RACK ARMOR™

U.S. PATENT 9,466,190

Powered by PremiSys™

Installation and Setup Manual

Table of Contents

While every precaution has been taken during the preparation of this setup and operations manual to ensure the accuracy of its contents, IDenticard Systems and Brady Worldwide assume no responsibility for errors or omissions. We continually strive for improved product quality and performance, so IDenticard Systems and Brady Worldwide reserve the right to change at any time the specifications and performance features of this product without notice or obligation. In addition, IDenticard Systems and Brady Worldwide shall not under any circumstances be liable for any incidental or consequential damages arising from loss of property or other damages or losses owing to the failure of this product, beyond the cost of repair or replacement of any defective product.

Introduction to Rack Armor™

Rack Armor is a product of IDenticard Systems and provides card access control and electronic monitoring of server rack cabinet doors. Rack Armor is powered by PremiSys software, version 2.15 or higher. Rack cabinet access control hardware is mounted on the *outside* of the server rack door, within a patent-pending enclosure. The proximity card reader is integrated with the door's electronic lock, swing handle and latch. Power is provided via POE through the PremiSys controllers and boards.

Cardholders are enrolled in the PremiSys software. Server cabinet door access is restricted and monitored by PremiSys hardware. PremiSys can be configured to send an email alert or link an audible sounder upon a Rack Armor alarm. PremiSys provides comprehensive system reports for auditing purposes. With DVR integration, PremiSys can call up live video cameras or retrieve video clips from cameras associated with Rack Armor points and events.

For system sales or to schedule a demonstration, contact your Authorized IDenticard Partner, Access Regional Sales Manager or Manufacturer Representative. Marketing materials and training videos are available online at www.IDenticard.com, or call (855) 367-4721.

1. Hardware Installation

1.1 PremiSys Hardware Preparation

Complete POE controller and POE board layout diagrams, drawings and programming instructions are provided in the PremiSys Hardware Manual.

For POE Controllers

- Before installing PremiSys controllers on the rack cabinet doors, be sure to program each controller with a static IP address using the web configurator.
- Be sure the controller voltage input jumper is set to POE.

For POE Reader Boards

- Before installing POE Reader Boards, program each with a static IP address using MR51eAddressTool.exe in the Utilities folder of the PremiSys software installation CD. Step by step instructions are provided in Section 2 of this document.
- Be sure the board input voltage jumper is set to POE.
- Prepare wiring for cabinet door position contacts. For RACK1 kit, The back door’s POE reader board Input 1 is used for the front cabinet door contact. Input 2 is used for the back cabinet door contact.

1.2 Rack Armor Door Preparation and Mounting

A graphic guide of these steps is provided in the Rack Armor hardware kit, or refer to Appendix B.

Installation Preparation: Remove existing latch. Refer to the cabinet manufacturer's instructions. Keep existing cam or rod system. Verify that door prep measurements are 25mm x 150mm. Make modifications if needed. Before mounting the hardware enclosures, ensure **PREM-RA-CTLR1POE** (Kit #1) and **PREM-RA-BRD1POE** (Kit #2) have been programmed static IP addresses. Any future change to its static IP address will require dismantling and re-mounting the hardware enclosure. For your reference, a MAC address label is affixed to the outside bottom of each enclosure.

Step 1: Tape supplied template to mark 7/8" and 21/64" drill holes with center punch. Insert nylon bushing into 7/8" hole from inside the door.

Step 2: Route Ethernet cable *(not supplied)* through nylon bushing. Do not secure cable; you will need to remove slack after enclosure is installed on door. Leave slack for cable placement. *(Ethernet cable cannot have a boot/hood.)*

Step 3: Install trim ring into position for either right or left swing door, placing the fill plate in the unused side.

Step 4 (optional): Connect the optional enclosure tamper switch.

Step 5: Route Ethernet cable through back of the enclosure and plug into the Ethernet port.

Step 6: Connect door position input. Route two jumper cables from board through the back of the Kit#2 enclosure and nylon bushing. See wiring detail.

Step 7: Secure enclosure with the four supplied screws.

Step 8: Insert electronic swing handle with reader into trim ring and door.

Step 9: Secure the reader to the door using the two supplied brackets.

Step 10: Connect the two wiring harnesses to electronic swing handle/reader.

Step 11: Insert snap rivet through the back of door into the back of the enclosure. Tighten the snap rivet to secure the enclosure to the door. Secure wires and Ethernet cable. All cables need to be secured.

Step 12: Place existing cam or rod system from the mechanical latch onto the new electronic swing handle. The supplied cam extender can be used to adjust the depth of the cam so that the latch catches the frame. The direction the swing handle opens is dictated by how the locking ring is seated. Simply rotate it 90 degrees if the direction needs to be changed.

PREM-RA-RACK1 connections and swing handle detail

The first Rack Armor cabinet is item PREM-RA-RACK1 and provides one Kit #1 for the front door, and one Kit #2 for the back door. With one PREM-RA-RACK1, up to seven additional cabinets can be added on the same subnet using item PREM-RA-RACK2 (two Kit #2s).

Kit #1 – Front door of a RACK1

The PoE Controller comes pre-mounted inside a Rack Armor enclosure. Install the enclosure on the exterior of the server cabinet's front door. The Controller is prewired with quick connectors for reader, lock actuator and swing handle. To monitor the physical position of the front cabinet door, the *front* door's contact is wired to the PoE One-Door Reader Board installed on the *back* cabinet door. See next page. Supervision type for all lock status inputs is normally-closed.

PREM-RA-CTLR1POE (Kit #1)

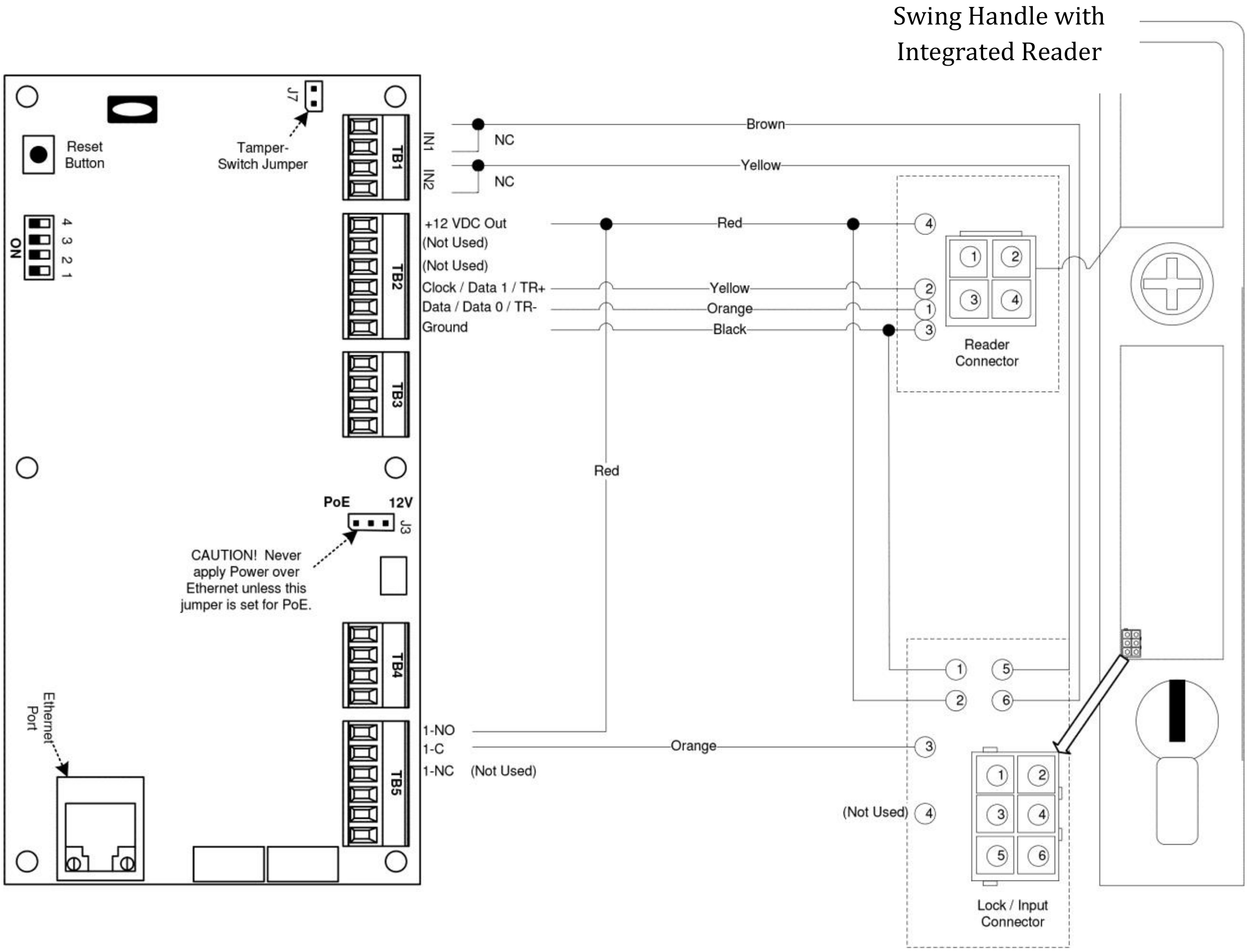


Figure 1.2.1 RACK1 front door (Rack Armor Kit #1) connection details

Terminations	Purpose
TB1 pre-wired quick connect	Input 1 = front electronic lock status (swing handle), wired normally closed Input 2 = front mechanical lock status (key), wired normally closed
TB2 pre-wired quick connect	Reader port 1 = front integrated reader
TB3 & TB4	Reader port 2 is not used
TB5 pre-wired quick connect	Relay 1 = front electronic lock, wired common and normally open Relay 2 is not used (available as a general purpose relay)

PREM-RA-RACK1 Kit #2 - Back door of a RACK1

The PoE One-Door Reader Board is pre-mounted inside a Rack Armor enclosure. Install the enclosure on the exterior of the server cabinet's *back* door. The PoE One-Door Reader Board is prewired with quick connectors for reader, lock actuator and swing handle. Supervision for cabinet door position indicator is configurable.

Swing Handle with
Integrated Reader

PREM-RA-BRD1POE (Kit #2)

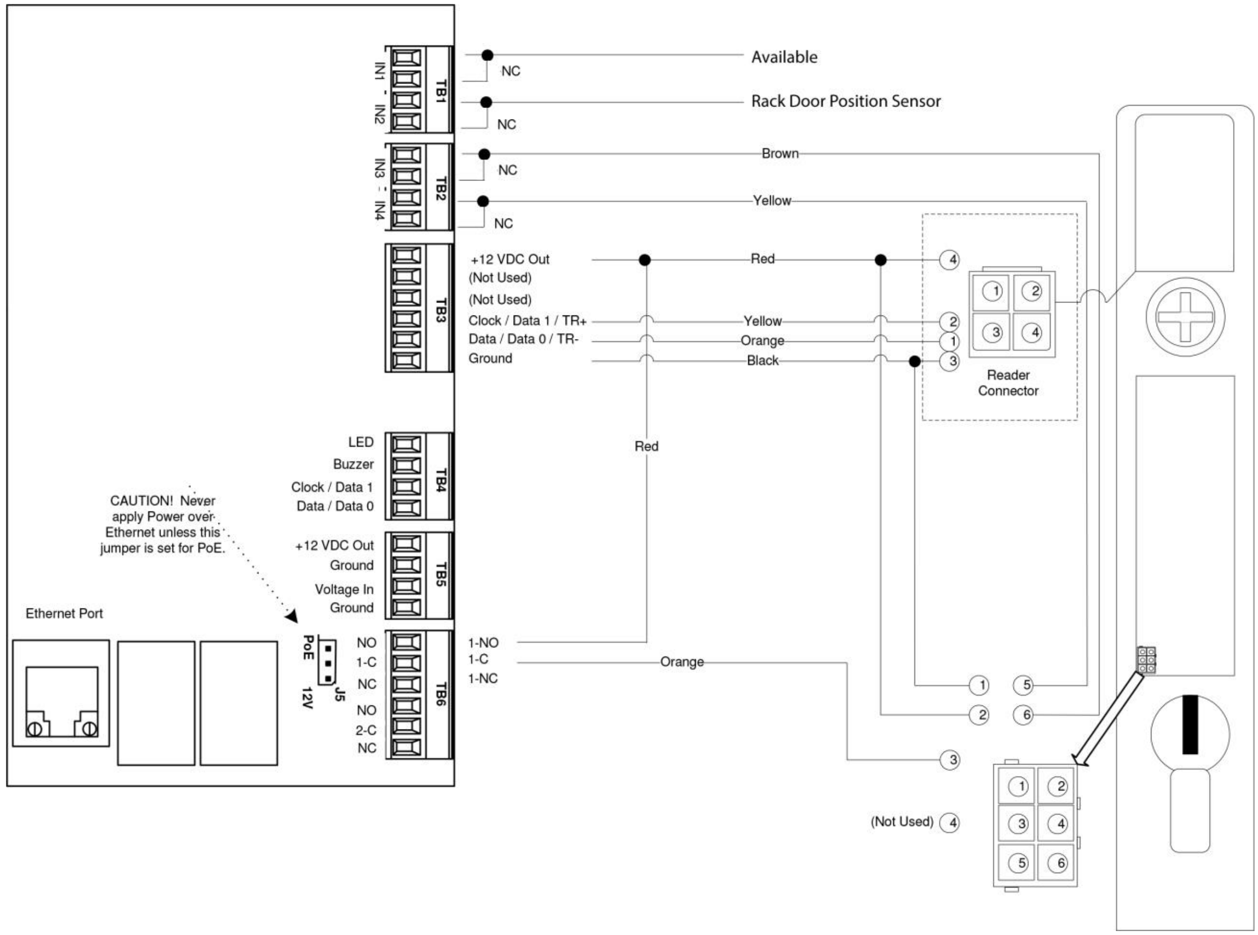


Figure 1.2.2 RACK1 back door (Kit #2) connection detail

Terminations	Purpose
TB1	Input 1 = front door position indicator, wire normally closed* Input 2 = back door position indicator, wire normally closed*
TB2 pre-wired quick connect	Input 3 = back electronic lock status, wired normally closed Input 4 = back mechanical lock status, wired normally closed
TB3 pre-wired quick connect	Reader port 1 = back door integrated reader
TB4	Reader port 2 (not used)
TB5 pre-wired quick connect	Relay 1 = back electronic lock, wired common and normally open Relay 2 is not used (available as a general purpose relay)

*Suggested wiring is NC. These inputs are software-configurable.
Supported supervision types are: NC; NO; 1K normal, 2K active; or 2K normal, 1K active

PREM-RA-RACK2 connections and swing handle detail

For each PREM-RA-RACK1 cabinet, up to seven additional server cabinets may be added to the system as PREM-RA-RACK2. A RACK2 cabinet has a Kit #2 on the front door and a Kit #2 on the back door.

Kit #2 - Front door or back door of a RACK2

PREM-RA-BRD1POE (in Kit #2)

Swing Handle with
Integrated Reader

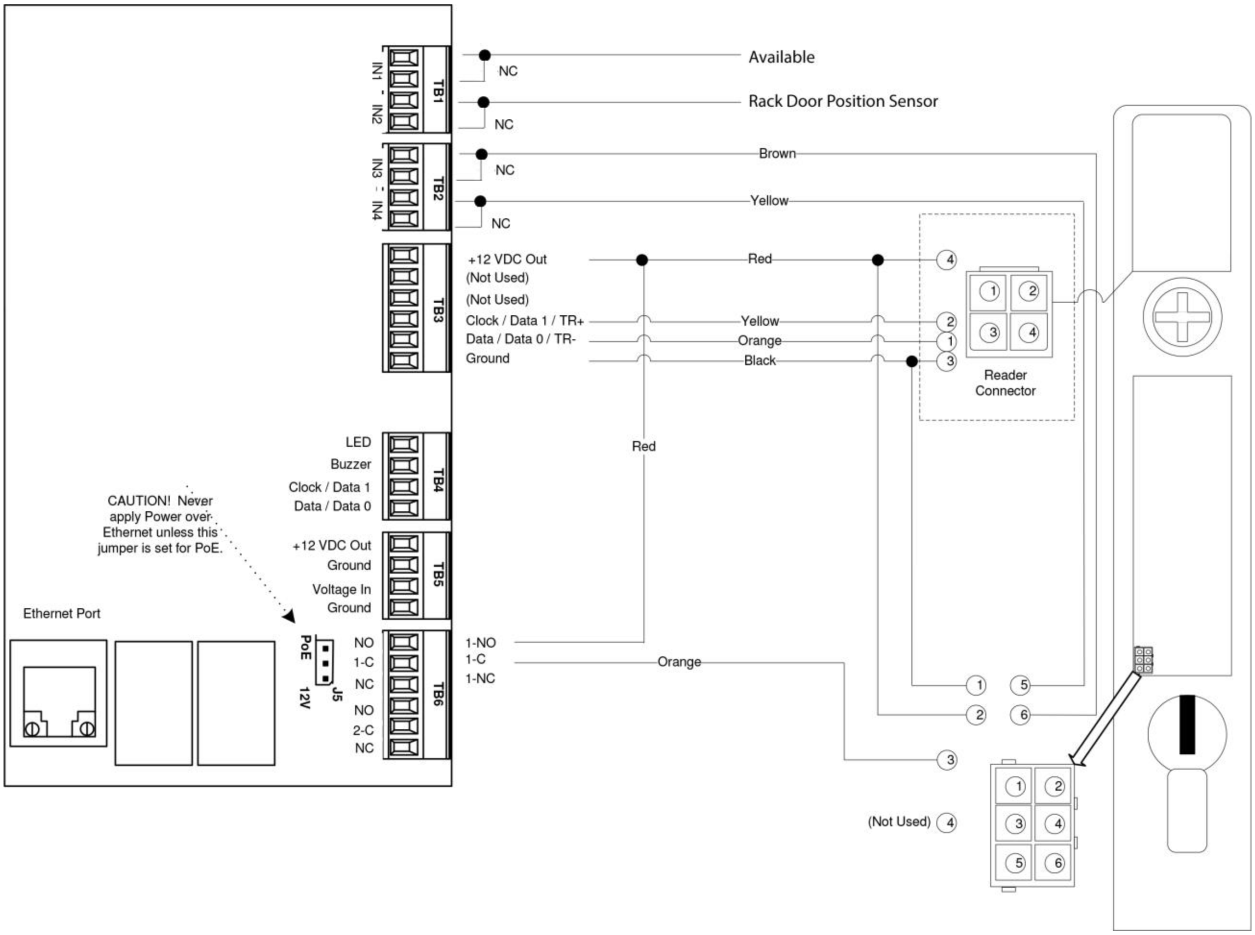


Figure 1.2.3 RACK2's front door or back door connection details

Terminations	Purpose
TB1	Input 1 = available*, can be used for monitoring top or side panel Input 2 = door position sensor*
TB2 pre-wired quick connect	Input 3 = electronic lock status, wired normally closed Input 4 = mechanical lock status, wired normally closed
TB3 pre-wired quick connect	Reader port 1 = integrated reader
TB4	Reader port 2 (not used)
TB5 pre-wired quick connect	Relay 1 = electronic lock, wired common and normally open Relay 2 is not used (available as a general purpose relay)

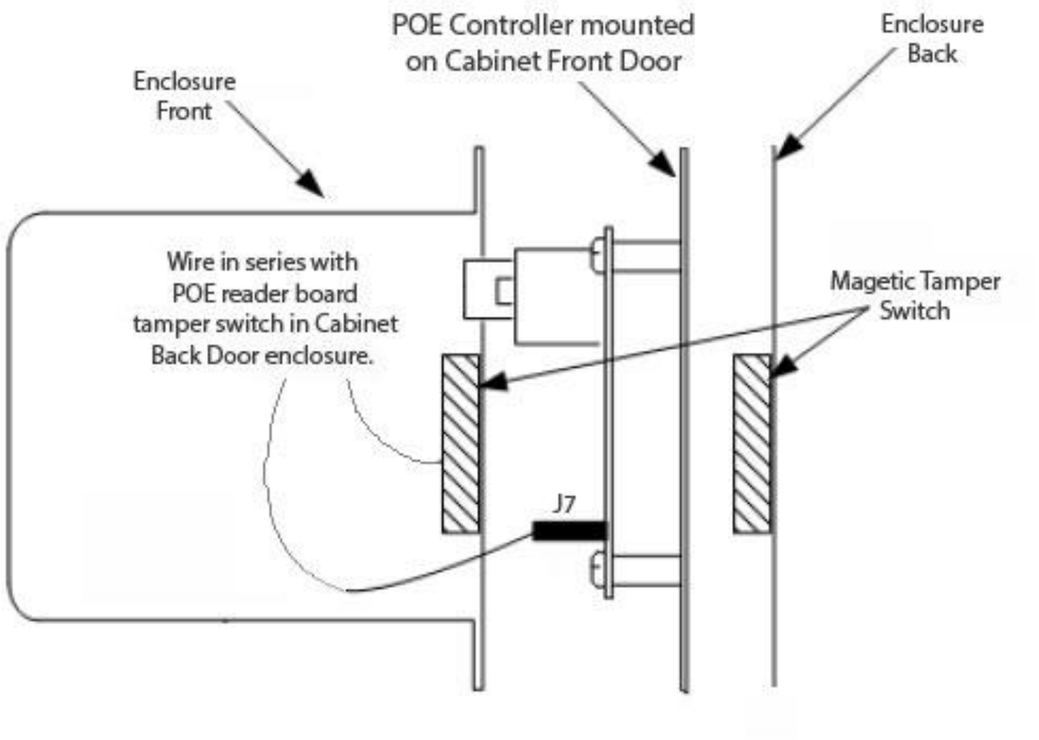
*Suggested wiring is NC. These inputs are software-configurable. Supported supervision types are: NC; NO; 1K normal, 2K active; or 2K normal, 1K active

Option tamper installation

The PoE Controller installed on the RACK1 front door has an onboard jumper for a monitoring tamper switch. It generates a tamper alarm event when a Rack Armor enclosure opens. The PoE One-Door Reader Board on the back door *does not* have a dedicated onboard component to monitor tamper alarm.

However, the front door PoE Controller may be used to monitor *both* the front *and* back tamper switches. Do this by wiring *two* normally-closed (NC) magnetic tamper switches in series, see Figure 1.2.4. Rack Armor magnetic tamper switches are sold separately, item PREM-POETAMPER.

Set Jumper J3 On. Wire magnetic tamper switches in series to Jumper J7 on the PoE Controller, as shown in Figure 1.2.3. This activates an alarm if either cover is removed. A closed loop (no resistors) is reported as secure. Open contacts log a "Tamper Alarm on Controller" event, whether it occurs at the front enclosure or back enclosure.


POE Controller mounted on Cabinet Front Door
Enclosure Back
Enclosure Front
Wire in series with POE reader board tamper switch in Cabinet Back Door enclosure.
Magetic Tamper Switch
J7

1.3 Hardware Point Supervision

Rack Armor distinguishes between normal events and alarm events based on changes-of-state to the PremiSys hardware onboard components. Alarm events are therefore determined by certain *combinations* of hardware conditions, and generated in a particular *sequential order*. Table 1.3.1 indicates how cabinet door activity reports, based on the initial sequence of events.

Table 1.3.1 Cabinet supervision on rack door opening

Events	Solenoid actuates	Swing handle opens	Door contact opens
Normal			
Rack - Door Unlocked	first		
Rack - Latch Open		second	
Rack - Door open			third
Alarm			
Rack - Key used		first*	
Rack - Forced open			first*

*An atypical event generates a rack alarm.

Technicians usually access server cabinets for variable periods of time. Therefore, when a cabinet door opens normally – without an alarm – Rack Armor will not generate a time-based alarm while the door stays physically open. If administrators require time-based notifications, configure custom trigger/procedures.

Racks are also monitored to log events as the cabinet doors become locked and secured again, see Table 1.3.2. If either the physical door or the swing handle is not closed within 10 seconds of the other, Rack Armor logs a "Rack not Secure" alarm event.

Table 1.3.2 Cabinet supervision on rack door closing

Event	Swing handle closed	Door contact closed
Normal		
Rack - Latch Closed	yes	
Rack - Door Closed		yes
Rack - Door Locked	yes	yes
Alarm		
Rack not Secure - Door Left Open*	yes	no, after 10 seconds
Rack not Secure - Swing Handle*	no, after 10 seconds	yes

*These alarms can be suppressed on a per cabinet basis, see checkbox in lower-left corner of Figure 2.4.2.

For a complete list of Rack Armor transactions, refer to Appendix A.

2. Software Setup

2.1 Installation and Specifications

Rack Armor is 'powered by PremiSys'. Rack Armor is feature available in PremiSys version 2.15. For PC specifications, refer to the read-me files and software installation instructions related to PremiSys. This manual covers features specific to Rack Armor and is a supplement to the comprehensive PremiSys software manual *IDentiHelp.chm*.

Authorized IDenticard Partners may access all available product documentation from *www.identicard.com*, click "Partner Login." Enter username and password, or register for a login. Once at the main Partner Resource Page, click "Find by Products" menu and select "PremiSys."

2.2 Rack Armor Licensing

Rack Armor is licensed per cabinet. A single cabinet license includes both front and back door, whether both doors are used or not. The purchase of a Rack Armor kit includes the corresponding reader license. However, these reader licenses must be activated in order to enable cabinets to be added in the software. As a result, PremiSys Try Mode does not support Rack Armor setup.

Activate licenses
To activate Rack Armor licenses, call IDenticard Technical Support while you are seated at the *PremiSys server machine* and *logged into PremiSys*. Know your Partner account number ready, and be ready to provide the customer's main software license code (printed on the start-up kit purchased invoice).

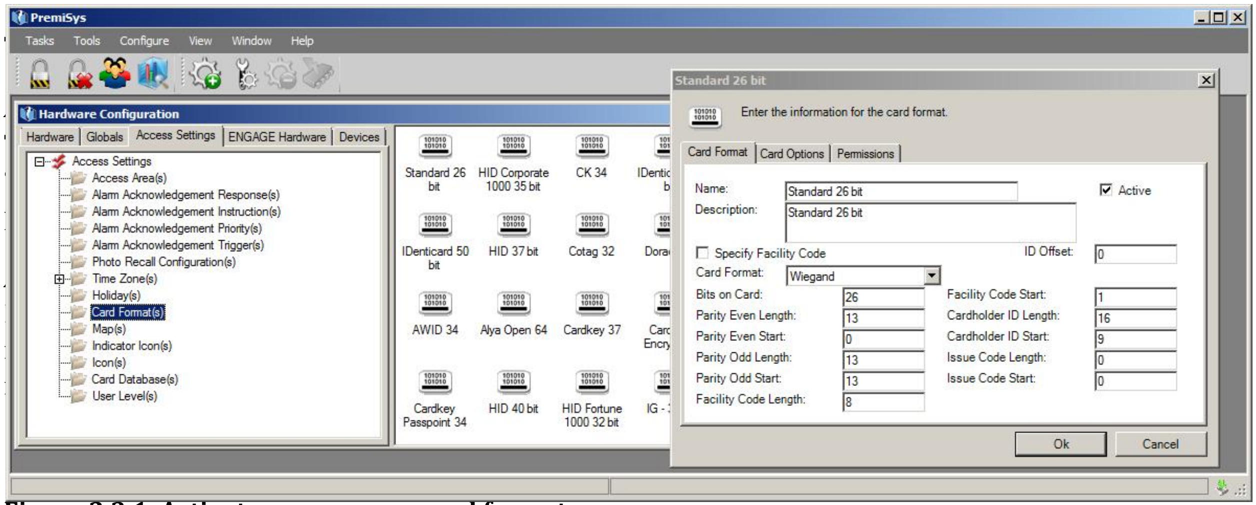
Look up licenses
To look up the number of existing Rack Armor licenses in the software, both *Total* and *Remaining*. Log in on any PremiSys client PC. Go to Help > License Upgrade. Click "Hardware" tab.

Transfer a license
If a customer needs to replace their PremiSys server machine, contact Technical Support in order to be able to activate PremiSys and Rack licenses on the new machine. Have your Partner number and system license number (found on the system invoice) ready when calling in.

2.3 Site Tree Setup

You do not need to have the physical hardware installed before start setting up the software. However, you will need to know the name of the cabinets, and the static IP addresses of your POE hardware.

Activate Card Format(s)
To begin, activate a card format, go to the *Tasks* pull-down menu, select *Hardware Configuration* and click on “Access Settings” tab. Locate and click on the folder “Card Format(s).” The window on the right displays preconfigured card formats. Double-click on the card format that matches your access credentials. Check the “Active” checkbox. If using a site code, i.e. facility code, check the “Facility Code” checkbox and enter one facility code in the field that appears.



Enter the information for the card format.

Name: Standard 26 bit

☑ Active

Description: Standard 26 bit

□ Specify Facility Code

ID Offset: 0

Card Format: Wiegand

Bits on Card:	26	Facility Code Start:	1
Parity Even Length:	13	Cardholder ID Length:	16
Parity Even Start:	0	Cardholder ID Start:	9
Parity Odd Length:	13	Issue Code Length:	0
Parity Odd Start:	13	Issue Code Start:	0
Facility Code Length:	8		

Figure 2.3.1 Activate one or more card formats

Add a Card Database

Go to the *Tasks* pull-down menu, select *Hardware Configuration* and click on "Access Settings" tab. Locate and right-click on the folder "Card Database(s)." Select "Add Card Database." Default settings meet most systems' needs. Click the F1 button on your keyboard to read descriptions of selectable Card Database fields. Click "OK" to save your new Card Database.

Add a site

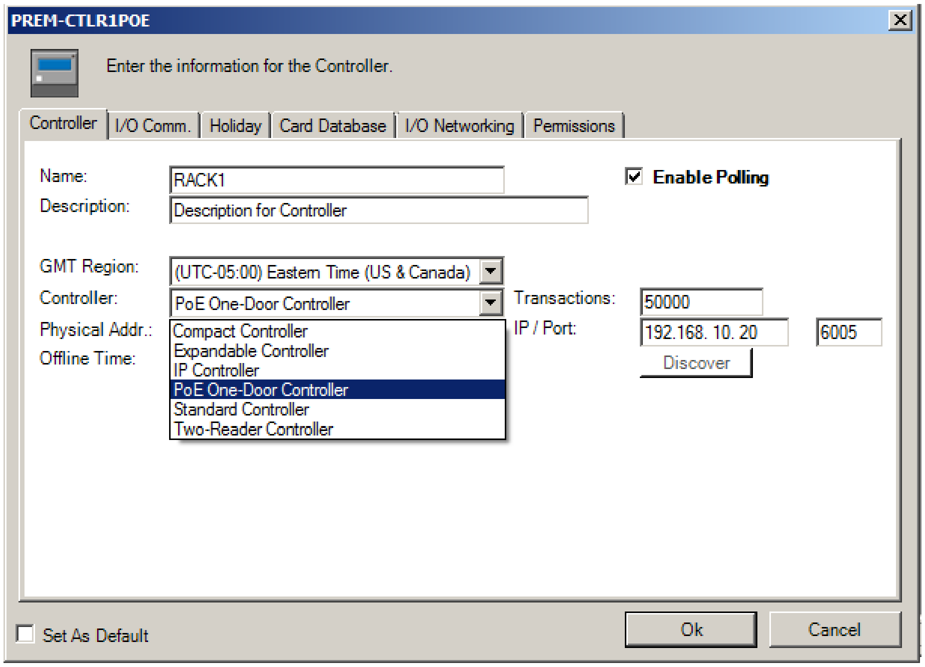
Go to the Tasks pull-down menu, select Hardware Configuration. Under the "Hardware" tab, right-click on "Site(s)" folder and add a site. A good name for the site is the physical building name. Site names can be used for reporting and hardware filters.

Add a channel

Right-click the "Channel" folder and add a channel. Each PoE Controller of a RACK1 Kit 1 will have its own channel. The best name for the channel depends on the following: if you have a RACK1 by itself, name it "A-101." If you will have a RACK1 with one to seven RACK2s downstream, name the controller "A-101 to A-108." For the other channel field, leave the default settings; *Comm. Type* should be set to "Network Out." Click "OK" to save the channel.

Add a controller (RACK1, Kit #1)

Right-click the "Controller(s)" folder and add a Controller. The best name for the controller will match the name of the channel in the previous step. A new controller setup window is shown in Figure 2.3.2.



PREM-CTLR1POE

Enter the information for the Controller.

Name: RACK1

Description: Description for Controller

☑ Enable Polling

GMT Region: (UTC-05:00) Eastern Time (US & Canada)

Controller: PoE One-Door Controller

Transactions: 50000

IP / Port: 192.168. 10. 20 6005

Physical Addr.:

Offline Time:

□ Set As Default

Figure 2.3.2 Controller setup window

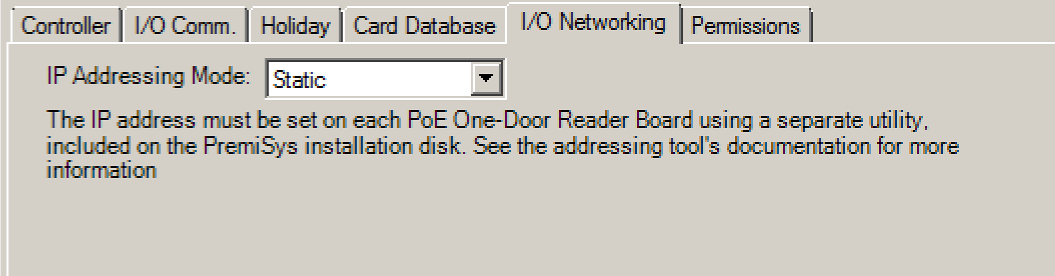
"Controller" tab is used to specify controller type and IP/TCPIP settings. Select "PoE One-Door Controller" for controller type. Enter IP address and TCPIP address. Always program the controller's IP address *before* connecting it to the customer's network. See the PremiSys Hardware Manual for instructions on programming controllers with the Web Configurator.

"I/O Comm." tab defaults are appropriate for most Rack Armor applications. Do not check "Enable Downstream Communication" unless you will install additional PREM-BRD-IN boards or PREM-BRD-OUT boards either for: 1) "linked cabinets" where a single reader controls all doors in a row, or 2) to monitor cabinet top and side panels.

"DST/Holiday" tab is used to set Daylight Savings and Holidays. Daylight savings must be updated each year, sometime between November and March. Holidays are normally not necessary for Rack Armor systems.

"Card Database" tab requires a card database be selected. If you don't see one, create a new one under Tasks > Hardware Configuration > Access Settings tab > Card Databases folder. Right-click “Add Card Database” and “Save.”

"I/O Networking" tab sets the controller to communicate with POE reader boards via Static IP. POE reader boards are installed on the RACK1 back cabinet door and all RACK2 doors, front and back. Select “Static” in the IP Addressing Mode drop-down menu, as shown in Figure 2.3.3.



IP Addressing Mode: Static

The IP address must be set on each PoE One-Door Reader Board using a separate utility, included on the PremiSys installation disk. See the addressing tool's documentation for more information

Figure 2.3.3 Choose Static

Use a separate program utility called "MR51eAddressTool.exe" to program a POE reader board with its static IP address. This utility is found in the Utilities folder of the PremiSys software installation CD or ZIP contents. Instructions for using this utility are found later in this chapter.

Click "OK" to save the controller. Expand the site tree under the new controller. You will see an "Onboard I/O Board" auto-generated. Be sure to change the default name "Onboard I/O board" to be the cabinet door name.

Rename the onboard I/O board for RACK1 front door

! IMPORTANT ! Right-click "Onboard I/O Board" under the "I/O Board(s)" folder, and choose Edit. Rename it "[Your Cabinet Name] Front" E.g. A-101. Click OK. When prompted to "Automatically Rename Associated Points," select "Yes." See Figure 2.3.4.

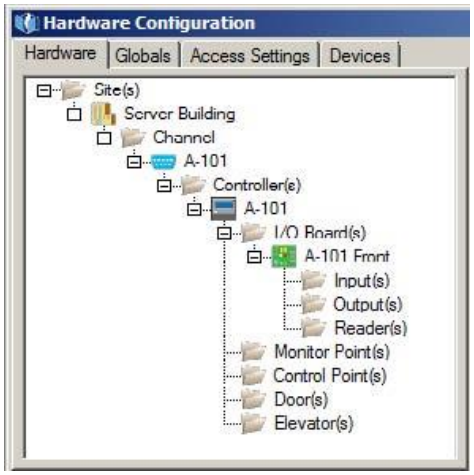
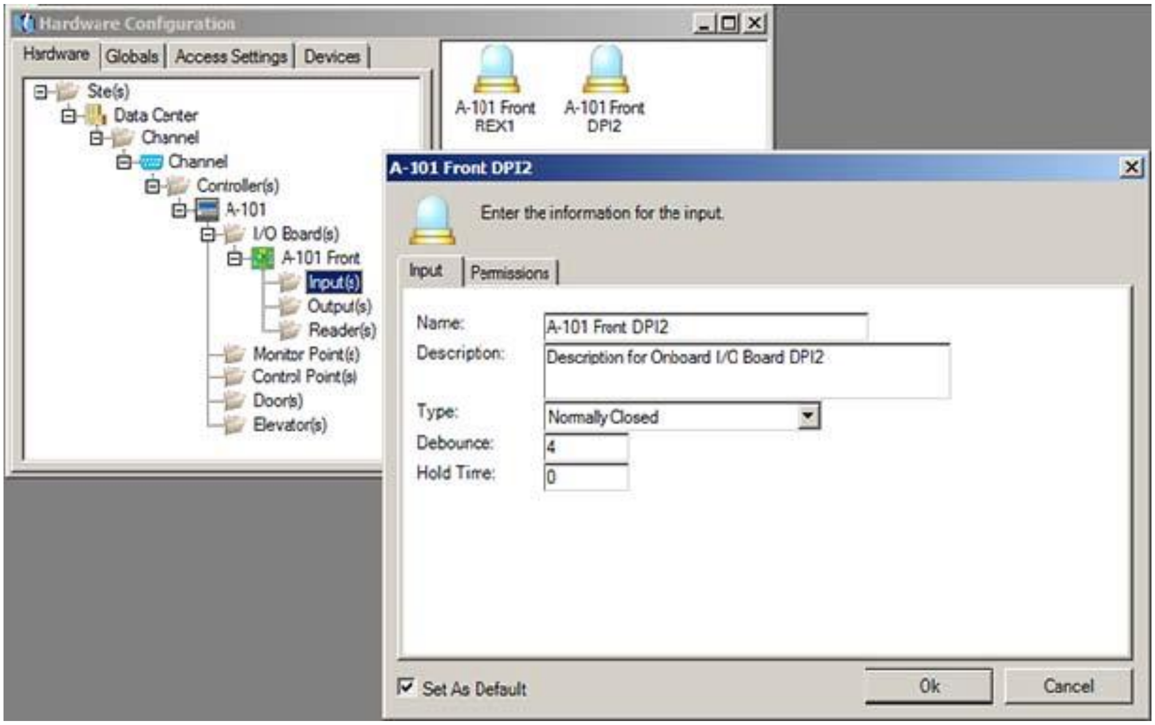


Figure 2.3.4 Controller named A-101 with its onboard I/O renamed A-101 Front

Edit input supervision type

The Rack Armor hardware quick connects are supervised Normally Closed. Click once on the Inputs folder below your new I/O board (green icon). If you don't see the Inputs folder, click on "+" next to the green I/O board icon.

Two inputs appear in the right-hand window. Double-click on each input icon and set type to "Normally Closed." Be sure to check the "Set As Default" checkbox as shown in Figure 2.3.5. This way, as new Rack Armor hardware is added, the new inputs will automatically default to Normally Closed supervision type.



Enter the information for the input.

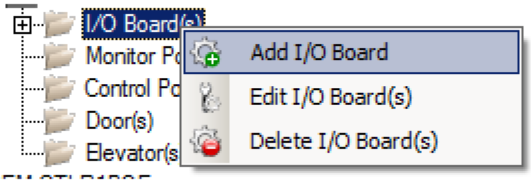
Name: A-101 Front DPI2
Description: Description for Onboard I/O Board DPI2
Type: Normally Closed
Debounce: 4
Hold Time: 0

☑ Set As Default

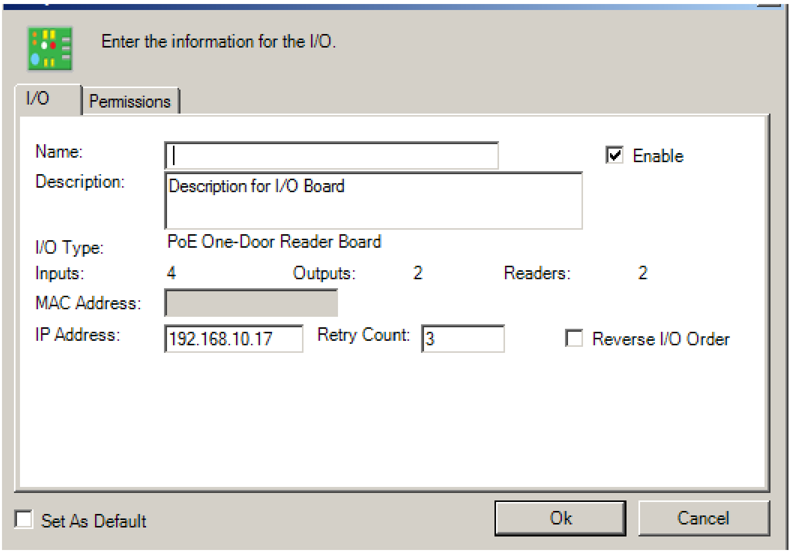
Figure 2.3.5 Set input supervision type to Normally Closed and check "Set As Default"

Add the POE reader board for Rack1's back door

Right-click on the "I/O Board(s)" folder, and choose Add.



Name it "[Your Cabinet Name] Back" E.g. A-101 Back. Enter the static IP address for this POE reader board, as shown below.



Enter the information for the I/O.

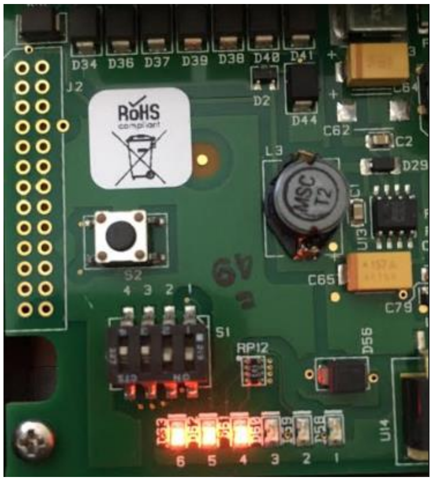
Name: |
☑ Enable
Description: Description for I/O Board
I/O Type: PoE One-Door Reader Board
Inputs: 4 Outputs: 2 Readers: 2
MAC Address:
IP Address: 192.168.10.17 Retry Count: 3 □ Reverse I/O Order

□ Set As Default

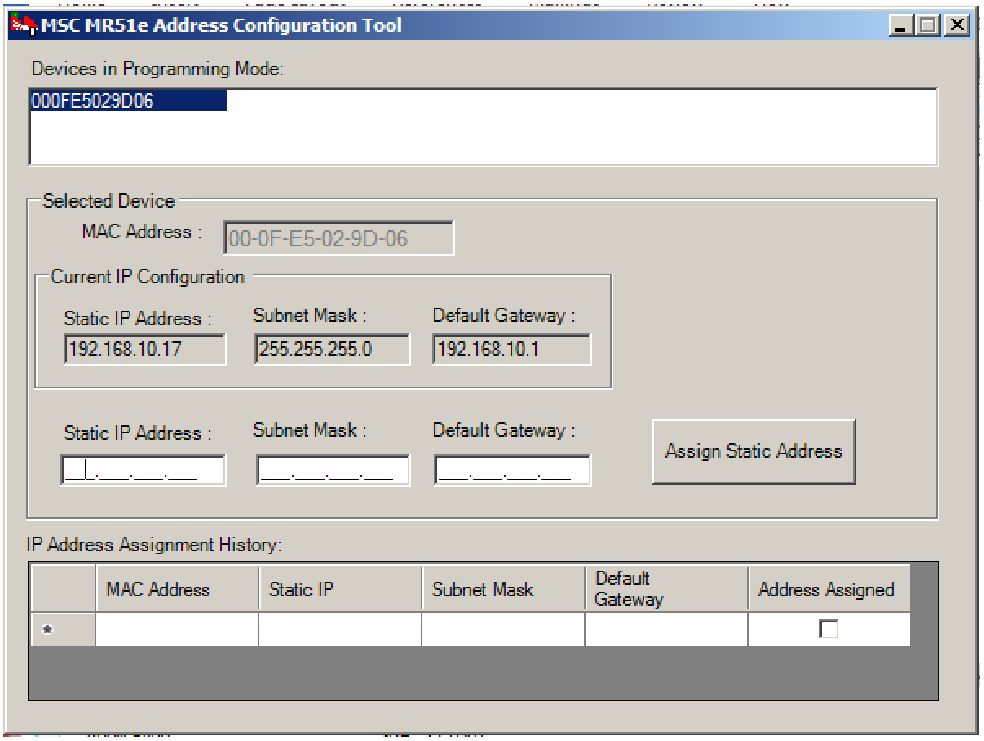
! IMPORTANT ! Be sure to program each POE reader board with a static IP address *before mounting it and its enclosure onto the Rack cabinet door*. To program it:

Step 1. Browse into the PremiSys installation files to PremiSys – Released > Utilities folder. Launch **MR51eAddressTool.exe** and choose "Local Area Connection" when prompted for Network Interface Selection.

Step 2. Power the POE reader board, connect network cable to a local LAN port, set reader board DIP switches to: 1-ON 2-ON 3-OFF 4-OFF. Press and release the reset button next to the switches.



Step 3. Highlight MAC address in "Devices" field and then enter desired IP address, subnet mask and default gateway in the fields below. Click "assign Static Address" button.



Devices in Programming Mode:

000FE5029D06

Selected Device

MAC Address : 00-0F-E5-02-9D-06

Current IP Configuration

Static IP Address : 192.168.10.17

Subnet Mask : 255.255.255.0

Default Gateway : 192.168.10.1

Static IP Address : ___.___.___.___

Subnet Mask : ___.___.___.___

Default Gateway : ___.___.___.___

IP Address Assignment History:

	MAC Address	Static IP	Subnet Mask	Default Gateway	Address Assigned
*					□

Step 4. Set the POE Reader Board DIP switches to 1-OFF 2-ON 3-OFF 4-OFF. Press and release the reset button next to the switches.

Delete auto-generated doors

Browse to the Door(s) folder below your new controller. Right-click and delete any doors labeled with your cabinet names, e.g. "A-101 Front" and "A-101 Back." If prompted to download to controller, select “download later.”

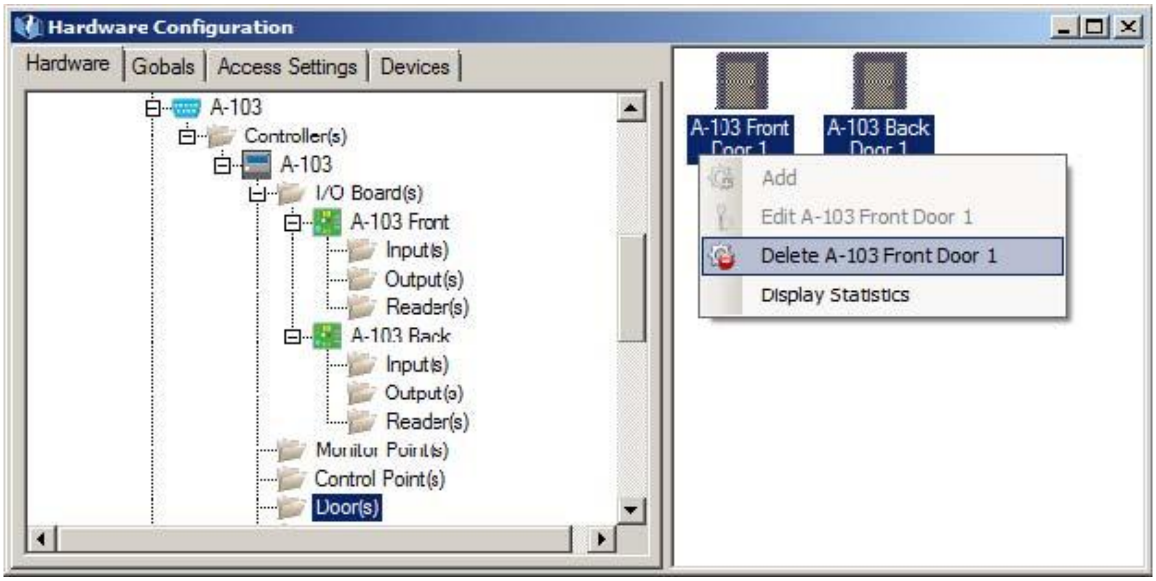


Figure 2.3.6 Contents of the Controller's Door(s) folder. Right-click to delete auto-generated doors.

You may continue to add fourteen more I/O boards (representing additional Kit #2s for each front and back door of up to seven RACK2s) per RACK1 controller. If adding RACK2s, edit name of the RACK1 controller to indicate the name of this group of racks. See Figure 2.3.7.

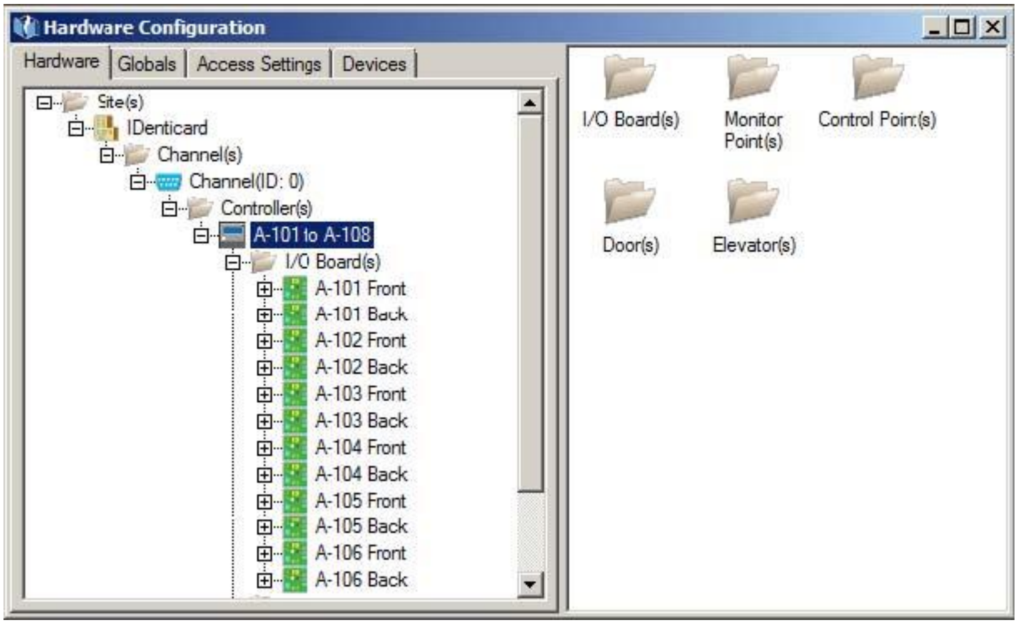


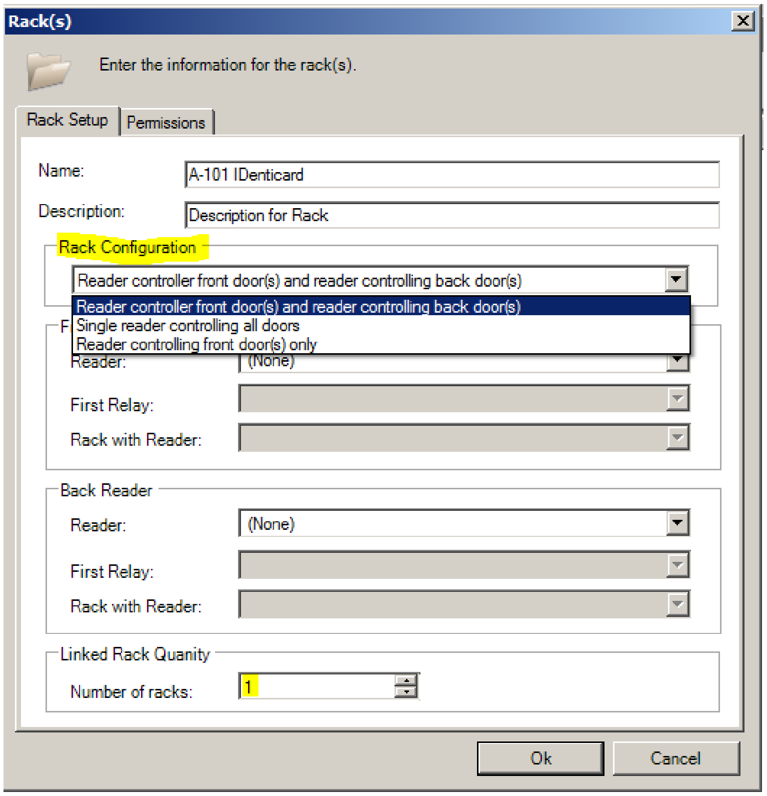
Figure 2.3.7 If RACK1 has multiple RACK2s below it, name the controller to describe the range of racks.

2.4 Cabinet Setup

Go to the *Hardware Configuration* Task, then to the *Globals* tab.

Add Rack - using the wizard

Under *Rack Armor*, right-click *Rack(s)* and Add. This will launch a wizard to generate one or more cabinets. See Figure 2.4.1. Enter an intuitive name for your rack(s). If you are creating a RACK1 or RACK2, enter a name to represent this cabinet. For typical rack setup, choose "Reader controlling front door and reader controlling back door." If you will install rack hardware only on one side of the cabinet, choose "Reader controlling front door only."



Enter the information for the rack(s).

Name: A-101 IDenticard

Description: Description for Rack

Rack Configuration

Reader controller front door(s) and reader controlling back door(s)

- Reader controller front door(s) and reader controlling back door(s)
- Single reader controlling all doors
- Reader controlling front door(s) only

F

Reader: (None)

First Relay:

Rack with Reader:

Back Reader

Reader: (None)

First Relay:

Rack with Reader:

Linked Rack Quanity

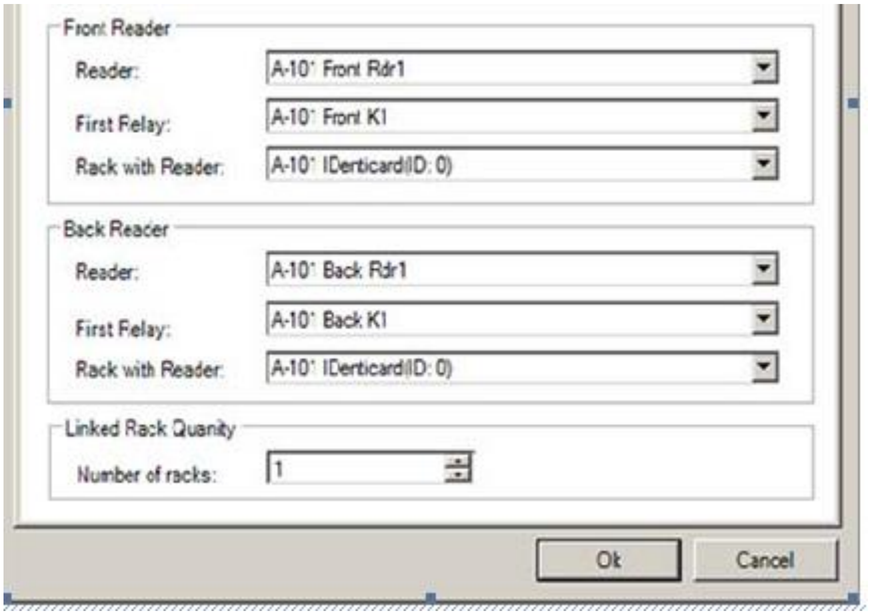
Number of racks: 1

Figure 2.4.1 Rack Setup Wizard

Less common is end-or-row configuration where one reader controls multiple rack doors. In this case, choose "Single reader controlling all doors" and enter a Rack Row name in the Name field instead and enter number of racks in the "Linked Rack Quantity" setting.

! IMPORTANT ! If this Rack is leased out to a customer, add the customer name to the rack or row name, e.g. "A-101 IDenticard" *This simplifies setting up hardware filters later for card access, reports and alerts, etc.*

Use Figure 2.4.2 below as a guide to selecting readers and relays. For Front and Back Reader drop-downs, be sure reader and relay names match the rack you named at the top, for example "A-101 *Front* Rdr 1" with "A-101 *Front* K1"; and *"A-101 Back* Rdr 1" with "A-101 *Back* K1". If you don't see matching names to select, STOP now and go back to the site tree and rename your "On-board I/O Board."



Front Reader

Reader: A-101 Front Rdr1

First Relay: A-101 Front K1

Rack with Reader: A-101 IDenticard(ID: 0)

Back Reader

Reader: A-101 Back Rdr1

First Relay: A-101 Back K1

Rack with Reader: A-101 IDenticard(ID: 0)

Linked Rack Quanity

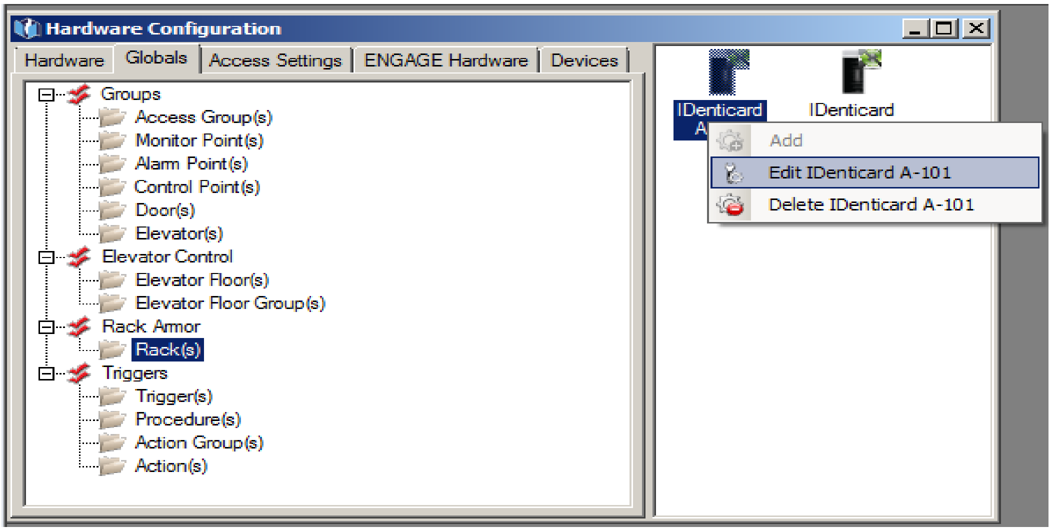
Number of racks: 1

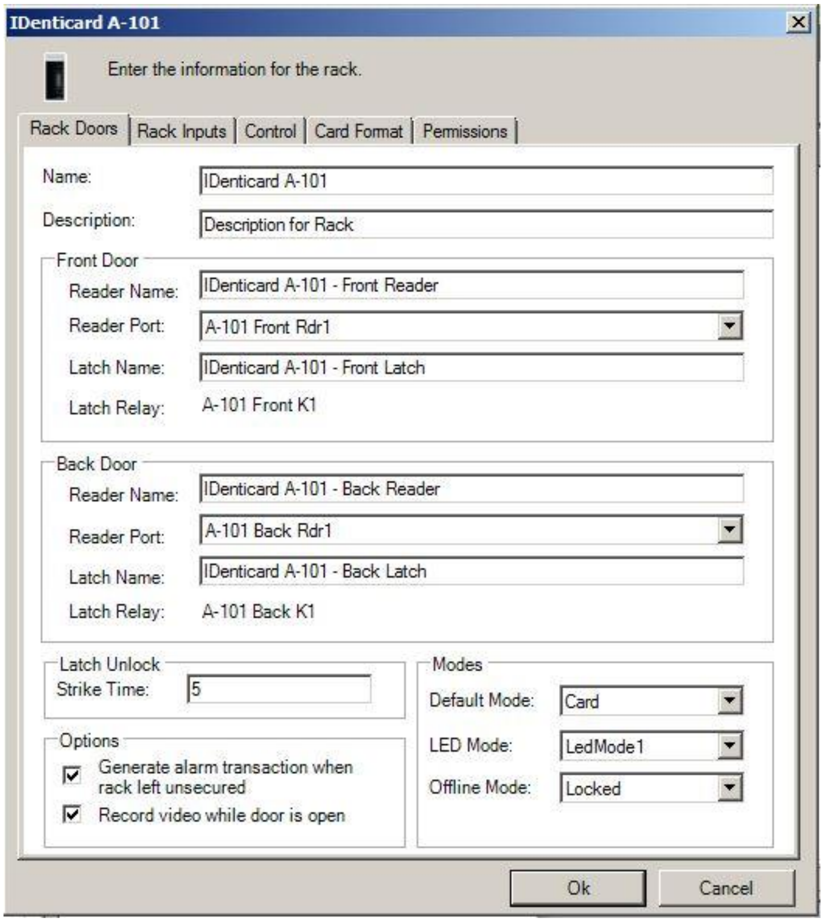
Figure 2.4.2 Cabinet configuration of rack doors with typical configuration of reader and latch settings.

About linked racks

Increasing "Number of racks" in Figure 2.4.1 to two or more will generate *linked racks*. Do this only IF you have enough hardware in your site tree so far. You must link racks IF you have one reader controlling multiple doors in a row using PREM-BRD-IN and PREM-BRD-OUTs (less common system architecture). Beware: if you delete one rack in a "linked row of racks," the entire row will be deleted!

Once clicking "OK," the wizard window will close revealing your new rack icon in the rack folder window. Edit each rack by right-clicking on a rack icon to complete its configuration. Certain settings have been carried over from the wizard and cannot be changed without deleting the rack, such as the associated latch relays.





IDenticard A-101

Enter the information for the rack.

Name: IDenticard A-101

Description: Description for Rack

Front Door

Reader Name: IDenticard A-101 - Front Reader

Reader Port: A-101 Front Rdr1

Latch Name: IDenticard A-101 - Front Latch

Latch Relay: A-101 Front K1

Back Door

Reader Name: IDenticard A-101 - Back Reader

Reader Port: A-101 Back Rdr1

Latch Name: IDenticard A-101 - Back Latch

Latch Relay: A-101 Back K1

Latch Unlock

Strike Time: 5

Options

☑ Generate alarm transaction when rack left unsecured

☑ Record video while door is open

Modes

Default Mode: Card

LED Mode: LedMode1

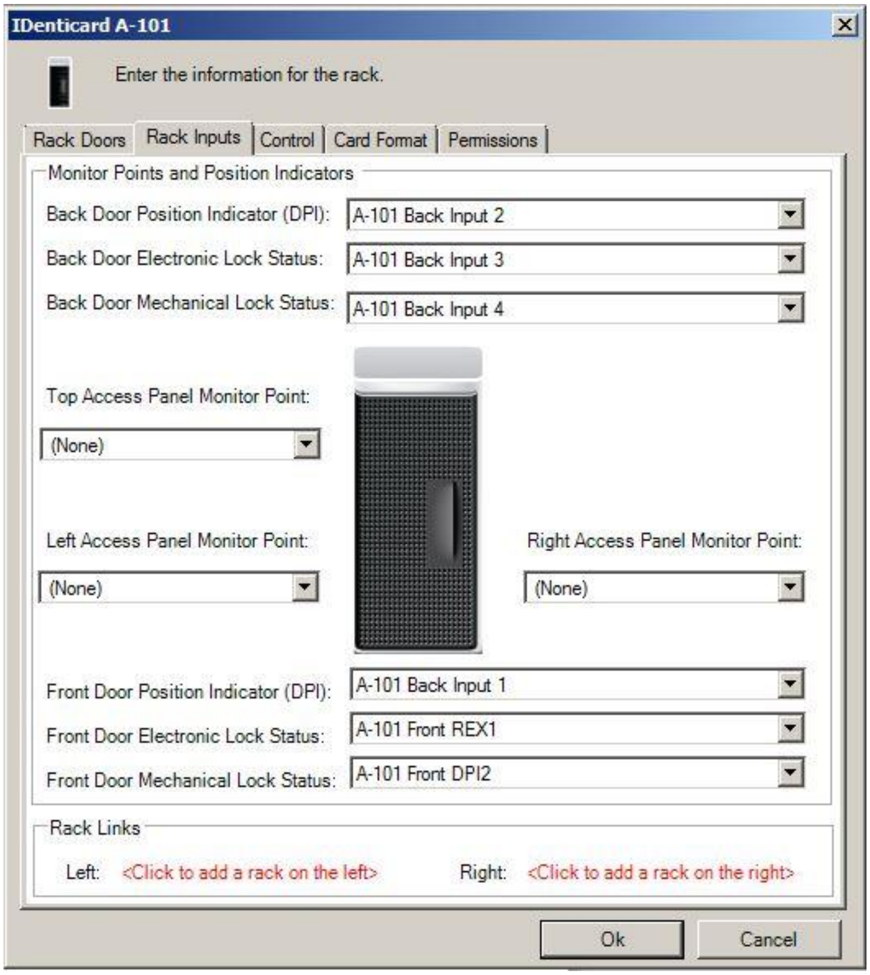
Offline Mode: Locked

View upon opening the rack setup window.

"Rack Doors" tab sets the corresponding readers and relays. The default settings have been carried over from the wizard. You may want to fine tune the name, e.g. A-101 IDenticard(ID: 0). This auto-generated ID# is a helpful suffix to identify *linked racks* in sequential order, but is not necessary for single cabinets.

"Latch Unlock" indicates the time in seconds the cabinet will unlock for a valid card (Access Granted event), and a momentary unlock (User Action).

"Default Mode" is set to "Card" by default. This allows cabinet doors to unlock momentarily when a valid card is presented to the rack cabinet door reader. The checkbox "Generate alarm transaction when rack left unsecured" produces a "Rack not Secure" if either the physical door or the swing handle is not closed within 10 seconds of the other.



IDenticard A-101

Enter the information for the rack.

Monitor Points and Position Indicators

Back Door Position Indicator (DPI): A-101 Back Input 2

Back Door Electronic Lock Status: A-101 Back Input 3

Back Door Mechanical Lock Status: A-101 Back Input 4

Top Access Panel Monitor Point: (None)

Left Access Panel Monitor Point: (None)

Right Access Panel Monitor Point: (None)

Front Door Position Indicator (DPI): A-101 Back Input 1

Front Door Electronic Lock Status: A-101 Front REX1

Front Door Mechanical Lock Status: A-101 Front DPI2

Rack Links

Left: <Click to add a rack on the left> Right: <Click to add a rack on the right>

Figure 2.4.3 Cabinet Configuration of RACK1 “Rack Inputs” tab

"Racks Inputs" tab determines which inputs are associated with rack monitoring components. Follow Figure 2.4.3 as a guide to select the correct corresponding inputs for the rack's DPI (door contacts), electric lock status (solenoids), and mechanical lock status (swing handles).

While your rack name will be different, suffix of the point names should match Figure 2.4.3, i.e. [Rack Name] **Back DPI2**. Play close attention to **Back** versus **Front**, and the final digit **1, 2, 3 or 4**.

"Access Panel" fields are used <u>only IF</u> you are monitoring the top and/or side panels for physical breeches. These point are set up as monitor points in the site tree, then selected here.

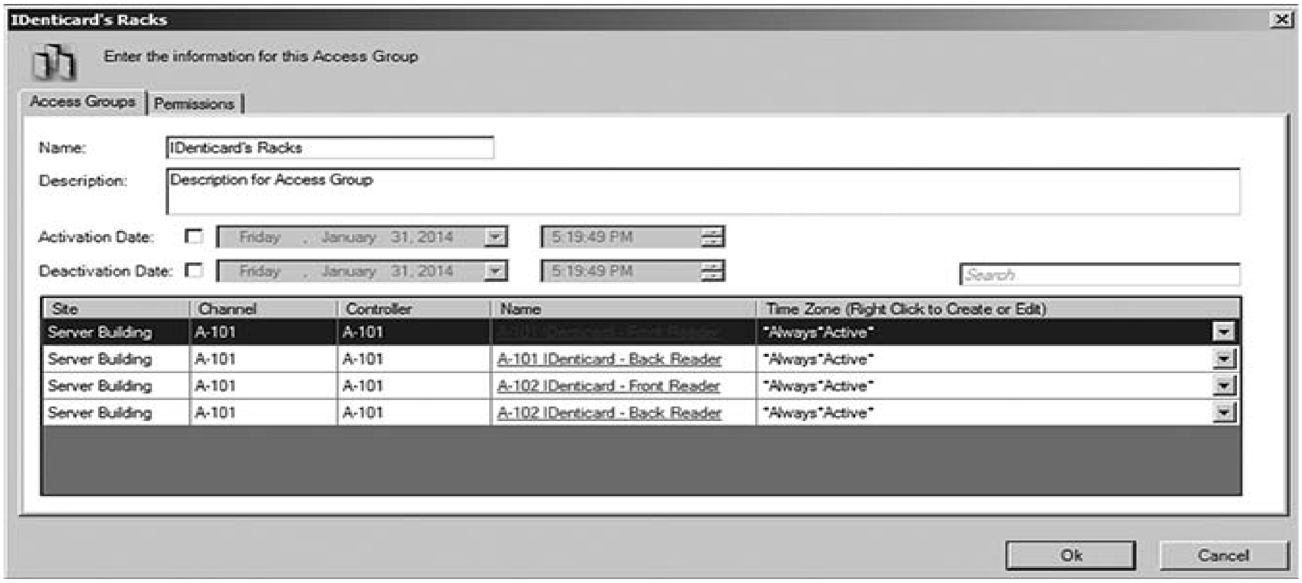
DO NOT click on the text in red (under “Rack Links”) unless you have a "reader at end of row" system architecture. Select <u>only IF</u> you need to add additional cabinets to a linked row. If you inadvertently click on <Click to add a rack on the left [or right]>, click cancel or you will need to delete the rack icon and begin adding the rack again.

"Control" tab in Figure 2.4.3 contains options for rack access. Choose "two man" checkbox if you want to require two valid cards presented within 10 seconds in order to unlock the cabinet door.

"Card Format" tab must have at least one card format checked. Rack Armor is compatible with HID® or Mifare™ card formats. If you don't see any card formats, create at least one in Tasks > Hardware Configuration > Access Settings tab.

2.5 Create an Access Group

Cards will be assigned one or more Access Groups, see Figure 2.4.4. Access Groups will be assigned to access cards and will determine which cabinet(s) the card will unlock and at what times. Name the group intuitively.



Name: IDenticard's Racks

Description: Description for Access Group

Activation Date: □ Friday , January 31, 2014 5:19:49 PM

Deactivation Date: □ Friday , January 31, 2014 5:19:49 PM

Site	Channel	Controller	Name	Time Zone (Right Click to Create or Edit)
Server Building	A-101	A-101	A-101 IDenticard - Front Reader	"Always"Active"
Server Building	A-101	A-101	A-101 IDenticard - Back Reader	"Always"Active"
Server Building	A-101	A-101	A-102 IDenticard - Front Reader	"Always"Active"
Server Building	A-101	A-101	A-102 IDenticard - Back Reader	"Always"Active"

Figure 2.4.4 Access Group Setup

Pair each front and back reader with a time zone to allow cards with this access group to unlock these cabinets. You will see all rack readers site-wide in this list. Only the readers with a paired time zone will be included in the group. Use the *Search* box to search by customer name.

Download
Remember to download to a controller when any changes are made to hardware configuration. Changes are not applied to a controller until downloaded. For more information, see the PremiSys IDentiHelp.chm on-screen help file located at the Help pull-down menu > Contents.

2.5 Dynamic Maps and Indicator Icons

Dynamic Maps and Indicator Icons provide a convenient way to browse hardware and visually monitor any number of racks. Prepare facility floor-plans as images to be imported as a background on the map. Supported files types include .bmp, .emf, .gif, .jpg, .png, .tif, .wmf. Icons are then placed on maps to represent a single rack (rack icon) or multiple racks (indicator icon).

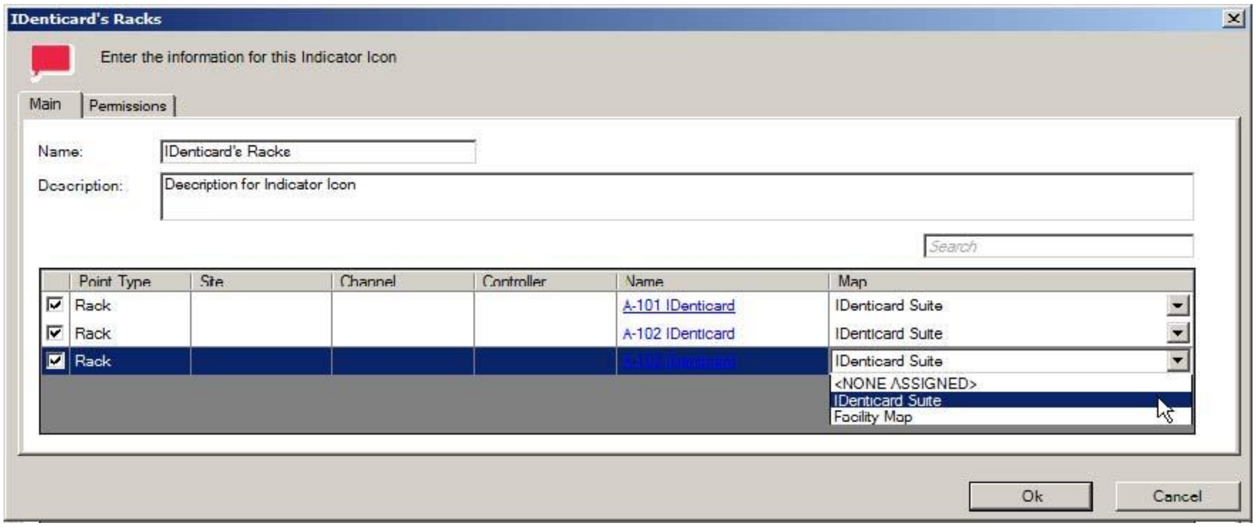
Creating maps

Decide how many maps will represent your facility. Typical systems have one map representing the facility's overall floor-plan, then one map per suite. An indicator icon placed on the overall map links down to the corresponding suite map in the event of an alarm condition at any rack in the suite. The indicator icon automatically changes from green to red to indicate current rack alarm condition(s) in the suite. To configure map-linking with an indicator icon, you must have at least two maps.

To set up maps, Go to Tasks pull-down menu > Hardware Configuration > Access Settings tab. Right-click "Maps," and Add. Name it intuitively, e.g. "Facility Map" or "Suite A." Maps can also be created for a particular customer's group of racks within a suite, e.g. "IDenticard Racks." Click "Browse" to import the background image. With the map open, place individual rack icons on the map by clicking and dragging each one from the *Globals > Racks* folder window. Any *linked racks* will drag over to the map together, useful for large numbers of racks.

Creating indicator icons

You must have your lower suite-level maps created first. Right-click "Indicator Icons" and Add. All monitored devices system-wide will appear in this list (racks, panel monitor points, and doors). If you've included the customer name in the rack name, use the *Search* field to filter for the customer's list of racks. Pair each selected rack with a map from the drop-down menu on the right, see Figure 2.5.1. Or multi-select racks using the CTRL key, then right-click in the map column and select "assign all."



Name: IDenticard's Racks

Description: Description for Indicator Icon

	Point Type	Site	Channel	Controller	Name	Map
☑	Rack				A-101 IDenticard	IDenticard Suite
☑	Rack				A-102 IDenticard	IDenticard Suite
☑	Rack				[illegible]	IDenticard Suite

Figure 2.5.1 Indicator Icon Setup

Not all racks selected for this indicator icon must link to the same map. Use the drop-down menu to choose the map to be associated with the checked point. If you check the box next to the "Point Type" column, do not leave its Map field set to <NONE ASSIGNED> or else this indicator icon will not link to another map when this point is in alarm. Click "OK" to save the indicator icon.

Next, open the higher-level map, e.g. "Facility Map," and drag the indicator onto the map. See Figure 2.5.2.

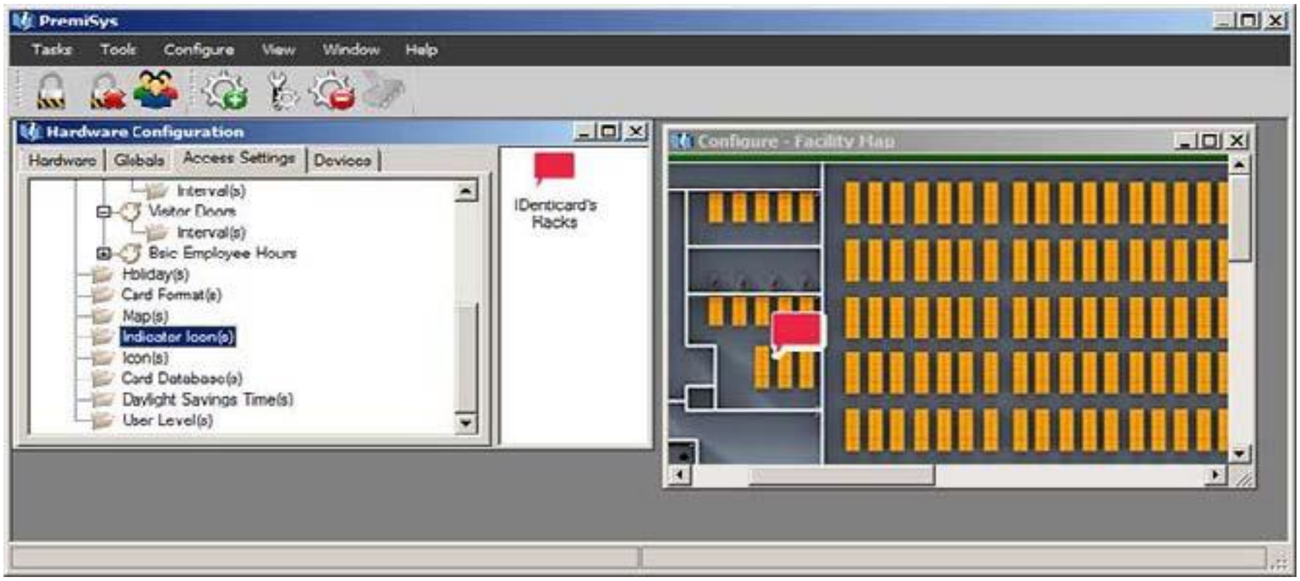


Figure 2.5.2 Click, drag and drop the indicator icon from the folder window onto a map.

2.6 Alarm Acknowledgements

Alarm Acknowledgements guide operators through acknowledging important system events. Email notification can be used to alert remote operators about important events. Configuring Alarm Acknowledgements is optional. Benefits include quickly alerting users to alarms, and providing a method for users to record comments related to alarms. With video integration, the alarm acknowledgment window provides video clips and live-streaming camera views of the rack in alarm.

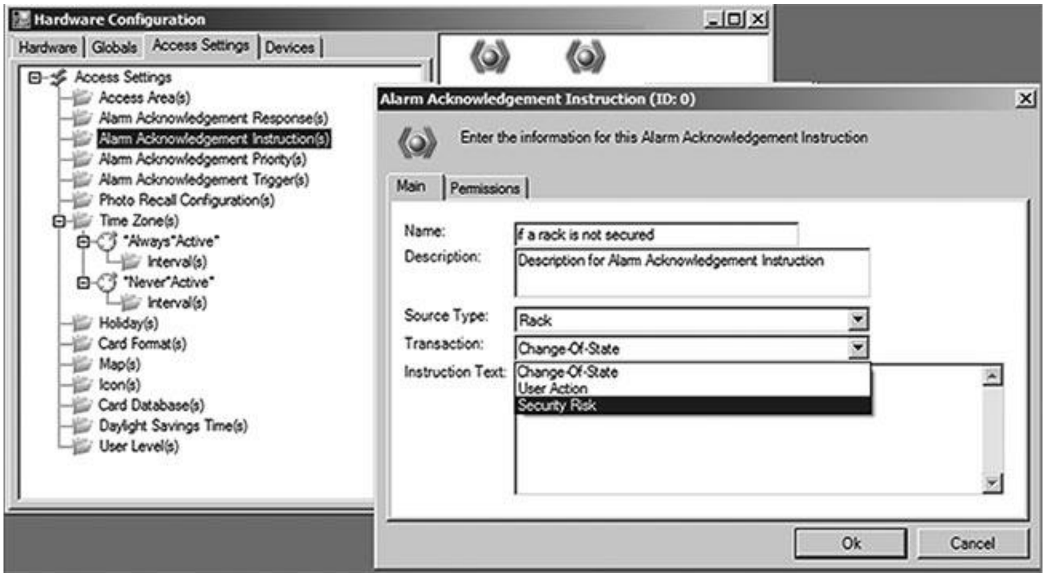
Go to Hardware Configuration > Access Settings

Alarm Acknowledgement Response(s)

Responses are optional. These allow users to select from a drop-down menu of related, common "canned" responses to speed up user response time.

Alarm Acknowledgement Instruction(s)

Instructions are required. Choose "Rack" as Source type. "Transaction" is the alarm's transaction type, refer to Appendix A. For example, to create instructions for a "Door Left Open" alarm, select "Security Risk." To create instructions for a "Momentary Unlock" event, select "User Action." See Figure 2.6.1.



Alarm Acknowledgement Instruction (ID: 0)

Enter the information for this Alarm Acknowledgement Instruction

Name: If a rack is not secured
Description: Description for Alarm Acknowledgement Instruction
Source Type: Rack
Transaction: Change-Of-State
Instruction Text:

Change-Of-State
User Action
Security Risk

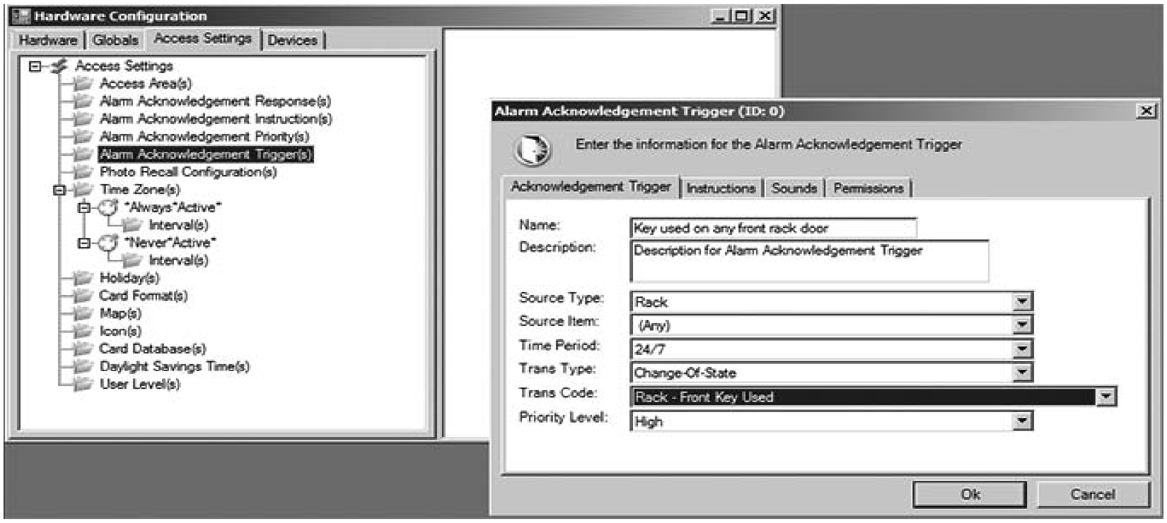
Figure 2.6.1 Alarm Acknowledgement Instructions setup window

Priority levels

 You must create at least one priority level. The priority level determines: 1) sort order for multiple alarms in the queue with the most important alarms at the top; and 2) whether notes and/or user password is required to acknowledge and/or clear the alarm. Low level alarms can be set to allow "one-step acknowledge" and/or "one-step clear."

Acknowledgment Triggers

Acknowledgement triggers define the specific events to appear in the alarm queue. Choose "Rack" as "Source Type." Figure 2.6.2 shows an alarm trigger configured for key used at any rack. Select priority level and instructions (required), A trigger can be set for "Any Rack" or one specific rack.



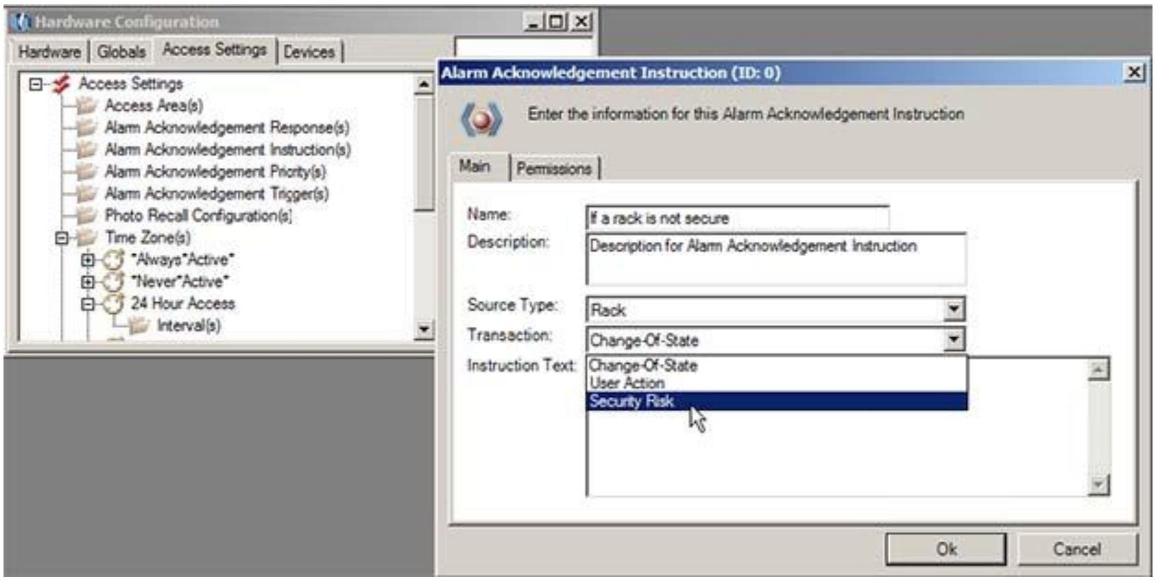
Alarm Acknowledgement Trigger (ID: 0)

Enter the information for the Alarm Acknowledgement Trigger

Name: Key used on any front rack door
Description: Description for Alarm Acknowledgement Trigger
Source Type: Rack
Source Item: (Any)
Time Period: 24/7
Trans Type: Change-Of-State
Trans Code: Rack - Front Key Used
Priority Level: High

Figure 2.6.2 Alarm Acknowledgement Trigger setup window

Key Used is a typical event that system administrators will want to be alerted about immediately.


Hardware Configuration
Hardware
Globals
Access Settings
Devices
Access Settings
Access Area(s)
Alarm Acknowledgement Response(s)
Alarm Acknowledgement Instruction(s)
Alarm Acknowledgement Priority(s)
Alarm Acknowledgement Trigger(s)
Photo Recall Configuration(s)
Time Zone(s)
"Always"Active"
"Never"Active"
24 Hour Access
Interval(s)
Alarm Acknowledgement Instruction (ID: 0)
Enter the information for this Alarm Acknowledgement Instruction
Main
Permissions
Instruction Text:
Change-Of-State
User Action
Security Risk
Ok
Cancel

Name: If a rack is not secure
Description: Description for Alarm Acknowledgement Instruction
Source Type: Rack
Transaction: Change-Of-State

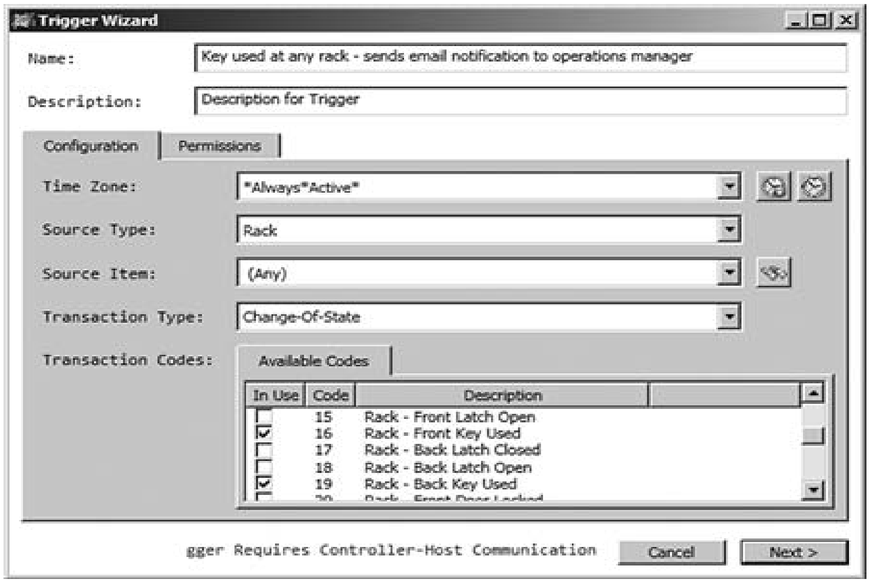
Figure 2.6.2 An alarm acknowledgement trigger set for "key used"

2.7 Event-based Email Notification

Any rack "change-of-state" transaction can be configured to automatically send an email with event details. Refer to Appendix A for the reference list of rack "change-of-state" events. Email notification requires the PremiSys server have a network connection to an SMTP server.

To set up event-based email notifications, first configure the Email Server from "Tasks" > "Hardware Configuration" > "Devices" tab. Right-click "SMTP mail server." Consult a local IT administrator for SMTP server details. Then, set up the email trigger in "Globals" tab > "Trigger(s)."

Rack Armor uses PremiSys *Trigger and Procedures* to generate event-based email notifications. Figure 2.7.1 shows an example trigger setting for a key used at any rack. Click "Next" to select a procedure to send the email.



Name: Key used at any rack - sends email notification to operations manager

Description: Description for Trigger

Time Zone: *Always*Active*

Source Type: Rack

Source Item: (Any)

Transaction Type: Change-Of-State

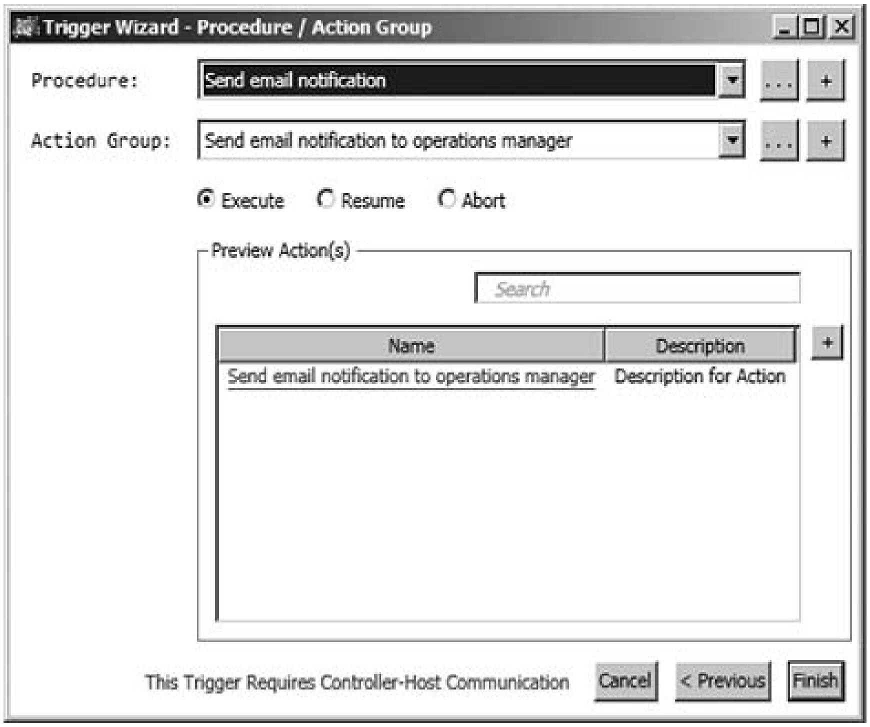
Transaction Codes: Available Codes

In Use	Code	Description
□	15	Rack - Front Latch Open
☑	16	Rack - Front Key Used
□	17	Rack - Back Latch Closed
□	18	Rack - Back Latch Open
☑	19	Rack - Back Key Used
□	20	Rack - Front Door Locked

gger Requires Controller-Host Communication

Figure 2.7.1 An event trigger set for "key used" at any rack

If you don't see a procedure like the one shown in Figure 2.7.2, use the "+" button to launch the Procedure Setup Wizard to guide you through setting up the Procedure's Action Group(s) and Action(s).



Procedure: Send email notification

Action Group: Send email notification to operations manager

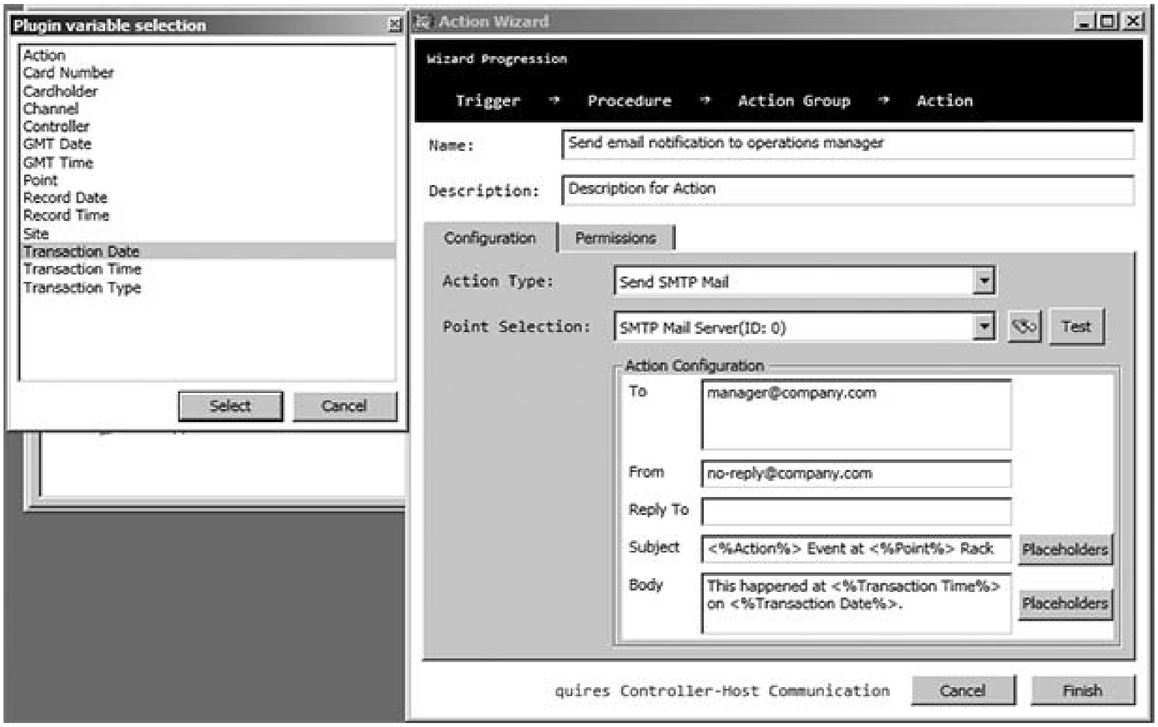
● Execute ○ Resume ○ Abort

Name	Description
Send email notification to operations manager	Description for Action

This Trigger Requires Controller-Host Communication

Figure 2.7.2

The email action can be configured to pass variables from the transaction event into the subject line and body of the email message. See Figure 2.7.3. "Placeholders" allow the email to contain the Rack name, time and date details. This allows you to reuse the same action in other action groups or procedures. The "Test" button is a convenient way to test sending the email, without needing to physically generate the associated alarm.



Name: Send email notification to operations manager

Description: Description for Action

Action Type: Send SMTP Mail

Point Selection: SMTP Mail Server(ID: 0)

To: manager@company.com

From: no-reply@company.com

Reply To:

Subject: <%Action%> Event at <%Point%> Rack

Body: This happened at <%Transaction Time%> on <%Transaction Date%>.

quires Controller-Host Communication

Figure 2.7.3

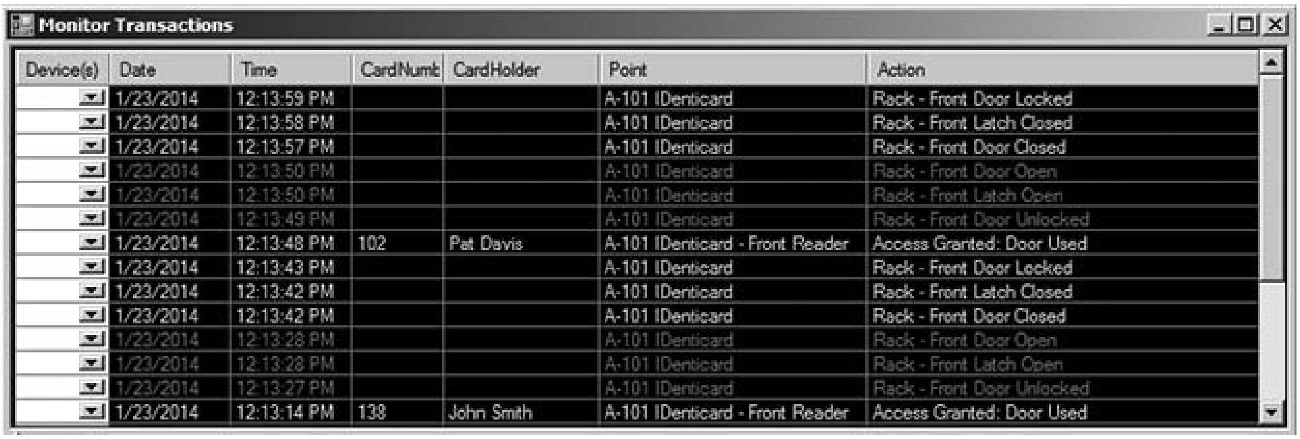
3. System Monitoring

The "Monitor and Control" Task provides views of live transactions, real-time rack status on dynamic maps, and alarm monitoring. With video integration, access video clips and live camera views. A detailed rack status window provides details on cabinet door and swing handle positions, and allows users to unlock and lockout cabinets.

To launch, go to the Tasks pull-down menu > Monitor and Control.

3.1 Live Transactions Screen

Live transactions scroll into the transaction screen. See Figure 3.1.1. A complete list of all Rack Transactions is provided in Appendix A. Right-click an event in the transaction screen to open a Filter window. Transactions can be filtered by type or by controller. Scroll direction and number of events can also be modified. By default, the most recent event is at the top and scrolls down.



Device(s)	Date	Time	CardNumb	CardHolder	Point	Action
	1/23/2014	12:13:59 PM			A-101 IDenticard	Rack - Front Door Locked
	1/23/2014	12:13:58 PM			A-101 IDenticard	Rack - Front Latch Closed
	1/23/2014	12:13:57 PM			A-101 IDenticard	Rack - Front Door Closed
	1/23/2014	12:13:50 PM			A-101 IDenticard	Rack - Front Door Open
	1/23/2014	12:13:50 PM			A-101 IDenticard	Rack - Front Latch Open
	1/23/2014	12:13:49 PM			A-101 IDenticard	Rack - Front Door Unlocked
	1/23/2014	12:13:48 PM	102	Pat Davis	A-101 IDenticard - Front Reader	Access Granted: Door Used
	1/23/2014	12:13:43 PM			A-101 IDenticard	Rack - Front Door Locked
	1/23/2014	12:13:42 PM			A-101 IDenticard	Rack - Front Latch Closed
	1/23/2014	12:13:42 PM			A-101 IDenticard	Rack - Front Door Closed
	1/23/2014	12:13:28 PM			A-101 IDenticard	Rack - Front Door Open
	1/23/2014	12:13:28 PM			A-101 IDenticard	Rack - Front Latch Open
	1/23/2014	12:13:27 PM			A-101 IDenticard	Rack - Front Door Unlocked
	1/23/2014	12:13:14 PM	138	John Smith	A-101 IDenticard - Front Reader	Access Granted: Door Used

Figure 3.1.1

If the system provides video integration, camera icons appear in the devices column next to events with associated cameras, and link to video clips.

Figure 3.1.1 shows a normal progression of events as actions are logged when a technician accesses rack A-101, leased to IDenticard. Logged is date and time, card number, cardholder number, which cabinet door, and what happened. If a system user manually unlocks a door in the software, his or her username will be logged and displayed.

3.2 Dynamic Maps

Launch maps from the "Monitor and Control Hardware" window > "Access Settings" tab, as shown in Figure 3.2.1. Any number of maps can be open at the same time.

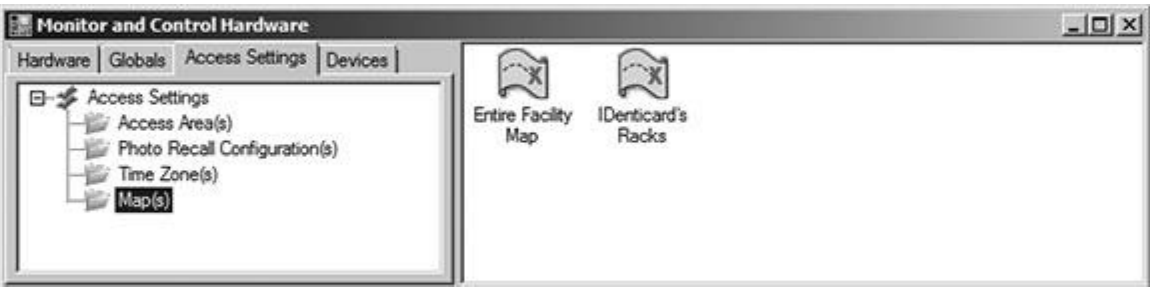


Figure 3.2.1

In Figure 3.2.2, key features are marked here by lettered call-outs. Use the buttons on the tool bar (A) to increase or decrease the size of the active map. The active map is the map last clicked. If you don't see these buttons, click on a map. Use the drop-down menu in the tool bar (B) to switch from one map to another. On dynamics maps, view indicator icons (C) and rack icons (D).

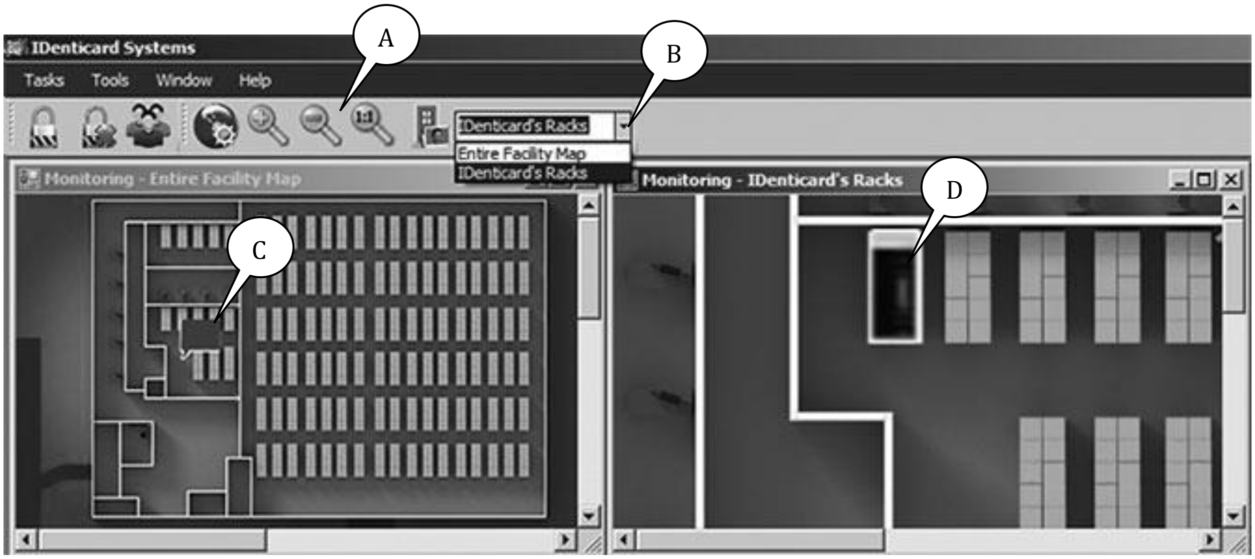


Figure 3.2.2

Live indicator icon is shown in Figure 3.2.3. An indicator icon will turn from green to red when any rack associated with the icon is in an alarm condition. A number appears over the indicator icon, to indicate how many racks associated with the icon are currently in alarm. Mouse-over an indicator icon to view more details, e.g. "A-101 IDenticard: Key Used." The indicator icon will link to another map only during the time a current alarm exists at one or more of its associated points (cabinets, doors, monitor points).

Live rack icon is shown in Figure 3.2.3. A rack icon changes to reflect the current status of the rack, e.g. "Front Key Used." Mouse-over the rack icon to view details. Double-click on the rack icon to open the cabinet details view window, see Figure 3.3.2.

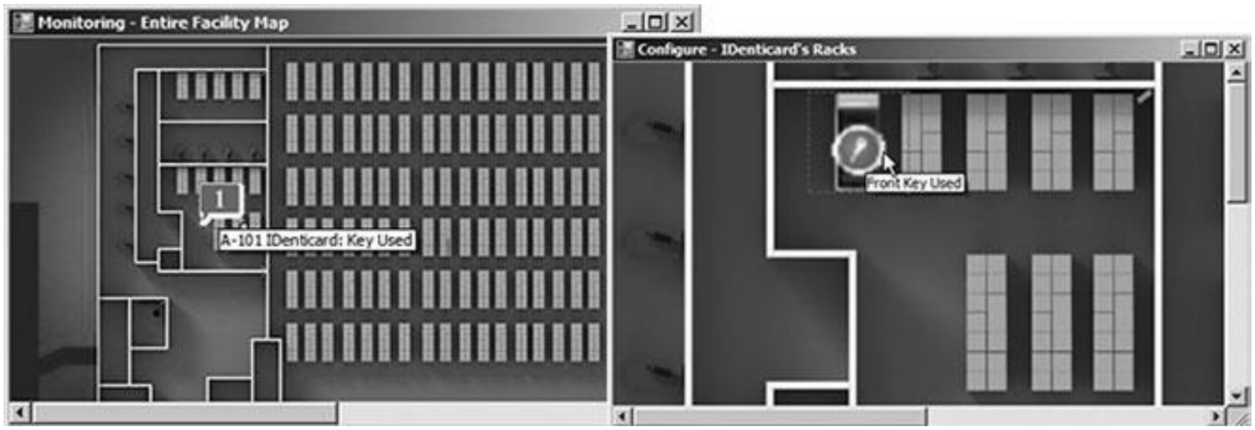

Monitoring - Entire Facility Map
Configure - IDenticard's Racks
1
A-101 IDenticard: Key Used
Front Key Used

Figure 3.2.3

3.3 Cabinet Details View

The rack details view can be opened from any rack icon on a dynamic map, or from the Globals > Racks folder, shown in Figure 3.3.1.

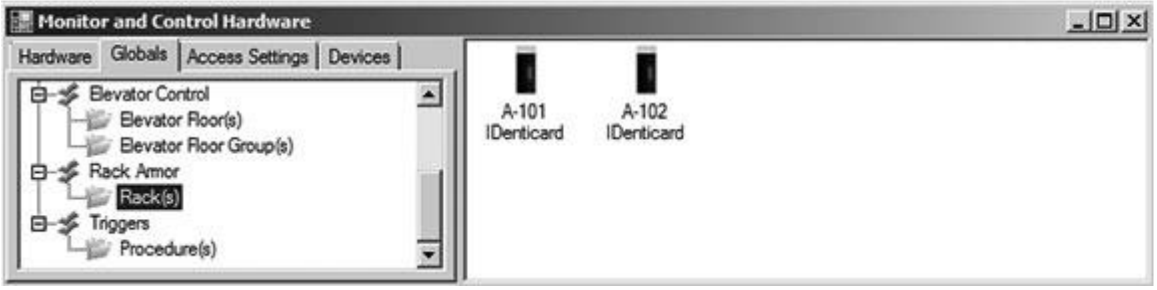
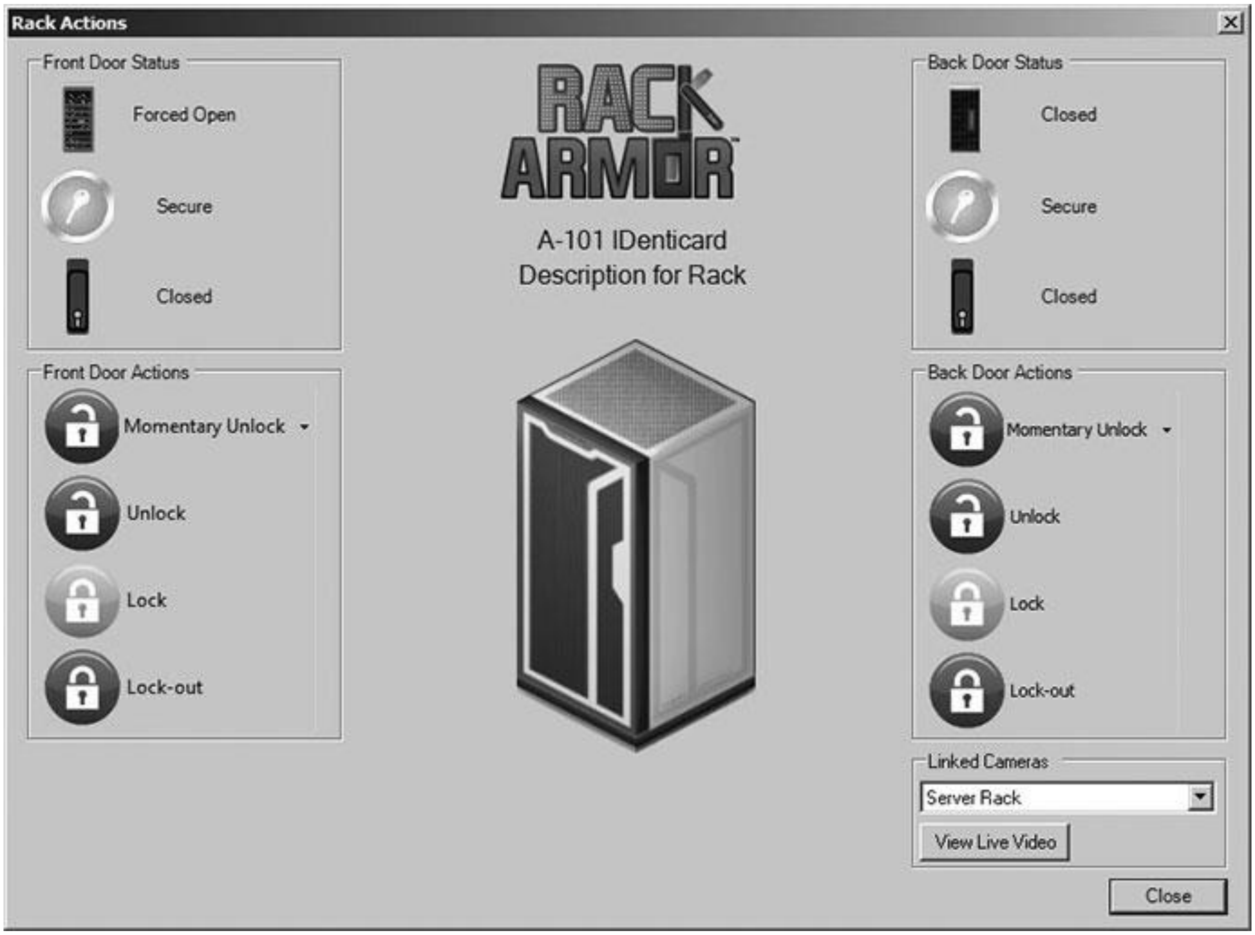


Figure 3.3.1

The rack details window shows rack status, and provides rack access control options to lock, unlock or momentarily unlock the front or back cabinet door. See Figure 3.3.2.

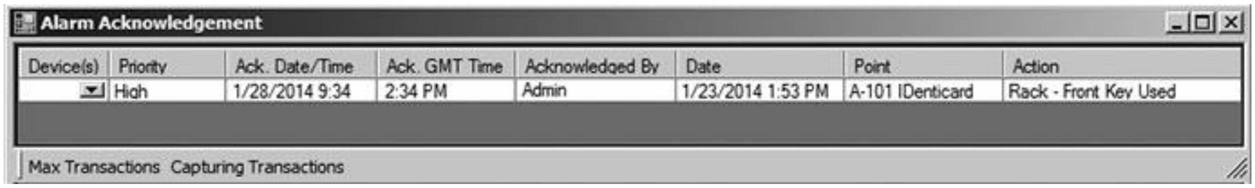


See Figure 3.3.2

In the rack details window, *front door status* and control is on the left side. *Back door status* and control is on the right side. If one or more cameras are associated with this cabinet, *Linked Cameras* in the lower-right corner opens associated cameras. If top, left or right panels are monitored, corresponding icons would appear in the lower-left corner of this window.

3.4 Alarm Acknowledgement Window

Events pre-configured for alarm acknowledgement causes the live alarm to be logged in the Acknowledgement window, shown in Figure 3.4.1. System users double-click on the line item to acknowledge or clear the alarm. Right-clicking an event in the alarm queue opens a Filter window, to customize the queue by controller or to change the column details displayed.



Device(s)	Priority	Ack. Date/Time	Ack. GMT Time	Acknowledged By	Date	Point	Action
▼	High	1/28/2014 9:34	2:34 PM	Admin	1/23/2014 1:53 PM	A-101 IDenticard	Rack - Front Key Used

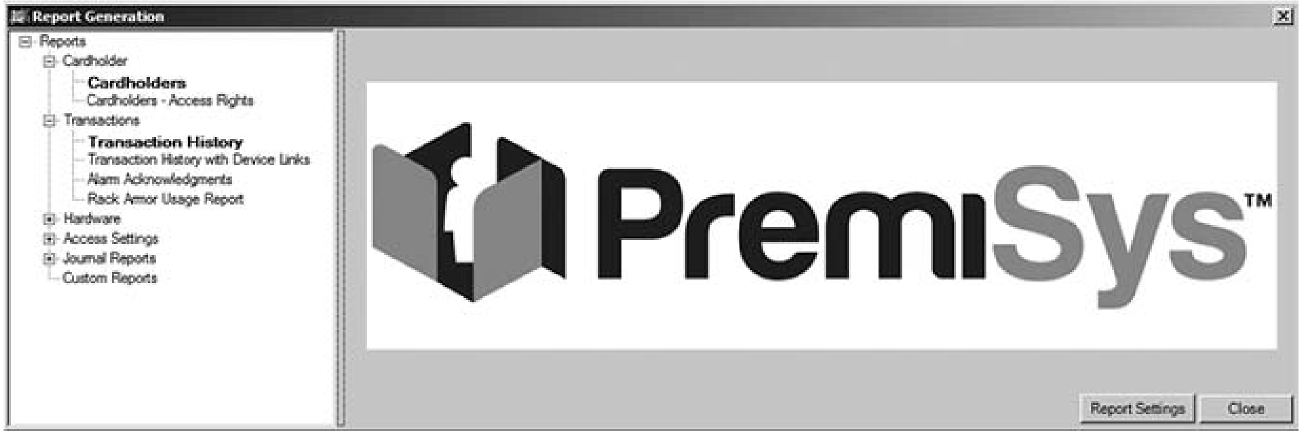
Figure 3.4.1

For systems utilizing video integration, the *Devices* column provides links to associated video clips. And, system users can access video clips and live camera views within the alarm acknowledgement details window.

4. Running Reports

Reports provide important information about who can access racks, when racks were accessed, who responded to alarms, and more. Every report can be printed or exported and saved as a local file in the following formats: .rpt, .pdf, .xls, .doc, or .rtf. To access reports, go to "Tasks" pull-down menu > Report Generation.

The most common Rack Armor reports are found under the *Cardholder* and *Transactions* categories, shown in Figure 4.1. These reports can be scheduled to send email results automatically on a specified schedule, see section 4.5 Scheduled Reports. Click on a report type to display the report setup window, Figure 4.2.

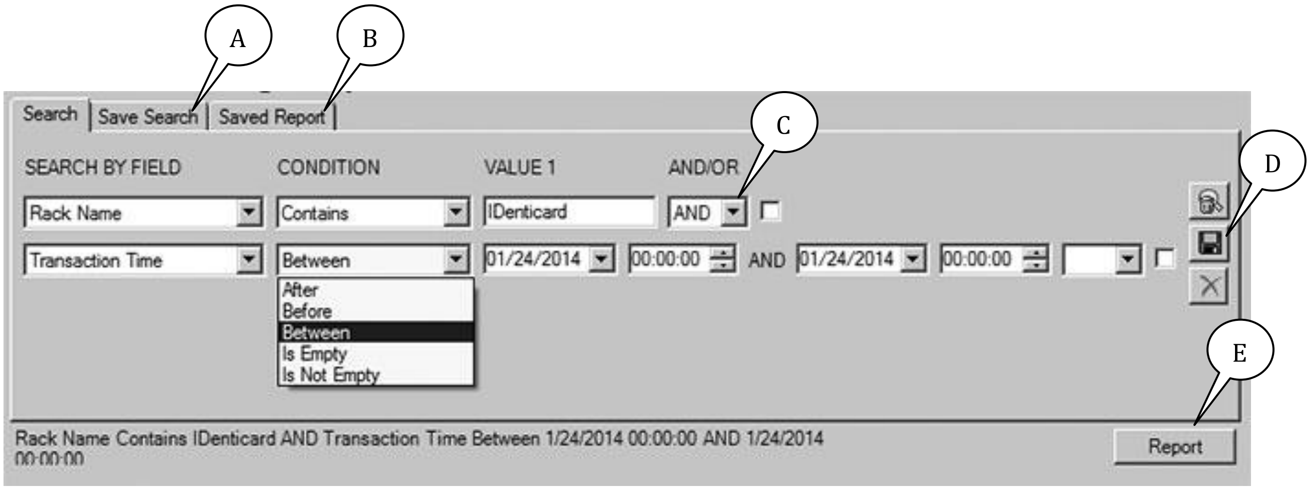


Report Generation

- Reports
  - Cardholder
    - **Cardholders**
    - Cardholders - Access Rights
  - Transactions
    - **Transaction History**
    - Transaction History with Device Links
    - Alarm Acknowledgments
    - Rack Armor Usage Report
  - Hardware
  - Access Settings
  - Journal Reports
  - Custom Reports

Figure 4.1

Figure 4.2 shows an example report setup window. Cardholder and transaction reports provide filters for finding specific information by one or more criteria using AND/OR (C). Filtering a report is not required. Search filters can be saved (D). Retrieve saved filters (A), and saved report layouts (B). Filters are saved *per user login*. Hit the "Report" button (E) to run the report.



SEARCH BY FIELD	CONDITION	VALUE 1	AND/OR
Rack Name	Contains	IDenticard	AND
Transaction Time	Between	01/24/2014 00:00:00 AND 01/24/2014 00:00:00	

Rack Name Contains IDenticard AND Transaction Time Between 1/24/2014 00:00:00 AND 1/24/2014 00:00:00

Figure 4.2

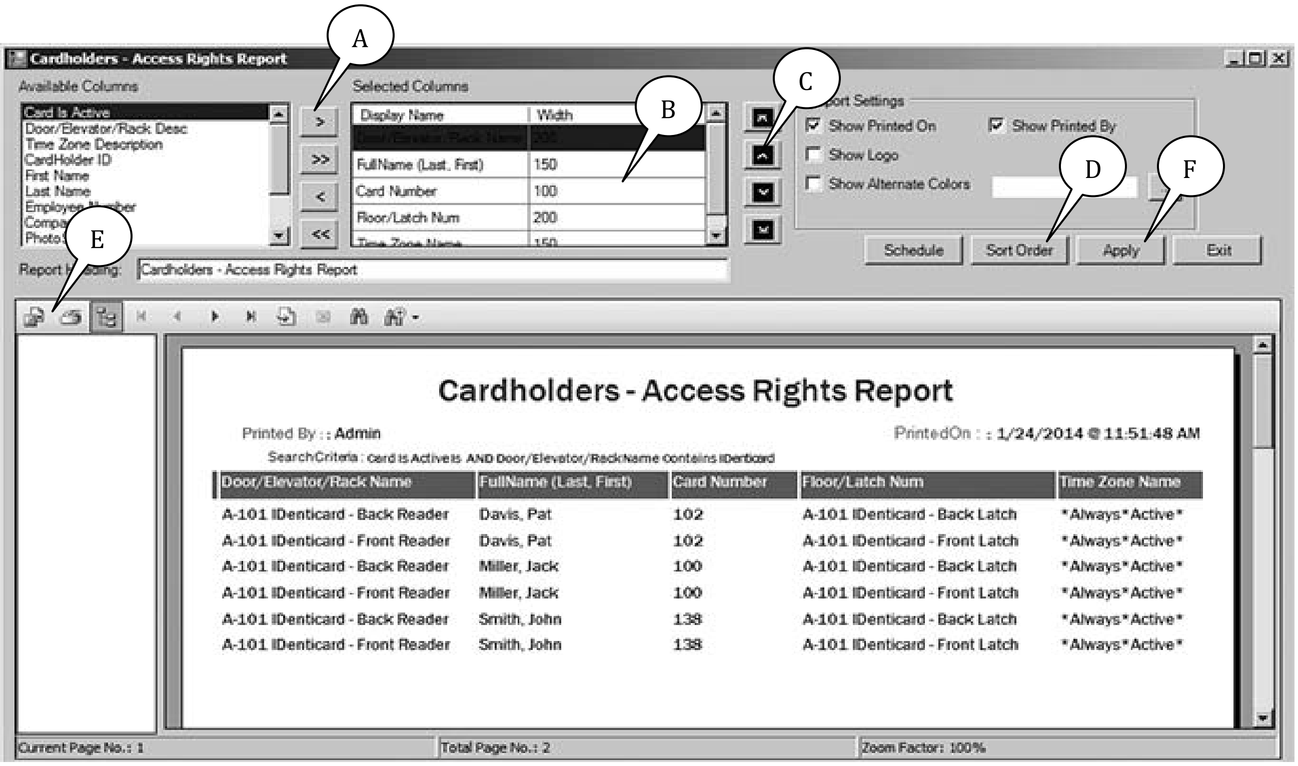
The "Search by Field" is a pull-down menu to select an available field for filtering. The "Condition" setting provides options to include or exclude terms or date/time spans. Enter a specific term in "Value," such as a company name for the "Rack Name" field. Fields available to search depend on the type of report selected.

4.1 Cardholder Reports

The *Cardholder - Access Rights* report is useful to view details on which cardholders can access which racks. Expand the Cardholders category shown in Figure 4.1, and click on *Cardholder - Access Rights*. Enter search criteria, such as the rack lease-holder or technician's company, or a combination. Then click the "Report" button.

An example of a *Cardholders - Access Rights* report is shown in Figure 4.1.1. Searchable fields include: card is active (yes or no), card number, cardholder ID, company, department description, department name, rack or door, rack name, rack description, employee number, first name, full name, last name, photo, time zone name, time zone description.

The other "Cardholder" report, called *Cardholders*, does not provide rack access rights details, nor history transactions. However, searchable fields provided are: any field in the Cardholders table; custom-created cardholder fields and tables; access card details including card number, card is active (yes or no), card is primary (yes or no), and card issue date. To run *Cardholders* report, choose "Detail" (one cardholder per page) or "List."



Available Columns: Card Is Active, Door/Elevator/Rack Desc, Time Zone Description, CardHolder ID, First Name, Last Name, Employee Number, Compa..., Photo...

Display Name	Width
Door/Elevator/Rack Name	200
FullName (Last, First)	150
Card Number	100
Floor/Latch Num	200
Time Zone Name	150

...ort Settings
☑ Show Printed On ☑ Show Printed By
□ Show Logo
□ Show Alternate Colors

Report Heading: Cardholders - Access Rights Report

Cardholders - Access Rights Report

Printed By : : Admin PrintedOn : : 1/24/2014 @ 11:51:48 AM

SearchCriteria : Card is ActiveIs AND Door/Elevator/RackName contains IDenticard

Door/Elevator/Rack Name	FullName (Last, First)	Card Number	Floor/Latch Num	Time Zone Name
A-101 IDenticard - Back Reader	Davis, Pat	102	A-101 IDenticard - Back Latch	*Always*Active*
A-101 IDenticard - Front Reader	Davis, Pat	102	A-101 IDenticard - Front Latch	*Always*Active*
A-101 IDenticard - Back Reader	Miller, Jack	100	A-101 IDenticard - Back Latch	*Always*Active*
A-101 IDenticard - Front Reader	Miller, Jack	100	A-101 IDenticard - Front Latch	*Always*Active*
A-101 IDenticard - Back Reader	Smith, John	138	A-101 IDenticard - Back Latch	*Always*Active*
A-101 IDenticard - Front Reader	Smith, John	138	A-101 IDenticard - Front Latch	*Always*Active*

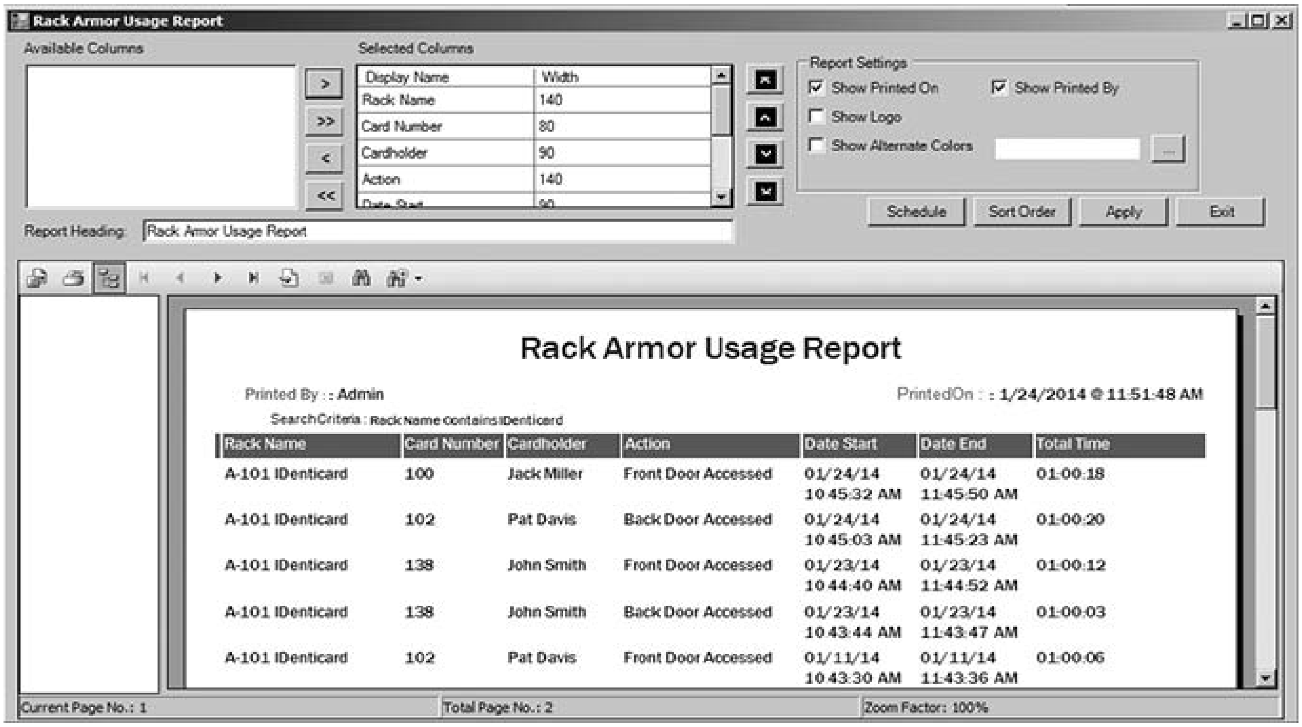
Current Page No.: 1 Total Page No.: 2 Zoom Factor: 100%

Figure 4.1.1

Report results can be customized by selecting columns (A), column widths (B), column order (C), and sort order (D). Hit the "Apply" button to apply changes (F). When applying changes, a prompt provides the optional save the report layout. If a "Save Not Successful" error is displayed, shorten the default name. Buttons (E) are provided to print or export the report. This report can set to run and email automatically on a schedule, see section 4.5 Scheduled Reports.

4.2 Rack Armor Usage Report

The Rack Armor Usage Report allows auditing of which racks were accessed when, by whom, and for how long. To access this report, expand "Transactions" and click on *Rack Armor Usage Report*. shown in Figure 4.1. Search filters include action (transaction name), card number, cardholder, company, department name, rack name, and transaction time (date/time span). Figure 4.2.1 shows an example rack usage report.



Rack Armor Usage Report

Available Columns

Selected Columns

Display Name	Width
Rack Name	140
Card Number	80
Cardholder	90
Action	140
Date Start	90

Report Settings

☑ Show Printed On ☑ Show Printed By

☐ Show Logo

☐ Show Alternate Colors

Report Heading: Rack Armor Usage Report

Rack Armor Usage Report

Printed By : : Admin

PrintedOn : : 1/24/2014 @ 11:51:48 AM

SearchCriteria : Rack Name contains IDenticard

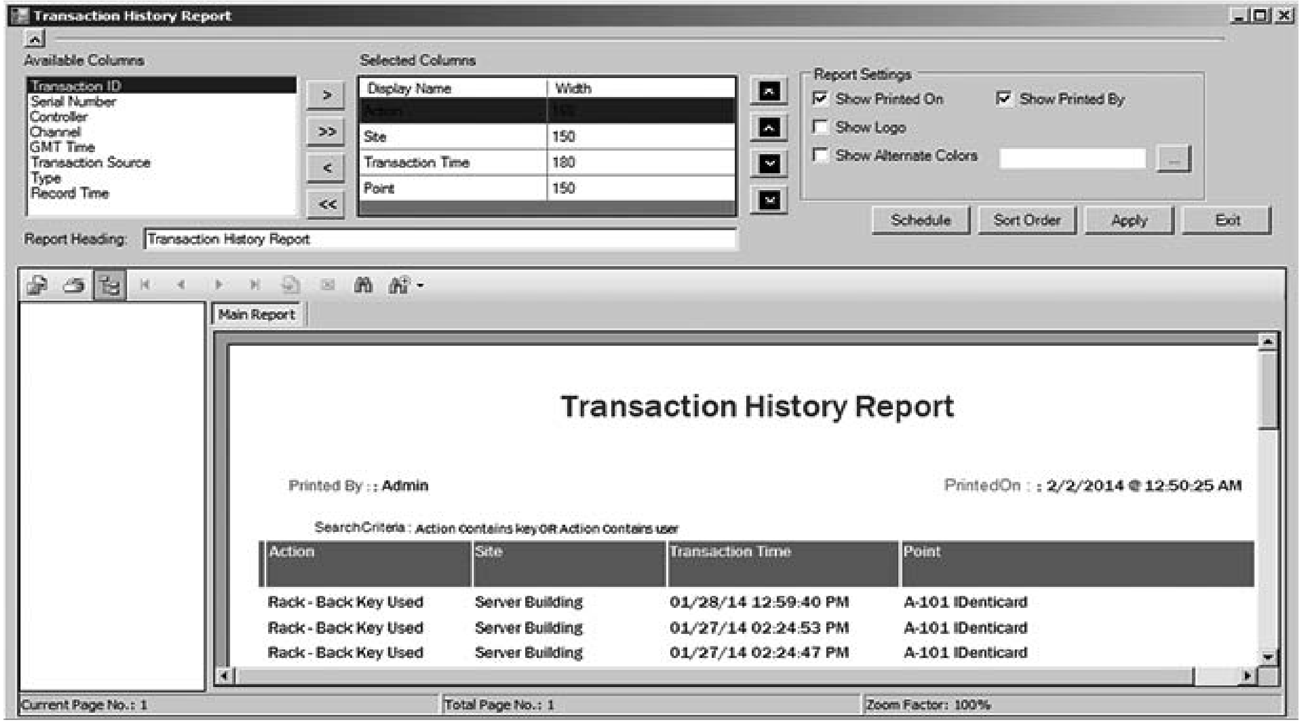
Rack Name	Card Number	Cardholder	Action	Date Start	Date End	Total Time
A-101 IDenticard	100	Jack Miller	Front Door Accessed	01/24/14 10:45:32 AM	01/24/14 11:45:50 AM	01:00:18
A-101 IDenticard	102	Pat Davis	Back Door Accessed	01/24/14 10:45:03 AM	01/24/14 11:45:23 AM	01:00:20
A-101 IDenticard	138	John Smith	Front Door Accessed	01/23/14 10:44:40 AM	01/23/14 11:44:52 AM	01:00:12
A-101 IDenticard	138	John Smith	Back Door Accessed	01/23/14 10:43:44 AM	01/23/14 11:43:47 AM	01:00:03
A-101 IDenticard	102	Pat Davis	Front Door Accessed	01/11/14 10:43:30 AM	01/11/14 11:43:36 AM	01:00:06

Current Page No.: 1 Total Page No.: 2 Zoom Factor: 100%

Figure 4.2.1

4.3 Rack Armor Transaction Report

Audit what happened at which racks, when and by whom or what. Results can include: when keys were used; when system users unlocked cabinets from the software; when cabinet doors were secured or unsecured. Report filters are constructed like the other reports, see Figure 4.2. The History Transaction report can also be customized, as shown in Figure 4.1.1. For an example transaction report, see Figure 4.3.1.



Available Columns:

- Transaction ID
- Serial Number
- Controller
- Channel
- GMT Time
- Transaction Source
- Type
- Record Time

Selected Columns:

Display Name	Width
Action	150
Site	150
Transaction Time	180
Point	150

Report Settings

☑ Show Printed On ☑ Show Printed By

☐ Show Logo

☐ Show Alternate Colors

Report Heading: Transaction History Report

Transaction History Report

Printed By :: **Admin**

PrintedOn :: **2/2/2014 @ 12:50:25 AM**

SearchCriteria : Action contains key OR Action Contains user

Action	Site	Transaction Time	Point
Rack - Back Key Used	Server Building	01/28/14 12:59:40 PM	A-101 IDenticard
Rack - Back Key Used	Server Building	01/27/14 02:24:53 PM	A-101 IDenticard
Rack - Back Key Used	Server Building	01/27/14 02:24:47 PM	A-101 IDenticard

Current Page No.: 1 | Total Page No.: 1 | Zoom Factor: 100%

Figure 4.3.1

4.4 Video Links Report

Video links reports are only applicable with video integration. Results include links to video clips associated with events generated by cabinet doors linked to camera(s). Details and report filters for Video Links Reports include these fields: action (transaction name); card number; cardholder; controller; plugin device name; plugin name; point (cabinet name); site; transaction time; type (such as change-or-state, user action, security risk, etc.).

4.5 Scheduled Reports

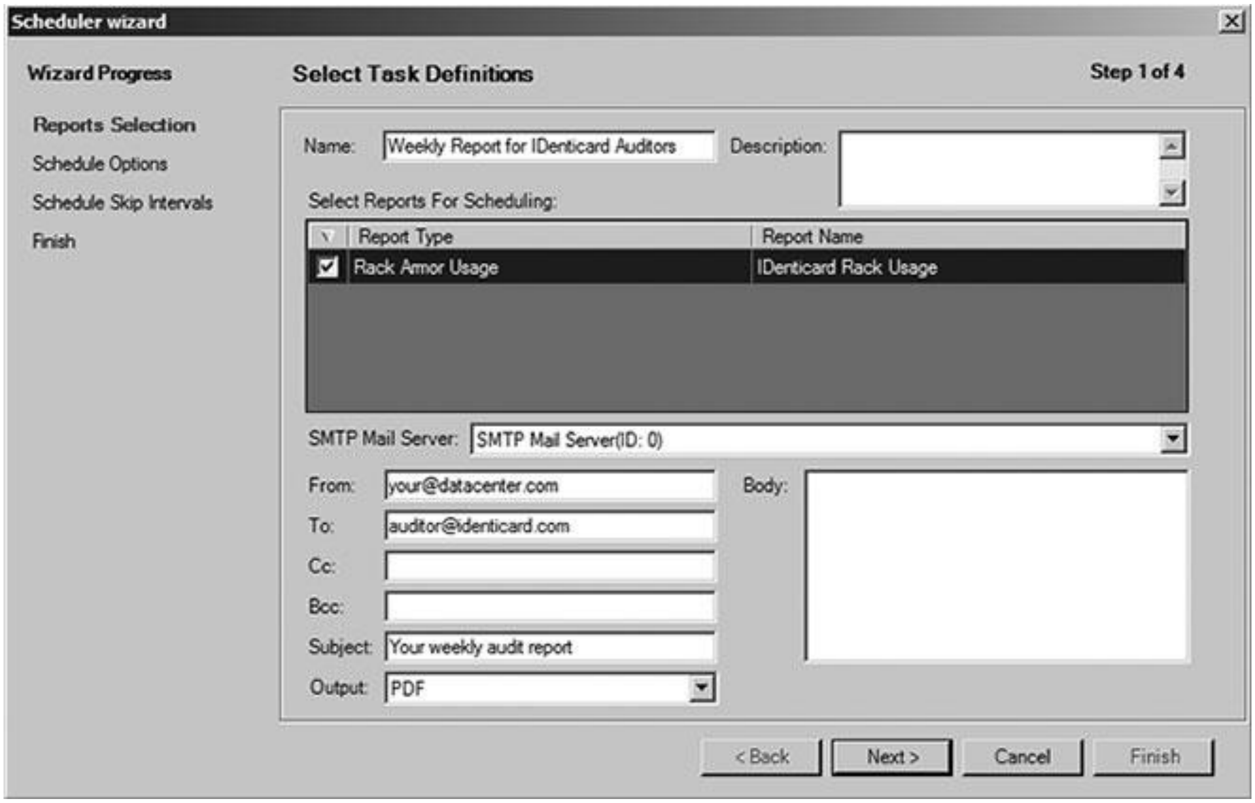
Scheduled reports provide the ability to automatically email any number of *Cardholders* or *Transactions* reports, at any frequency, using any saved report filters, to any number of recipients. Report results are received as a PDF or Excel file attachment. The "Scheduler" task from the *Tasks* pull-down menu, see Figure 4.5.3, provides a centralized listing of all existing scheduled reports, as well as the option to add, edit or delete. To configure scheduled reports, there must be existing saved *Report Layouts* and an existing *SMTP Mail Server*.

To configure an Email Server, go to the *Hardware Configuration* Task > *Devices*. Right-click "SMTP mail server" and Add. Consult the local IT administrator for their system specific SMTP server details. If scheduled reports are to be sent to multiple recipients, set up group distribution lists on the email server.

Scheduled reports require that at least one save *Report Layout* exist for the type of report to be scheduled, see Figure 4.2 (B). The option to save a report layout is provided when applying changes to report results, see Figure 4.1.1 (F). If a "Save Not Successful" error is displayed, shorten the default name.

To schedule reports from the reports results window

Manually run a report first, see Figure 4.2 (E). While viewing the report results window, locate the "Schedule" button. This launches the *Scheduled Report Wizard* to configure this report (layout and filter) to run on a schedule, Figure 4.5.1.



Name: Weekly Report for IDenticard Auditors

Description:

Select Reports For Scheduling:

	Report Type	Report Name
☑	Rack Armor Usage	IDenticard Rack Usage

SMTP Mail Server: SMTP Mail Server(ID: 0)

From: your@datacenter.com

To: auditor@identicard.com

Cc:

Bcc:

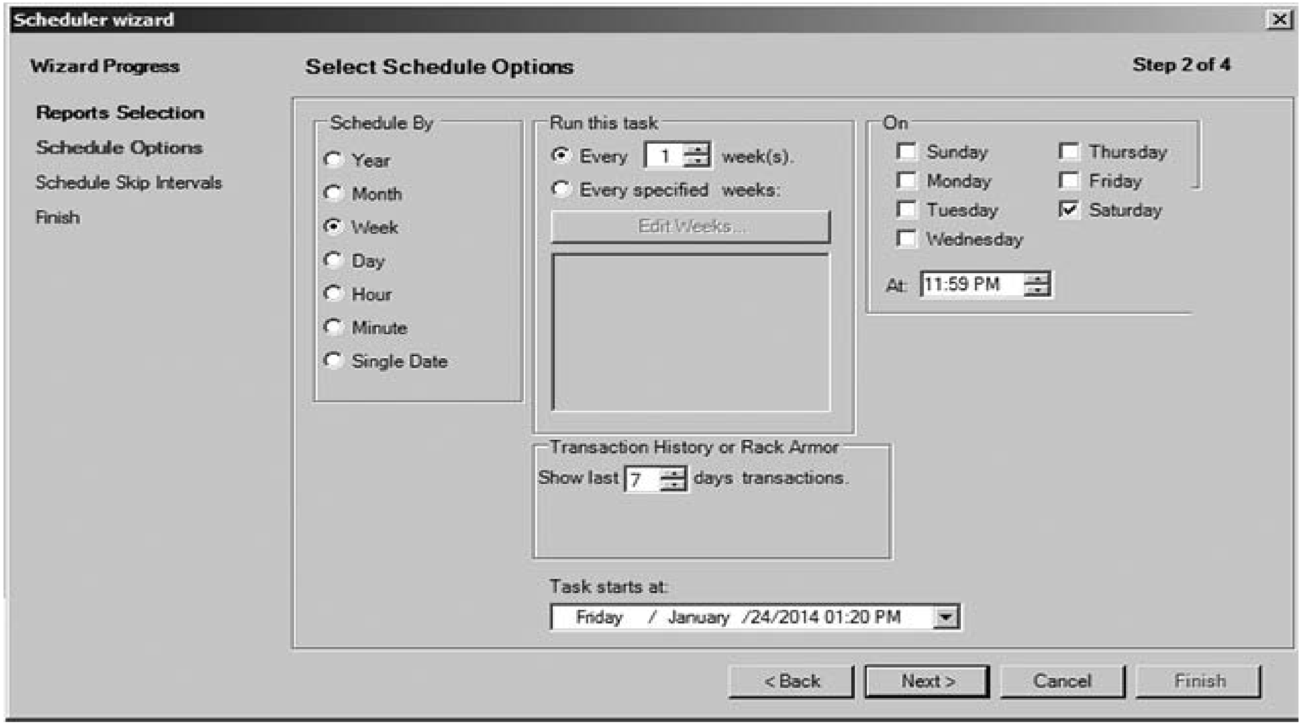
Subject: Your weekly audit report

Output: PDF

Body:

Figure 4.5.1

Name the scheduled report intuitively. The *From*, *To* and *Subject* fields are required. For multiple recipients, you must enter a single distribution list. Entering multiple addresses delimited by commas is not supported. Select "PDF" or "Excel" from the *Output* drop-down menu to choose the report file attachment format. You may optionally include a *Description* and email message *Body*. Click the "Next" button to configure the schedule, Figure 4.5.2.



Scheduler wizard

Wizard Progress

Reports Selection

Schedule Options

Schedule Skip Intervals

Finish

Select Schedule Options

Step 2 of 4

Schedule By

○ Year
○ Month
● Week
○ Day
○ Hour
○ Minute
○ Single Date

Run this task

● Every 1 week(s).
○ Every specified weeks:

Edit Weeks...

On

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

At: 11:59 PM

Transaction History or Rack Armor

Show last 7 days transactions.

Task starts at:

Friday / January /24/2014 01:20 PM

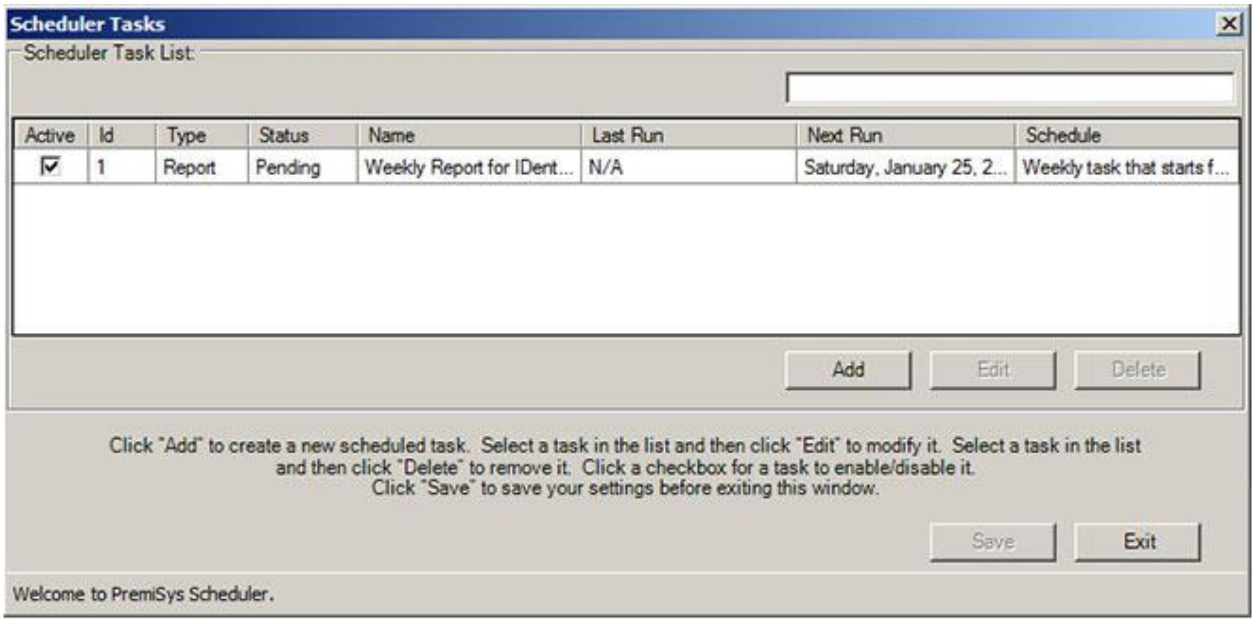
< Back | Next > | Cancel | Finish

Figure 4.5.2

Figure 4.5.2 shows an example transaction report set to run weekly at 11:59 every Saturday, and to include the last seven days worth of events. Click "Next" and follow prompts to complete the setup. Review the scheduled report summary on the final screen, and click "Finish" to save it.

To manage scheduled reports from the Scheduler Task

The best way to review, manage, edit or delete existing scheduled reports is from the *Tasks* pull-down menu > *Scheduler*, shown in Figure 4.5.3. Be sure to click the "Save" button after making any changes here.



Scheduler Tasks

Scheduler Task List:

Active	Id	Type	Status	Name	Last Run	Next Run	Schedule
☑	1	Report	Pending	Weekly Report for IDent...	N/A	Saturday, January 25, 2...	Weekly task that starts f...

Add | Edit | Delete

Click "Add" to create a new scheduled task. Select a task in the list and then click "Edit" to modify it. Select a task in the list and then click "Delete" to remove it. Click a checkbox for a task to enable/disable it.
Click "Save" to save your settings before exiting this window.

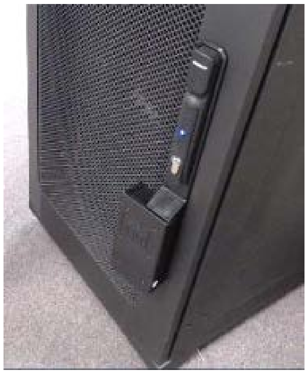
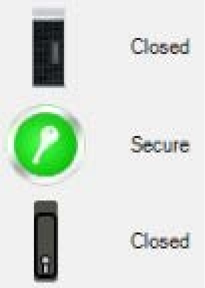
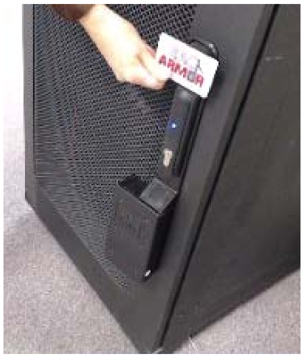
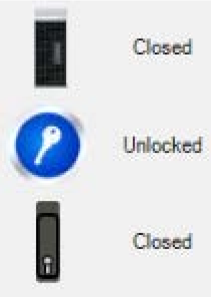
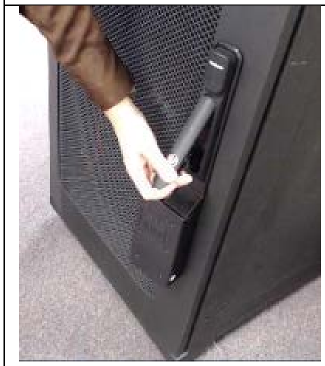
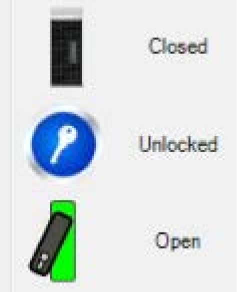
Save | Exit

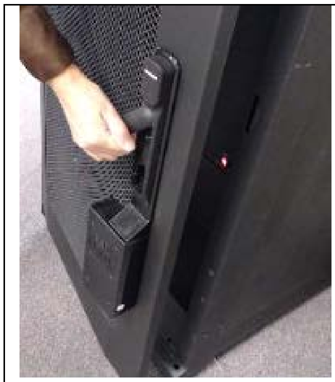
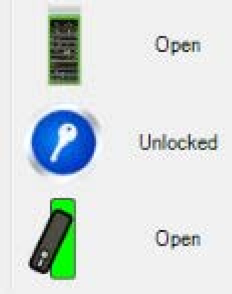
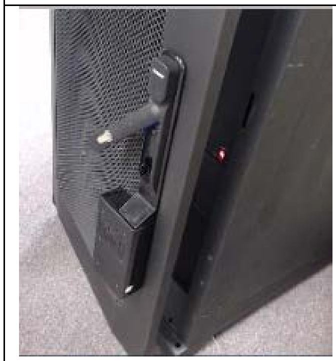
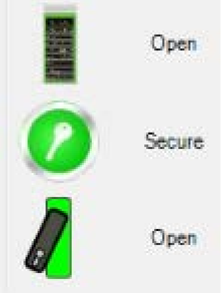
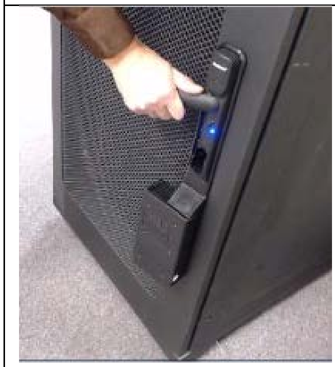
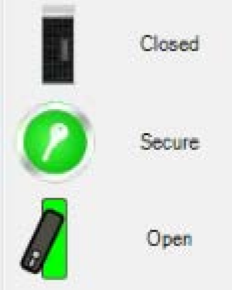
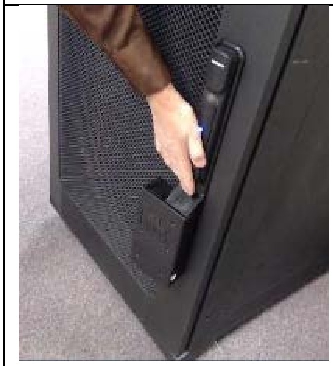
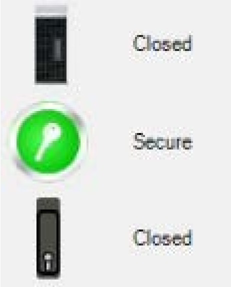
Welcome to PremiSys Scheduler.

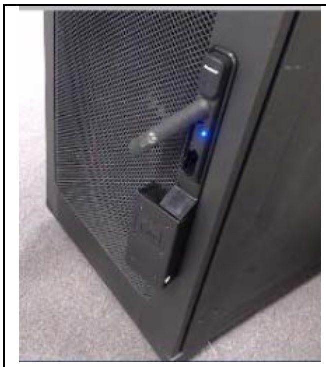
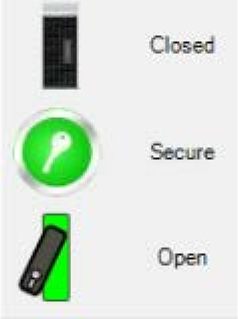
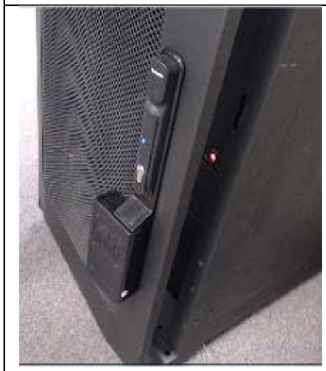
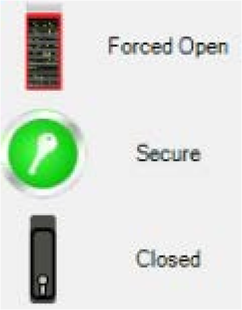
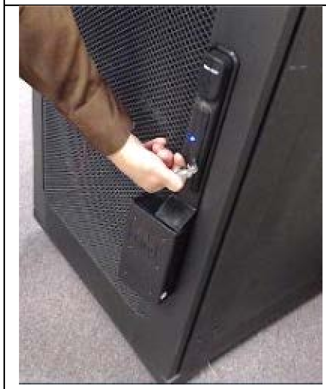
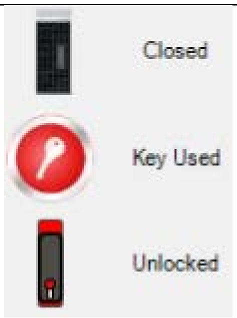
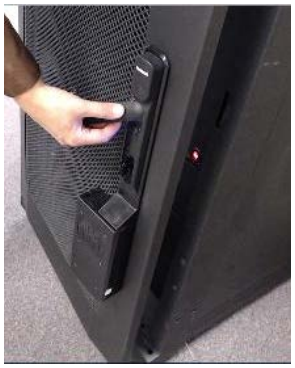
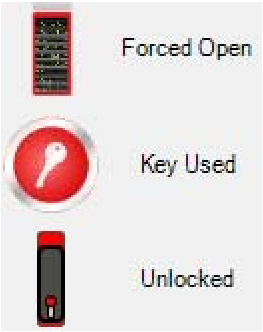
Figure 4.5.3

Appendix A: Rack Armor Transactions and Icons

Source type	Transaction type	Action (transaction name)	Default color
Rack	Change-Of-State	Rack - Front Door Closed Rack - Front Door Open Rack - Front Door Forced Rack - Back Door Closed Rack - Back Door Open Rack - Back Door Forced Rack - Front Latch Closed Rack - Front Latch Open Rack - Front Key Used Rack - Back Latch Closed Rack - Back Latch Open Rack - Back Key Used Rack - Front Door Locked Rack - Front Door Unlocked Rack - Back Door Locked Rack - Back Door Unlocked Rack - Top Panel Secure Rack - Top Panel Open Rack - Left Panel Secure Rack - Left Panel Open Rack - Right Panel Secure Rack - Right Panel Open	Green change-of-state events include: "closed" "secure" "locked" Red change-of-state events include: "open" "key" "forced"
Rack	User Action	Manual Action : Rack Front Momentary Unlock Manual Action : Rack Front Unlock Manual Action : Rack Front Lock Manual Action : Rack Front Lock-out Manual Action : Rack Back Momentary Unlock Manual Action : Rack Back Unlock Manual Action : Rack Back Lock Manual Action : Rack Back Lock-out	All user action events are in white
Rack	Security Risk	Rack Not Secured : Front Swing Handle Rack Not Secured : Front Door Left Open Rack Not Secured : Back Swing Handle Rack Not Secured : Back Door Left Open	All security risk events are in red

Physical State	Details View Icons	Map icon	Description and Action
	 Closed Secure Closed	🔒	When there is no activity at the cabinet door, the server rack icons would appear as shown here. The cabinet door is secure: the swing handle is closed and locked; and, the cabinet door is closed.
	 Closed Unlocked Closed	🔓	A valid card is presented to the integrated reader, unlocking the electronic lock. The door is still closed and the swing handle is closed. Action reported is Access Granted: Door Used Rack - Front Door Unlocked
	 Closed Unlocked Open	🔓	The swing handle is released but the door is still closed. Action reported is Rack - Front Latch Open

	 Open Unlocked Open	🔓	The door is physically open, the swing handle is released, and the pulse time for the electronic lock has not yet ended. Action reported is Rack - Front Door Open
	 Open Secure Open	🔓	During the time the cabinet is open after a valid card presentation. The door and swing handle are open, and the electronic lock is no longer actuated. Action reported is Rack - Front Door Locked Note: "locked" does not indicate the door is physically closed and locked. Rather, this action logs when the lock pulse time ends regardless of door position
	 Closed Secure Open	🔓	The technician has 10 seconds to secure the swing handle after closing the door. Action reported is Rack - Front Door Closed
	 Closed Secure Closed	🔒	The technician has closed the swing handle within 10 seconds after closing the door. Action reported Rack - Front Latch Closed

	 Closed Secure Open		This door is closed but the swing handle has been left open for more than 10 seconds. Action reported Rack not secured - Front Swing Handle
	 Forced Open Secure Closed		This latch is closed but the door is ajar. Action reported Rack not secured - Front Door Left Open
	 Closed Key Used Unlocked		A key is inserted and turned. Action reported Rack - Front Key Used
	 Forced Open Key Used Unlocked		The door opens after the key is used. Action reported Rack - Front Door Forced