the Navigation pane. Then, click on the IP locksets item in the hardware tree. All of the IP locksets will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button within the ribbon or select new from the right click menu.

Editing an IP Lockset

To edit an IP lockset, go to the IP locksets entry screen by clicking on the IP Lockset icon within the Hardware group of the Navigation pane. Then, click on the IP locksets item in the

hardware tree. All of the IP locksets will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the IP lockset to be edited and click on the edit button within the ribbon, or double click the IP lockset to be edited. You can also select edit from the right click menu.

Deleting an IP Lockset

To delete an IP lockset, go to the IP locksets entry screen by clicking on the IP Lockset icon within the Hardware group of the Navigation pane. Then, click on the IP locksets item in the hardware tree. All of the IP locksets will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the IP lockset to be deleted and click on the delete button within the ribbon or select delete from the right click menu.

Printing IP Lockset Reports

To print reports for IP locksets, go to the IP locksets entry screen by clicking on the IP Lockset icon within the Hardware group of the Navigation pane. Then, click on the IP locksets item in the hardware tree. All of the IP locksets will then be displayed in the right window pane of the Access It! Universal desktop. Select the IP locksets to print reports for and click on the print button on the toolbar or select print from the file option on the system menu or from the right click menu. The following reports are available:

- *Access By IP Lockset* - This report provides a list of cardholders and cards that have access to the selected IP locksets. This report includes the timezone that corresponds to the selected IP locksets.
- *Access Levels By IP Lockset* - This report provides a list of all access levels that contain the selected IP locksets. This report includes the timezone that corresponds to the selected IP lockset.
- *IP Lockset Access Denied Events* - This report provides a list of all access denied card usage events for the selected IP locksets.
- *IP Lockset Access Events* - This report provides a list of all access card usage events for the selected IP locksets.
- *IP Lockset Access Granted Events* - This report provides a list of all access granted card usage events for the selected IP locksets.
- *IP Lockset Activity* - This report provides a list of all access granted card usage events for the selected IP locksets.
- *IP Lockset Audit History* - This report provides a list of all database updates and user issued commands for the selected IP locksets.
- *IP Lockset Listing* - This report provides a list of the selected IP Locksets and their various properties.
- *IP Lockset Listing with Battery Voltage* - This report provides a list of the selected IP Locksets and their various properties, including battery voltage.

IP Lockset Commands

To send a command to an IP lockset, go to the hardware tree by either clicking on the hardware toolbar button within the main group on the toolbar, or by selecting hardware from the go option on the system menu. Then, click on the IP locksets item in the hardware tree. All of the IP locksets will then be displayed in the right window pane of the Access It! Universal desktop. Select the IP lockset to send a command to and click on the IP locksets command drop down next to the refresh button on the toolbar or select commands from the right click menu. Select the command to be issued from the list and click on the command to be sent to the IP lockset. You can also send a command by selecting commands from the file option on the system menu and selecting the command to be sent.

The following IP lockset commands are supported:

Unlock

The door will be unlocked if the IP lockset is currently online.

Lock

The door will be locked if the IP lockset is currently online.

IP Locksets Detail

IP Locksets

IP locksets are used to define the serial number and operational parameters for each of the IP locksets in the system. If the main IP lockset item is selected in the hardware tree, live status information is displayed in the right window pane of the Access It! Universal.NET desktop for each of the IP locksets. The IP lockset icon will also display the current alarm state for each of the IP locksets.

Access to this screen is determined by the settings for the currently logged in user. IP lockset permissions inherit their settings from the reader settings for the user group. For more information on users, see the [Users](#) help file topic.

IP Lockset Name

Enter the name to be used for this IP lockset. It is recommended that a friendly name be assigned to all of the IP locksets being used. An example of a friendly name would be "Dorm Room 101". The IP lockset name can be up to 50 characters in length.

Serial Number

Enter the serial number for this IP lockset. This number will be automatically populated if the IP lockset is being added after it has been discovered on the network automatically.

It is very important that the serial number entered matches the serial number of the lockset being installed. Entering the wrong serial number could result in system malfunctions.

Hardware Server

The hardware server name is used to specify the network name of the ASSA ABLOY communication server that will be hosting the IP locksets. It is usually but not necessarily the same computer that will be hosting the database.

Inbound Port Number

The TCP port that the comm server will listen on for incoming IP lockset connections and communication traffic.

If a firewall is in place this port will need to be configured for incoming (lockset to comm server) TCP traffic.

Outbound Port Number

The TCP port that the comm server will use for outbound IP lockset connections and

communication traffic.

If a firewall is in place this port will need to be configured for outbound (comm server to lockset) TCP traffic.

IP Address

The IP address that has been assigned to the lockset.

An IP address must be assigned to the lockset using the Network Configuration Tool and the Lock Configuration Tool prior to lockset communications.

Communications Mode

Select the communication mode to be used for this lockset. The following communication modes are supported:

- *Host Initiated* - Communication between the lockset and the comm server computer is initiated by the comm server. This mode is generally used with POE locksets and wireless locksets that are always powered.
- *Lock Initiated* - Communication between the lockset and the comm server computer is initiated by the lockset. This mode is generally used with battery powered wireless locksets.

Last Contact Time

This field will display the last date and time that communications were established with the lockset. This field is for display purposes only and cannot be edited.

Battery Voltage

This field will display the lockset battery voltage as of the last time that communications were established with the lockset. This field is for display purposes only and cannot be edited.

Auxiliary Voltage

This field will display the lockset auxiliary voltage as of the last time that communications were established with the lockset. This field is for display purposes only and cannot be edited.

IP Lockset Time Zone

Select the local time zone for the location that the IP lockset is being installed.

The time zone that the server computer is located in and the time zone that the IP lockset is installed at may be different. Be sure and select the time zone for the location that the IP

lockset is being physically installed and not the time zone that the server computer is located in.

Automatically adjust for DST Changes

Select (check) this option if the IP lockset should automatically adjust its time settings when Daylight Savings Time starts or ends.

Contact Schedule

Select the contact schedule to be used for communications with the IP lockset. Contact schedules determine how often and when IP lockset communications occur between the comm server computer and the lockset. Click on the edit button to modify existing contact schedules or to add new contact schedules. The following contact schedule parameters are supported:

- *Radio Always On* - Communications between the comm server computer and the IP lockset will be continuous and transactions and updates to the lockset will occur in real time.
- *Simple ("x" minutes off, "y" seconds on scheduler)* - Communications between the comm server computer and the IP lockset will occur for the amount of time specified for awake time and then communications will reoccur after the amount of time specified for the sleep period.
- *Day of Month* - Communications between the comm server computer and the IP lockset will occur on the days of the month specified at the time specified and continue for the awake time specified.
- *Day of Week* - Communications between the comm server computer and the IP lockset will occur on the days of the week specified at the time specified and continue for the awake time specified.
- *Comm User Only* - Communications between the comm server computer and the IP lockset will only occur when a comm user credential is presented or entered at the IP lockset for the awake time specified.

Treat as Communication Failure After

Enter the amount of time that must pass if an IP lockset has not been contacted before a communication failure event or alarm will be generated.

Scheduled Unlock Timezone

Select the scheduled unlock timezone for this IP lockset. The IP lockset will unlock at the start of the selected timezone and re-lock at the end of the selected timezone. This option works in conjunction with the unlock mode parameter.

Unlock Mode

Select the unlock mode for this IP lockset. The following unlock mode parameters are supported:

- *Auto unlock on schedule* - The IP lockset will unlock at the start of the timezone specified in the scheduled unlock timezone and re-lock at the end of the timezone specified in the scheduled unlock timezone. If the scheduled unlock timezone is set to <None> then the lockset will not automatically unlock.
- *Unlock on first person through* - The IP lockset will unlock when the first valid credential is presented at the lockset. This is commonly used when it is desirable to have a specific person or persons in an area and then unlock the door so that other people may enter without having to use a card.

iClass reader mode

Select the iClass mode to be used by the lockset.

Apartment mode

Select (check) this option to enable the feature where every time you leave the room the door unlocks itself and you have to use your card from the outside to lock it. This is required in most Canadian residential situations.

Visible Keypad Feedback

Select (check) this option to enable visible keypad feedback. Visible keypad feedback will light up the key on the IP lockset keypad being pressed briefly to give the user confirmation of pressing the key.

Enable Panic Mode

Select (check) this option to enable panic mode. Panic mode will lock down the IP lockset preventing regular users from entering and lock the door. Only master users and emergency users will be allowed access to the IP lockset. If a master user presents a credential at the IP lockset panic mode will be cleared. For more information on lockset user types see the [Cards](#) help file topic.

Normal Unlock Time

Select or enter the unlock time for this IP lockset. The unlock time is the amount of time that the door will remain unlocked after a valid card has been presented, or an access granted command has been issued. This time can range from 1 to 255 seconds.

Extended Unlock Time

Select or enter the extended unlock time for this IP lockset. The extended unlock time is the extended amount of time that the door will remain unlocked after a valid card has been presented. This time will be added on to the standard unlock time for all cards that have the extended access times option checked. This time can range from 1 to 255 seconds.

Door Ajar Time

Select or enter the door ajar time for this IP lockset. The door ajar time is the amount of time that the door can be open after a valid card has been presented. This time can range from 1 to 255 seconds.

2nd Credential Timeout

Select or enter the 2nd credential timeout for this IP lockset. The 2nd credential timeout is the amount of time the IP lockset will wait for a PIN number to be entered if the card is set up for Card and PIN access mode or Card Then PIN access mode. For more information on card access modes, see the [Cards](#) help file topic.

Lockout After x Failed Attempts

Select or enter the lockout after "x" failed attempts for this IP lockset. The lockout after "x" failed attempts will lock out a card holder if the card presentation or PIN entry fails consecutively for the number of times specified in the field. This value can range from 0 to 255 attempts.

Lockout Duration

Select or enter the lockout duration for this IP lockset. The lockout duration is the amount of time that a card holder will be locked out after exceeding the number of attempts specified in the lockout after "x" failed attempts field. This value can range from 1 to 255 seconds.

RX-Held

Select (check) this option to enable RX-held.

RX-Held Shunt Delay

Select or enter the RX-held shunt delay for this IP lockset. This value can range from 1 to 9999 seconds.

Remote Authentication

Select (check) this option to enable the remote authentication feature. When enabled, the lockset will automatically awake on an Access Denied event and will contact the server to check if the card presented is a new card that has not yet been downloaded into the lock. If a valid record is found the lock will then grant access.

Comm Behavior

Comm behavior determines what event types during what IP lockset cycle will force the IP lockset to communicate with the host computer.

The following IP lockset contact event types are supported:

- *Contact Host on RX held event* - The IP lockset will communicate with the host computer when the RX has been held during the selected lockset cycles.
- *Contact Host on Access Granted* - The IP lockset will communicate with the host computer when a valid credential has been presented and access has been granted during the selected lockset cycles.
- *Contact Host on Access Denied* - The IP lockset will communicate with the host computer when an invalid credential has been presented and access has been denied during the selected lockset cycles.
- *Contact Host on Door Secured* - The IP lockset will communicate with the host computer when the door has been secured during the selected lockset cycles.
- *Contact Host on Door Forced* - The IP lockset will communicate with the host computer when the door has been forced open during the selected lockset cycles.
- *Contact Host on Key Override* - The IP lockset will communicate with the host computer when a key has been used to open the door during the selected lockset cycles.
- *Contact Host on Door Ajar* - The IP lockset will communicate with the host computer when the door has been left ajar (held open) during the selected lockset cycles.
- *Contact Host on Low Battery* - The IP lockset will communicate with the host computer when the battery is low during the selected lockset cycles.

Event Type

IP lockset events (transactions) are recorded in the event file every time there is a card or PIN presented at the IP lockset. IP lockset events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Access Granted Regular User* - A credential has been presented by a regular user type at the IP lockset and access has been granted to the door.
- *Access Granted Use Limit User* - A credential has been presented by a use limit user

type at the IP lockset and access has been granted to the door.

- *Access Granted* - A credential has been presented by a user at the IP lockset and access has been granted to the door.
- *Valid Entry* - A credential has been presented by a user at the IP lockset and access has been granted to the door and the door has been used.
- *Access Denied Invalid PIN* - A credential has been presented at the IP lockset and access has been denied because the PIN number entered is invalid.
- *Access Denied Wrong Time* - A credential has been presented at the IP lockset and access has been denied because the user is not allowed access to this door at this time.
- *Access Denied Lockout* - A credential has been presented at the IP lockset and access has been denied because the user has been locked out due to too many failed access attempts.
- *Access Denied Expired User* - A credential has been presented at the IP lockset and access has been denied because the user has used an expired credential.
- *Access Denied Suspended User* - A credential has been presented at the IP lockset and access has been denied because the user is suspended.
- *Access Denied Door Bolted* - A credential has been presented at the IP lockset and access has been denied because the door is bolted.
- *Access Denied Lock in Panic Mode* - A credential has been presented at the IP lockset and access has been denied because the lockset is in panic mode. Only emergency and master user types will have access.
- *Access Denied Lock in Passage Mode* - A credential has been presented at the IP lockset and access has been denied because the door is already unlocked.
- *Access Denied Lock not in Passage Mode* - A credential has been presented and access has been denied because the user is a relock user and the door is not unlocked.
- *Access Denied Bad Access Mode* - A credential has been presented at the IP lockset and access has been denied because the users access mode is incorrect. For example, the user entered a PIN and the access mode is set to card only for the credential.
- *Access Denied* - A credential has been presented at the IP lockset and access has been denied.
- *Access Denied Bad Credential* - A credential has been presented at the IP lockset and access has been denied because the credential is not recognized.
- *Access Denied Emergency User Radio Busy* - A credential has been presented at the IP lockset and access has been denied for a emergency user because the lockset is currently communicating with the comm server.
- *Access Denied Supervisor Radio Busy* - A credential has been presented at the IP lockset and access has been denied for a supervisor user because the lockset is currently communicating with the comm server.
- *Access Denied Use Limit User Radio Busy* - A credential has been presented at the IP lockset and access has been denied for a use limit user because the lockset is currently communicating with the comm server.
- *Access Denied Radio Busy* - A credential has been presented at the IP lockset and access has been denied because the lockset is currently communicating with the comm

server.

- *Access Denied Panic User Radio Busy* - A credential has been presented at the IP lockset and access has been denied for a panic user because the lockset is currently communicating with the comm server.
- *Access Denied REX Radio Busy* - A request to exit has been requested at the IP lockset and access has been denied because the lockset is currently communicating with the comm server.
- *Access Denied Lockout User Radio Busy* - A credential has been presented at the IP lockset and access has been denied for a lockout user because the lockset is currently communicating with the comm server.
- *Access Denied Relock User Radio Busy* - A credential has been presented at the IP lockset and access has been denied for a relock user because the lockset is currently communicating with the comm server.
- *Door Forced* - The door has been forced open without either a valid credential being presented.
- *Door Ajar* - The door has been open longer than the allowed door ajar time setting for this IP lockset.
- *Door Secured* - The door has been secured after being in an alarm state (forced open, held open, etc.).
- *Door Opened* - The door has been opened.
- *Door Closed* - The door has been closed.
- *Invalid Entry* - An invalid entry has been made at the IP lockset.
- *Scheduled Unlock* - The door has been unlocked because a scheduled unlock timezone assigned to the lockset has started.
- *Scheduled Relock* - The door has been relocked because a scheduled unlock timezone assigned to the lockset has ended.
- *Panic Button Pushed* - The IP lockset has been put in to panic mode. Panic mode results in the door being locked and only master and emergency user types will be granted access.
- *Lockout Begin* - The IP lockset has started a lockout for a user. That user will not be granted access until the lockout period ends.
- *Lockout End* - The IP lockset has ended a lockout for a user. If the user is authorized they will now be granted access.
- *Lock Reset* - The IP lockset has been reset.
- *Emergency Code Entered* - An emergency code has been entered at the IP lockset.
- *Relock Code Entered* - A relock code has been entered at the IP lockset.
- *Master Code Entered* - A master code has been entered at the IP lockset.
- *Supervisor Code Entered* - A supervisor code has been entered at the IP lockset.
- *Key Override* - A key has been used at the IP lockset to open the door rather than a credential.
- *Bolt Thrown* - The bolt has been thrown at the IP lockset.
- *Bolt Retracted* - The bolt has been retracted at the IP lockset.

- *Bolt Opened* - The bolt has been opened at the IP lockset.
- *Bolt Closed* - The bolt has been closed at the IP lockset.
- *Latch Opened* - The latch has been opened at the IP lockset.
- *Latch Closed* - The latch has been closed at the IP lockset.
- *REX opened* - A request to exit has been initiated for the IP lockset by the associated request to exit device.
- *REX Closed* - A request to exit has been canceled for the IP lockset by the associated request to exit device.
- *Battery Low* - The battery is low in the IP lockset.
- *Battery Dead* - The battery is dead in the IP lockset.
- *Battery Replaced* - The battery has been replaced in the IP lockset.
- *Clock Set Back* - The clock has been set back in the IP lockset.
- *Clock Set Forward* - The clock has been set forward in the IP lockset.
- *Communication Session Started* - A connection has been established with the IP lockset and communications have started.
- *Communication Session Ended* - A connection has been established with the IP lockset and communications have ended.
- *Connection Attempt* - An attempt to connect to the IP lockset has been started.
- *Connection Established* - A connection has been established with the IP lockset.
- *Connection Attempt Failed* - An attempt to connect to the IP lockset has been failed.
- *Lockset Online* - The IP lockset is now online with the comm server.
- *Lockset Offline* - The IP lockset is now offline with the comm server.
- *Communication Exception* - A communication exception has occurred at the IP lockset.
- *Decryption Failure* - A decryption failure has occurred at the IP lockset.
- *Comm User Activated* - A credential has been presented at the IP lockset for a comm user and a communication session has been requested.
- *DPAC Disabled* - The DPAC has been disabled at the IP lockset.
- *MCC Programming Mode Entered* - The IP lockset has entered MCC programming mode.
- *MCC Programming Mode Exited* - The IP lockset has exited MCC programming mode.
- *Serial Receiver Overrun* - A serial receiver overrun has occurred at the IP lockset.
- *DPAC Receiver Overrun* - A DPAC receiver overrun has occurred at the IP lockset.
- *NVRAM is cleared by push button* - The NVRAM has been cleared manually at the IP lockset by pushing the button on the lockset.
- *NVRAM is cleared by revision* - The NVRAM has been cleared by revision at the IP lockset.
- *NVRAM wasn't changed* - The NVRAM was not changed at the IP lockset.
- *Radio Timed Out - Remote Login* - The radio has timed out during a remote login at the IP lockset.
- *Error Reading RTC* - An error reading the RTC has occurred at the IP lockset.
- *Remote Unlock* - The IP lockset has been remotely unlocked.
- *Time Zone Exceptions Disabled* - Holidays have been disabled at the IP lockset.

- *Performing checksum on configuration NVRAM* - A checksum is being performed on the NVRAM in the IP lockset.
- *Performing checksum on timezone data* - A checksum is being performed on the timezone data in the IP lockset.
- *Battery Check Not Performed* - A battery check was not performed at the IP lockset.
- *Firmware Update Aborted* - A firmware updated has been aborted at the IP lockset.
- *Firmware Update Error* - A firmware update error has occurred at the IP lockset.
- *Firmware Download Timeout* - A firmware download has timed out at the IP lockset.
- *Firmware Upgrade Started* - A firmware upgrade has been started at the IP lockset.
- *Firmware Upgrade Finished* - A firmware upgrade has finished at the IP lockset.
- *Firmware Upload Failed* - A firmware upload has failed at the IP lockset.
- *Remote Authorization Request Made* - A remote authorization request has been made at the IP lockset.
- *Mortise State Machine Failure* - A mortise state machine failure has occurred at the IP lockset.
- *User Added or Changed* - A user or card holder has been added to or updated in the IP lockset.
- *User Deleted* - A user or card holder has been deleted in the IP lockset.
- *Date and Time Set* - The date and time has been set in the IP lockset.
- *Event Log Cleared* - The event log has been cleared in the IP lockset.
- *User Database Reset* - The user database has been reset in the IP lockset.
- *User Replaced* - A user has been replaced in the IP lockset.
- *User Updated* - A user has been updated in the IP lockset.
- *Event Log wrapped* - The event log has wrapped in the IP lockset.
- *Declined Log wrapped* - The declined log has wrapped in the IP lockset.
- *Alarm Log wrapped* - The alarm log has wrapped in the IP lockset.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information etc. There is no limit as to how long a notes field can be.

[IP Locksets](#)

Card Groups

[Card Groups Detail](#)

Card groups are used to group a single card or many cards together. The card group will group together cards with the same card group assigned to them. The card group can then be used to have a single card or a group of cards perform tasks when a card number from a certain card group is presented at a reader. The card group can also be used to set up mandatory or default card activation and expiration dates. The task to be performed by the card group and the conditions under which to perform the task are defined in the tasks screen. For more information on tasks, see the [Tasks](#) help file topic.

Card groups must be enabled in the sites screen in order to function. For more information on sites, see the [Sites](#) help file topic. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Card Group

To add a card group, go to the card groups entry screen by clicking on the Card Groups icon within the Main group of the Navigation pane. All of the card groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the toolbar or select new from the right click menu.

Editing a Card Group

To edit a card group, go to the card groups entry screen by clicking on the Card Groups icon within the Main group of the Navigation pane. All of the card groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the card group to be edited and click on the edit button on the toolbar, or double click the card group to be edited. You can also select edit from the right click menu.

Deleting a Card Group

To delete a card group, go to the card groups entry screen by clicking on the Card Groups icon within the Main group of the Navigation pane. All of the card groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the card group to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu.

Printing Card Group Reports

To print reports for a card group, go to the card groups entry screen by clicking on the Card Groups icon within the Main group of the Navigation pane. All of the card groups in the

database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the card groups to print reports for and click on the Reports button within the ribbon or select print reports from the right click menu. The following reports are available:

- *Card Group History* - This report provides a list of all database update events for the selected card groups.
- *Card Group Listing* - This report provides a list of the selected card groups and their various properties.

Card Groups Detail

Card Groups

Card groups are used to group a single card or many cards together. The card group will group together cards with the same card group assigned to them. The card group can then be used to have a single card or a group of cards perform tasks when a card number from a certain card group is presented at a reader. The card group can also be used to set up mandatory or default card activation and expiration dates. The task to be performed by the card group and the conditions under which to perform the task are defined in the tasks screen. For more information on tasks, see the [Tasks](#) help file topic.

Card groups must be enabled in the sites screen in order to function. For more information on sites, see the [Sites](#) help file topic. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Card Group Name

Enter the name to be used for this card group. All of the card groups have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the card groups being used. An example of a friendly name would be "South Building Contractors". The card group name can be up to 50 characters in length.

Require Active/Expire Dates

Select (check) this option to require an activation and or expiration date when a card is entered that is being assigned to this card group. This option is useful when you want the operator to be forced to enter an expiration date for a card that might be in a temporary contractors group.

Predefined Active Date

Select (check) this option to force the entry of a predefined activation date when a card is being entered that is being assigned to this card group. The operator will be forced to use an activation date and will not be able to change the date when this option is used.

Predefined Expire Date

Select (check) this option to force the entry of a predefined expiration date when a card is being entered that is being assigned to this card group. The operator will be forced to use an expiration date and will not be able to change the date when this option is used.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Cancel Buttons

Clicking on the save button will save the changes made to the card group. Clicking on the cancel button will not save the changes made to the card group.

SALTO Doors

[SALTO Doors Detail](#)

The SALTO SHIP (SALTO Host Interface Protocol) is an integration between SALTO ProAccess SPACE and Access It! Universal.NET. This integration allows for managing users and basic hardware configuration of offline and online SALTO locksets within the Access It! Universal.NET application. SALTO keys are referred to as cards within Access It! Universal.NET. The SHIP integration allows the key/card to encode its own access database and event trail directly to the card. This allows for offline locks to be used without the need for a central repository.

The SHIP integration requires Doors, Timezones, and Calendars be managed within ProAccess SPACE.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a SALTO Door

To add a SALTO Door, go to the SALTO Doors entry screen by clicking on the SALTO Doors icon within the Hardware group of the Navigation pane. Then, click on the SALTO Doors item in the hardware tree. All of the SALTO Doors will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button within the ribbon or select new from the right click menu.

Editing a SALTO Door

To edit a SALTO Door, go to the SALTO Doors entry screen by clicking on the SALTO Door icon within the Hardware group of the Navigation pane. Then, click on the SALTO Doors item in the hardware tree. All of the SALTO Doors will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the SALTO Door to be edited and click on the edit button within the ribbon, or double click the SALTO Door to be edited. You can also select edit from the right click menu.

When a modification to an offline lock is made it must be updated using the SALTO Programming device (PPD).

Deleting a SALTO Door

To delete a SALTO Door, go to the SALTO Doors entry screen by clicking on the SALTO Door icon within the Hardware group of the Navigation pane. Then, click on the SALTO Doors item in the hardware tree. All of the SALTO Doors will then be displayed in the right

window pane of the Access It! Universal.NET desktop. Select the SALTO Door to be deleted and click on the delete button within the ribbon or select delete from the right click menu.

Once a SALTO Door has been deleted, cards will continue to be granted access until deleted within the SALTO ProAccess SPACE application.

SALTO Doors Detail

[SaltoDoors](#)

The SALTO SHIP (SALTO Host Interface Protocol) is an integration between SALTO ProAccess SPACE and Access It! Universal.NET. This integration allows for managing users and basic hardware configuration of offline and online SALTO locksets within the Access It! Universal.NET application. SALTO keys are referred to as cards within Access It! Universal.NET. The SHIP integration allows the key/card to encode its own access database and event trail directly to the card. This allows for offline locks to be used without the need for a central repository.

The SHIP integration requires Doors, Timezones, and Calendars be managed within ProAccess SPACE.

Access to this screen is determined by the settings for the currently logged in user. SALTO Door permissions inherit their settings from the reader settings for the user group. For more information on users, see the [Users](#) help file topic.

SALTO Door Name

Enter the name to be used for this SALTO Door. It is recommended that a friendly name be assigned to all of the SALTO Doors being used. An example of a friendly name would be "Dorm Room 101". The SALTO Door name can be up to 24 characters in length.

SALTO Door Description

Enter the friendly description to be used for this SALTO Door. This field is used for informational purposes only. The SALTO Description name can be up to 54 characters in length.

Open Mode

The open mode defines how the SALTO Door functions. The available modes are:

- Standard - *The lock only opens when an authorized key is used.*
- Office - *The lock can be unlocked by any user who has the Office option selected in their user profile and has access to the door. To activate Office mode, present the key to the lock, while keeping the inner handle pressed down. To disable the Office mode, repeat the procedure.*
- Timed Office - *This is the same as the Office mode detailed above except that the Office mode is only allowed during defined time periods (e.g., 08:00 to 15:00). The time periods must be previously defined.*

- *Automatic Opening - The lock unlocks automatically at specific times and remains open during a defined time period (e.g., 08:00 to 18:00). At the end of each time period, the lock closes and reverts to Standard mode. It is essential to set an access point timed period for this mode.*
- *Toggle - The lock can be unlocked by any authorized user that presents a valid key. You do not need to hold down the inner handle. The next authorized key presented then closes the door. This continues switching (toggling) on presentation of each valid key.*
- *Timed Toggle - This mode operates in the same way as the Toggle mode described above. However, you can only toggle the option on and off within set access point timed periods.*
- *Keypad Only - The lock can be opened at any time by typing a valid code on a keypad. The keypad code must contain between one and eight digits and is the same for every user. When you select the Keypad only option from the Open mode drop-down list, a keypad code field is displayed in which you can define the code. The lock can also be opened with a valid key.*
- *Timed Keypad - This mode is the same as the Keypad only mode described above except that the Keypad only mode is only allowed during a defined timed period. The lock can be opened with a key at any time.*
- *Key + PIN - The lock can only be opened using both a valid key and by typing a valid PIN on the keypad. This acts as a dual security control. If the PIN code is incorrect, access will not be granted. The PIN must be defined in the cards screen.*
- *Timed Key + PIN - This is the same as the Key + PIN mode above except that the Key + PIN mode is only allowed during specific time periods. Outside of these time periods, the lock operates in Standard mode.*
- *Automatic Opening + Office - This mode works in the same way as the Automatic opening mode. However, outside of the timed period, the lock reverts to Office mode rather than Standard mode.*
- *Automatic Opening + Toggle - This mode is the same as Automatic + Office mode except that outside of the timed period the lock reverts to the Toggle mode.*
- *Automatic Changes - This 'mode' acts as an indication that the lock will work with a mixture of modes during certain time periods throughout the day. The combination of modes are defined in an automatic changes entry, for example, Automatic change#001. Automatic change schedules must be defined in SALTO ProAccess SPACE.*

Open Period

The open period is the time schedule to be used in conjunction with timed open modes.

Keypad Code

The keypad code is the code used in conjunction with keypad open modes.

Open Time

The open time is the amount of time that the door handle will remain active after a valid key has been presented. The door locks as soon as the handle is released, even if the time value is not reached. The default time value is six seconds. The value can be increased or decreased in the range 0 to 255 seconds.

Increased Open Time

Enter the amount of time that the door handle will remain active after a valid key, that has the extended access times option enabled, has been presented. Used typically for ADA solutions.

Audit on keys

Select (check) this option in order for offline locks to log the key's access events upon presentation as long as the key's memory is not full. When the key is used at an online lock, the event history is uploaded to Access It! Universal.NET. This requires the Audit openings in the key option to be enabled within the cardholders card screen.

Antipassback enabled

SALTO license dependent feature. Select (check) this option to enable the use of Antipassback (APB) and have the lock move a key from the inside to outside area. Ensures that a user cannot enter through the same door multiple times until they have first exited the door (or until a specified time period has passed). This is to prevent a key being used by a number of different users.

Outward antipassback

SALTO license dependent feature. Select (check) this option to enable the use of Antipassback (APB) and have the lock move a key from the outside to inside area. Ensures that a user cannot enter through the same door multiple times until they have first exited the door (or until a specified time period has passed). This is to prevent a key being used by a number of different users.

Update required

Indicates if an offline lock is pending an update. Updates require the use of the SALTO Portable Programming Device (PPD).

Battery status

Indicates the current battery status of the lock.

Event Type

SALTO Door events (transactions) are recorded in the event file every time there is a card or PIN presented at the SALTO Door. SALTO Door events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

When using offline locks, the Audit on key option must be enabled for the both lock and card in order for the event transaction to be recorded.

The following event types are supported:

- *End of DLO (door left opened).*-A door closed after being held open
- *Door left opened (DLO).*-A door entered a held open state
- *Door programmed with spare key.*-A door was programmed using a spare key
- *Hotel guest cancelled.*-A hotel guest key was cancelled
- *Blacklisted key deleted.*-A key on the blacklist was presented to a online reader and deleted
- *Access denied: hotel guest key cancelled.*-A key was denied because it was originally a hotel guest can and has since been cancelled
- *Access denied: key does not override privacy.*-A key was denied because it was presented while the lock was in privacy mode
- *Access denied: antipassback.*-A key was denied because of a violation to Antipassback (APB) procedures
- *Access denied: invalid PIN.*-A key was denied due to an invalid PIN being entered
- *Access denied: out of time.*-A key was denied due to being presented outside of its valid schedule
- *Access denied: key cancelled.*-A key was denied due to it being cancelled
- *Access denied: key not allowed in this door.*-A key was denied due to not having access to the door
- *Access denied: key no activated.*-A key was denied due to not yet being activated
- *Access denied: unable to audit on the key.*-A key was denied due to the audit trail being unable to be stored onto the key
- *Access denied: key with data manipulated.*-A key was denied due to the data onboard being corrupted or manipulated
- *Access denied: door in emergency state.*-A key was denied due to the door being in a state of emergency
- *Access denied: key expired.*-A key was denied due to the key being expired
- *Access denied: run out of battery.*-A key was denied due to the lock battery being critically low
- *Expiration automatically extended (offline).*-A key was presented at an offline lock and

was revalidated

- *Warning: key has not been completely updated (online).* -A key was presented to a online lock and did not fully complete a data update
- *Key deleted (online).* -A key was presented to an online reader and deleted
- *Key updated (online).* -A key was presented to an online reader and internal data was updated
- *End of privacy.* -A lock ended privacy mode
- *Start of privacy.* -A lock entered privacy mode
- *Key updated in "out of site" mode (online).* -A lock operating in out of site mode updated a key
- *Guest new key.* -A new guest key was created
- *New hotel guest key.* -A new hotel guest key was issued
- *End of office mode.* -A offline lock ended office mode
- *Start of office mode.* -A offline lock entered office mode
- *Door has restored communication with the host.* -A online door resumed communicating to the host
- *Door has lost communication with the host.* -A online door stopped communicating to the host
- *End of office mode (online).* -A online lock ended office mode
- *Start of office mode (online).* -A online lock entered office mode
- *Closing not allowed: door in emergency state.* -A relock command was issued but unable to complete due to the door being in a state of emergency
- *RF Lock updated.* -A RF Lock was updated
- *PPD connection.* -A SALTO Programming device connected to a lock
- *Door closed: key.* -Door mode configured for toggle and relocked through the use of a key
- *Door closed: key and keyboard.* -Door mode configured for toggle and relocked through the use of a key and keypad
- *Door closed: keyboard.* -Door mode configured for toggle and relocked through the use of a keypad
- *Low battery level.* -The battery level of a lock is low
- *Door opened: key and keyboard.* -The door opened through use of a key presented and a keyboard entered
- *Door opened: key.* -The door opened through use of a key presented to the reader
- *Door opened: inside handle.* -The door opened through use of the inside handle
- *Door opened: online command.* -The door was opened through use of a command from the host software
- *Door opened: spare card (hotel).* -The door was opened through use of a hotel spare key
- *Door opened: mechanical key.* -The door was opened through use of a mechanical key
- *Door opened: multiple guest key.* -The door was opened through use of a multi-issued guest key
- *Door opened: PPD.* -The door was opened through use of the SALTO programming

device (PPD)

- *Host has lost communication with the door.*-The host lost communication to a door
- *Host has restored communication with the door.*-The host resumed communication to a door
- *End of forced closing (online).*-The lock ended emergency closing mode
- *End of forced opening (online).*-The lock ended emergency opening mode
- *Start of forced closing (online).*-The lock entered emergency closing mode
- *Start of forced opening (online).*-The lock entered emergency opening mode
- *Automatic change.*-The lock went through an automatic change of door mode
- *Time modified (daylight saving time).*-The time of a lock changed due to daylight savings
- *RF Lock date and time updated.*-The time on a RF lock was changed
- *Door opened: unique opening.*-
- *Door opened: switch.*-
- *Door opened: keyboard.*-
- *Door most probably opened: key and PIN.*-
- *Access denied: key out of date.*-
- *Access denied: old hotel guest key.*-
- *Access denied: no associated authorization.*-
- *Access denied: unique opening key already used.*-
- *Access denied: key with old renovation number.*-
- *Access denied: locker occupancy timeout.*-
- *Access denied: denied by host.*-
- *Door closed: switch.*-
- *Key inserted (energy saving device).*-
- *Key removed (energy saving device).*-
- *Room prepared (energy saving device).*-
- *Alarm: intrusion (online).*-
- *End of intrusion.*-
- *Alarm: tamper (online).*-
- *End of tamper.*-
- *Online peripheral updated.*-
- *New renovation code for key (online).*-
- *New renovation code.*-
- *Incorrect clock value.*-

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

[Salto Doors](#)

Access Levels

[Access Levels Detail](#)

Access levels are combinations of timezones, floor codes and readers (doors/elevators) that are used to give a cardholder access to a door, elevator or a group of doors or elevators during a certain time. Access It! Universal.NET supports up to 32,767 access levels for each site.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding an Access Level

To add an access level, go to the access levels entry screen by clicking on the Access Levels icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu.

Editing an Access Level

To edit an access level, go to the access levels entry screen by clicking on the Access Levels icon within the Configuration group of the Navigation pane. Select the access level to be edited and click on the edit button on the toolbar, or double click the access level to be edited. You can also select edit from the right click menu.

Deleting an Access Level

To delete an access level, go to the access levels entry screen by clicking on the Access Levels icon within the Configuration group of the Navigation pane. All of the access levels in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the access level to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu.

Printing Access Level Reports

To print reports for an access level, go to the access levels entry screen by clicking on the Access Levels icon within the Configuration group of the Navigation pane. All of the access levels in the database will then be displayed in the right window pane of the Access It! Universal desktop. Select the access levels to print reports for and click on the Reports button within the ribbon or from the right click menu select print reports. The following reports are available:

- *Access By Access Level* - This report provides a list of all card holders and cards that

have been assigned the selected access levels.

- *Access Level History* - This report provides a list of all database updates for the selected access levels.
- *Access Level Listing* - This report provides a list of the selected access levels and their various properties.
- *Temporary Access By Access Level* - This report provides a list of all cardholders and cards that have been assigned the selected temporary access levels.

Access Levels Detail

Access Levels

Access levels are combinations of timezones, floor codes and readers (doors/elevators) that are used to give a card or a cardholder access to a door, elevator or a group of doors or elevators during a certain time. Access It! Universal.NET supports up to 32,000 access levels for each site.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Access Level Name

Enter the name to be used for this access level. It is recommended that a friendly name be assigned to all of the access levels being used. An example of a friendly name would be "All Doors During Office Hours". The access level name can be up to 50 characters in length.

Timezone

Select the timezone to be used for all of the selected readers being assigned to the access level. Only one timezone can be selected at a time, so when readers are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned reader it must be moved back to the available window, then re-assigned with the new timezone.

Readers/Timezone Access

To assign readers to an access level, select the timezone and the desired reader(s), then "move" the readers that you wish to be assigned to the access level from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected readers from the available window to the assigned window. The "<<" button will move all selected readers from the assigned window to the available window. Multiple readers can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired readers.

Only readers that are not setup with an elevator access configuration type will be displayed on this tab. For more information on reader access configurations, see the [Readers](#) help file topic.

Reader/Floor Code Access

Select the floor code to be used for all of the selected elevator readers being assigned to the access level. Only one floor code can be selected at a time, so when elevator readers are

being assigned for different floor codes, they must be selected individually or in groups by the desired floor code. To change a floor code for an assigned elevator reader it must be moved back to the available window, then re-assigned with the new floor code.

Available/Assigned Readers/Floor Codes

To assign elevator readers to an access level, select the floor code and the desired elevator reader(s), then "move" the elevator readers that you wish to be assigned to the access level from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected elevator readers from the available window to the assigned window. The "<<" button will move all selected elevator readers from the assigned window to the available window. Multiple elevator readers can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired elevator readers.

Only readers that are setup with an elevator access configuration type will be displayed on this tab. For more information on reader access configurations, see the [Readers help file topic](#).

IP Lockset/Timezone Access

Select the timezone to be used for all of the selected IP locksets being assigned to the access level. Only one timezone can be selected at a time, so when IP locksets are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned IP lockset it must be moved back to the available window, then re-assigned with the new timezone.

IP lockset licenses much be purchased separately. This tab will only be visible if one or more IP lockset licenses have been purchased.

Available/Assigned IP Locksets/Timezones

To assign IP locksets to an access level, select the timezone and the desired IP lockset(s), then "move" the IP locksets that you wish to be assigned to the access level from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected IP locksets from the available window to the assigned window. The "<<" button will move all selected IP locksets from the assigned window to the available window. Multiple IP locksets can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired IP locksets.

IP lockset licenses much be purchased separately. This tab will only be visible if one or more IP lockset licenses have been purchased.

SALTO Door/Timezone Access

Select the timezone to be used for all of the selected SALTO Doors being assigned to the

access level. Only one timezone can be selected at a time, so when SALTO Doors are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned SALTO Door it must be moved back to the available window, then re-assigned with the new timezone.

SALTO Door integrated reader licenses must be purchased separately. This tab will only be visible if the SALTO integration is enabled.

Timezones must be configured within SALTO ProAccess SPACE.

Available/Assigned SALTO Doors/Timezones

To assign SALTO Doors to an access level, select the timezone and the desired SALTO Door(s), then "move" the SALTO Doors that you wish to be assigned to the access level from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected SALTO Doors from the available window to the assigned window. The "<<" button will move all selected SALTO Doors from the assigned window to the available window. Multiple SALTO Doors can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired SALTO Doors.

SALTO Door integrated reader licenses must be purchased separately. This tab will only be visible if the SALTO integration is enabled.

Timezones must be configured within SALTO ProAccess SPACE.

Activate Date/Time

If this box is checked, the Access Level will become active at the date/time entered. When used there must be a corresponding Deactivate Date/Time.

Deactivate Date/Time

If this box is checked, the Access Level will become inactive at the date/time entered. When used there must be a corresponding Activate Date/Time.

Escort Mode

The escort mode is used to create access levels which require a cardholder to have an escort. When a cardholder requires an escort, a cardholder with escort privileges must present their card at the same reader within 15 seconds of the cardholder requiring escort. If multiple access levels for the same reader/door are applied to the same card, the most restrictive access level will take precedence. For instance, if a card or cardholder or some combination of card and cardholder is assigned an access level which makes that card an escort but that same card/cardholder is also assigned an access level that requires an escort, that card will require an escort.

- *Cards with this Access Level are not an escort* - If this option is selected, cardholders assigned this access level will not be escorts. If a cardholder who is not an escort

presents their card within 15 seconds following a cardholder requiring an escort, they will not be granted access unless an escort card is presented. They have the option of presenting their card again after receiving an access denied, at which time they should be granted access, provided a cardholder requiring an escort does not present before them.

- *Cards with this Access Level are an escort* - If this option is selected, cardholders assigned this access level will be escorts.
- *Cards with this Access Level require an escort* - If this option is selected, cardholders assigned this access level will require an escort for doors assigned this access level.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Company

Select the company that this access level will be assigned to. If a company is selected only users with permissions to the selected company will have access to this access level. This access level can also be assigned to all companies which is useful for a shared perimeter access level. Companies are used to partition access levels within a site. For more information on companies, see the [Companies](#) help file topic. For more information on users, see the [Users](#) help file topic.

Companies licenses must be purchased separately. This tab will only be visible if the Company feature has been purchased.

Save/Close Buttons

Clicking on the save button will save the changes made to the access level. Clicking on the cancel button will not save the changes made to the access level.

[Access Levels](#)

Floor Codes

[Floor Codes Detail](#)

Floor Codes are combinations of timezones and outputs (floors) that are used to give a card holder access to an elevator or a group of elevators. Access It! Universal.NET supports up to 255 floor codes per site. Each of the floor codes can support up to 64 outputs (floors).

The name of the No Floor Access floor code can be changed but the data cannot be edited. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Floor Code

To add a floor code, go to the floor code entry screen by clicking on the Floor Code within the Configuration group of the Navigation pane. All of the floor codes in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the toolbar or select new from the right click menu.

Editing a Floor Code

To edit a floor code, go to the floor code entry screen by clicking on the Floor Code within the Configuration group of the Navigation pane. All of the floor codes in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the floor code to be edited and click on the edit button on the toolbar, or double click the floor code to be edited. You can also select edit from the right click menu.

Deleting a Floor Code

To delete a floor code, go to the floor code entry screen by clicking on the Floor Code within the Configuration group of the Navigation pane. All of the floor codes in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the floor code to be deleted and click on the delete button on the toolbar or select delete from the right click menu.

Printing Floor Code Reports

To print reports for a floor code, go to the floor code entry screen by clicking on the Floor Code within the Configuration group of the Navigation pane. All of the floor codes in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the floor codes to print reports for and click on the Report button within the ribbon or select print reports from the right click menu. The following reports are available:

- *Floor Code History* - This report provides a list of all database updates for the selected floor codes.
- *Floor Code Listing* - This report provides a list of the selected floor codes and their various properties.

Floor Codes Detail

Floor Codes

Floor Codes are combinations of timezones and outputs (floors) that are used to give a card holder access to an elevator or a group of elevators. Access It! Universal.NET supports up to 255 floor codes per site. Each of the floor codes can support up to 64 outputs (floors).

The name of the No Floor Access floor code can be changed but the data cannot be edited. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Floor Code Name

Enter the name to be used for this floor code. All of the floor codes have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the floor codes being used. An example of a friendly name would be "Floors 5-8 During Office Hours". The floor code name can be up to 50 characters in length.

Timezone

Select the timezone to be used for all of the selected outputs (floors) being assigned to the floor code. Only one timezone can be selected at a time, so when outputs are being assigned for different timezones, they must be selected individually or in groups by the desired timezone. To change a timezone for an assigned output it must be moved back to the available window, then re-assigned with the new timezone.

Reader

Select the reader to display the floor descriptions from. If no reader is selected floor names will be displayed by output number instead of the "friendly" floor name assigned to the individual elevator readers.

Available/Assigned Outputs/Timezones

To assign outputs (floors) to a floor code, select the timezone and the desired output(s), then "move" the outputs that you wish to be assigned to the floor code from the available window to the assigned window. This is accomplished by using the ">>" and "<<" buttons. The ">>" button will move all selected outputs from the available window to the assigned window. The "<<" button will move all selected outputs from the assigned window to the available window. Multiple outputs can be selected by holding down the <Ctrl> key on the keyboard while selecting (clicking) the desired outputs.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the floor code. Clicking on the close button will not save the changes made to the floor code.

Intervals

[Intervals Detail](#)

Intervals are used to determine when timezones will be active or inactive. All intervals can be set up to accommodate varying time schedules on different days of the week and during holidays. Access It! Universal.NET supports an unlimited number of intervals per site. The Always interval is predefined and assigns 24 hours a day to all days of the week including holidays.

The name of the "Always" interval can be changed but the data cannot be edited and it cannot be deleted. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. For more information on timezones, see the [Timezones](#) help file topic.

Adding an Interval

To add an interval, go to the intervals entry screen by clicking on the Intervals icon within the Configuration group of the Navigation pane. All of the intervals in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button within the ribbon or from the right click menu.

Editing an Interval

To edit an interval, go to the intervals entry screen by clicking on the Intervals icon within the Configuration group of the Navigation pane. All of the intervals in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the interval to be edited and click on the edit button within the ribbon, or double click the interval to be edited. You can also select edit from the right click menu.

Deleting an Interval

To delete an interval, go to the intervals entry screen by clicking on the Intervals icon within the Configuration group of the Navigation pane. All of the intervals in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the interval to be deleted and click on the delete button on the toolbar or select delete from the right click menu.

Intervals Detail

Intervals

Intervals are used to determine when timezones will be active or inactive. All intervals can be set up to accommodate varying time schedules on different days of the week and during holidays. Access It! Universal supports an unlimited number of intervals per site. The Always interval is predefined and assigns 24 hours a day to all days of the week including holidays.

The name of the "Always" interval can be changed but the data cannot be edited and it cannot be deleted. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. For more information on timezones, see the [Timezones](#) help file topic.

Interval Name

Enter the name to be used for this interval. It is recommended that a friendly name be assigned to all of the intervals being used. An example of a friendly name would be "M,Tu,W,Th,F 08:00-16:59". The interval name can be up to 50 characters in length. When building a new Interval, the Interval name is dynamically created,

Start Time

Select or enter the start time for this interval. The start time is the time at which any timezones that contain this interval will become active on the days of the week and holiday groups specified.

End Time

Select or enter the end time for this interval. The start time is the time at which any timezones that contain this interval will become inactive on the days of the week and holiday groups specified.

Days of Week

Select the days of the week to be used for this interval. The days of the week are the days at which any timezones that contain this interval will become active or inactive on the selected days at the start and end times specified.

Holiday Groups

Select the holiday groups to be used for this interval. When a holiday group is included (checked) in an interval, all of the holidays that belong to the selected holiday group will be

included in the interval. This means that any timezones that contain this interval will be active on any of the holidays in the holidays file that belong to the corresponding holiday group at the start and end times specified.

When a holiday group is selected within an interval, an entry must be made within the holidays data entry screen to define any dates as holidays that are to be included within this interval. For more information on holidays, see the [Holidays](#) help file topic.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the interval. Clicking on the close button will not save the changes made to the interval.

Timezones

[Timezones Detail](#)

Timezones are used to determine when a card holder has access to a door, or when a door is to be unlocked. All timezones can have up to twelve intervals that can be set up to accommodate varying time schedules on different days of the week. Access It! Universal.NET supports up to 255 timezones per site. The Always timezone has the predefined interval named "Always", which assigns 24 hours a day to all days of the week including holidays. The Never timezone has no predefined intervals and will never allow access to, or unlock any doors during any days of the week. The calendar and graph at the bottom of the timezones window determines whether a timezone is active or inactive during a specific day and time. Green sections on the graph display when the selected timezone will be active. Red sections on the graph display when the selected timezone will be inactive. **The name of the "Always" and "Never" timezones can be changed but the data cannot be edited and they cannot be deleted. Access to this screen is determined by the settings for the currently logged in user. For more information on intervals, see the [Intervals](#) help file topic. For more information on users, see the [Users](#) help file topic.**

Adding a Timezone

To add a timezone, go to the timezones entry screen by clicking on the Timezones icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu.

Editing a Timezone

To edit a timezone, go to the timezones entry screen by clicking on the Timezones icon within the Configuration group of the Navigation pane. Select the timezone to be edited and click on the edit button on the toolbar, or double click the timezone to be edited. You can also select edit from the right click menu.

Deleting a Timezone

To delete a timezone, go to the timezones entry screen by clicking on the Timezones icon within the Configuration group of the Navigation pane. All of the timezones in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the timezone to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu.

Printing Timezone Reports

To print reports for a timezone, go to the timezones entry screen by clicking on the Timezones icon within the Configuration group of the Navigation pane. All of the timezones in the database will then be displayed in the right window pane of the Access It! Universal desktop. Select the timezones to print reports for and click on the Reports button within the ribbon or from the right click menu select print reports. The following reports are available:

- *Timezone History* - This report provides a list of all database updates for the selected timezones.
- *Timezone Listing* - This report provides a list of the selected timezones and their various properties.
- *Timezone Utilization Listing* - This report provides a list of the selected timezones as well as where the timezones are being used.

Timezones Detail

Timezones

Timezones are used to determine when a card holder has access to a door, or when a door is to be unlocked. All timezones can have up to twelve intervals that can be set up to accommodate varying time schedules on different days of the week. Access It! Universal.NET supports up to 255 timezones per site. The Always timezone has the predefined interval named "Always", which assigns 24 hours a day to all days of the week including holidays. The Never timezone has no predefined intervals and will never allow access to, or unlock any doors during any days of the week. The calendar and graph at the bottom of the timezones window determines whether a timezone is active or inactive during a specific day and time. Green sections on the graph display when the selected timezone will be active. Red sections on the graph display when the selected timezone will be inactive. **The name of the "Always" and "Never" timezones can be changed but the data cannot be edited and they cannot be deleted. Access to this screen is determined by the settings for the currently logged in user. For more information on intervals, see the [Intervals](#) help file topic. For more information on users, see the [Users](#) help file topic.**

Timezone Name

Enter the name to be used for this timezone. It is recommended that a friendly name be assigned to all of the timezones being used. An example of a friendly name would be "Office Hours". The timezone name can be up to 50 characters in length.

Default Timezone Mode

Select the default timezone mode for this timezone. The default timezone mode sets the manner in which a timezone will respond to the intervals defined for the timezone. The following default timezone modes are supported:

- *Always Inactive* - The timezone will always be inactive and any defined intervals will be ignored. When set to this mode, the timezone can only be activated using a task. This mode is generally used for special timezones that are only to be activated when a card holder from a specific card group enters the area first.
- *Always Active* - The timezone will always be active and any defined intervals will be ignored. When set to this mode, the timezone can only be deactivated using a task. This mode is generally used for special timezones that are only to be deactivated during "threat level" or hazardous situations.
- *Normal* - The timezone will operate normally and all defined intervals will be processed according to the defined days and times. This is the most common setting.
- *One-Time Event* - The timezone will only if the Activate Date matches the current date

AND any of the defined Start/End Time intervals is active.

The default timezone mode will take effect whenever a change is made to any timezone's settings, or when the SCP panel has been reset or lost power. Any timezone commands sent will only result in a temporary timezone mode change.

Activate Date

Specify the date for which this Timezone will be active. This entry is only available for Timezone Mode -- One-Time Event.

Start Time/End Time

Specify the Start and End Times that this Timezone will be active during. This entry is only available for Timezone Mode -- One-Time Event

Intervals

Click on the add intervals button to add intervals to this timezone. Only one interval needs to be set up to enable a timezone, but up to 12 can be used if desired. The start time for the interval being added is when the timezone will become active and the end time for the interval being added is when the timezone will become inactive. For example, if a door has an unlock during timezone set to a timezone that has a start time of 08:00 AM and an end time of 05:00 PM, then the door will be unlocked from 08:00 AM to 05:00 PM on the specified days of the week or holidays. Intervals are only available for Timezone Modes of *Always Active*, *Always Inactive* and *Normal*

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the timezone. Clicking on the close button will not save the changes made to the timezone.

Holidays

[Holidays Detail](#)

Holidays are used to define specified dates as holidays. Dates defined as holidays can be used within timezone intervals to be controlled by a timezone. A day becomes a holiday instead of the day of the week in a timezone interval when the specified holiday date matches the current system date. Access It! Universal.NET supports up to 255 holidays per site.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Holiday

To add a holiday, go to the holidays entry screen by clicking on the Holidays icon within the Configuration group of the Navigation pane. All of the holidays in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the toolbar or select new from the right click menu.

Editing a Holiday

To edit a holiday, go to the holidays entry screen by clicking on the Holidays icon within the Configuration group of the Navigation pane. All of the holidays in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the holiday to be edited and click on the edit button on the toolbar, or double click the holiday to be edited. You can also select edit from the right click menu.

Deleting a Holiday

To delete a holiday, go to the holidays entry screen by clicking on the Holidays icon within the Configuration group of the Navigation pane. All of the holidays in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the holiday to be deleted and click on the delete button on the toolbar or select delete from the right click menu.

Printing Holiday Reports

To print reports for a holiday, go to the holidays entry screen by clicking on the Holidays icon within the Configuration group of the Navigation pane. All of the holidays in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the holidays to print reports for and click on the print button on the toolbar or select print from the right click menu. The following reports are available:

- *Holiday History* - This report provides a list of all database updates for the selected holidays.
- *Holiday Listing* - This report provides a list of the selected holidays and their various properties.

Holidays Detail

[Holidays](#)

Holidays are used to define specified dates as holidays. Dates defined as holidays can be used within timezone intervals to be controlled by a timezone. A day becomes a holiday instead of the day of the week in a timezone interval when the specified holiday date matches the current system date. Access It! Universal.NET supports up to 255 holidays per site.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Holiday Name

Enter the name to be used for this holiday. All of the holidays have predefined names that can be used if desired. It is recommended however, that a friendly name be assigned to all of the holidays being used. An example of a friendly name would be "Schnauzer Appreciation Day". The holiday name can be up to 50 characters in length.

Holiday Date

Select or enter the date to be defined as a holiday. To enable the holiday date field, either click on the drop down to bring up the calendar, or click the check box in the holiday date field and enter a date manually.

Holiday Duration

Select the duration in days of the holiday. All of the days for the number of days selected for the holiday duration, starting with the holiday date will be defined as a holiday. The holiday duration is useful if a holiday spans several days or weeks so that only one holiday entry needs to be defined to cover the entire holiday duration. The holiday duration can range from 1 day to 364 days.

Holiday Groups

Select (check) the holiday groups in which this holiday should be included. When a holiday is included in a holiday group, any of the holidays in the same holiday group will automatically override as a holiday instead of the day of the week within any of the timezones that have the same holiday group selected. A holiday can belong to a single group or multiple groups. Holiday groups are useful when two or more groups of employees have differing holiday schedules throughout the year.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the holiday. Clicking on the close button will not save the changes made to the holiday.

Badge Types

Badge types are used to determine the physical layout, appearance and contents of a card when it is printed or previewed. Badge types can range from simple visitor cards with static text, to complex card designs with corporate logos, pictures and signatures. Badge types are designed with the badge designer, for more information on the badge designer, see the [Badge Designer](#) help file topic.

Badging is an optional feature and will not be displayed if not purchased. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Badge Type

To add a badge type, go to the badge types screen by clicking on the badge types toolbar button within the configuration group on the toolbar. All of the badge types in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the toolbar or select new from the right click menu.

Editing a Badge Type

To edit a badge type, go to the badge types entry screen by clicking on the Badge Types icon within the Configuration group of the Navigation pane. All of the badge types will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the badge type to be edited and click on the edit button on the toolbar, or double click the badge type to be edited. You can also select edit from the right click menu.

Deleting a Badge Type

To delete a badge type, go to the badge types entry screen by clicking on the Badge Types icon within the Configuration group of the Navigation pane. All of the badge types will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the badge type to be deleted and click on the delete button on the toolbar, or hit the delete key on the keyboard. You can also select delete from the right click menu.

The next step is to use the badge designer to edit the design of the badge type. For more information on using the badge designer, see the [Badge Designer](#) help file topic.

Badge Designer

The badge designer is used to create new or modify existing badge type designs. Badge types can be designed with many different styles and functions. For more information on badge types, see the [Badge Types](#) help file topic.

Objects are added to the badge type design and properties are set to determine the functionality of these objects. Single or dual sided badge types are fully supported.

The first step when designing a badge type is to set the overall badge properties. These properties control the way the card is formatted and printed. For more information on badge properties, see the [Badge Properties](#) help file topic.

The second step when designing a badge type is to add objects to the badge type design and set their properties. For more information on badge designer objects see any of the badge designer object help file topic.

The third step when designing a badge type is to save the changes to the badge type and preview the card to see the results. For more information on previewing cards, see the [Previewing Cards](#) help file topic.

The following formatting functions are supported in the badge designer and can be accessed in the toolbar or right click menus:

Align

The align function is used to align a single object or multiple objects with either each other or the badge designer grid. To access the align functions, either click on one of the align function toolbar buttons. In addition, when an object is dragged and placed near another object, friendly grid lines appear to assist in aligning objects together. The following align functions are supported:

- *To Grid* - This function will align a single or multiple objects to the closest grid snap location. To select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected.
- *Lefts* - This function will left align multiple objects to the same left badge location. To select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.
- *Centers* - This function will center align multiple objects to the same center badge location. To select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.
- *Rights* - This function will right align multiple objects to the same right badge location. To

select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.

- *Tops* - This function will top align multiple objects to the same top badge location. To select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.
- *Middles* - This function will middle align multiple objects to the same middle badge location. To select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.
- *Bottoms* - This function will bottom align multiple objects to the same bottom badge location. To select multiple objects to align, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.

Make Same Size

The make same size function is used to make multiple objects the same physical size. To access the make same size functions, either click on one of the make same size function toolbar buttons, or by selecting make same size from the format...make same size option on the system menu. The following make same size functions are supported:

- *Widths* - This function will make the widths of multiple objects the same physical size. To select multiple objects to make the same size, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.
- *Heights* - This function will make the heights of multiple objects the same physical size. To select multiple objects to make the same size, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.
- *Both* - This function will make both the widths and the heights of multiple objects the same physical size. To select multiple objects to make the same size, hold down the <Ctrl> key while clicking on each of the objects to be selected. If only one object is selected, this function will not be available.

Horizontal Spacing

The make horizontal spacing equal function is used to make multiple objects spaced out evenly across a horizontal plane. To access the make horizontal spacing equal function, select the make horizontal spacing equal function from the horizontal spacing...make equal option on the system menu. If two or fewer objects are selected, this function will not be available.

Vertical Spacing

The make vertical spacing equal function is used to make multiple objects spaced out evenly across a vertical plane. To access the make vertical spacing equal function, select the make vertical spacing equal function from the vertical spacing...make equal option on the system menu. If two or fewer objects are selected, this function will not be available.

Order

The order function is used to set the front to back (top to bottom) order of a single object or multiple objects. To access the order functions, select the order functions from the order option on the system menu.

- *Send to Front* - This tool will bring the selected object(s) to the top of the designer and will be in front of all other objects.
- *Send to Back* - This tool will bring the selected object(s) to the bottom of the designer and will be behind of all other objects.

Badge Properties

The badge properties control the way a badge type design is formatted and printed. To access the badge properties, either click on the properties toolbar button with no objects selected, or by selecting properties from the file option on the system menu.

The following badge properties are supported:

Designer

- *Show grid*
This function turns on and off the display of the formatting grid.
- *Snap to grid*
This function turns on and off the snap to grid option of the formatting grid. It is recommended that this option be left on to make it easier to line up objects within the map design.
- *Grid Spacing*
This option controls for how close the grid dots or lines are spaced between each other.
- *Grid mode*
This option controls how the background grid is displayed. Available options are dots or lines.
- *Show dimension lines*
This option controls if dimension lines are displayed when an object is dragged and dropped in the designed. Dimension lines are the measurements displayed in relation to the edge of the badge designer.
- *Snap to line*
This option controls if an object will snap to the grid as it is dragged and dropped in the designer.
- *Designer Units*
This option determines if measurements in the designer will use inches or centimeters.

Badge

- *Printer*
Select the printer to be used as the default when printed.
- *Card Size*
Select the card size to be displayed in the designer. Available options are printer specific.
- *Card Bin*
Select the card bin to be used when printing. Available options are printer specific.
- *Height*

Used in conjunction with the custom page size. Sets the height of the page in the designer.

- *Width*

Used in conjunction with the custom page size. Sets the width of the page in the designer.

- *Orientation*

This option controls if the page will be orientated as portrait or landscape. Select portrait for top to bottom orientation or landscape for left to right orientation.

- *Dual Sided*

Select this option if the badge being created has both a front and back to be designed. When selected, the option to design the back of the badge will be available in the left-hand explorer window.

Verify that the printer selected supports duplex printing before using this option.

- *Prompt for alternate printer when printing*

Select this option to populate a print dialog box when printing the badge type. This allows for specifying different printers and printer-specific settings upon print.

Margins

- *Left*

Configure the margin space to be used for the left of the badge.

- *Right*

Configure the margin space to be used for the right of the badge.

- *Top*

Configure the margin space to be used for the top of the badge.

- *Bottom*

Configure the margin space to be used for the bottom of the badge.

Script

Enter any desired optional code for the badge type design. Code can be used for things such as mag stripe encoding when a card is being printed.

Badge type code can be very complex and is only recommended for advanced users. Improper use of the code function can result in erratic card printing and application malfunction.

Photo

The photo object is used to add a badge holder picture to the badge type design. To add a picture object to the badge type design, expand the badge data menu by clicking on badge data, then click on the photo icon and drag it to the desired location on the badge type design. A picture object will then be placed on the badge type design at the default size. The picture object should then be moved to the correct location on the badge type design by clicking anywhere inside the picture object and dragging it to the desired location. The picture object should then be resized by clicking on any of the handles on the picture object and dragging it to the desired size. The picture object properties should then be set by modifying the object properties in the right-hand properties menu.

The following properties are supported for the picture object:

Image

- *Size mode*
This option adjusts the size of the picture. Options are to fit the photo to match the objects size (fit), fit the photo to match the object size and retain proportions (fit proportional), or retain the images size, but force to be in the objects shape (clip).
- *Horizontal alignment*
This option controls how the photo is horizontally aligned in the objects shape. Options are to align left, center, or right.
- *Vertical alignment*
This option controls how the photo is vertically aligned in the objects shape. Options are to align top, middle, or bottom.
- *Transparency Tolerance*
This option determines how "transparent" the picture will be. Valid entries are from 0 (not transparent) to 255 (completely transparent). This option is generally used to obtain "floating head" or "security badges", making the badge more difficult to duplicate. This option is most useful when the pictures are taken against a solid colored background.
- *Flip/rotate*
This option allows for flipping or rotating the image. Options are None, Rotate 90, Rotate 180, Rotate 270, Flip Horizontally, Rotate 90 Flip Horizontally, Flip Vertically, and Rotate 90 Flip Vertically,
- *Image transparency*
This option controls the transparency of the photo. Valid entries are 0 (completely transparent) and 255 (no transparent). This is typically used for "ghosting" images. (who ya gonna call?)

Border

- *Style*
This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.
- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.
- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*

This option controls the height of the selected item.

Signature

The signature object is used to add a badge holder picture to the badge type design. To add a signature object to the badge type design, expand the badge data menu by clicking on badge data, then click on the signature icon and drag it to the desired location on the badge type design. A signature object will then be placed on the badge type design at the default size. The signature object should then be moved to the correct location on the badge type design by clicking anywhere inside the signature object and dragging it to the desired location. The signature object should then be resized by clicking on any of the handles on the signature object and dragging it to the desired size. The signature object properties should then be set by modifying the object properties in the right-hand properties menu.

The following properties are supported for the signature object:

Image

- *Size mode*
This option adjusts the size of the signature. Options are to fit the signature to match the objects size (fit), fit the signature to match the object size and retain proportions (fit proportional), or retain the images size, but force to be in the objects shape (clip).
- *Horizontal alignment*
This option controls how the signature is horizontally aligned in the objects shape. Options are to align left, center, or right.
- *Vertical alignment*
This option controls how the signature is vertically aligned in the objects shape. Options are to align top, middle, or bottom.
- *Transparency Tolerance*
This option determines how "transparent" the signature will be. Valid entries are from 0 (not transparent) to 255 (completely transparent). This option is generally used to obtain "floating head" or "security badges", making the badge more difficult to duplicate. This option is most useful when the signature is captured against a solid colored background.
- *Flip/rotate*
This option allows for flipping or rotating the signature. Options are None, Rotate 90, Rotate 180, Rotate 270, Flip Horizontally, Rotate 90 Flip Horizontally, Flip Vertically, and Rotate 90 Flip Vertically,
- *Image Transparency*
This option controls the transparency of the photo. Valid entries are 0 (completely transparent) and 255 (no transparency). This is typically used for "ghosting" images. (who ya gonna call?)

Border

- *Style*
This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.
- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.
- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*

This option controls the height of the selected item.

Embedded Image

The embedded image object is used to add an image (graphic) file to the badge type design. To add an embedded image object to the badge type design, expand the embedded images menu by clicking on the embedded image menu, then click on the plus sign. A browser window will then be displayed to select or enter the image file name to be added as an embedded image. Supported file types are: BMP, JPG, JPEG, GIF, and PNG. An embedded image will then be placed in the embedded images menu and can be dragged onto the badge designer. The static image object should then be moved to the correct location on the badge type design by clicking anywhere inside the static image object and dragging it to the desired location. The static image object should then be resized by clicking on any of the handles on the static image object and dragging it to the desired size. The static image object properties should then be set by using the properties menu on the right-hand pane.

The following properties are supported for the static image object:

Image

- *Size mode*
This option adjusts the size of the picture. Options are to fit the photo to match the objects size (fit), fit the photo to match the object size and retain proportions (fit proportional), or retain the images size, but force to be in the objects shape (clip).
- *Horizontal alignment*
This option controls how the photo is horizontally aligned in the objects shape. Options are to align left, center, or right.
- *Vertical alignment*
This option controls how the photo is vertically aligned in the objects shape. Options are to align top, middle, or bottom.
- *Use Transparent Color*
When selected, the transparent color will be used in conjunction with the transparency tolerance.
- *Transparent color:*
The selected color will be transparent when the image is printed.
- *Transparency tolerance*
The tolerance for the transparent color. Values are 0 (no transparency) and 255 (completely transparent)

Border

- *Style*

This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.

- *Width*

This option sets the thickness for the border. Values are entered in points (pt).

- *Color*

This option sets the color for the border around the selected item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*

This option controls what layer the selected item will be on.

- *Left*

This option controls how far from the left the selected item will be placed.

- *Top*

This option controls how far from the top the selected item will be placed.

- *Width*

This option controls the width of the selected item.

- *Height*

This option controls the height of the selected item.

Lines

The line object is used to add a horizontal or vertical line to the badge type design. To add a line object to the badge type design, expand the tools branch by clicking on the tools menu, then click on the line icon and drag it to the desired location on the badge type design. A line object will then be placed on the badge type design at the default size. The line object should then be moved to the correct location on the badge type design by clicking anywhere inside the line object and dragging it to the desired location. The line object should then be resized by clicking on any of the handles on the line object and dragging it to the desired size. The line object properties should then be set by clicking the object and adjusting the properties within the right-hand properties menu.

The following properties are supported for the line object:

Line

- *Style*
This option will change the style of the line. The options are Solid, Dashed, Dotted, DashDot, and DashDotDot.
- *Color*
This option will set color of the line.
- *Width*
This option will set the size of the lines width. Values are entered in points (pt)

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.

- *Top*
This option controls how far from the top the selected item will be placed.
- *Right*
This option controls how far from the right the selected item will be placed.
- *Button*
This option controls how far from the bottom the selected item will be placed.

Lines

The line object is used to add a horizontal or vertical line to the badge type design. To add a line object to the badge type design, expand the tools branch by clicking on the tools menu, then click on the line icon and drag it to the desired location on the badge type design. A line object will then be placed on the badge type design at the default size. The line object should then be moved to the correct location on the badge type design by clicking anywhere inside the line object and dragging it to the desired location. The line object should then be resized by clicking on any of the handles on the line object and dragging it to the desired size. The line object properties should then be set by clicking the object and adjusting the properties within the right-hand properties menu.

The following properties are supported for the line object:

Line

- *Style*
This option will change the style of the line. The options are Solid, Dashed, Dotted, DashDot, and DashDotDot.
- *Color*
This option will set color of the line.
- *Width*
This option will set the size of the lines width. Values are entered in points (pt)

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.

- *Top*
This option controls how far from the top the selected item will be placed.
- *Right*
This option controls how far from the right the selected item will be placed.
- *Button*
This option controls how far from the bottom the selected item will be placed.

Shapes

The shape object is used to add a custom shape object to the badge type design. To add a shape object to the badge type design, expand the tools menu by clicking on tools, then click on the shape icon and drag it to the desired location on the badge type design. A square object will then be placed on the badge type design at the default size. The object properties should be configured by using the properties menu on the right-hand pane and then be moved to the correct location on the badge type design by clicking anywhere inside the object and dragging it to the desired location. The object should then be resized by clicking on any of the handles on the oval object and dragging it to the desired size. by clicking the object properties button on the badge designer toolbar.

The following properties are supported for the shape object:

Shape

- *Shape style*
Select the style of the shape. Available options are Rectangle, Round Rectangle, and Ellipse.
- *Rounding radius*
This option determines how round the corners of the shapes will be.

Color

- *Background*
Select the background color for the shape.

Border

- *Style*
This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.
- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.
- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*
This option controls the height of the selected item.

Shapes

The shape object is used to add a custom shape object to the badge type design. To add a shape object to the badge type design, expand the tools menu by clicking on tools, then click on the shape icon and drag it to the desired location on the badge type design. A square object will then be placed on the badge type design at the default size. The object properties should be configured by using the properties menu on the right-hand pane and then be moved to the correct location on the badge type design by clicking anywhere inside the object and dragging it to the desired location. The object should then be resized by clicking on any of the handles on the oval object and dragging it to the desired size. by clicking the object properties button on the badge designer toolbar.

The following properties are supported for the shape object:

Shape

- *Shape style*
Select the style of the shape. Available options are Rectangle, Round Rectangle, and Ellipse.
- *Rounding radius*
This option determines how round the corners of the shapes will be.

Color

- *Background*
Select the background color for the shape.

Border

- *Style*
This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.
- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.
- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*
This option controls the height of the selected item.

Shapes

The shape object is used to add a custom shape object to the badge type design. To add a shape object to the badge type design, expand the tools menu by clicking on tools, then click on the shape icon and drag it to the desired location on the badge type design. A square object will then be placed on the badge type design at the default size. The object properties should be configured by using the properties menu on the right-hand pane and then be moved to the correct location on the badge type design by clicking anywhere inside the object and dragging it to the desired location. The object should then be resized by clicking on any of the handles on the oval object and dragging it to the desired size. by clicking the object properties button on the badge designer toolbar.

The following properties are supported for the shape object:

Shape

- *Shape style*
Select the style of the shape. Available options are Rectangle, Round Rectangle, and Ellipse.
- *Rounding radius*
This option determines how round the corners of the shapes will be.

Color

- *Background*
Select the background color for the shape.

Border

- *Style*
This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.
- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.
- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*
This option controls the height of the selected item.

Static Text

The static text object is used to add static text, conditional text or labels to the badge type design. To add a static text object to the badge type design, expand the text branch by clicking on the plus sign, then click on the static text icon and drag it to the desired location on the badge type design. A window will then be displayed to enter the text to be added to the badge type design. The text can be up to 255 characters in length. A static text object will then be placed on the badge type design at the default size. The static text object should then be moved to the correct location on the badge type design by clicking anywhere inside the static text object and dragging it to the desired location. The static text object should then be resized by clicking on any of the handles on the static text object and dragging it to the desired size. The static text object properties should then be set by either double clicking anywhere inside the static text object, or by clicking the object properties button on the badge designer toolbar. The static text object properties can also be accessed by selecting properties from the edit option on the badge designer menu.

The following properties are supported for the static text object:

Text Alignment

This option sets the horizontal text alignment within the static text object frame. Select either left for left justified text, center for centered text or right for right justified text.

Text Angle

- *0 Degrees* - This option will not rotate the text.
- *90 Degrees* - This option will rotate the text by 90 degrees or 1/4 turn
- *180 Degrees* - This option will rotate the text by 180 degrees or 1/2 turn.
- *270 Degrees* - This option will rotate the text by 270 degrees or 3/4 turn.

Back Style

This option sets the back style of the static text object frame. Select either transparent for a "see through" static text object frame or opaque for a solid colored static text object frame. This option is almost always set to transparent unless text is being printed on a colored background or a picture background.

Expression

This option determines what will be printed within the static text object frame. By default, the text entered when the static text object is initially added to the badge is entered here.

Optionally, an expression could be entered here to conditionally print text based on a set of conditions. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Print When The Following Expression Is True

This option determines whether or not the text will print or preview based on the result of an expression. If the expression entered returns a true result, then the text will be printed. If the expression entered returns a false result, then the text will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Back Color

This option sets the back color of the text. Select the text back color by either clicking on one of the standard colors or by clicking on the edit custom color button and selecting a custom color from the palette.

Fore Color

This option sets the fore color of the text. Select the text fore color by either clicking on one of the standard colors or by clicking on the edit custom color button and selecting a custom color from the palette.

Font

This option sets the font and any special formatting characters for the text. Choose the desired font, size and any special effects for the text.

**The fonts available are based upon the fonts installed on the local computer.
Only True Type fonts are supported.**

Expression Builder

The expression builder is used to create advanced functions for use on badge type designs. To build an expression, click on the category, then double click on the field, function or operator to be added to the expression. The expression will be built in the expression builder window as the items are selected. Syntax help will be displayed in the syntax help window whenever a category and item have been selected.

Use of the expression builder can be very complex and is only recommended for advanced users. Further assistance regarding the use of expressions can be found in any documentation for the VBScript scripting language. Further discussion of the VBScript scripting language and expressions is beyond the scope of this help text.

The following categories are supported for the expression builder:

Data Fields

This category displays all of the card holder and card data fields that are available to build expressions. Select the card holder or card data field to be added to the expression by double clicking on the desired field.

Built-in Functions

This category displays all of the built-in functions that are available to build expressions. Expand the Built-in Function node to list the different functions and their definitions. Select the built-in function to be added to the expression by double clicking on the desired function.

Badge Functions

This category displays all of the badge functions that are available to build expressions. Expand the Badge Function node to list the different functions. Select the badge function to be added to the expression by double clicking on the desired function.

Operators

This category displays all of the operators that are available to build expressions. Expand the Operators node to list the different operators and their definitions. Select the operator to be added to the expression by double clicking on the desired operator.

Constants

This category displays all of the constants that are available to build expressions. Expand the Constant node to list the different constants and their definitions. Select the constant to be

added to the expression by double clicking on the desired constant.

Magstripe Encoding

This category displays all of the constants that are available to build ABA Track 2 or ABA Track 3 encoding expressions. Expand the Magstripe Encoding node to list the different encoding options and their definitions. Select the option to be added to the expression by double clicking on the desired option.

Badge Data

The badge data object is used to add badge holder data fields to the badge type design. To add a badge data object to the badge type design, expand the badge data branch by clicking on Badge Data, then click on the badge data field that is to be added and drag it to the desired location on the badge type design. A badge data object will then be placed on the badge type design at the default size. The badge data object should then be moved to the correct location on the badge type design by clicking anywhere inside the badge data object and dragging it to the desired location. The badge data object should then be resized by clicking on any of the handles on the badge data object and dragging it to the desired size. The badge data object properties should then be set by either double clicking anywhere inside the badge data object, or by clicking the object properties button on the badge designer toolbar. The badge data object properties can also be accessed by selecting properties from the edit option on the badge designer menu.

The badge data fields that are available will vary based upon the user fields that are being used.

The following properties are supported for the badge data object:

The following properties are supported for the badge data common expressions object:

Data

- *Source*
When used with Common Expressions, the source should be set to Expression.
- *Expression*
The scripting required to generate the required common expression. This will automatically be populated when the field is placed in the designer. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Alignment

- *Horizontal*
This option sets the horizontal data alignment within the badge data common expressions object frame. Select either left for left justified data, center for centered data or right for right justified data.

- *Vertical*

This option sets the vertical data alignment within the badge data common expressions object frame. Select either left for left justified data, center for centered data or right for right justified data.

Color

- *Background*

This option sets the back color of the data. Select the data back color by either clicking on one of the standard colors or by clicking on the edit custom color button and selecting a custom color from the palette.

- *Text*

This option sets the fore color of the data. Select the data fore color by either clicking on one of the standard colors or by clicking on the edit custom color button and selecting a custom color from the palette.

Text

- *Font*

This option sets the font and any special formatting characters for the data. Choose the desired font, size and any special effects for the data. Fonts are dependent on what is installed within the machines operating system and only True Type fonts are supported.

- *Decoration*

This option sets the decoration for the text. Available options are None, Underline, Overline, or Strike through.

Border

- *Style*

This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.

- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Behavior

- *Angle*
This option sets the angle of the specified item. Values can range between 0 (no rotate) - 360 (fully rotated).
- *Shrink to fit*
This option will force the text of the item to fit based on the items height/width.
- *Word wrap*
This option will force text to wrap to the next line once it reaches the width limit of the item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "..." button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.

- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*
This option controls the height of the selected item.

Badge Data Common Expressions

The badge data common expressions object is used to add commonly used combinations of badge holder data fields to the badge type design. To add a badge data common expression object to the badge type design, expand the badge data common expressions branch by selecting Common Expressions, then click on the badge data common expression that is to be added and drag it to the desired location on the badge type design. A badge data common expression object will then be placed on the badge type design at the default size. The badge data common expression object should then be moved to the correct location on the badge type design by clicking anywhere inside the badge data common expression object and dragging it to the desired location. The badge data common expression object should then be resized by clicking on any of the handles on the badge data common expression object and dragging it to the desired size. The badge data common expression object properties should then be set by either double clicking anywhere inside the badge data common expression object, or by clicking the object properties button on the badge designer toolbar. The badge data common expressions object properties can also be accessed by selecting properties from the edit option on the badge designer menu.

The following properties are supported for the badge data common expressions object:

Data

- *Source*
When used with Common Expressions, the source should be set to Expression.
- *Expression*
The scripting required to generate the required common expression. This will automatically be populated when the field is placed in the designer. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Alignment

- *Horizontal*
This option sets the horizontal data alignment within the badge data common expressions object frame. Select either left for left justified data, center for centered data or right for right justified data.

- *Vertical*

This option sets the vertical data alignment within the badge data common expressions object frame. Select either left for left justified data, center for centered data or right for right justified data.

Color

- *Background*

This option sets the back color of the data. Select the data back color by either clicking on one of the standard colors or by clicking on the edit custom color button and selecting a custom color from the palette.

- *Text*

This option sets the fore color of the data. Select the data fore color by either clicking on one of the standard colors or by clicking on the edit custom color button and selecting a custom color from the palette.

Text

- *Font*

This option sets the font and any special formatting characters for the data. Choose the desired font, size and any special effects for the data. Fonts are dependent on what is installed within the machines operating system and only True Type Fonts are supported.

- *Decoration*

This option sets the decoration for the text. Available options are None, Underline, Overline, or Strike through.

Border

- *Style*

This option sets the decoration for a border around the selected item. Available options are None, Dotted, Dashed, Solid, Double, Groove, Ridge, Inset, WindowInset, and Outset.

- *Width*
This option sets the thickness for the border. Values are entered in points (pt).
- *Color*
This option sets the color for the border around the selected item.

Behavior

- *Angle*
This option sets the angle of the specified item. Values can range between 0 (no rotate) - 360 (fully rotated).
- *Shrink to fit*
This option will force the text of the item to fit based on the items height/width.
- *Word wrap*
This option will force text to wrap to the next line once it reaches the width limit of the item.

Print When

This option determines whether or not the data will print or preview based on the result of an expression. If the expression entered returns a true result, then the data will be printed. If the expression entered returns a false result, then the data will not be printed. An expression can either be typed in manually or built using the expression builder by clicking on the "... " button. For more information on the expression builder, see the [Expression Builder](#) help file topic.

Layout

- *Layer*
This option controls what layer the selected item will be on.
- *Left*
This option controls how far from the left the selected item will be placed.

- *Top*
This option controls how far from the top the selected item will be placed.
- *Width*
This option controls the width of the selected item.
- *Height*
This option controls the height of the selected item.

User Groups

[User Groups Detail](#)

Users groups are used to define groups of system operators, various operator settings and security levels. Access permissions can be set up that will control the level of access that members of the user group will have to all of the data files, configuration files and utilities. Members can also be given access to a single site (data partition) or a number of sites. In addition, members can be given access to all or none of the cardholder user fields (including Cardholder Access Levels). Cardholder user fields and data entry controls can also be customized for each user group. For more information on editing cardholder user fields, see the [Cardholder User Fields](#) help file topic. For more information on sites, see the [Sites](#) help file topic. For more information on users, see the [Users](#) help file topic.

The default user group "Administrators" has access to all areas of the software and should only be assigned to system administrators. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a User Group

To add a user group, go to the User Groups entry screen by clicking on the User Group icon within the Configuration group of the Navigation pane. All of the user groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the ribbon or select new from the right click menu.

Editing a User Group

To edit a user group, go to the User Groups entry screen by clicking on the User Group icon within the Configuration group of the Navigation pane. All of the user groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the user group to be edited and click on the edit button on the ribbon, or double click the user group to be edited. You can also select edit from the right click menu.

Deleting a User Group

To delete a user group, go to the User Groups entry screen by clicking on the User Group icon within the Configuration group of the Navigation pane. All of the user groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the user group to be deleted and click on the delete button on the ribbon or select delete from the right click menu.

Printing User Group Reports

To print reports for a user group, go to the User Groups entry screen by clicking on the User Group icon within the Configuration group of the Navigation pane. All of the user groups in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the user groups to print reports for and click on the Reports button on the ribbon or select print reports from the right click menu. The following reports are available:

- *User Group History* - This report provides a list of all database updates for the selected user groups.
- *User Group Listing* - This report provides a list of the selected user groups and their various properties.
- *User Group Listing With Users* - This report provides a list of the selected user groups and the users that belong to those groups.

User Groups Detail

User Groups

Users groups are used to define groups of system operators, various operator settings and security levels. Access permissions can be set up that will control the level of access that members of the user group will have to all of the data files, configuration files and utilities. Members can also be given access to a single site (data partition) or a number of sites. In addition, members can be given access to all or none of the cardholder user fields. Cardholder user fields and data entry controls can also be customized for each user group. For more information on editing cardholder user fields, see the [Cardholder User Fields](#) help file topic. For more information on sites, see the [Sites](#) help file topic. For more information on users, see the [Users](#) help file topic.

The default user group "Administrators" has access to all areas of the software and should only be assigned to system administrators. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

User Group Name

Enter the name to be used for this user group. The user group name can be up to 50 characters in length.

Inactivity Logout Time

Enter the inactivity logout time for this user group. The inactivity logout time is the amount of time in minutes that a system user that belongs to this group will be automatically logged out of the system if no mouse or keyboard activity has been detected. The inactivity logout time can range from 0 to 99 minutes with 0 meaning never automatically log the user off.

Minimum Password Length

Enter the minimum password length for this user group. The minimum password length determines the minimum number of password characters that will be required for a valid user password. The minimum password length can range from 0 to 99 characters with 0 meaning that no minimum length is required.

Maximum Password Age

Enter the minimum password age for this user group. The minimum password age determines the number of days for which a password will be valid. The maximum password age can range from 0 to 999 days with 0 meaning that passwords will not expire.

Maximum Concurrent Logins

Enter the maximum number of concurrent logins allowed for this user group.

Maximum unsuccessful login

Enter the maximum number of unsuccessful login attempts allowed before the user belonging to this group is locked out. Once locked out another user must log in to reset the account.

Allow web client login

Select to allow users in this user group to have the ability to log into the web client.

Enforce Strong Password

If this option is checked, the User password will be required to contain 1 upper case character, 1 lower case character, 1 numeric character, 1 special character, and be a minimum of 6 characters.

Default Card Group

Select the default card group for this user group. The default card group will be the default card group assigned when cards are being added to the system. Any users that are assigned to this user group will automatically default to this value when adding cards. For more information on card groups, see the [Card Groups](#) help file topic.

Default Companies

Select the default company for this user group. The default card company will be the default company assigned when cards are being added to the system when using the companies feature. Any users that are assigned to this user group will automatically default to this value when adding cards. For more information on card groups, see the [Companies](#) help file topic.

Home Page

Select the home page to be displayed when logging into the application or web client. Valid options are the System Status, Cardholders, Cards, or a blank screen.

Default Card Status

Select the default card status for this user group. The default card status will be the default

card status assigned when cards are being added to the system. Any users that are assigned to this user group will automatically default to these values when adding cards. For more information on cards status, see the [Cards](#) help file topic.

Permissions

To assign permissions for the user group, select the desired category in the permissions tree or expand the tree using the "+" sign to assign individual field permissions and menu access permissions. When the corresponding circle is green the user group has full permissions to the category. When the corresponding circle is half green the user group has restricted permissions to the category. When the circle is white or empty the user group has no permissions to the category. The following permission categories are supported:

- *Cardholder Fields* - Select the main cardholder fields branch (do not expand) to modify the cardholder user fields on the cardholders form. Select the field to be modified and click on the "Edit Field" button to change the display name and the type of data editing control being used. The display order of the cardholders form can also be modified by using the up and down arrow buttons. Expand the cardholder fields branch using the ">" sign to assign access permission for the individual fields. For more information on cardholder user fields, see the [Cardholder User Fields](#) help file topic.
- *Card Fields* - Select the main card fields branch to modify the cards form (do not expand). Select the field to be modified and click on the "Edit Field" button to change the display name and the type of editing control being used. Expand the card fields branch using the ">" sign to assign access permission for the individual fields.
- *Cardholders* - Select the main Cardholders branch to assign access permissions to the global cardholders screen.
- *Cards* - Select the main Cards branch to assign access permissions to the global cards screen.
- *Card Groups* - Select the main Card Groups branch to assign access permissions to the card groups screen or individual card groups.
- *Reports* - Select the main reports branch to assign access permissions to the reports screen or individual reports.
- *Badge Types* - Select the main badge types branch to assign access permissions to the badge types screen or individual badge types.
- *Servers* - Select the main servers branch to assign access permissions to the servers screen.
- *Workstations* - Select the main workstations branch to assign access permissions to the workstations screen.
- *Sites* - Select the main sites branch to assign access permissions to the sites screen.
- *User Groups* - Select the main sites branch to assign access permissions to the user groups screen.
- *Users* - Select the main sites branch to assign access permissions to the users screen.
- *Recipients* - Select the main sites branch to assign access permissions to the recipient

screen.

- *Companies* - Select the main sites branch to assign access permissions to the companies screen.
- *Data Exchange Packages* - Select the main sites branch to assign access permissions to the data exchange packages screen.
- *Diagnostics* - Select the main sites branch to assign access permissions to the diagnostics screen.
- *Change Alarm/Event Filters* - Select the main sites branch to assign access permissions to the Alarm/Event Filters screen.
- *Instant Messaging* - Select the main sites branch to assign access permissions to send instant messaging between workstations.
- *Import Card Data* - Select the main Import Card Data branch to assign access permissions to the optional Import Cards feature.
- *Export Card Data* - Select the main Export Card Data branch to assign access permissions to the optional Export Cards feature.
- *Main or Site Branches* - Select the main (site) branch to set permission for all of the site based screens or expand the tree using the "+" sign to assign individual screen access permissions for each of the sites.

Within each of the categories the following options are supported:

- *No Access* - The user group will not be able to view the category or field and will not be able to add, edit or delete items.
- *View* - The user group will be able to view the category or field but will not be able to add, edit or delete items.
- *View Only* - The user group will be able to view only the selected items.
NOTE: The ability to view selected Readers/Inputs/Outputs requires the Enterprise edition of Access It! Universal.NET
- *New* - The user group will be able to view the category or field and add items without the ability to edit existing items or delete items.
- *Edit* - The user group will be able to view the category or field and edit existing items without the ability to add or delete items.
- *Delete* - The user group will be able to view the category or field and delete existing items without the ability to add or edit items.
- *Execute Commands* - The user group will be able to execute commands (i.e. grant access) for the category.

The above options can be used together for any combination of the above permissions.

Some of the special site-specific category privileges are described below:

- *Change Alarm/Event Filters* - In the miscellaneous category the events that are displayed in the event window and the alarms displayed in the alarm window can have a default filter created to filter events by either the event type or the location that the event

occurred. This is accomplished by clicking on the setup filters button. Select the desired event type(s) and location(s) to be displayed. The default filter can then be turned on or off by selecting the current filter (Default) in the events or alarms window pane. An example of event filtering would be if this workstation is used as a photo id verification workstation for positive identification purposes, it may be desirable to filter the event locations for this workstation to only the readers that are being used for verification purposes.

- *Alarm Delay* - In the alarms category alarm delays are used to "route" or "bump" alarms from one workstation to another based upon a time schedule. Alarm delays are useful when one or more sites are unmanned during a certain time of day and it is necessary to send the alarms to a different site for operator handling. For more information on alarm delays, see the [Alarm Delay](#) help file topic.

Alarm Colors

Alarm colors control how alarms are displayed in the alarms window. Four priority ranges can be set with a low and high limit for both pending and acknowledged alarms. Both the background (highlight) color and the font or text color can be set. This option is useful so that higher priority alarms can be set up so that they draw more attention than lower priority alarms.

Event Colors

Event colors control how events are displayed in the events window. Five different categories of events can be set. Both the background (highlight) color and the font or text color can be set. This option is useful in situations where many events are being monitored and attention can be drawn to a certain category of events.

Default Event Reporting Template

The Default Event Reporting Template allows for a default template of event reporting for each device category. This template only applies to creating new devices, and does not have an effect on existing event reporting.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be

useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Cancel Buttons

Clicking on the save button will save the changes made to the user group. Clicking on the cancel button will not save the changes made to the user group.

[User Groups](#)

Users

[Users Detail](#)

Users are used to define system operators, passwords and their security role or user group. Security levels are determined by the user group that the user is a member of. For more information on user groups, see the [User Groups](#) help file topic. Access It! Universal.NET comes with one default user "Admin" which has no password assigned. This user has been granted access to all areas of the system and should only be used by system administrators. It is recommended that a user be set up for each operator that will be using the system. All editing, deleting and adding of data in the system is recorded in the events database along with the name of the user that performed the action. This is useful for tracking data updates within the system and who performed them.

It is strongly recommended that a password be assigned to the "Admin" user or the user be removed as soon as the software is installed. The "Admin" user has been assigned to the "Administrators" user group granting them access to all screens and areas in the system and should only be used by system administrators. Access to this screen is determined by the settings for the currently logged in user. All users can change their own passwords whether or not they have access to the users screen.

Adding a User

To add a user, go to the users data entry screen by clicking on the Users icon within the Configuration group of the Navigation pane. All of the users in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the ribbon or from the right click menu.

Editing a User

To edit a user, go to the users data entry screen by clicking on the Users icon within the Configuration group of the Navigation pane. All of the users in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the user to be edited and click on the edit button on the ribbon, or double click the user to be edited. You can also select edit from the right click menu.

Deleting a User

To delete a user, go to the users data entry screen by clicking on the Users icon within the Configuration group of the Navigation pane. All of the users in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the user to be deleted and click on the delete button on the ribbon or select delete from the right click menu.

Setting a Password for a User

To set a password for a user, select the user then click on the change password for user button on the ribbon and enter the new password and then confirm the new password. You can also select change password from the right click menu. To change the password for the account currently logged in, select Change Password from the File menu.

Passwords for domain users can only be managed with the operating system administration tools. The ability to change passwords is determined by the user group for the currently logged in user. For more information on user groups, see the [User Groups](#) help file topic.

Printing User Reports

To print reports for a user, go to the users data entry screen by clicking on the Users icon within the Configuration group of the Navigation pane. All of the users in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the users to print reports for and click on the Reports button on the ribbon or select Print Reports from the right click menu. The following reports are available:

- *Alarm Acknowledgments And Clears* - This report provides a list of all alarm acknowledgments and clears for the selected users.
- *User Listing* - This report provides a list of the selected users and their various properties.
- *User Transaction History* - This report provides a list of all transactions for the selected users including database updates, commands to devices and alarm processing.

Users Detail

Users

Users are used to define system operators, passwords and their security role or user group. Security levels are determined by the user group that the user is a member of. For more information on user groups, see the [User Groups](#) help file topic. Access It! Universal.NET comes with one default user "Admin" which has no password assigned. This user has been granted access to all areas of the system and should only be used by system administrators. It is recommended that a user be set up for each operator that will be using the system. All editing, deleting and adding of data in the system is recorded in the events file along with the name of the user that performed the action. This is useful for tracking data updates within the system and who performed them.

It is strongly recommended that a password be assigned to the "Admin" user or the user be removed as soon as the software is installed. The "Admin" user has been assigned to the "Administrators" user group granting them access to all screens and areas in the system and should only be used by system administrators. Access to this screen is determined by the settings for the currently logged in user. All users can change their own passwords whether or not they have access to the users screen.

User Name

Enter the name to be used for this user. The user name can be up to 50 characters in length. This is the login name that the system operator will use to gain access to the application.

User Group Name

Select the user group name for this user. The user group name will assign the user to a user group and that user group will determine the security level or security role for the user. For more information on user groups, see the [User Groups](#) help file topic.

Full Name

Enter the full name for this user. The full name can be up to 50 characters in length and is strictly used for informational purposes. The full name can be used to identify the system user by real name for demographics purposes instead of by user name.

Domain User

Select (check) this option if this user is a domain user. A domain users password will be authenticated by the domain selected in the login screen instead of with a password stored in the application database. This is useful for centralized password and user management. The

default domain "Access It! Universal.NET" should be used when a non-domain user is being authenticated at the login screen.

User Enabled

Select (check) this option if this user is to be enabled. If the user enabled option is checked, the user is enabled and can log in to the system with the proper credentials. If the user enabled option is not checked, the user is disabled and cannot log in to the system even if the proper credentials are entered. This is useful for temporarily disabling a user from logging in to the system without having to delete the user.

Require Password Change at Next Login

Select (check) this option to force the user to change their password upon the next login.

Active Date

Enter the active date for this user. The user will become active at midnight on the date entered in the active date field. This is useful for temporary system users that only need access to the system for a specified period of time.

Expire Date

Enter the expire date for this user. The user will become inactive at midnight on the date entered in the expire date field. This is useful for temporary system users that only need access to the system for a specified period of time.

Password

If the User is assigned to a User Group that requires strong password enforcement, that password will be required to contain 1 upper case character, 1 lower case character, 1 numeric character, 1 special character, and be a minimum of 6 characters and they will receive an error message until these criteria have been met.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be

useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the user. Clicking on the close button will not save the changes made to the user.

[Users](#)

Reports

Reports are used to create and edit all reports and to run certain reports that are not related to data entry screens. All reports can be sent to either the screen or a system printer. Most reports should be run from their respective data entry screens. For example, a report that contains all of the access granted events for a specific reader would be run from the readers screen with the appropriate readers selected.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Running Reports

To run a report, either select the reports data entry screen by clicking the Reports icon in the configuration menu of the navigation pane. Reports can also be ran by clicking the reports button within the ribbon or selecting print reports from right click menu. Next, select the report to be run and click on the print button on the toolbar or select print from the file option on the system menu or from the right click menu.

The following reports can only be ran from the reports screen (all other reports should be run from their respective data entry screens):

Alarm Listing - This report provides a list of alarms for the selected events as well as who acknowledged them and who cleared them.

Evacuation Report - This report provides a list of cardholders that are currently IN the selected areas.

Event Listing - This report provides a list of all user selectable events.

Report Listing - This report provides a list of all reports available, as well as report category and a description.

Unused Cards - This report provides a list of all cards that have not been used for a user inputted number of days or have never been used.

Designing Reports

To create new reports or edit existing reports, from the right click menu select show all reports then click on the new button to create a new report or select a report to modify and click on the edit button on the toolbar to run the report designer. For more information on designing reports, see the Report Designer help file topic.

Report designer licenses must be purchased separately.

Recipients

[Recipients Detail](#)

Notification recipients are used to set up individuals or groups of individuals to be notified by email or pager when a system event or alarm occurs. Recipients can be notified by executing a macro when an event or alarm occurs. Notifications can also be set up to only occur during a specified schedule.

An external email or paging service is necessary in order for notification to function. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Recipient

To add a recipient, go to the recipients entry screen by clicking on the Recipients icon within the Configuration group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu.

Editing a Recipient

To edit a recipient, go to the recipients entry screen by clicking on the Recipients icon within the Configuration group of the Navigation pane. Select the recipient to be edited and click on the edit button on the toolbar, or double click the recipient to be edited. You can also select edit from the right click menu.

Deleting a Recipient

To delete a recipient, go to the recipients entry screen by clicking on the Recipients icon within the Configuration group of the Navigation pane. All of the recipients in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the recipient to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu.

Printing Recipient Reports

To print reports for a recipient, go to the recipients entry screen by clicking on the Recipients icon within the Configuration group of the Navigation pane. All of the recipients in the database will then be displayed in the right window pane of the Access It! Universal desktop. Select the recipients to print reports for and click on the Reports button within the ribbon or from the right click menu select print reports. The following reports are available:

- *Recipient History* - This report provides a list of all database updates for the selected

recipients.

- *Recipient Listing* - This report provides a list of the selected recipients and their various properties.

Recipients Detail

Recipients

Notification recipients are used to set up individuals or groups of individuals to be notified by email or pager when a system event or alarm occurs. Recipients can be notified by executing a macro when an event or alarm occurs. Notifications can also be set up to only occur during a specified schedule.

An external email or paging service is necessary in order for notification to function. Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Recipient Name

Enter the name to be used for this recipient. The recipient name should be the name of the individual that is being notified or the name of the group for which multiple individuals are being notified. The recipient name can be up to 50 characters in length.

Email Service

Select the email service to be used to notify the recipient or group. Email services can be added and maintained by clicking the edit button next to the email service name. The following email service parameters are supported:

- *Email Service Name* - Enter the name to be used for this email service. The email service name can be up to 50 characters in length.
- *SMTP Server* - Enter the name of the SMTP (Simple Mail Transfer Protocol) server being used to send notification email. This information is usually obtained from your internet provider or network administrator.
- *Mail From* - Enter the name that you wish to appear in the "from" field of the notification email. **NOTE: This field must be in standard email format e.g. someone@somewhere.com.**
- *Default Subject* - Enter the default subject that you wish to appear in the "subject" field of the notification email if no subject is available for the event being sent.
- *Authentication Type* - Select the authentication type for the SMTP server. This information is available from your ISP or network administrator.
- *POP Server* - Enter the name of the POP (Post Office Protocol) server being used to send notification email. This information is usually obtained from your internet provider or network administrator.
- *User Name* - Enter the user name to be used for authentication to the email server.
- *Password* - Enter the password to be used for authentication to the email server.
- *Charset* - Enter the character set to be used with the email server. The default is "us-

ascii" which is for the United States ASCII format. Most email servers will accept this format.

- *TCP Port* - Enter the TCP port to be used for communications with the email server. Most SMTP mail servers use TCP port 25 by default.

Email Address

Enter the email address to be used for this recipient.

Enable Email Schedule

Select the days of the week and times to be used for each of the 4 intervals. Only 1 interval needs to be set up to enable a notification schedule, but all 4 can be used if desired. Enter the appropriate start time and end time for any of the intervals being used. The start time is when notification will become active and the end time is when the notification will become inactive.

Paging Service

Select the paging service to be used to notify the recipient or group. Paging services can be added and maintained by clicking the edit button next to the paging service name. The following paging service parameters are supported:

- *Paging Service Name* - Enter the name to be used for this paging service. The paging service name can be up to 50 characters in length.
- *Baud Rate* - Enter the baud rate to be used for this paging service. This information is usually obtained from your paging provider.
- *Service Type* - Select the service type to be used for this paging service. This information is usually obtained from your paging provider.
- *Access Number* - Enter the access telephone number to dial in to the paging service provider. This is not the number for the individual pager but the number for the paging service itself. This information is usually obtained from your paging provider.
- *Max Characters per Block* - Enter the maximum characters per block that this paging service will support. This information is usually obtained from your paging provider.

Pager ID

Enter the pager number or pager identification number for this recipient. This is not the number for the paging service but the number for the individual pager to be used for notification.

Default Page Message

Enter the default message that you wish to appear on the pager if no message is available for the event being sent.

Enable Paging Schedule

Select the days of the week and times to be used for each of the 4 intervals. Only 1 interval needs to be set up to enable a notification schedule, but all 4 can be used if desired. Enter the appropriate start time and end time for any of the intervals being used. The start time is when notification will become active and the end time is when the notification will become inactive.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Cancel Buttons

Clicking on the save button will save the changes made to the recipient. Clicking on the cancel button will not save the changes made to the recipient.

[Recipients](#)

Data Exchange Packages

Data exchange packages is a utility used to import or update records within the Access It! Universal.NET database via an external data source. Once created, data exchange packages can be executed manually or on a schedule. The six types of external data sources currently supported are: Microsoft Access, Microsoft Excel, Text File, Text File over FTP, SQL Server, ODBC, and Microsoft Active Directory. Card and cardholder data and associated fields, including access levels and images, may be added, updated or deleted via this utility. **When using Windows Authentication, the Windows user logged on to the workstation must have permission to modify the Access It! Universal.NET database to utilize the Data Exchange Packages feature.**

Importing/Exporting Data Exchange Packages

After a Data Exchange Package has been created and saved it can be exported to a XML file by right clicking the page and selecting Export. By right clicking and selecting Import, the XML file can then be loaded. This is beneficial for systems that use several canned packages that need to be installed on sub systems.

Package Name

Specify the name of the data exchange package. A user-friendly name is recommended.

Package Type

- *Import - Microsoft Access* - Select the data source file name. If the database is password protected, enter the User Name and Password. Select the Table/Query using the dropdown list. Check/uncheck the delete rows after execution option as needed.
- *Import - Microsoft Excel* - Select the data source file name. Use the drop-down list to choose the worksheet name. Check/uncheck the First row contains column headers and Delete file after execution options as needed.
- *Import - Microsoft SQL Server* - Use the dropdown list to choose the SQL Server, Authentication mode, Database, and Table. If SQL Server authentication is chosen, enter the User Name and Password. Check/uncheck the Delete rows after execution option as needed.
- *Import - Text File* - Select the data source text file. Check/uncheck the First row contains column headers and Delete file after execution option buttons as needed.
- *Import - Active Directory* - Enter the path to the Active Directory data source. For additional information on path syntax, see the [Active Directory Path](#) help file topic. Use the drop-down list to choose a Selection Type. If the Full Import selection type is chosen, all rows in the data source will be processed. If the Updates/Deletes Only

selection type is chosen, all rows in the data source will be processed the FIRST time the data package is executed. During subsequent executions of the data exchange package, only records that have been inserted, updated, or deleted since the last time the data exchange package was executed will be processed. **Active Directory synchronization is performed using the "DirSync" control. To use the "DirSync" control, the caller to Active Directory must have the "directory get changes" right assigned on the root of the partition being monitored. By default, this right is assigned to the Administrator and LocalSystem accounts on domain controllers. The caller must also have the "DS-Replication-Get-Changes" extended control access right.**

- *Import - ODBC* - Use the drop-down lists to select a System DSN and Table/View of the data source. If the data source is password protected, enter the Login ID and Password. It is also possible to specify a single schema owner or return all tables. If necessary, add table and column identifiers.
- *Export - Text File* - Select the location for the exported file. Check/uncheck the First row contains column headers and Delete file after execution option buttons as needed. Delimiters supported are comma, space, pipe, tab, and semicolon.

Selection Type

Selection Type options vary based on source data type.

- *Full Import* - Import all records from the source data.
- *Updates/Deletes Only* - Import only updated data
 - *Selection Column* - Select the specified column the Data Exchange Package will reference to detect updates
 - *Selection Criteria Type*
 - *Selection Columns Data > Last Processed* - Used when the Selection Column is a datetime field. The Data Exchange Package will only process records that have a datetime newer than the last time the Data Exchange Package executed.
 - *Selection Columns Data > (Value)* - Used when the Selection Column is not a datetime field. A custom value must be entered that the Data Exchange Package will use to reference which records need to be processed.
 - *Value* - The custom value that the Data Exchange Package will use to reference which records need to be processed.
 - *Update Mode* - Controls if the custom value should be updated after the Data Exchange Package executes
 - *Don't Update* - The custom value will not be updated
 - *Null* - The custom value will be set to null
 - *Empty String* - The custom value will be set to an empty (blank) string
 - *Specify Value* - The custom value will be set to a specified value
 - *Specify Update Value* - The value that the custom defined value will be set to

Exception Logging Mode

- *Log to Folder* - A unique exception log will be created each time the data exchange package is executed. The file name will be the data exchange package name concatenated with a date/timestamp and a .log extension. An example of a file name for a data exchange package named Microsoft Access Import would be Microsoft Access Import 2012-01-06-11-54-28.log.
- *Log to File* - The exception log will be created, if one does not exist, or overwritten for each execution of the data exchange package. The file name will be the data exchange package name with the .log extension. For example, if the data exchange package name is Microsoft Excel Import, the filename will be Microsoft Excel Import.log.

Exception Log Path

Enter the destination folder name for exception logs. If left empty, the default location will be: C:\ProgramData\RS2 Technologies, LLC\Access It! Universal.NET\

Package Enabled

Select (check) the package enabled checkbox to enable or disable the data exchange package.

Key Field

The key field can be selected from any of the mapped fields. For more information on field mapping, see the [Field Mapping](#) help topic file. For example, assume there is a field called EmployeeID in the data source that is mapped to UserText11 (which has been renamed EmpID in the Access It! Universal Cardholders table). EmpID would be selected as the key field. During execution of the data exchange package, the executor will search for an EmpID in Access It! Universal.NET that matches the EmployeeID from the data source. If a match is located, an update will be performed (or a delete, depending upon the delete mode/delete control/delete control value specified). If a match is not located and the "insert record if it doesn't exist" checkbox is checked, an insert will be performed. If the checkbox is not checked, the record is ignored.

Card Modification Rule

This option will be functional only if the key field is a field in the Cardholders database AND the card number and facility code are mapped. The selected option will determine how processing will proceed when a cardholder already has existing cards in the database and an import or update is to be performed.

- *Insert/Update Card* - The cardholder's existing cards will not be modified.

- *Replace Existing Card(s)* - Any existing cards for the cardholder will be deleted.
- *Deactivate Existing Card(s)* - The cardholder's existing cards will remain in the database but will be deactivated.

Access Level Modification Rule

This option will not be available if the key field is not defined via Field Mapping. If one or more Access Level fields is mapped, the Access Level Modification Rule dictates how the access levels will be processed when the data exchange package is executed. If the key field is the Card Number or Card Number/Facility Code, the access level modification rule will apply to the card being processed. If the key field is mapped to a cardholder field, as in the example of UserText11 above, the modification rule will affect all cards belonging to the cardholder.

- *Insert/Update Access Level(s)* - access levels will be added to the card specified in the record being processed.
- *Replace Access Level(s)* - All existing access levels for the card will be replaced with the access levels from the data source.
- *Delete Access Level(s)* - The specified access levels, if they exist, will be deleted for the card
- *Insert/Update Cardholder Access Level(s)* - access levels will be added to the cardholder specified in the record being processed.
- *Replace Cardholder Access Level(s)* - All existing access levels for the cardholder will be replaced with the access levels from the data source.
- *Delete Cardholder Access Level(s)* - The specified access levels, if they exist, will be deleted for the cardholder

Access Level Creation Rule

This option will not be available if the key field is not defined via Field Mapping. If one or more Access Level fields is mapped, the Access Level Creation Rule dictates how the access levels will be handled when the source access level does not exist within Access It! Universal.NET

- *Don't Create* - Access Levels will not be created if they do not exist within Access It! Universal.NET
- *Create in specified sites* - Access Levels will be created in only the specified sites if they do not exist within Access It! Universal.NET
- *Create in all sites* - Access Levels will be created in all sites if they do not exist within Access It! Universal.NET

Insert Record If It Doesn't Exist

Check this box if, during the execution of the data exchange package, a record is encountered on the data source file that does not have a corresponding record, by key field, in the Access It! Universal.NET database.

Delete Control Field/Delete Control Value

When a key field is defined, a mapped field can be designated as a delete control field. For example, EmployeeStatus is mapped to UserText5. Valid EmployeeStatus values are EMPLOYEE, CONTRACTOR, VENDOR, TERMINATED. With the delete control field set to EmployeeStatus and the delete control value set to TERMINATED, any record containing TERMINATED in the EmployeeStatus field will be deleted. Use the dropdown list to select the delete control field. Enter the desired value for the delete control value.

Delete Mode

The delete mode determines whether just an individual card or the cardholder and all of their associated cards are deleted.

- *Delete Cardholder*- If this option is selected, the cardholder and all of the associated cards will be deleted.
- *Delete Card* - If this option is selected, the individual card will be deleted.

Record Selection (export only)

The record selection allows for specifying if all records or just select records should be exported when the Data Exchange Package is executed.

Selection of Last Modified Records (export only)

The selection of last modified records is used in conjunction with the record selection and allows for specifying if only records recently modified should be exported.

Field Mappings

For more information on field mapping, see the [Field Mapping](#) help topic file.

Preprocessing Step

Click the Add step button to add a pre-processing step. A Pre-processing step can execute an EXE, BAT, VB, or PS1 file which performs any required initialization before the data exchange package executes.

Postprocessing Step

Click the Add step button to add a post-processing step. A Post-processing step can execute an EXE, BAT, VB, or PS1 file which performs any required cleanup after the data exchange package executes.

Schedule Type

- *None* - The data exchange package will not be executed and will not be scheduled to execute.
- *Run Once* - The data exchange package will be executed one time only at the specified date and time.
- *Minutely* - The data exchange package will be executed beginning on the selected date for the interval (in minutes) selected.
- *Hourly* - The package will be executed beginning on the selected date for the interval (in hours) selected.
- *Daily* - The package will be executed daily beginning on the selected date at the selected time.
- *Weekly* - The package will be executed weekly on the selected day of the week, beginning on the selected date, at the selected time.
- *Monthly* - The package will be executed on the selected day of the month beginning on the selected date and time.

Event Type

Data Exchange events (transactions) are recorded in the event file every time a package executes. Events can also be displayed in the events window or produce a system alarm. For more information on events, see the [Events](#) help file topic. For more information on alarms, see the [Alarms](#) help file topic.

The following event types are supported:

- *Data exchange package succeeded* - The data exchange package executed and ran without error.
- *Data exchange package succeeded with error* - The data exchange package executed successfully and one or more records failed to import.
- *Data exchange package failed* - The data exchange package failed to execute.

Notes

Notes can be used to record miscellaneous text information about the Data Exchange Package. This field can be useful for recording what type of processing the data exchange package will perform, hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Auditing

The auditing tab will automatically record when and by whom the Data Exchange Package was created, when and by whom the last time that package was modified, and when the package was last executed.

Companies Detail

Companies

Companies are used to control access to or partition cardholders, cards and access levels. Cardholders, cards and access levels can either be assigned to no company or to a specific company. Only users with access to the company that a cardholder, card or access level has assigned to them will be able to view, modify or delete those items.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Company Name

Enter the name to be used for this company. The company name should be the name of the company or partition. This normally that the name of a tenant in a multi-tenant building or the name of a company when a central system is being used to manage multiple companies. The company name can be up to 50 characters in length.

Auditing

The auditing tab will automatically record the last time that a record was modified and who was logged in to the system when the record was modified. This information is recorded each time a record is added or changed and stored in the system database.

Notes

Notes can be used to record miscellaneous text information for a record. This field can be useful for recording hardware service intervals, personnel information, general system information, etc. There is no limit as to how long a notes field can be.

Save/Close Buttons

Clicking on the save button will save the changes made to the company. Clicking on the close button will not save the changes made to the company.

Companies

[Companies Detail](#)

Companies are used to control access to or partition cardholders, cards and access levels. Cardholders, cards and access levels can either be assigned to no company or to a specific company. Only users with access to the company that a cardholder, card or access level has assigned to them will be able to view, modify or delete those items.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Company

To add a company, go to the Companies entry screen by clicking on the Companies icon within the Configuration group of the Navigation pane. All of the companies in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the toolbar or select new from the file option on the system menu or from the right click menu.

Editing a Company

To edit a company, go to the Companies entry screen by clicking on the Companies icon within the Configuration group of the Navigation pane. All of the companies in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the company to be edited and click on the edit button on the toolbar, or double click the company to be edited. You can also select edit from the right click menu.

Deleting a Company

To delete a company, go to the Companies entry screen by clicking on the Companies icon within the Configuration group of the Navigation pane. All of the companies will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the company to be deleted and click on the delete button on the toolbar or select delete from the right click menu.

Alarm Event Filters

[Alarm Event Filters Detail](#)

Alarm/Event filters allow for the creation of custom filtering of the events and/or alarms displayed within the workstation. A Filter can be a combination of specific event types and specific event locations. Access It! Universal.NET allows for an unlimited amount of filters to be created.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding an Alarm Event Filter

To add an alarm event filter, go to the Alarm/Event filters data entry screen by clicking on the Alarm/Event filter icon within the Configuration group of the Navigation Pane. Click on the new button on the ribbon or select new from the right click menu.

Servers

[Servers Detail](#)

Servers are used to create new or maintain existing regional or standalone servers by specifying the computer that will poll the panels and host the site, specifying various server parameters and specifying the TCP communications options. Each server can host up to 255 sites. The first server on a new system is automatically created in the database with all of the default settings the first time the application is run.

NOTE: Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. Regional server licenses must be purchased separately for each server.

Adding a Server

Servers are automatically added each time the services are started on the machine and rarely require manual entry into the application. To manually add a server, go to the servers entry screen by clicking on the servers icon within the System group of the Navigation pane. Click on the new button on the toolbar or select new from the right click menu.

Editing a Server

To edit a server, go to the servers entry screen by clicking on the servers icon within the System group of the Navigation pane. Select the server to be edited and click on the edit button on the toolbar, or double click the server to be edited. You can also select edit from the right click menu.

Deleting a Server

To delete a server, go to the servers entry screen by clicking on the servers icon within the System group of the Navigation pane. All of the servers in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the server to be deleted and click on the delete button on the toolbar or select delete from the file option on the system menu or from the right click menu. Deleting a server will not delete any of the sites associated with the server.

Printing Server Reports

To print reports for a server, go to the servers entry screen by clicking on the servers icon within the System group of the Navigation pane. All of the servers in the database will then be displayed in the right window pane of the Access It! Universal desktop. Select the servers to print reports for and click on the Reports button within the ribbon or from the right click

menu select print reports. The following reports are available:

- *Server Listing* - This report provides a list of the selected servers and their various properties.

Servers Detail

Servers

Servers are used to create new or maintain existing regional or standalone servers by specifying the computer that will poll the panels and host the site, specifying various server parameters and specifying the TCP communications options. Each server can host up to 255 sites. The first server on a new system is automatically created in the database with all of the default settings the first time the application is run.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic. Regional server licenses must be purchased separately for each server.

Server Name

The server name is used to specify the network name of the Access It! Universal.NET server that will be hosting the site(s). This is also the server that will communicate or poll the hardware panels. It is usually but not necessarily the same computer that will be hosting the database.

Card Update Interval

Select or enter the external card update checking interval to be used. The external card update checking interval is the amount of time in seconds that the system will check to see if any cards have been automatically deactivated by the unused card expiration threshold option and send the updates to the SCP panels. The external card update checking interval can range from 0 to 86400 seconds. If this option is set to zero, external card updates will never be automatically sent to the SCP panels.

This option must be set to a non-zero value in order for the unused card expiration option to function. This option can also be used to send card updates to the SCP panels if the cards have been updated directly in the database by an external source such as a Human Resource Management (PeopleSoft) program.

Unused Card Expiration Threshold

Select or enter the unused card expiration threshold to be used. The unused card expiration threshold is the amount of time in days that an unused card is allowed to remain active in the system. If a card has not been used at any of the readers in the system for the time in days set here, the card will automatically be set to inactive and will no longer work at any of the readers in the system. The unused card expiration threshold can range from 0 to 300 days. If this option is set to zero, cards will never be automatically deactivated.

TCP Notification Port

Enter the TCP notification port for the server. The TCP notification port is the port where the server will "listen" for attached workstations and send events and alarms to them as long as they are set up to receive events and alarms.

If a firewall is installed in the system this port will need to be enabled for two-way TCP traffic in order for alarms and events to be sent to workstations.

Enforce Unique PIN Numbers

Select (check) this option to require unique PIN numbers. This option should be used if any of the readers in the system are going to be used in PIN only or Card or PIN mode. This will ensure that all PIN numbers are unique and can only be assigned to one card. This option cannot be enabled if duplicate PIN's already exist in the system (PIN 0000 is not considered a duplicate)

Sites Detail

Sites

Sites are used to create new or maintain existing sites within a database and specify various site capacities and parameters. A site is used to segregate (partition) data in a database. Only the hardware installed at a specific site will be available when connected to that site. To switch between the various sites, select the desired site from the current site drop down located just under the system menu. Multiple sites may be viewed at once by disabling the option 'allow selection of only a single site' within the File | Options menu.

Any changes made at the site level will prompt for a reset all of the SCP panels in the site when changes are saved. If a reset is not performed, a Macro can be scheduled to reset all the SCPs at a later point in time. Access to individual sites is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Site Name

Enter the name to be used for this site. It is recommended that a name be assigned to all of the sites based on the location of the site. An example site name might be "Chicago" or "Child Care Wing". The site is used to partition data based on the location of the attached hardware. Each site will contain its own set of hardware, access levels, floor codes, timezones, holidays, maps and macros. All card holders, cards, card groups, badge types, reports, recipients, user groups and users will be globally contained in all sites. The site name can be up to 50 characters in length.

Site Online

Select (check) this option if the site is to be active or online. When a site is not online, it will not be available from within Access It! Universal.NET and no communications will take place with any of the hardware attached to the site. When a site is marked as off-line it will not be deleted from the database and can be brought back online at any time.

Regional Server

The regional server is used to select the network name of the Access It! Universal.NET server that will be hosting the site and acting as the server for the site. It is usually but not necessarily the same computer that will be hosting the database.

Holiday Count

Enter the number of holidays for this site. The number of holidays per site can range from 32 to 255.

Timezone Count

Enter the number of timezones for this site. The number of timezones per site can range from 128 to 255.

Access Level Count

Enter the number of access levels for this site. The number of access levels per site can range from 255 to 32,000.

Floor Code Count

Enter the number of floor codes for this site. The number of floor codes per site can range from 0 to 32,767.

Alarm Expiration Threshold

Select or enter the alarm expiration threshold to be used. The alarm expiration threshold is the amount of time in hours that an alarm will be displayed in the alarms window prior to being acknowledged. If the alarm has not been acknowledged after the time in hours set here, the alarm will automatically be "expired" or removed and will no longer be displayed in the alarms window. The alarm expiration threshold can range from 0 to 99 hours. If this option is set to zero, alarms will never be automatically "expired".

Escort timeout (seconds)

Select or enter the escort timeout value to be used. The escort time is the amount of time an escorted cardholder has to present their card after an escort's card presentation. Values can range from 0-60 seconds.

Multi-card timeout (seconds)

Select or enter the multi-card timeout value to be used. The multi-card time is the amount of time allowed for a second card swipe to be presented while the reader is in "require 2 cards at this reader" mode. Values can range from 0-60 seconds.

Biometric Reader Type

Select the biometric reader type to be used with the system. Selecting a biometric reader type will allow biometric templates to be stored within each of the SCP panels. For more information on SCP panel biometric template capacities, see the [SCP's](#) help file topic.

Biometric licenses must be purchased separately in order for biometric support to take

effect.

Use Precision Access

Select (check) this option if precision access is to be used for this site. Precision access provides the ability to assign door access to a card by specifying individual doors and time codes. Precision access can be used in conjunction with, or instead of access levels. Precision access is generally used when an access level contains most of the doors that a card needs access to, but needs to have one or more additional doors added. This allows the assigning of the additional door without the need to create an entire new access level for the special access need of a card. For more information on access levels, see the [Access Levels](#) help file topic. For more information on cards, see the [Cards](#) help file topic.

Enabling precision access greatly reduces the total card capacity of the SCP panel(s) in the site. Once precision access is enabled, all SCP panel(s) in the site will use precision access. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Use Limit

Select (check) this option if use limits are to be used. Use limits will limit the number of times that the card can be used at any reader that has the non-zero use limit option set. Each time the card is granted access at any of these readers the number of uses remaining will be decremented by one. For more information on readers requiring non-zero use limits, see the [Readers](#) help file topic.

Enabling use limits reduces the total card capacity of the SCP panel(s) in the site. Once use limits are enabled, all SCP panel(s) in the site will use Use Limits. For more information on SCP panel card capacities, see the [SCP's](#) help file topic. Use limits are specific to each of the SCP panels in the site. If a card has a use limit of 20 and has access to readers set up to for use limits that are attached to two different SCP's, the card will have 20 uses at each of the SCP's. In addition, if an SCP panel is reset, the use limit will be reset to it's original value.

Use Large Card Numbers

Select (check) this option if large card numbers are to be used. When large card number support is enabled, the card number can range from 1 to 9223372036854775807. For more information on cards, see the [Cards](#) help file topic.

Enabling large card numbers reduces the total card capacity of the SCP panel(s) in the site. Once large card numbers are enabled, all SCP panel(s) in the site will use large card numbers. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Temporary Access Level

Select (check) this option if temporary access levels are to be used. Temporary access levels are combinations of timezones, floor codes and readers (doors/elevators) that are used to

give a card holder temporary (date based) access to a door, elevator or a group of doors or elevators. For more information on temporary access levels, see the [Cards](#) help file topic. Enabling temporary access levels reduces the total card capacity of the SCP panel(s) in the site. Once temporary access levels are enabled, all SCP panel(s) in the site will use temporary access levels. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Issue Levels

Select (check) this option if issue levels are to be used. When issue level support is enabled, the encoded issue level number on the card is used in addition to the card number and facility code to process access requests. If a card is lost or stolen, this enables the same card number to be re-used with a different issue level. Issue levels can range from 0 to 255. For more information on cards, see the [Cards](#) help file topic.

Enabling issue levels reduces the total card capacity of the SCP panel(s) in the site. Once issue levels are enabled, all SCP panel(s) in the site will use issue levels. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Temporary Card Deactivate

Select (check) this option if temporary card deactivations are to be used. Temporary card deactivation will temporarily deactivate a card based on a date or a date range. For more information on temporary card deactivation, see the [Cards](#) help file topic.

Enabling temporary card deactivation reduces the total card capacity of the SCP panel(s) in the site. Once temporary card deactivations are enabled, all SCP panel(s) in the site will use temporary card deactivation. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Antipassback

Select (check) this option if anti-passback functions are to be used. Anti-passback is used to prevent the "passing back" of a card from card holder to card holder when entering or leaving a designated area. If the card is used more than once, the card holder may or may not be granted access to the area and an anti-passback event (transaction) will be generated. For more information on anti-passback, see the [Readers](#) help file topic.

Enabling anti-passback reduces the total card capacity of the SCP panel(s) in the site. Once anti-passback is enabled, all SCP panel(s) in the site will use anti-passback. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Timed Antipassback

Select (check) this option if timed anti-passback is to be used. Timed anti-passback is used to prevent the "passing back" of a card from card holder to card holder when entering or

leaving a designated area for a certain period of time. If the card is used more than once, the card holder may or may not be granted access to the area and an anti-passback event (transaction) will be generated. For more information on timed anti-passback, see the [Readers](#) help file topic.

Enabling timed anti-passback reduces the total card capacity of the SCP panel(s) in the site. Once timed anti-passback is enabled, all SCP panel(s) in the site will use timed anti-passback. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Card Groups

Select (check) this option if card groups are to be used. Card groups will group together cards with the same card group number assigned to them. The card group number can then be used to have a single card or a group of cards perform tasks when a card number from a certain card group is presented at a reader. For example, the lights could be turned on in the area where an employee works when their card is presented at the reader for the entrance to that area. The task to be performed by the card group and the conditions under which to perform the task are defined in the tasks screen. For more information on tasks, see the [Tasks](#) help file topic.

Enabling card groups reduces the total card capacity of the SCP panel(s) in the site. Once card groups are enabled, all SCP panel(s) in the site will use card groups. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Use Companies

Select (check) this option if companies are to be used. Companies are used to control access to or partition cardholders, cards and access levels. Cardholders, cards and access levels can either be assigned to no company or to a specific company. Only users with access to the company that a cardholder, card or access level has assigned to them will be able to view, modify or delete those items. For more information on companies, see the [Companies](#) help file topic. For more information on users, see the [Users](#) help file topic.

Use Large Encoded Card ID

Select (check) this option if using PIV-I credentials. Large Encoded Card ID allows for a EP-series controller to not decode a card into a number and facility code, but to instead report the entire Encoded ID as the card number.

Card Activate/Expire Mode

Select the card activation and expiration mode. Either none, date only or date and time is supported. For more information on card activation and expiration, see the [Cards](#) help file topic. If none is selected date based card activation and expiration will not be supported.

Selecting date and time card activation and expiration reduces the total card capacity of the

SCP panel(s) in the site. Once date and time card activation and expiration is enabled, all SCP panel(s) in the site will use date and time card activation and expiration. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Access Levels Per Card

Select the maximum number of access levels that can be assigned to each card. The number is selectable from 1 through 128.

Increasing this option reduces the total card capacity of the SCP panel(s) in the site. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

PIN Digits Per Card

Enter or select the maximum number of PIN digits that can be used for a card. This option can be set from 4 to 9 digits long.

Setting this option to more than 4 reduces the total card capacity of the SCP panel(s) in the site. For more information on SCP panel card capacities, see the [SCP's](#) help file topic.

Holiday Group Names

Enter a friendly description for the eight different holiday groups. The friendly name is an informational field only, an example would be to name Holiday Group 1 "Contractor Holidays".

[Sites](#)

Workstations

[Workstations Detail](#)

Workstations are used to create new or maintain existing client workstations by specifying various local file locations, integration options and cardholder enrollment options. The first time a workstation successfully connects to a regional server a new entry is automatically created in the database with all of the default settings for a workstation.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Adding a Workstation

To add a workstation, go to the workstations screen by clicking on the Workstations icon within the System group of the Navigation pane. All of the workstations in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Click on the new button on the ribbon or select new from the right click menu.

Editing a Workstation

To edit a workstation, go to the workstations screen by clicking on the Workstations icon within the System group of the Navigation pane. All of the workstations in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the workstation to be edited and click on the edit button on the ribbon, or double click the workstation to be edited. You can also select edit from the right click menu.

Deleting a Workstation

To delete a workstation, go to the workstations screen by clicking on the Workstations icon within the System group of the Navigation pane. All of the workstations in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the workstation to be deleted and click on the delete button on the toolbar. You can also select delete from the right click menu.

Printing Workstation Reports

To print reports for a workstation, go to the workstations screen by clicking on the Workstations icon within the System group of the Navigation pane. All of the workstations in the database will then be displayed in the right window pane of the Access It! Universal.NET desktop. Select the workstations to print reports for and click on the Reports button from the ribbon. You can also select print from the right click menu. The following report is available:

- *Workstation Listing* - This report provides a list of the selected Workstations and their various properties.

Workstations Detail

Workstations

Workstations are used to create new or maintain existing client workstations by specifying various local file locations, integration options and cardholder enrollment options. The first time a workstation successfully connects to a regional server a new entry is automatically created in the database with all of the default settings for a workstation.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Workstation Name

The workstation name is used to specify the computer name of the Access It! Universal.NET client workstation.

Workstation Description

The workstation description is used to specify a friendly name to the Access It! Universal.NET client workstation.

Attachments Location

The attachments location is the location on the local machine or network folder where the attachment files are located. Attachments are used to store scanned images, graphics, electronic forms, etc. with a card holder record. To choose a location, either enter the full path name to the folder where the attachment files are located or click on the change button to browse for a folder.

Compression Factor

The compression factor controls the quality and size of the attachment files. The compression factor can range from 2 to 255 with 2 being the highest quality with the lowest amount of compression and 255 being the lowest quality with the highest amount of compression.

Receive TCP Events

Select (check) this option to receive events and alarms at this workstation. If this option is not selected, no events or alarms will be sent to this workstation from the server and the events and alarms windows will not be displayed within Access It! Universal.NET. This option only applies to the local workstation. Other workstations will continue to receive events and alarms

as long as they have this option selected.

Enable DVR Integration for this Workstation

Select (check) this option to enable DVR (Digital Video Recorder) integration for the local workstation. DVR integration allows the local workstation to interact with a variety of DVR recording devices.

DVR licenses must be purchased separately for each workstation.

Enable CCTV Integration for this Workstation

Select (check) this option to enable CCTV integration for the local workstation. CCTV integration allows the local workstation to interact with a variety of CCTV control devices.

CCTV integration licenses must be purchased separately for each workstation.

Enable Intercom Integration for this Workstation

Select (check) this option to enable intercom integration for the local workstation. Intercom integration allows the local workstation to interact with a variety of intercom control devices.

Intercom integration licenses must be purchased separately for each workstation.

Auto Connect Video Recorder (DVR)

Select (check) this option to have the associated DVR camera for an associated hardware device displayed on this workstation automatically when processing alarms or viewing maps for the associated site.

NOTE: DVR integration licenses must be purchased separately for each workstation.

Video Monitor # (CCTV)

The associated monitor is the device that will be used when CCTV functions are activated from this workstation. CCTV cameras can be activated from either the alarms screen or the maps screen. For more information on the alarms screen, see the [Alarms](#) help file topic. For more information on the maps screen, see the [Maps](#) help file topic.

CCTV integration licenses must be purchased separately for each workstation.

Video Switcher Pre-select String (CCTV)

Enter the pre-selection string to be associated with this workstation. The pre-selection string will be sent to the CCTV switcher prior to the camera and monitor selection commands.

CCTV integration licenses must be purchased separately for each workstation.

Video Switcher Post-deselect String (CCTV)

Enter the post de-selection string to be associated with this workstation. The post de-selection string will be sent to the CCTV switcher after to the camera and monitor selection commands.

CCTV integration licenses must be purchased separately for each workstation.

Auto Connect on Camera Select (CCTV)

Select (check) this option to have the associated CCTV monitor for this workstation automatically selected when processing alarms or viewing maps for the associated site.

CCTV integration licenses must be purchased separately for each workstation.

Associated Intercom Station (Intercom)

The associated intercom station is the device that will be used when intercom functions are activated from this workstation. Intercom stations can be activated from either the alarms screen or the maps screen. For more information on the alarms screen, see the [Alarms](#) help file topic. For more information on the maps screen, see the [Maps](#) help file topic.

Intercom integration licenses must be purchased separately for each workstation.

Auto Connect on Intercom Select (Intercom)

Select (check) this option to have the associated intercom station for this workstation automatically connected when processing alarms or viewing maps for the associated site.

Intercom integration licenses must be purchased separately for each workstation.

Recognition Handkey and Bioscrypt/L1/Morpho Settings

Select the comm port and baud rate setting for any RSI Handkey or IP/comm port for any Morpho/Bioscrypt biometric enrollment readers attached to this workstation. These settings can be obtained from the biometric device manufacturer.

Biometric licenses must be purchased separately in order for biometric support to take effect.

Enrollment Readers

Card enrollment readers are used to automatically fill in the encoded card number and facility code when a new card is presented at an enrollment reader and look up and display existing cards when presented. Check (select) any of the available enrollment readers for which options are to be defined. Next, select whether to display the cards screen or the card wizard when a new card is presented and whether to display the cards screen when an existing card is presented. Only readers configured for a reader mode Enrollment Reader are listed.

The Large Encoded Card ID Cards section is used for enrolling PIV-I formatted cards. This

requires the option of manually entering a friendly card number upon enrollment (Manual card number entry), or having the application automatically assign a card number and increment each enrolled card (automatic card number entry).

In order to enroll Large Encoded ID Cards, the site option Use Large Encoded Card ID must be enabled.

Encode/Enroll (Biometrics)

Define any encoding devices that are attached to this workstation. Encoders are used to either encode (burn) biometric and/or card information to smart cards or launch a third party biometric enrollment executable. Click New to create a new encode. Enter a friendly name for the encoder, select the encoder type and enter the appropriate parameters for the encoder. These settings can be obtained from the encoding device manufacturer.

The Encoding license much be purchased separately.

The Biometric license much be purchased separately.

Workstations

Diagnostics

Diagnostics are used to view the Access It! Universal software's communications with the SCP panel(s). Diagnostics are used for troubleshooting purposes only and should never be used for the daily operation of the system. All communications between the SCP panel and the Access It! Universal.NET software will be displayed in the diagnostics window.

Access to this screen is determined by the settings for the currently logged in user. For more information on users, see the [Users](#) help file topic.

Viewing Diagnostics

To view diagnostics, go to the diagnostics entry screen by clicking on the Diagnostics icon within the System group of the Navigation pane.

Debugging

Debugging is used to control the writing of diagnostic information to a text file on the computer hosting the access control server service. This text file is used by Access It! Universal.NET support personnel to help diagnose system problems. Debugging is used for diagnostic purposes only and should never be used for the daily operation of the system.

To turn on debugging, click the debug to file button on toolbar button in the diagnostics window. This will create two text files in the application folder on the server, called SCPDebug.txt and APCDebug.txt. This file may be requested by Access It! Universal.NET support personnel for troubleshooting purposes.

Leaving debugging turned on can decrease the overall performance of the system and the debug files on the server will get very large and consume hard disk space.

Direct Command

Direct commands are used to send direct numeric commands to the SCP panel(s). Direct commands are used for diagnostic purposes only and should never be used for the daily operation of the system. There are many direct commands available and discussing them here is beyond the scope of this documentation. Direct command usage may be requested by Access It! Universal support personnel.

To send a direct command, click within the direct command text box in the diagnostics window. Enter the direct command to be sent to the SCP panel. Click the Send to SCP DII button to send the command to the SCP panel immediately.

Direct commands can be very complex and are only recommended to be used by advanced users with the assistance of the Access It! Universal.NET technical support staff. Sending an invalid direct command can compromise the security and functionality of the system.

Panel Utility

The Access It! Universal.NET Panel Utility is used to set network parameters, perform diagnostics and download firmware into the system controller processor and sub panels. To run the Panel Utility, click on the windows start button, then choose the Panel Utility from the Access It! Universal.NET Client Utilities program folder.

Attach to Panel

Select the Attach button to open the Attach Panel properties screen

Panel Type

Select the type of SCP that is attached.

Comm Type

TCP/IP - The attached panel is communicating via TCP/IP

Hardwired - The attached panel is communicating via a RS-232 connection

Address

Select the address the SCP is configured for. The default Address is 0.

IP Address

Enter the IP address the SCP is configure for.

TCP Port

Enter the TCP port the SCP is configured for. The default port is TCP port 3001.

SIO Port Speed

Select the SIO Port speed the SCP and SIO's are configured for. The default baud rate is 38400

Detach

Select the Detach button to detach from a SCP.

Download SCP Firmware

Select the Download SCP Firmware button to browse for a firmware file to download to the SCP.

Set SCP OEM Code

Select the Set SCP OEM code button to load in a specified OEM code. the Authorization code to change the OEM is required and can only be obtained from RS2 Technical Support.

Request Status

Select the Request Status button to perform a request from the SCP. The response is then shown in the Messages tab.

Direct Command

Select the Direct Command button to send a direct command that can be sent to the SCP.

Add SIO

Select the Add SIO button to open the Add SIO properties screen

SIO Model

Select the model of the SIO that is being added.

SIO Address

Select the RS484 address of the SIO being added.

Refresh SIOs

Refresh the status of all installed SIOs

Dnld SIO F/W

Select the Dnld SIO F/W button to browse for a firmware file to download to the specified SIO.

Set SIO OEM

Select the Set SIO OEM code button to load in a specified OEM code. The Authorization

code to change the OEM is required and can only be obtained from RS2 Technical Support.

Programming a new IP address

To program a new IP address into a non-EP style panel, select the Lantronix COBOX Programmer from the Tools menu.

MAC Address

Enter the MAC address for the SCP panel. The MAC address is a unique number that identifies the SCP panel. This alpha-numeric number is printed on the SCP panel near the RJ45 network jack that connects the panel to the network. The number is in the format XX-XX-XX-XX-XX.

IP Address

Enter the IP address for the SCP panel. The IP address is a unique number that identifies the SCP panel on the network. The number will be provided by the system or network administrator. The number is in the format XXX.XXX.XXX.XXX.

Entering the wrong IP address can cause SCP panel malfunction and disrupt functionality of other devices on the network.

Gateway IP Address

Enter the gateway IP address for the SCP panel. The gateway IP address is a number that identifies the router for SCP panel on the network. The number will be provided by the system or network administrator. The number is in the format XXX.XXX.XXX.XXX.

Subnet Mask

Select the subnet mask for the SCP panel. The subnet mask is a number that identifies the local segment for the network. The number will be provided by the system or network administrator. The number is in the format XXX.XXX.XXX.XXX.

Panel Type

Select the model number of the SCP panel being programmed.

Disable Web Server

Check to disable the on-board Lantronix web server.

Telnet Password

If required, a telnet password can be set to prevent unauthorized access through telnet.

Set IP Configuration

Click on the set configuration button to send the entered network parameters to the SCP panel.

The SCP panel must be on the same subnet as the PC being used to program the SCP panel. If it is not, the IP programmer will respond with a timeout error due to the fact that it is unable to find the MAC address on the network.

System Status

The system status screen is used to display information about the access control system database, dongle (software key) and client workstations. To access the system status screen, go to the system status screen by either clicking on the system status toolbar button within the system group on the toolbar or select system status from the go option on the system menu. Several system statistics can be clicked on to navigate to a filtered view of the respective screen.

The following system status information is displayed:

System Statistics

- *Total Cards* - Displays the total number of cards in the system database.
- *Active Cards* - Displays the total number of active cards in the system database. Cards are considered active when the card status is set to either active or date based with a date range that falls within the current system date.
- *Installed SCPs* - Displays the total number of active SCP panels in the system database. An SCP is considered active when it's device installed check box has been checked (selected).
- *Installed SIOs* - Displays the total number of active SIO panels in the system database. An SIO is considered active when it's device installed check box has been checked (selected).
- *Installed Readers* - Displays the total number of active readers in the system database. A reader is considered active when the SIO panel that it is attached to has its device installed check box checked (selected).
- *Installed Inputs* - Displays the total number of active inputs in the system database. An input is considered active when the SIO panel that it is attached to has its device installed check box checked (selected).
- *Installed Outputs* - Displays the total number of active outputs in the system database. An output is considered active when the SIO panel that it is attached to has its device installed check box checked (selected).
- *Unlocked Doors* - Displays the total number of unlocked doors in the system.

System Warnings

- *Pending Alarms* - Displays the total number of system alarms that have not been acknowledged.
- *Unsecured Doors* - Displays the total number of doors in the system that are currently in an unsecured state. A door is considered unsecured when the door contact for the door is not in a normal state. The normal state is determined by the door contact

configuration option setting in the readers screen.

- *Unsecured Inputs* - Displays the total number of inputs in the system that are currently in an unsecured state. An input is considered unsecured when the input is not in a normal state. The normal state is determined by the input configuration option setting in the inputs screen.
- *Offline SCPs* - Displays the total number of SCP panels that are currently off-line. An SCP is considered off-line when its device installed check box has been checked (selected) and Access It! Universal cannot communicate with the SCP panel.
- *Offline SIOs* - Displays the total number of SIO panels that are currently off-line. An SIO is considered off-line when its device installed check box has been checked (selected) and the SCP panel that it is attached to cannot communicate with the SIO panel.

Today's Scheduled Events

- *Card Activations* - Displays the total number of cards that will be automatically activated in the system database. Automatic activation occurs on the current system date for any cards that have their date based activation date set to the current system date.
- *Card Deactivations* - Displays the total number of cards that will be automatically deactivated in the system database. Automatic deactivation occurs on the current system date for any cards that have their date based deactivation date set to the current system date.

Software License

- *Regional Server* - Displays the regional server that is hosting the currently selected site.
- *Server Version* - Displays the version number for the application server. If a client is running a different version than the server the word "Mismatch" is displayed in red.
- *Dongle Status* - Displays the current status of the attached dongle key. Displays "OK" if a key is present and is the correct version. Displays "Wrong Version" if the attached key is not for the currently installed software version. Displays "Not Attached" if a key is not detected and the software is running in demo mode.
- *Serial Number* - Displays the factory programmed serial number for the application software.
- *Key Revision* - Displays the factory programmed key revision number for the application software.
- *Max Sites* - Displays the number of sites (partitions) that have been licensed for the system.
- *Max SCPs* - Displays the maximum number of SCP panels that can be installed for each site.
- *Workstations* - Displays the total number of workstations that have been licensed for the system. A license must be purchased for each concurrent workstation that will be attached to the system.
- *DVR Integration* - Displays the total number of DVR (digital video recorder) control

workstations that have been licensed for the system. A license must be purchased for each concurrent DVR workstation that will be attached to the system.

- *Intrusion Panels* - Displays the total number of intrusion panels that have been licensed for the system.
- *Email/Paging Integration* - Displays whether or not email and paging integration is enabled within the application software.
- *Report Designer* - Displays whether or not the custom report designer is enabled within the application software.
- *MR-52 Alternate Wiring* - Displays whether or not alternate MR-52 wiring has been enabled within the application software. Alternate MR-52 wiring will change the location of the door contact, exit request and door strike relays so that re-wiring is not necessary when performing a retrofit installation.
- *ID Badging* - Displays whether or not ID badging has been enabled within the application software.
- *Biometric Support* - Displays whether or not any type of biometric reader support is enabled within the application software.
- *Encoder Support* - Displays whether or not any type of encoder support is enabled within the application software.
- *Barcode Support* - Displays whether or not barcodes can be added to badge types.
- *Terminal Server Support* - Displays whether or not clients can run the application via Windows Terminal Server.
- *Web Client Support* - Displays whether or not web client support is enabled within the application software.
- *Regional Server Support* - Displays whether or not multiple regional servers can be used within the system.
- *Time And Attendance* - Displays whether or not time and attendance functionality has been enabled within the application software.
- *Import/Export* - Displays whether or not the import/export utility is enabled within the application software.
- *Companies* - Displays whether or not companies are enabled within the application software.
- *OEM Codes* - Displays the OEM codes that the system has been licensed for. The application software will only communicate with hardware panels that match one of the OEM codes licensed in the key.
- *IP Locksets Enabled* - Displays whether or not the system will support ASSA ABLOY IP locksets. Reports Yes if enabled, No if not enabled, and Error if enabled but the ASSA ABLOY integration services are not running.
- *Integrated Reader Count* - Displays the total number of Integrated readers that have been licensed for the system. Integrated readers include SALTO, ASSA ABLOY, Allegion AD Series, Allegion NDE Series, SimonsVoss, Honeywell, Vanderbilt, Telaeris, KONE, and OTIS Elevator readers. A license must be purchased for each Integrated reader that will be attached to the system.
- *Data Exchange Utility* - Displays whether or not the Data Exchange Utility allowing for

scheduled imports is enabled within the application software.

- *Mercury PW/PRO Hardware* - Displays whether or not the ability to communicate to Honeywell hardware is enabled within the application software.
- *SALTO Integration* - Displays whether or not the ability to communicate to SALTO SHIP hardware is enabled within the application software.
- *Advanced Elevator Control* - Displays whether or not the ability to communicate to OTIS or KONE elevators is enabled within the application software.
- *PSIA Service* - Displays whether or not the ability to communicate using the PSIA service is enabled within the application software.

Workstations/Users/Options

Displays all of the currently attached (running) workstations, the users currently using the workstations and the options in use for the workstations. In addition, right clicking on a workstation will allow instant messages to be sent to other attached workstations if the currently logged in user has permission to perform this function. For more information on users, see the [Users](#) help file topic.