

PSA PRODUCT SCORECARD

The PSA Product Scorecard is a tool that contributes to the evaluation of a manufacturer or their product. Some evaluations will be comprehensive and based upon extensive bench-testing; some evaluations will not. The goal is to provide PSA integrators with a common means to aggregate evaluative information.

PRODUCT: Feenics | Keep—Access Control

Average Star Rating: 3.7

Company: Aronson Security Group
Tester Name: Scott Hanson

Testing Environment: Bench
Testing 2 weeks

Star Rating System
5 = Excellent (exceeded expectations)
4 = Pretty Good (better than other similar products)
3 = Acceptable (nothing to clearly differentiate it from similar products)
2 = Not so Good (poorer than other similar products)
1 = Unacceptable (did not meet minimum expectations)
0 = No opinion / Not applicable / Undetermined

Using the key above, rate the following:	Star Rating
Product's initial performance	4
Product's performance after 6 months	0
Product's performance after 12 months	0
Product's overall build quality	4
Product's feature set	4
Rate the product's "ease of use"	4
Quality of the product's documentation	3
Quality of the product's technical support	3
Availability of the product's technical support	3
Product's use of industry standards	4
Product's manufacturer rep. support	4
Product's price compared to value	0
Product's Warranty	0
Product's RMA process	0

Additional Comments:
 This product was evaluated using the hosted site from Feenics. Basic testing was for compatibility of Mercury Hardware, and the ease of use and functionality.
(See attached for more details)

Feenics Keep Access Control

Summary

The Feenics Keep Access Control system is a cloud based (Hosted) system. This system can be hosted by Feenics, or at a customer site. The system supports standard Mercury hardware as well as the HID Vertx Line of controllers. The field deployment is just like most standard Access Control systems with an Intelligent System Controller supporting the door controllers.

Testing Process

- System software was hosted on the Feenics Servers
- Access to the system was via web page on the internet
- Connected a single Mercury EP1501
 - Powered via PoE
 - (LNL-2210 Single Door Controller)
- Wired up an HID RP-40 Multiclass Reader
- Configured a single card holder using standard 26bit Wiegand format
- Ran a series of standard scenarios
 - Enrolling a card holder
 - Designing a badge Layout
 - Creating access levels
 - Door unlock schedules

Initial Setup

Server Configuration

Since this was a hosted configuration, there was no server to setup. Feenics provided a hosted environment. From there it was a basic web interface for all programming and monitoring of the access control system.

If this had been a system hosted at the site, a standard server configuration would need to be built, specifications for this build were not provided for this test.

Hardware Configuration

Feenics provided ASG with a single EP1501 (Single Door Controller). A HID RP-40 Multiclass reader was wired to the controller, and toggle switches to simulate the Door Contact and Request To Exit devices.. Door hardware was simulated by several toggle switches for input devices and lights for output devices.

Configuring

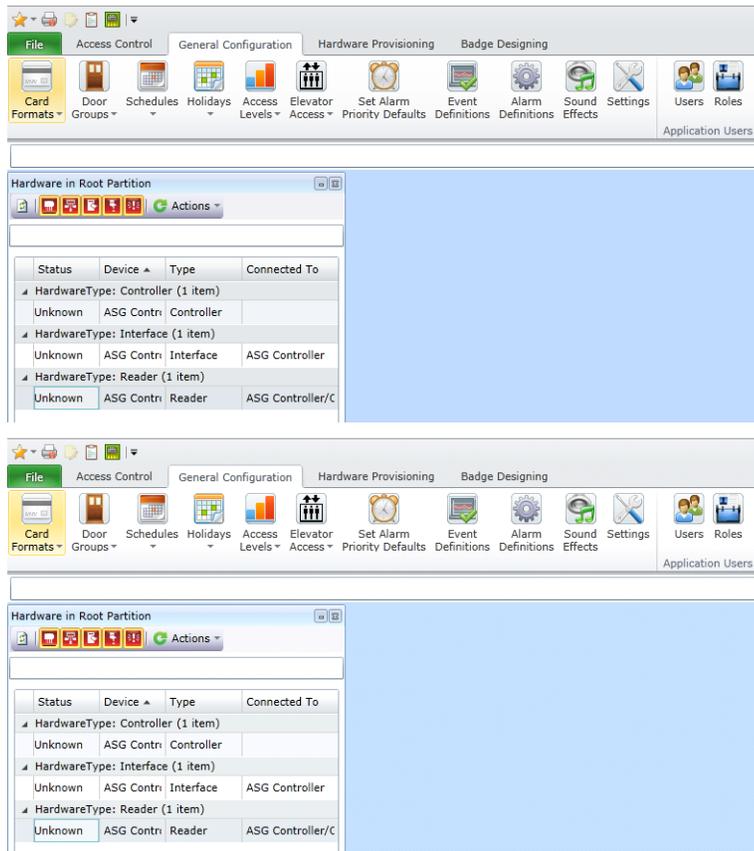
Once installed and configured the Keep Access Control system and ISC devices are accessed via a Web browser. The following are the steps required to allow a cardholder to gain access to a door.

1. Step 1 – Assign IP Address to EP1501

- a. The EP1501 IP configuration is accessible from the onboard web interface
 - i. Static default IP address is 192.168.0.251
 - ii. Default username/password: admin/password
- b. Programming is the same as a standard Mercury Board
- c. Assign IP address, Subnet Mask and Gateway
- d. Save settings

2. Step 2 – Add the Controller (ISC) in the software

- a. Hardware Provisioning Tab -> Controllers -> Select 'Add new controller'
 - i. Assign Unique name for the controller
 - ii. Choose Device Type
 - iii. Input the MAC address (IP is optional)
 - iv. Click Save on the bottom of the screen
- b. Verify that the door controller comes online via the 'View all Hardware' button

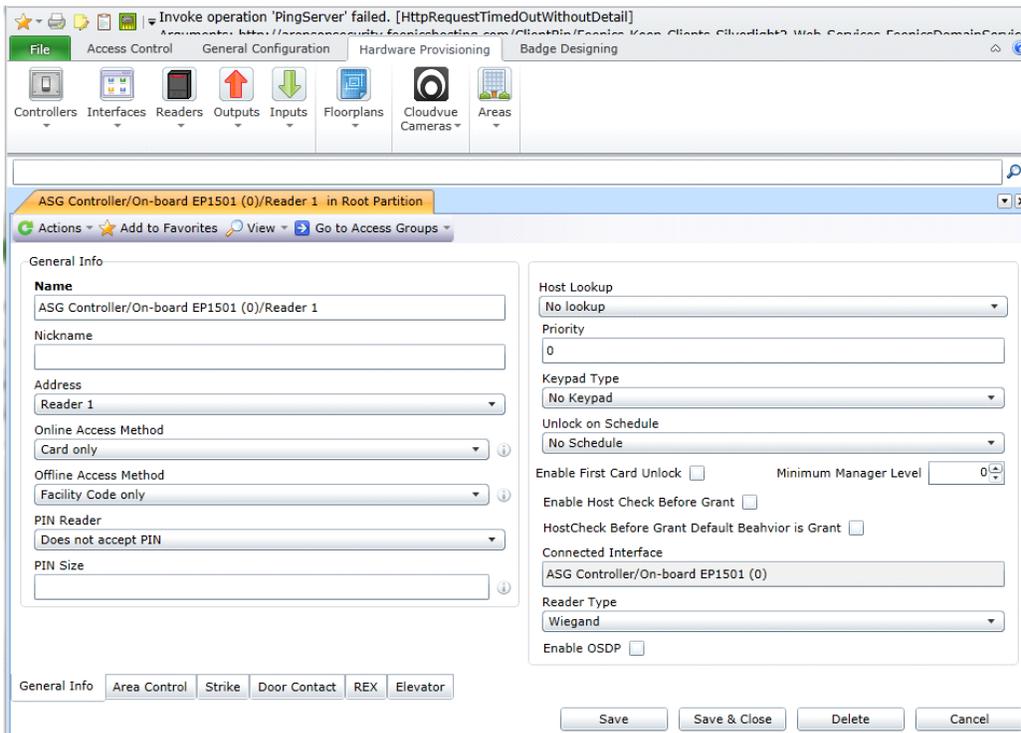
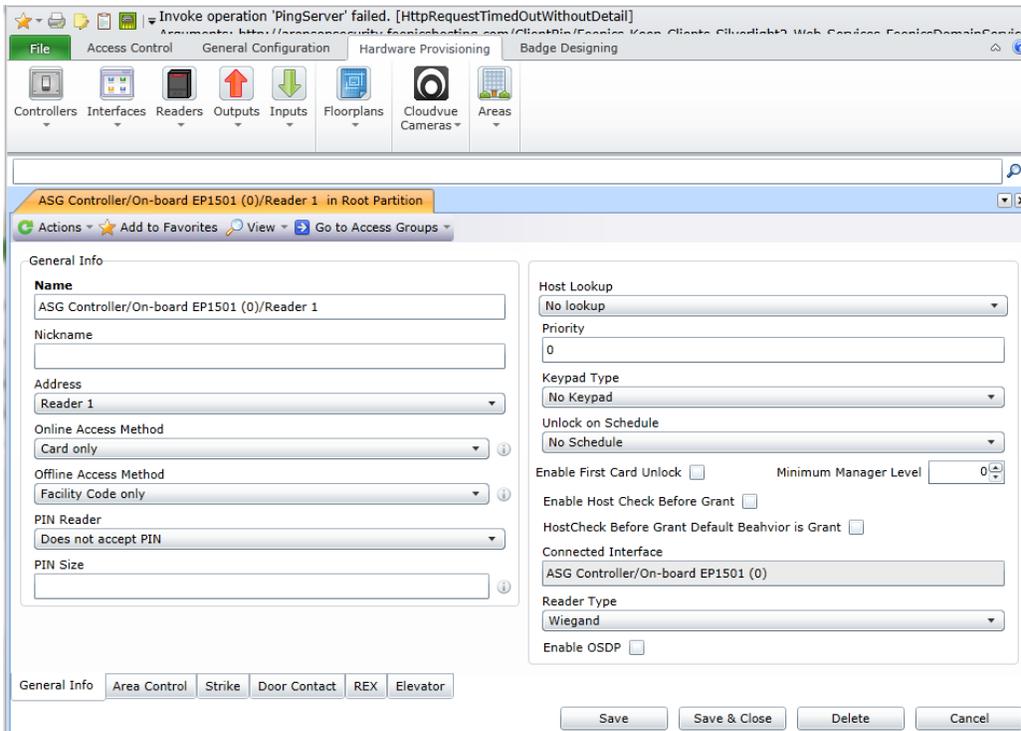


3. Step 3 – Add an Interface (Door Controller) to the Controller (ISC)

a. Hardware Provisioning Tab

- i. Double click on the Hardware Controller in the left pane
- ii. Click on Add Interface, and select 'On-board EP1501'
- iii. The information from the controller will auto fill this section
- iv. Select Save at the bottom of the screen

4. Step 4 – Add a reader to the controller



- a. Select Add Reader
 - i. Select Reader Port
 - ii. Input a Name / Description

- iii. Select options as required
- iv. Door unlock schedule is applied on this screen
- v. Click save on the bottom of the screen

The screenshot shows a window titled "Hardware in Root Partition" with a toolbar and a table of hardware components. The table has columns for Status, Device, Type, and Connected To. The hardware is grouped by HardwareType: Controller (1 item), Interface (1 item), and Reader (1 item). Each item's status is highlighted in green.

Status	Device	Type	Connected To
HardwareType: Controller (1 item)			
Online	ASG Controller	Controller	
HardwareType: Interface (1 item)			
Online	ASG Controller/On-bo	Interface	ASG Controller
HardwareType: Reader (1 item)			
Card Only	ASG Controller/On-bo	Reader	ASG Controller/C

vi.

This screenshot is identical to the one above, showing the same hardware configuration and status in the "Hardware in Root Partition" window.

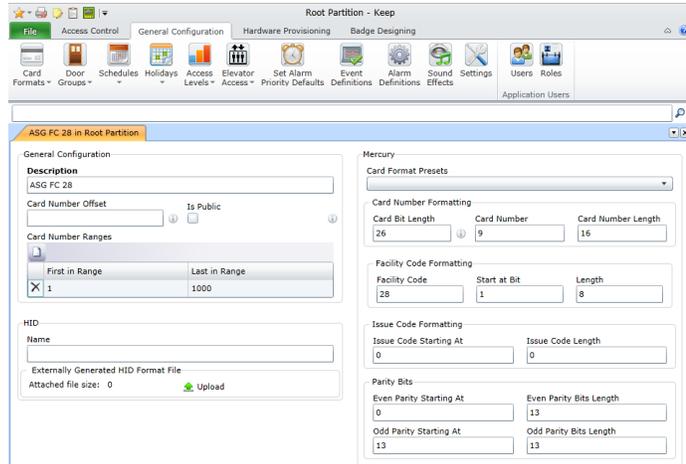
Status	Device	Type	Connected To
HardwareType: Controller (1 item)			
Online	ASG Controller	Controller	
HardwareType: Interface (1 item)			
Online	ASG Controller/On-bo	Interface	ASG Controller
HardwareType: Reader (1 item)			
Card Only	ASG Controller/On-bo	Reader	ASG Controller/C

Verify that all hard-

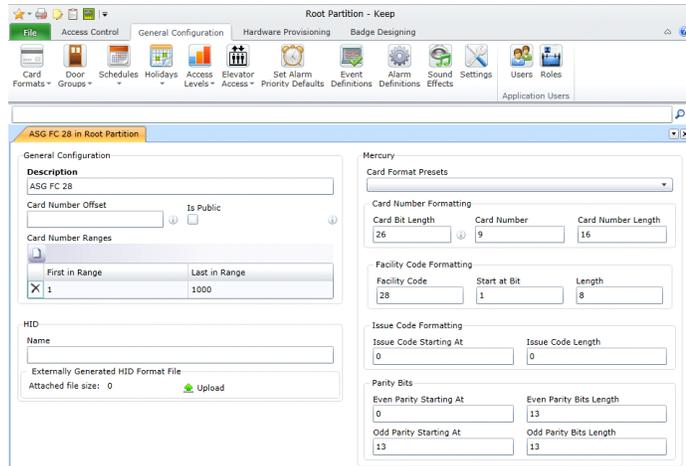
ware programmed is online

5. Step 5 – Card Formats

- a. General Configuration tab -> Card Formats -> Add new card format
 - i. Enter Description for the card format



ii.



Enter desired

range for the card format

- iii. Select Card Bit Length and starting bit and length
- iv. Select Card Facility code and starting bit and length
- v. Enter Parity settings
- vi. The Keep system comes preconfigured with default 26 bit and 37 bit HID cards

6. Step 6 – Create Door Group

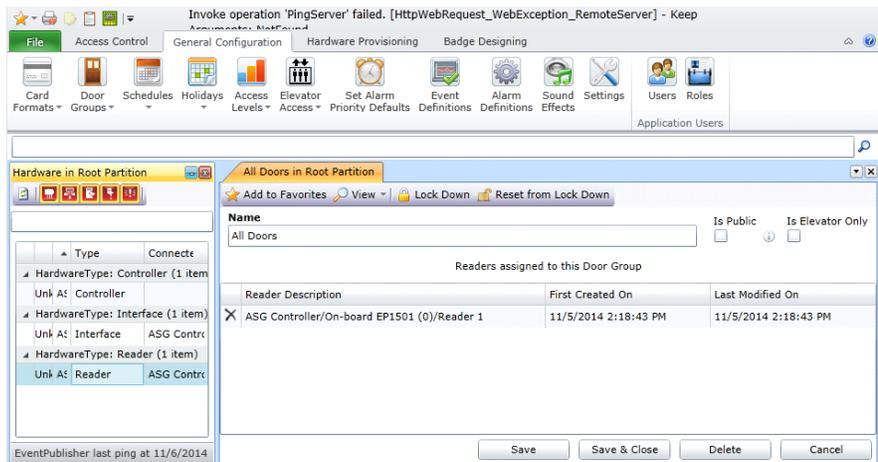
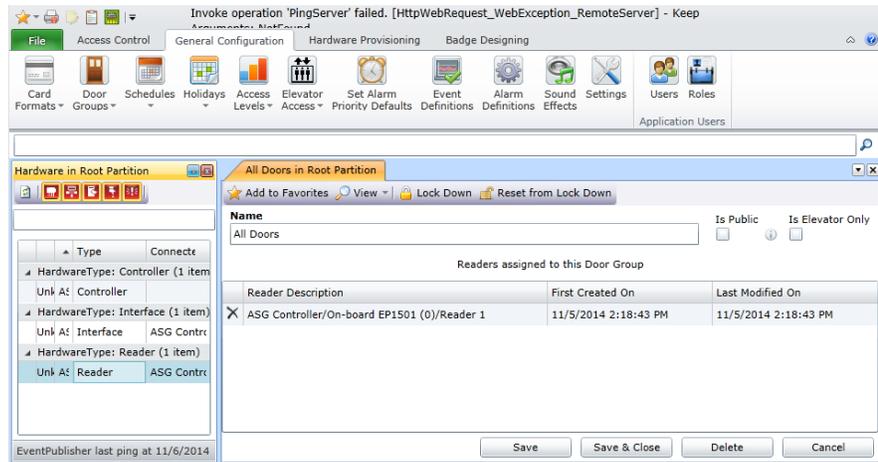
- a. Readers must belong to a door group in order to be assigned to a
- b. Open the device status window

c. **Select** General Configuration tab -> Door Groups -> Add new door group

i. Input a Door Group Name

ii. Drag and drop doors from status window to the door group window to add doors to the group

iii.



Select save at the bottom of the screen

7. Step 7 – Create Schedule

a. **Select** General Configuration tab -> Schedules -> Add new Schedule

b. Input a Name

c. Select function of schedule

i. Public

ii. Hardware

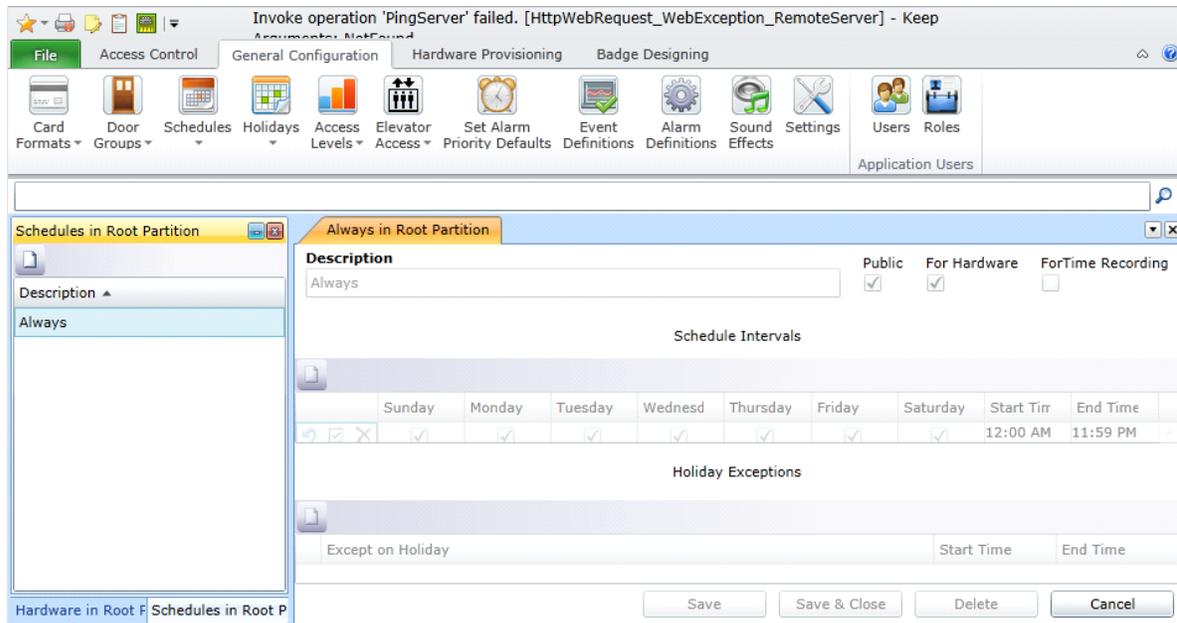
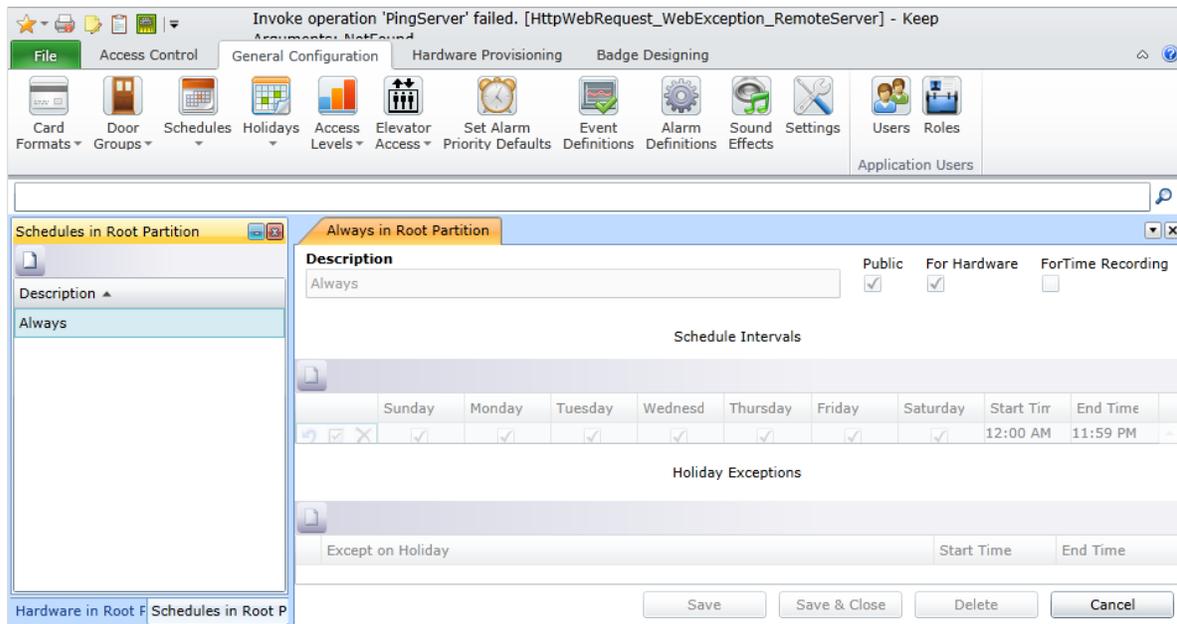
iii. Both

d. Create Schedule Intervals (Click on icon to add interval)

i. Select Days of week

ii. Select Time Intervals

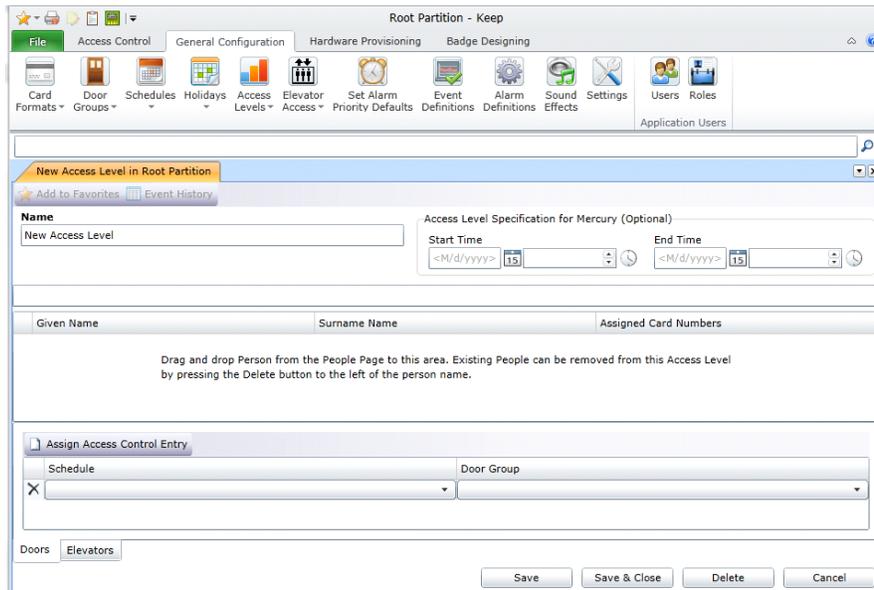
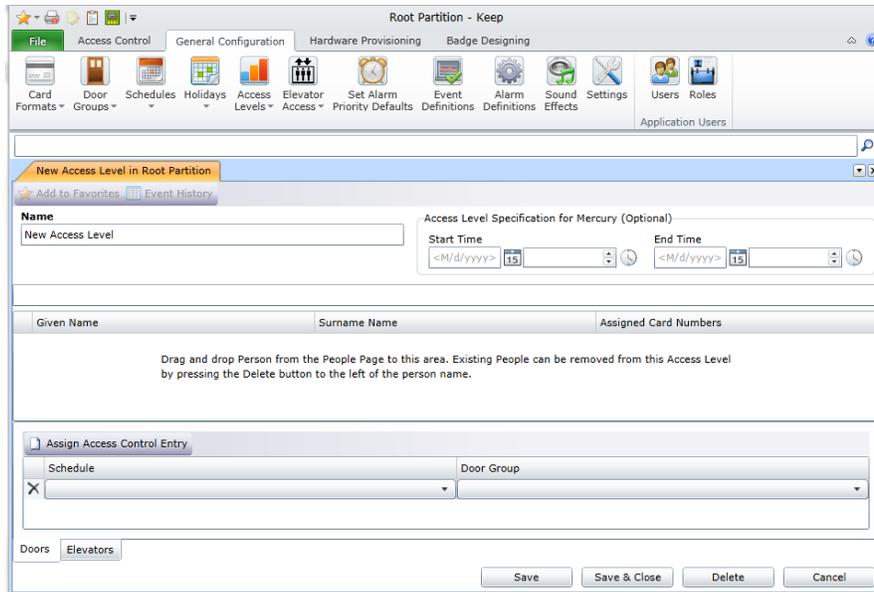
e.



Select Save

8. Step 8 – Create Access Levels

- a. **Select** General Configuration tab -> Access Levels -> Add new Access Level
- b. Input unique name
- c. Click on Assign Access Control Entry
 - i. Use drop down to select Schedule
 - ii. Use drop down to select Door Group
- d. Select save at the bottom of the screen



9. Step 9 – Create Card Holder

- a. **Select** Access Control tab -> New
- b. Input name
 - i. Given Name (First Name)
 - ii. Surname (Last Name)

iii.

Root Partition - Keep

File Access Control General Configuration Hardware Provisioning Badge Designing

New Batch List Cards Event History Live Monitoring View Floorplan Generate Reports Manage Reports

People Events & Alarm Monitoring Reporting

Technician, Joe

Cards Add to Favorites View

Name and Address

Given Name: Joe

Surname: Technician

File As: Technician, Joe Manager Level: 0

Email Address: Joe.technician@joes.com Mobile Phone: 222-222-2222

Office Phone: Home Phone:

Identification Photo

Upload Camera Discard

Assign Access Levels

ASG All Doors Always

Person Information Additional Information Badge Printing

Save Save & Close Delete Cancel

Root Partition - Keep

File Access Control General Configuration Hardware Provisioning Badge Designing

New Batch List Cards Event History Live Monitoring View Floorplan Generate Reports Manage Reports

People Events & Alarm Monitoring Reporting

Technician, Joe

Cards Add to Favorites View

Name and Address

Given Name: Joe

Surname: Technician

File As: Technician, Joe Manager Level: 0

Email Address: Joe.technician@joes.com Mobile Phone: 222-222-2222

Office Phone: Home Phone:

Identification Photo

Upload Camera Discard

Assign Access Levels

ASG All Doors Always

Person Information Additional Information Badge Printing

Save Save & Close Delete Cancel

Fill in other card holder information as required

- c. Add photo by clicking on Upload in Identification Photo area
- d. Click on Assign Access Levels Button
 - i. Use drop down to select Access Level
 - ii. Multiple Access Levels can be added



e.



Click on Cards button to add credential to cardholder (new windows opens)

i.

Click on Assign Card

(new window opens)

- ii. Use dropdown to select Badge Type
- iii. Input card number
- iv. Input Encoded Card Number if different
- v. Input PIN code if required
- vi. Select Active and Expiration dates and times
- vii. Select Save

10. User now has access to the reader per the schedule assigned

Basic Functionality

The Keep Access Control software is easy to migrate and function. The software is feature rich, and provides the basic and advanced functionality. Standard Mercury door functions are available and act similar to a Lenel installation. This makes this a much easier system to engineer and deploy if Standard Mercury hardware is used.

The advanced functionality includes:

1. Elevator control
2. Anti-passback
3. Maps
4. Badge Design

The web interface easy to navigate and is very intuitive. The lack of 'Right Click' context menus makes it a little harder to manipulate, but this is a learning curve that can easily be overcome with use and familiarity of the interface.

Conclusion

The Keep Access Control System appears is a fully functional and well thought out Access Control System. The only downside that I can see is in a hosted environment, the loss of internet means you have no way to control the system. The learning curve to functionality is minimal, and a customer's ability to create and assign access levels is easy to teach. The fact there is no hard client to install makes this system very adaptable, and easy to manage from any computer on the customer's network.