NanoAccess®

Access Control System
User Programming Guide

(revision 2c)

eyeLock®
Advanced Biometric Identity Authentication

Notices

It is IMPORTANT that this instruction manual be read and understood completely before installation or operation is attempted. It is intended that the installation of this unit will be performed only by persons trained and qualified in the installation of access control equipment. The IMPORTANT safeguards and instructions in this manual cannot cover all possible conditions and situations which may occur during installation and use. It must be understood that common sense and caution must be exercised by the person(s) installing, maintaining, and operating the equipment.

Standards Approvals

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

NanoAccess™ System

Installation Company Contact Information

Contents

1. Introduction

This manual contains information regarding the programming and configuration of the NanoAccess access control system. This system offers multi-station ability to secure doors, manage access of personnel, create and analyze reports, and monitor the system remotely from any Web browser. All monitored activity at the facility is recorded in the system memory — providing a record of all Card Holder entries and exits, input detection, and security or fire detection, if desired. The system can be seamlessly scaled up, via software keys, to provide increased door and reader capacity, enhanced features, and higher-level capabilities.

General Features

The following is a feature summary of the Controller:

- Browser-based management enables system status and updates from any location, with any supported OS, using any supported browser — Chrome® ver. 22 or higher; IE 9.0 or higher; Firefox® ver. 13 or higher; Safari® ver. 5.1.7 or higher.
- Supports access from iPhone®, iPad® and Android® devices.
- Intuitive Wizard allows for ultra-fast setup.
- Configure the system to perform automatic functions on specific days and times. For example, schedule when a door is unlocked or when an employee can gain access to the facility.
- Create, view, and print customized reports using the reporting tool.
- Create a set of instructions that the system will follow when an event occurs. For example, when a door is forced open the system can be instructed to turn on a camera and display a graphic.
- Configure the system to store custom information for each Card Holder such as phone number or employee ID.
- Define up to 30 holidays as special schedules. For example, schedule a door to remain locked during a holiday.
- Configure the system to send email and text message notifications.
- Software updates for new feature and product enhancements.

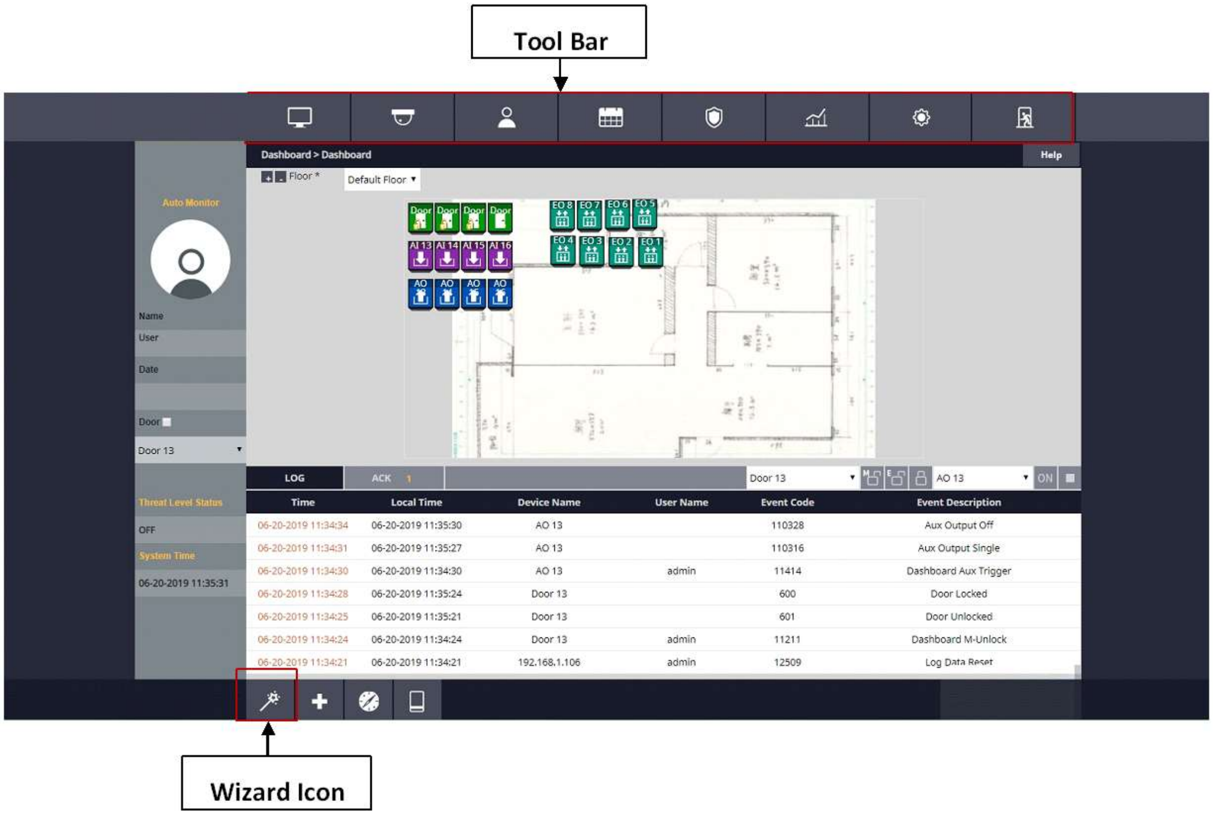
System Information

Feature	**System Capacities**	**System Capacities**
Model	**Base**	**Advanced**
Doors	32	128
Readers per system	64 (32 in / 32 out)	256 (128 in / 128 out)
Inputs	96	384
Outputs	64	512
Users (Card holders)	5,000	50,000
Access Levels	25	512
Time Schedules	25	250
Simultaneous system users	5	25
Online transactions	15,000	100,000
Elevator Control	Yes	Yes
Guard Tour	No	Yes
CCTV Integration	No	Yes
Mobile Phone as a credential	No	Yes
Real-time Graphic Floor Plans	No	Yes
Upgradeable	Yes	N/A

2. Software Layout

System Server Software

The Controller browser interface includes two methods available to the operator for programming and navigation. These methods include using the ***Toolbar*** and ***Wizard***. The Toolbar provides access to all configuration options; whereas the Wizard provides access to the core system components. The following illustration shows the location of the Toolbar and Wizard icon.



Threat Level Status: OFF

System Time: 06-20-2019 11:35:31

Time	Local Time	Device Name	User Name	Event Code	Event Description
06-20-2019 11:34:34	06-20-2019 11:35:30	AO 13		110328	Aux Output Off
06-20-2019 11:34:31	06-20-2019 11:35:27	AO 13		110316	Aux Output Single
06-20-2019 11:34:30	06-20-2019 11:34:30	AO 13	admin	11414	Dashboard Aux Trigger
06-20-2019 11:34:28	06-20-2019 11:35:24	Door 13		600	Door Locked
06-20-2019 11:34:25	06-20-2019 11:35:21	Door 13		601	Door Unlocked
06-20-2019 11:34:24	06-20-2019 11:34:24	Door 13	admin	11211	Dashboard M-Unlock
06-20-2019 11:34:21	06-20-2019 11:34:21	192.168.1.106	admin	12509	Log Data Reset

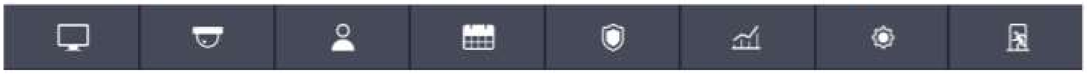
The first time the system is run, the Wizard will run automatically. This allows setting of the following core system components:

- System Language Selection
- System License
- Card Format Setup
- Holiday Group Setup
- Schedule Setup
- Door Setup
- Access Level Setup
- Card Holder Setup
- Card Setup
- Network Setup
- Dealer Registration
- System Startup Screen Selection

Refer to the Section in the rear of this manual "Using the Wizard" for details on each Wizard screen.

Toolbar Menu

The Toolbar provides access to all setup, programming, management, and reporting options of the Controller.



Dashboard: The default system software page, which is primarily used to monitor and acknowledge recent events.

NVR: view cameras and NVRs if installed.

Administration: 1)Add, edit or delete Card Holders and Access Levels .2)Export or import data using a CSV file.

Schedule: Add and edit time schedules, holidays and unlock schedules.

Threat Level: Enable and set Threat Level.

Report: Provides system ,event reporting and the result of smart reports.

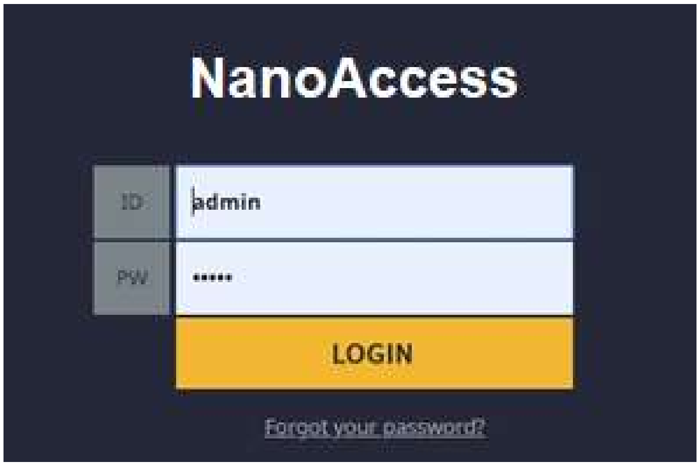
System Setting: Dashboard, NVR, Card Format, Event Action, Threat Level, Smart Report, User, Floor, System, Network, Device, Client & Site and Group Table setting.

Logout: Logs the operator out of the system.

3. System Programming

Connect to the Controller

Open a web browser on a local computer and enter the IP address of the Controller (Default = 192.168.0.250). The browser presents the login page as shown.

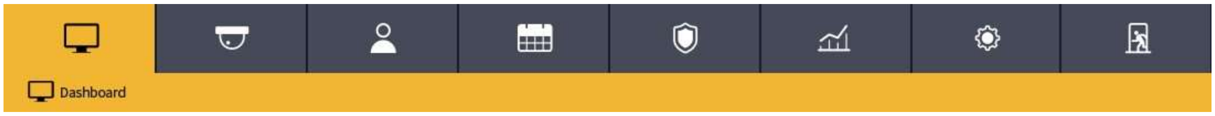


1. Enter the User ID.
   Default User ID = **admin**
2. Enter the Password.
   Default Password = **admin**
3. Click Login.

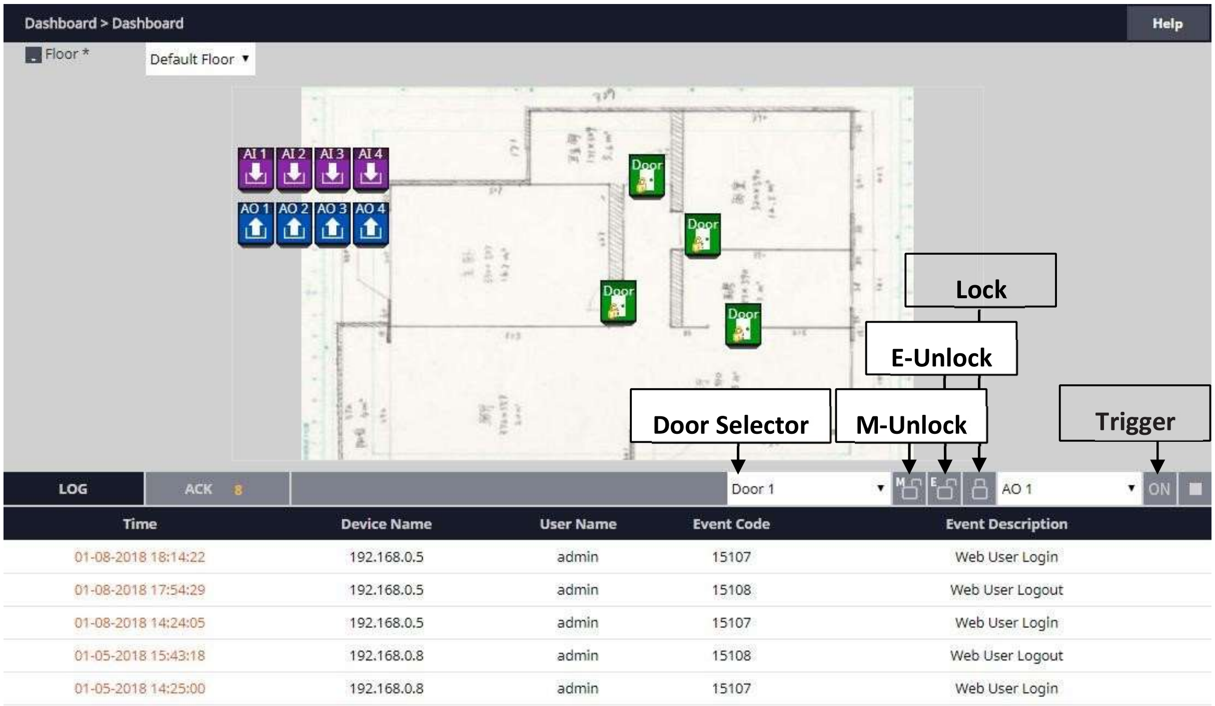
Just in case, a link will be displayed that will send a message to the NanoAccess Super Administrator for a forgotten password.

✓ NOTE: The Super Administrator password is set in Device Settings >Controller

Dashboard



Click the ***Dashboard*** icon to open the Dashboard window, which displays incoming events and allows users to view, acknowledge, and clear events. The Dashboard allows the operator to monitor real-time activities in the facility - for example, use of a valid card or a door forced open. The Dashboard also provides the ability to manually lock and unlock doors and activate outputs.



Time	Device Name	User Name	Event Code	Event Description
01-08-2018 18:14:22	192.168.0.5	admin	15107	Web User Login
01-08-2018 17:54:29	192.168.0.5	admin	15108	Web User Logout
01-08-2018 14:24:05	192.168.0.5	admin	15107	Web User Login
01-05-2018 15:43:18	192.168.0.8	admin	15108	Web User Logout
01-05-2018 14:25:00	192.168.0.8	admin	15107	Web User Login

M-Unlock: Unlocks the door for the time defined as the Door Unlock Time (default = 3 seconds). **E-Unlock:** Unlocks the door until the user clicks Lock.

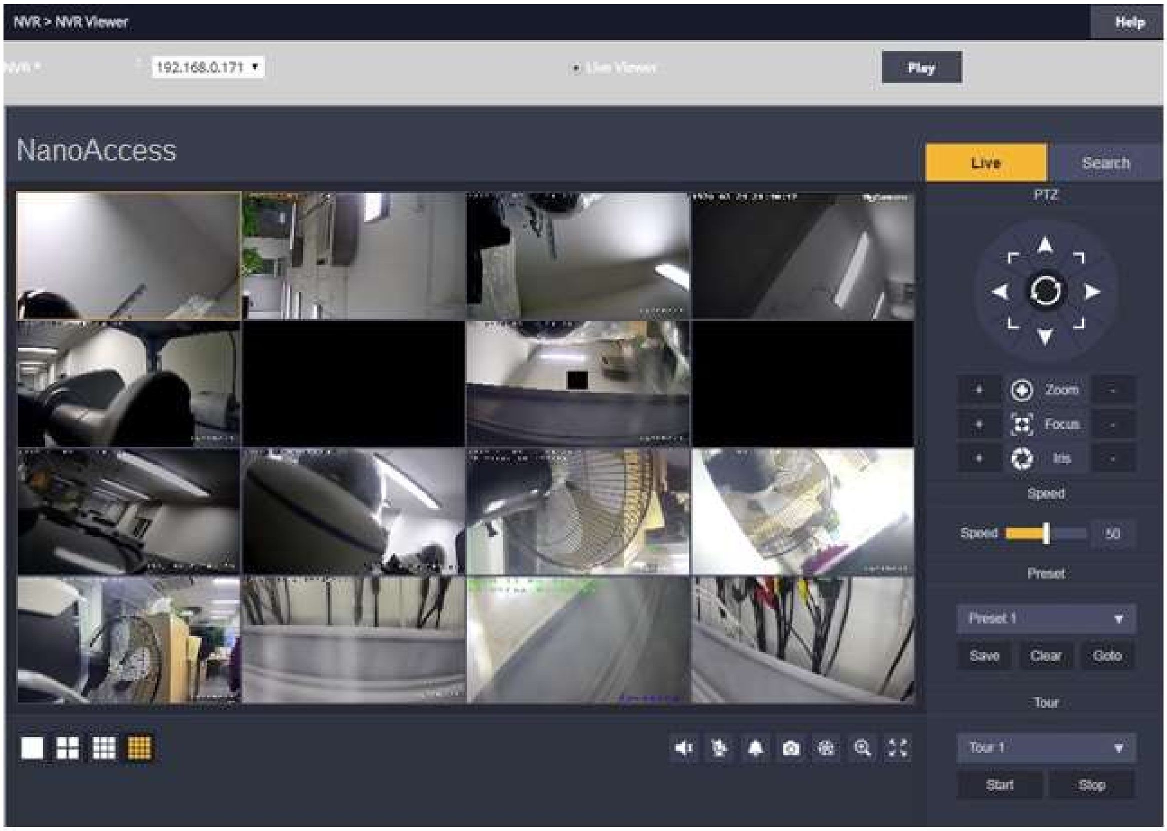
Lock: Locks the door.

Trigger: Activates the selected auxiliary or elevator output according to the ***Aux Output*** settings (see Aux Output to configure output settings).

NVR View

Optional Feature

NVR View allows the user to select defined IP NVR video matrix and different NVR views. **Refer to the NVR manual for programming information.**

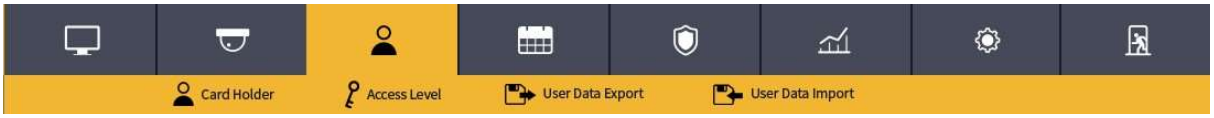

NVR * 192.168.0.171

Speed 50

Preset 1

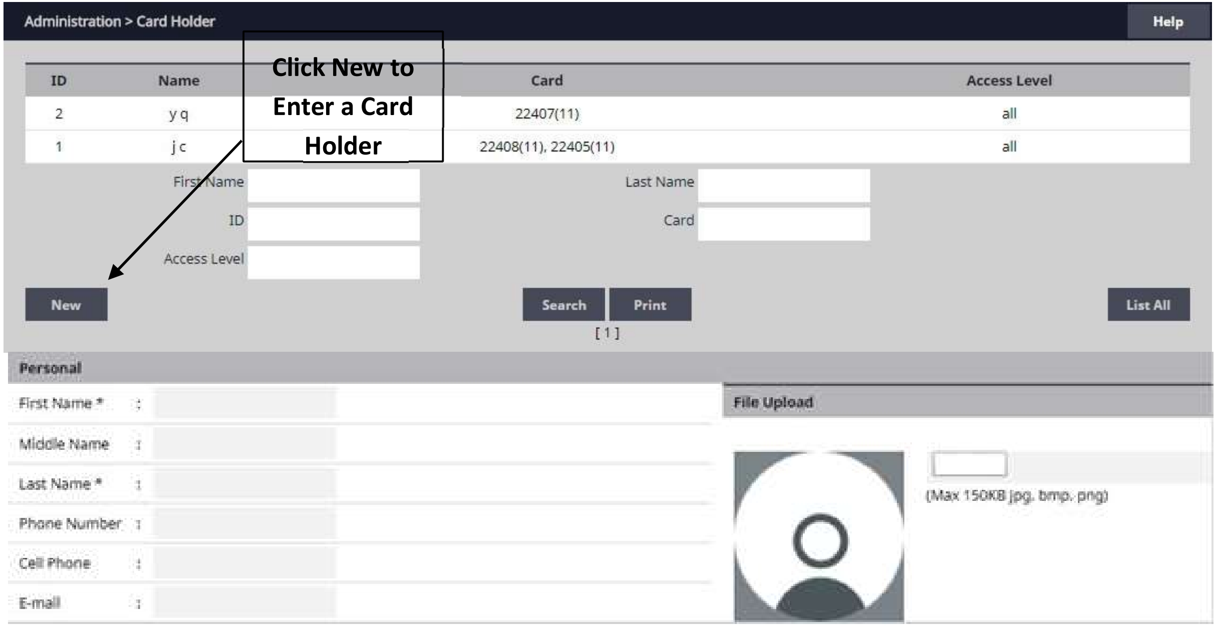
Tour 1

Card Holder



Card Holders are individuals who access the facility and are entered in the system. Access credentials are assigned to Card Holders

Creating a Card Holder



Administration > Card Holder

Help

ID	Name	Card	Access Level
2	y q	22407(11)	all
1	j c	22408(11), 22405(11)	all

Click New to Enter a Card Holder

First Name

Last Name

ID

Card

Access Level

New

Search

Print

List All

[1]

Personal

First Name * :

Middle Name :

Last Name * :

Phone Number :

Cell Phone :

E-mail :

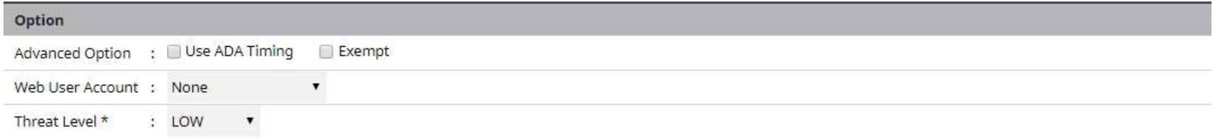
File Upload

(Max 150KB jpg, bmp, png)

1. Click **New**.
2. Enter the name and contact information of the Card Holder.
3. Click **File Upload** to select a file to assign an image to the Card Holder for identification purposes.

✓ ***NOTE:*** *Picture files can be 150 Kb maximum. JPG, BMP, or PNG formats.*

Card Holder Options



Option

Advanced Option : ☐ Use ADA Timing ☐ Exempt

Web User Account : None ▾

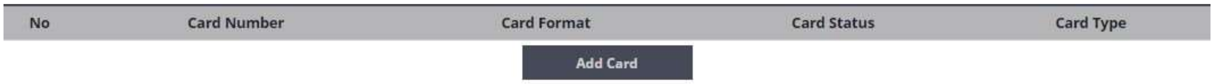
Threat Level * : LOW ▾

1. Select **ADA Timing** for extended timing for the door relay.
2. Select **Exempt** to allow the Card Holder to bypass Anti-Passback rules (except occupancy rules) if the Card Holder is allowed access to the region.
3. Select a **Web User Account** to give the Card Holder operator privileges to the Controller.
4. Choose the highest **Threat Level** that the Card Holder will be allowed access.

✓ ***NOTE:*** *A Card Holder cannot access a door if either the Door Threat Level or the System Threat Level is greater than the Card Holder Threat Level.*

5. Click **Save**.

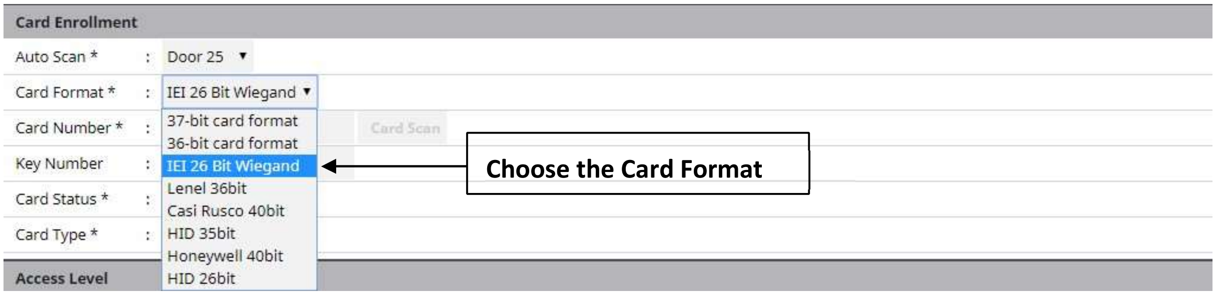
Assigning a Card to an Existing Card Holder



No	Card Number	Card Format	Card Status	Card Type

1. Select the Card Holder from the main window.
2. Click **Add Card**.

Card Format

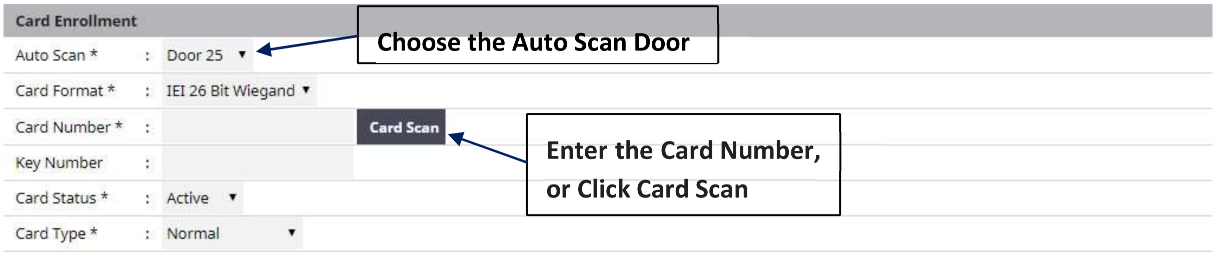


Card Enrollment		
Auto Scan *	:	Door 25 ▾
Card Format *	:	IEI 26 Bit Wiegand ▾
Card Number *	:	
Key Number	:	
Card Status *	:	
Card Type *	:	

Choose the Card Format

3. Select the appropriate **Card Format** from the drop-down field.

Card Number



Card Enrollment		
Auto Scan *	:	Door 25 ▾
Card Format *	:	IEI 26 Bit Wiegand ▾
Card Number *	:	
Key Number	:	
Card Status *	:	Active ▾
Card Type *	:	Normal ▾

Choose the Auto Scan Door

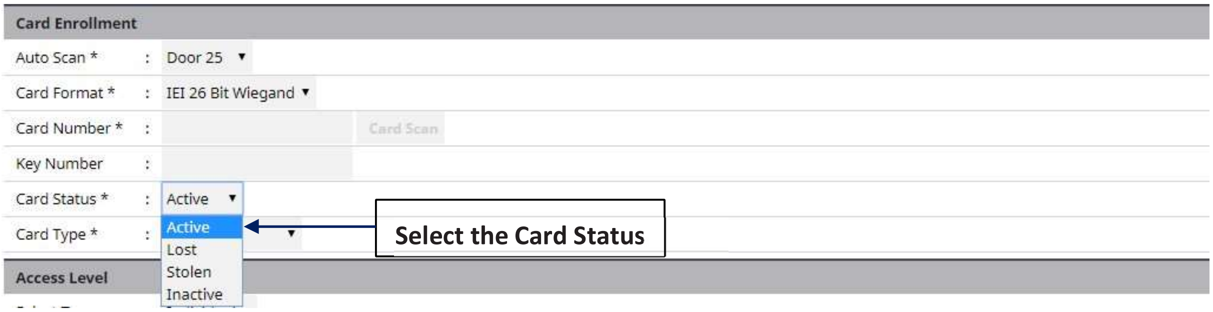
Enter the Card Number, or Click Card Scan

4. Enter the **Card Number** or use the Auto Scan feature.

Auto Scan

5. Choose the **Auto Scan** door reader where the card will be presented.
6. Click **Card Scan** and present the card to the reader. The new card number will populate the data field.

Card Status

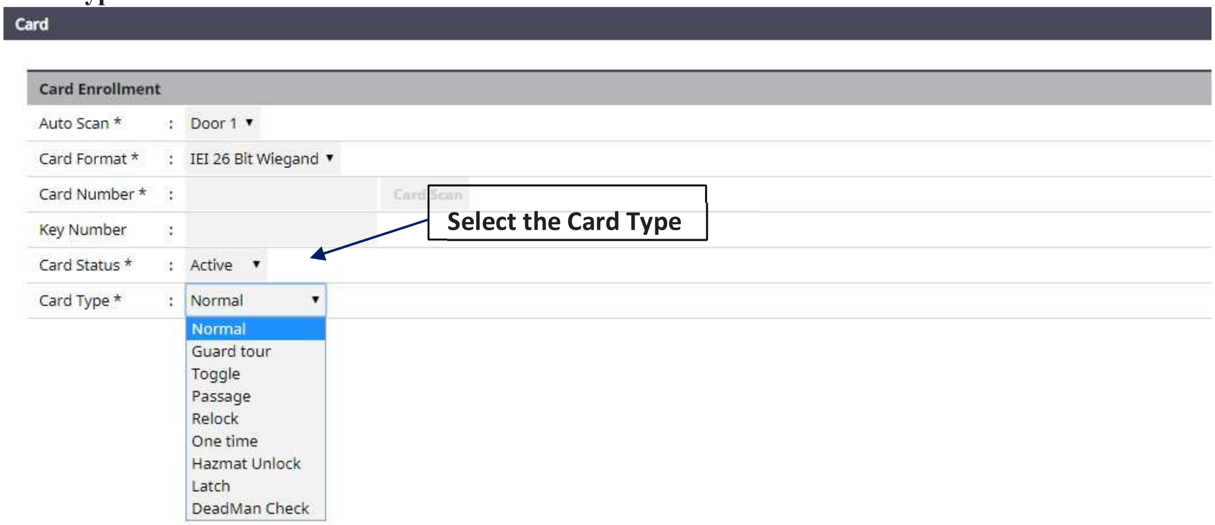


Card Enrollment		
Auto Scan *	:	Door 25 ▾
Card Format *	:	IEI 26 Bit Wiegand ▾
Card Number *	:	
Key Number	:	
Card Status *	:	Active ▾
Card Type *	:	

Select the Card Status

7. Select the current **Card Status**.

Card Type



Card

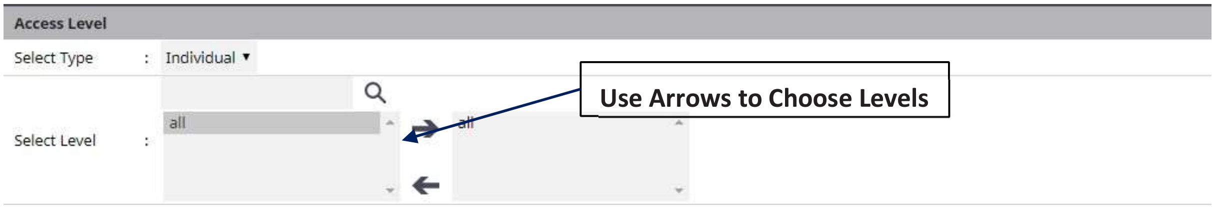
Card Enrollment

Auto Scan *	:	Door 1 ▾
Card Format *	:	IEI 26 Bit Wiegand ▾
Card Number *	:	
Key Number	:	
Card Status *	:	Active ▾
Card Type *	:	Normal ▾

Select the Card Type

8. Select the function for the card with **Card Type** dropdown.

Access Level



Access Level

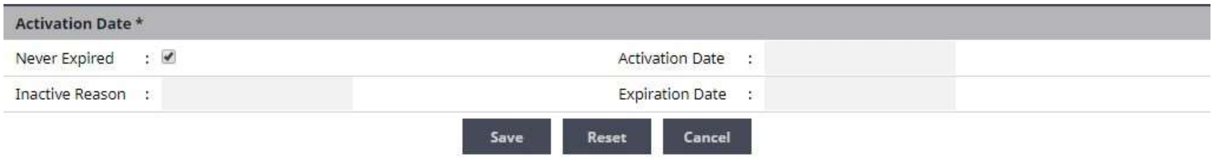
Select Type	:	Individual ▾
Select Level	:	all

Use Arrows to Choose Levels

9. For **Select Type** select Individual or Group access level.

10. For **Select Level** select the desired access levels (or use the search icon to find a specific access level) and click the right arrow to move the access level to the field on the right.

Activation Date



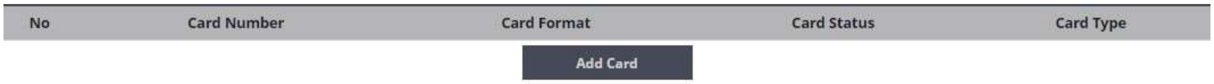
Activation Date *

Never Expired	: ☑		Activation Date	:	
Inactive Reason	:		Expiration Date	:	

11. Choose an optional activation and expiration date for the card.

12. Click **Save** to assign the card to the Card Holder.

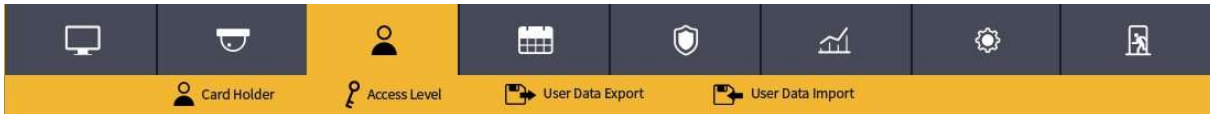
The added card will show on the card list for the Card Holder.



No	Card Number	Card Format	Card Status	Card Type

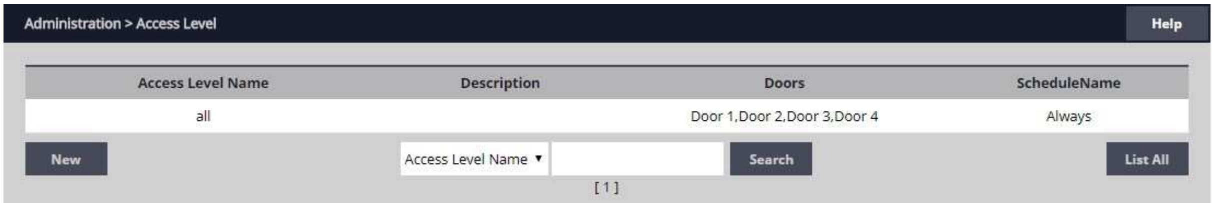
Click **Add Card** to add additional cards for the selected Card Holder.

Access level

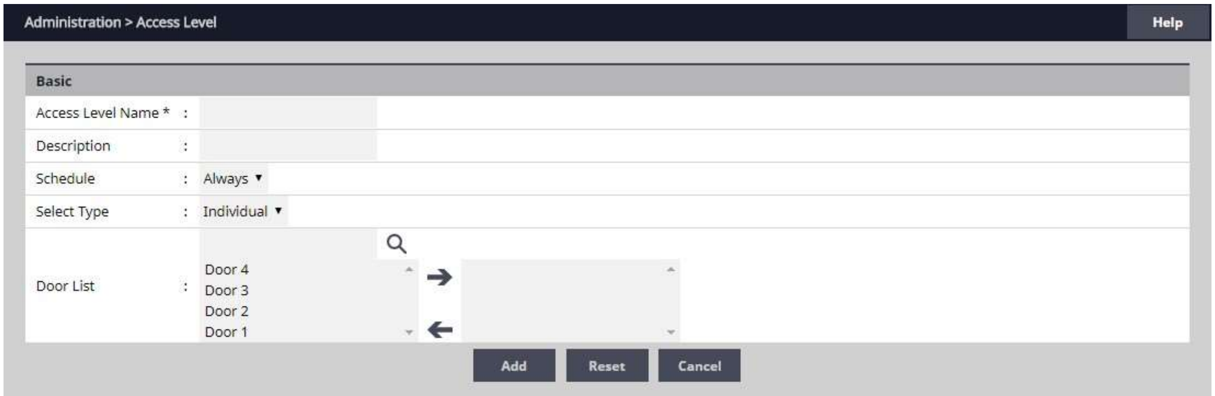


An ***Access Level*** establishes which doors the Card Holder can access and when they are allowed to access them. Access Levels are comprised of a time schedule and door(s).

Adding an Access Level



Access Level Name	Description	Doors	ScheduleName
all		Door 1,Door 2,Door 3,Door 4	Always



Access Level Name * :	
Description :	
Schedule :	Always ▾
Select Type :	Individual ▾
Door List :	Door 4 Door 3 Door 2 Door 1

1. Click **New**.
2. Enter the desired **Access Level Name and Description** (optional).
3. Assign a time schedule to the Access Level by choosing it from the **Schedule** dropdown menu.
4. Select Group or Individual for the Access Group **Type**.
5. For **Door List**, select the desired doors (or use the search icon to find a specific door) and click the right arrow to move the doors to the field on the right.

✓ ***Note:*** *Ctrl-click or shift-click will select multiple doors.*

6. Click Add to save the changes.

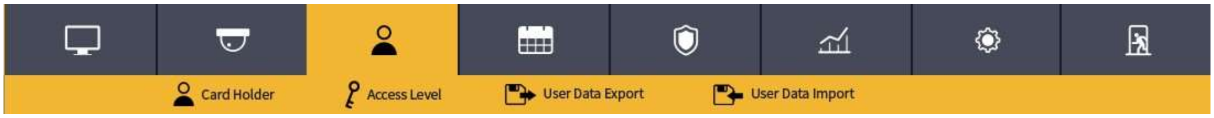
Editing an Access Level

1. Select an Access Level from the list and click **Edit**.
2. Make the desired edits.
3. Click **Save** to save the changes.

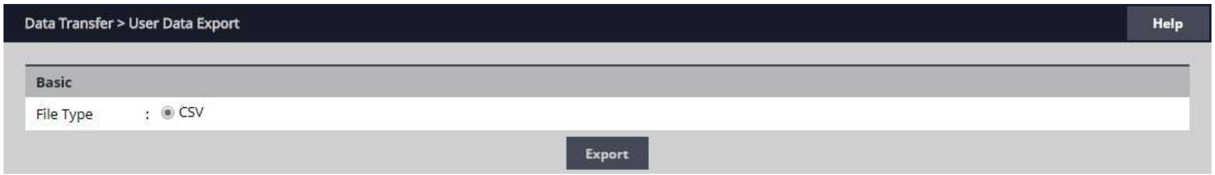
Deleting an Access Level

1. Select an Access Level from the list and click **Edit**.
2. Click **Delete**.
3. A confirmation window will pop up, click **OK** to delete the Access Level.

User Data Export



User Data Export provides the ability to export Card Holder data to a comma separated value (CSV) file.



Data Transfer > User Data Export

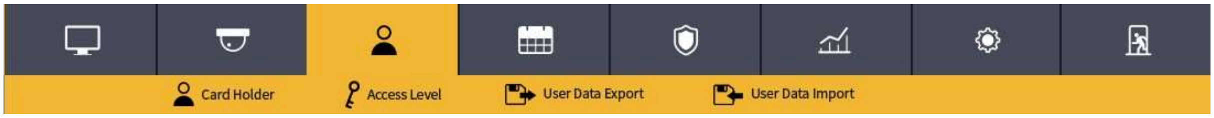
Basic

File Type : ◉ CSV

Exporting User Data

1. To export the Card Holder data, click Export.
2. The CSV file of the Card Holder data will be downloaded through the browser.

User Data Import



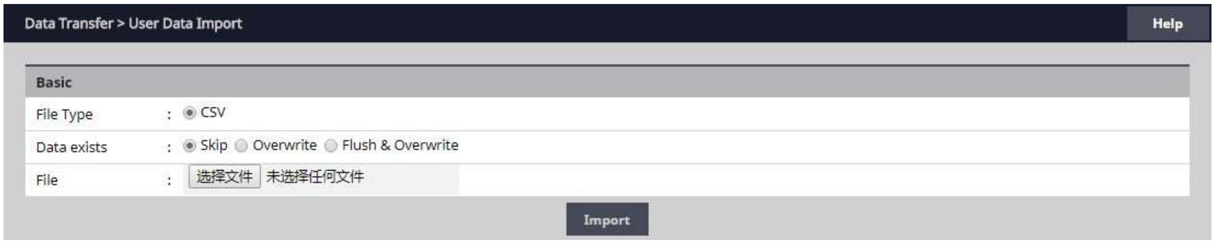
User Data Import provides the ability to import Card Holder data from a comma separated value (CSV) file.

To successfully import a file, the column headers must match those present in the User Data Export file. It is suggested to perform a data export and use it as a template for the import file.

You must have the related card formats and Access Levels configured before importing the file.

◆ ***WARNING:*** *Do not use special characters <>?{})(*&%#@ in any fields.*

✓ ***NOTE:*** *Data will not be imported unless the information is entered in the same manner in which it appears in the system software database (e.g., case sensitive and syntax sensitive).*

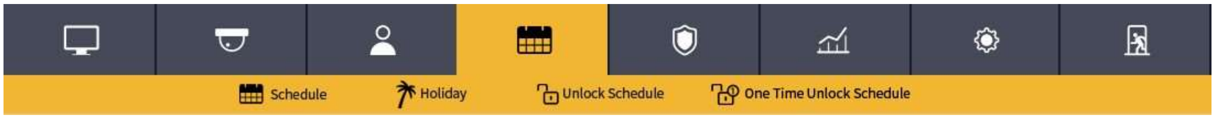


Basic

File Type :	● CSV
Data exists :	● Skip ○ Overwrite ○ Flush & Overwrite
File :	选择文件 未选择任何文件

Importing User Data

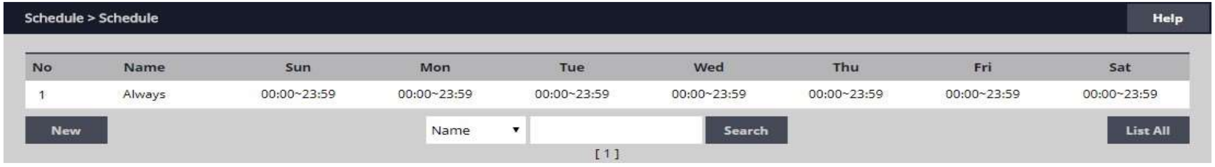
1. To skip Card Holder records that currently exist in the system, select Skip. To overwrite Card Holder records that currently exist in the system, select Overwrite.
2. Click Choose File and select the file to import.
3. Click Import.



Schedule

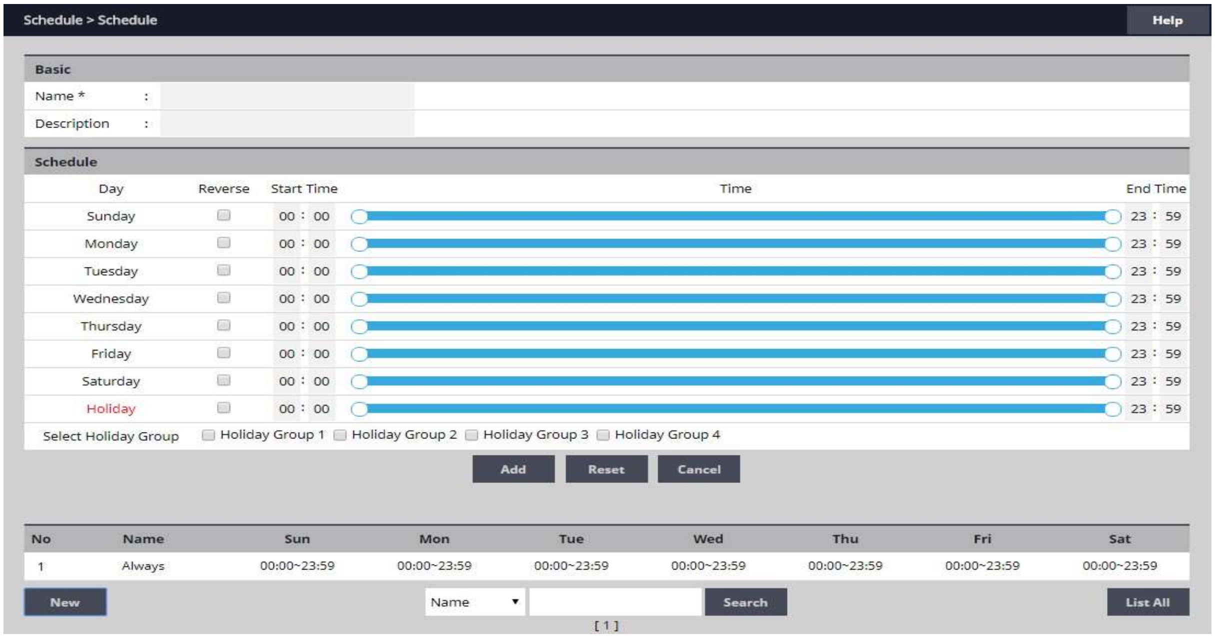
A ***Schedule*** is a combination of a time interval and one or more days of the week. Use schedules to identify the hours and days when inputs, outputs or door access are in operation. Assign holiday groups to the schedule to control when operations occur on holidays. There is one default time schedule of Always, which is defined as 00:00-23:59, seven days per week.

Adding a Schedule



Schedule > Schedule

No	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	Always	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59



Schedule > Schedule

Basic

Name * :

Description :

Schedule

Day	Reverse	Start Time	Time	End Time
Sunday	□	00 : 00		23 : 59
Monday	□	00 : 00		23 : 59
Tuesday	□	00 : 00		23 : 59
Wednesday	□	00 : 00		23 : 59
Thursday	□	00 : 00		23 : 59
Friday	□	00 : 00		23 : 59
Saturday	□	00 : 00		23 : 59
Holiday	□	00 : 00		23 : 59

Select Holiday Group □ Holiday Group 1 □ Holiday Group 2 □ Holiday Group 3 □ Holiday Group 4

No	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	Always	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59

1. Click **New**.
2. Enter the desired name and description (optional) for the schedule.
3. Adjust the sliders for the **Start Time** and **End Time** on days when the schedule is to be active. (Collapse slider for no access on that day.)
4. (Optional) Select a holiday group to allow access on the holidays in the group. If a holiday group is selected, identify a start and end time for holiday access.
5. Click **Add** to save the new schedule.

✓ ***Note:*** *To create a schedule with a "Midnight Crossing" (e.g., 16:00 to 00:30) click Reverse.*

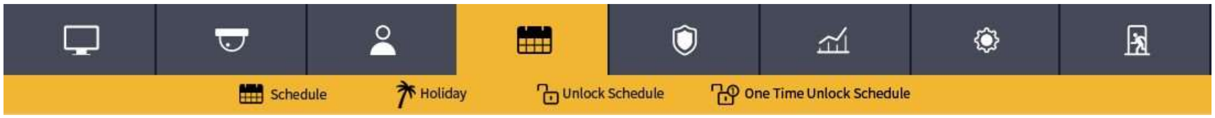
Deleting a Schedule

1. Select the schedule to be deleted.
2. The schedule will appear. Scroll to the bottom of the page and click **Delete**.
3. Click **OK** to confirm the deletion.

Editing a Schedule

1. Select the schedule to be edited and click **Edit**.
2. Perform the desired changes to the **Name, Description** and time intervals.
3. Scroll down and click **Save** to save the changes.

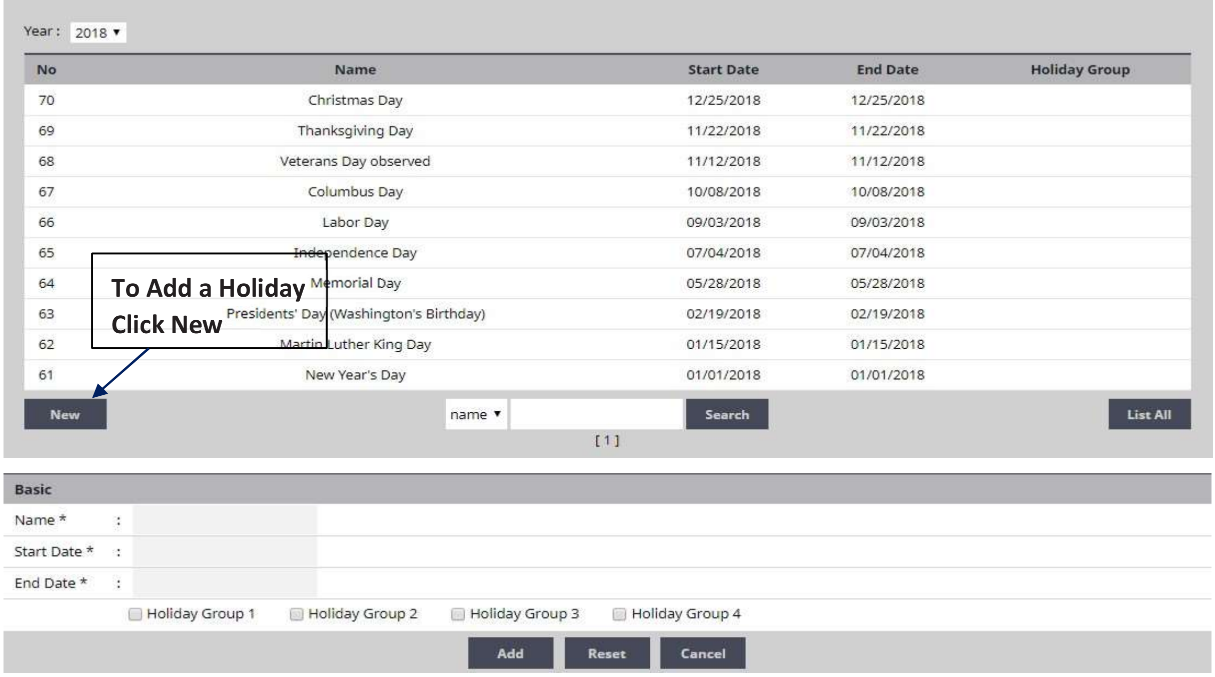
✓ ***NOTE:*** *When changing or deleting a schedule review the unlock schedules and Access Levels for possible changes.*



Holiday

Use ***Holiday*** to define days and times during the year when holiday hours are used. When the holiday starts, the Controller switches from regular hours to holiday hours. When the holiday ends, the regular hours resume. You can assign four holiday groups with up to 30 holidays total among the groups. A holiday can include any number of consecutive days within the same calendar year. The system Controller has preconfigured holiday groups based upon the country you selected in the Language section of the Wizard. The holiday groups are preconfigured through 2020 for quick setup.

Adding a Holiday



Year : 2018

No	Name	Start Date	End Date	Holiday Group
70	Christmas Day	12/25/2018	12/25/2018	
69	Thanksgiving Day	11/22/2018	11/22/2018	
68	Veterans Day observed	11/12/2018	11/12/2018	
67	Columbus Day	10/08/2018	10/08/2018	
66	Labor Day	09/03/2018	09/03/2018	
65	Independence Day	07/04/2018	07/04/2018	
64	Memorial Day	05/28/2018	05/28/2018	
63	Presidents' Day (Washington's Birthday)	02/19/2018	02/19/2018	
62	Martin Luther King Day	01/15/2018	01/15/2018	
61	New Year's Day	01/01/2018	01/01/2018	

To Add a Holiday Click New

Basic

Name * :	
Start Date * :	
End Date * :	

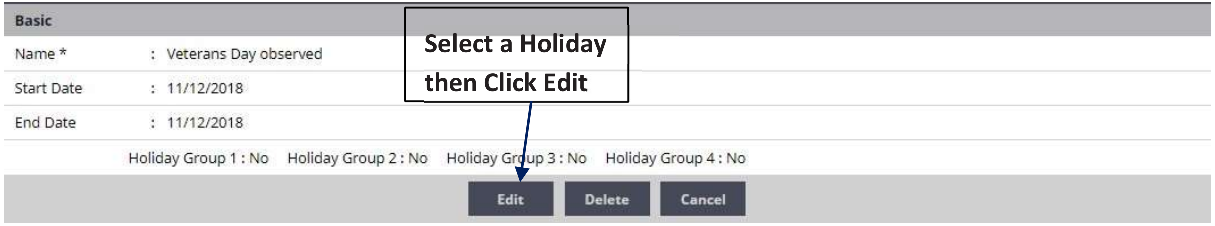
□ Holiday Group 1 □ Holiday Group 2 □ Holiday Group 3 □ Holiday Group 4

1. Click **New** and enter the desired name, start date and end date.
2. Select the desired holiday group for the new holiday.
3. Click **Add** to save the new holiday.

✓ NOTE: Access will be restricted on any holiday assigned to a holiday group.

See Schedules for information on how to allow access on holidays.

Editing a Holiday



Basic

Name * : Veterans Day observed

Start Date : 11/12/2018

End Date : 11/12/2018

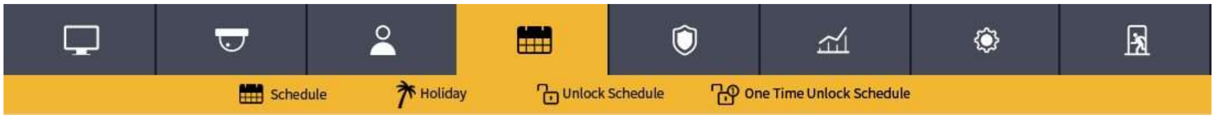
Holiday Group 1 : No Holiday Group 2 : No Holiday Group 3 : No Holiday Group 4 : No

Select a Holiday then Click Edit

1. Select the desired holiday and click **Edit**.
2. Change the start date and end date to the desired date.
3. Rename the holiday (it is recommended that pre-configured holidays be renamed when edited).
4. Click **Save**.

Deleting a Holiday

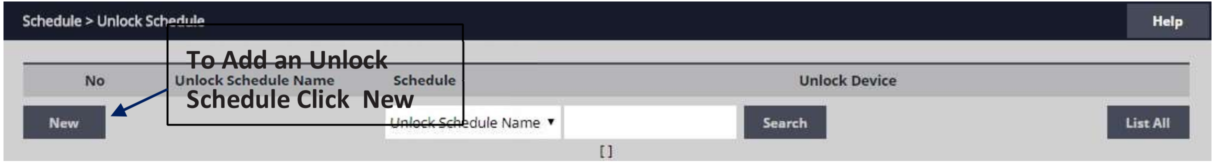
1. Highlight the holiday to be deleted.
2. Click **Delete**. A confirmation box will appear.
3. Click **OK** to confirm.



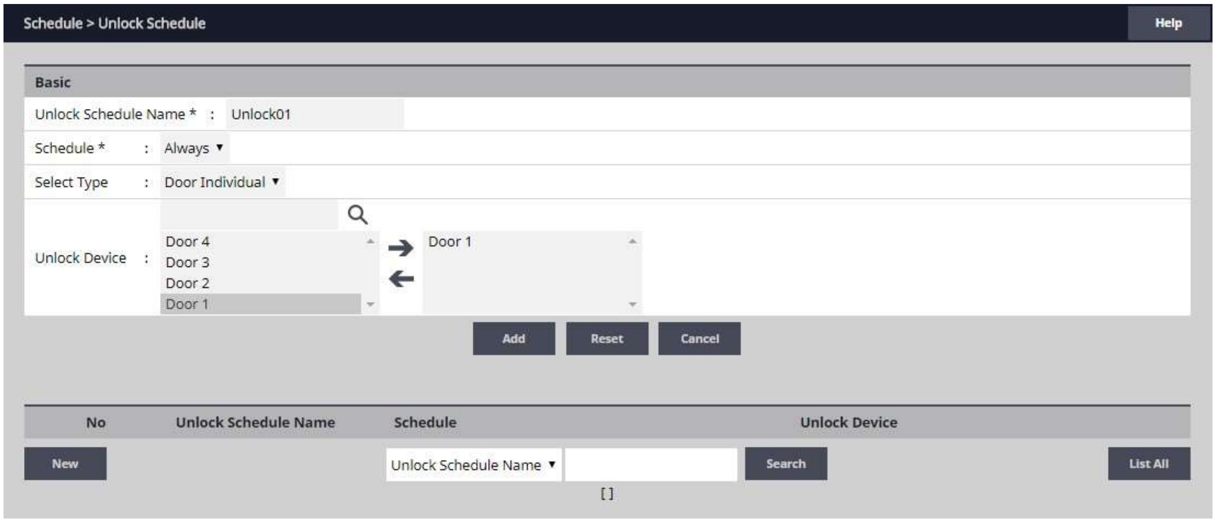
Unlock Schedule

An ***Unlock Schedule*** defines which Schedule will be used with selected access devices to automatically unlock one or more doors.

Adding an Unlock Schedule



To Add an Unlock Schedule Click New



Unlock Schedule Name * : Unlock01

Schedule * : Always ▾

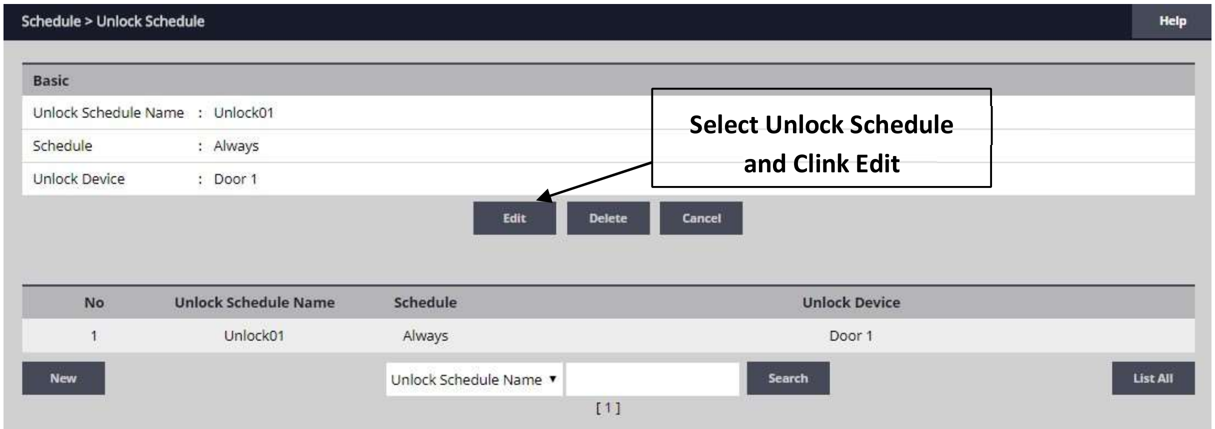
Select Type : Door Individual ▾

Unlock Device : Door 1

1. Click **New**.
2. Enter a Unlock Schedule **Name**.
3. Select the **Schedule** when the door will be unlocked.
4. Click the **Select Type** drop-down to select an individual door or a group of doors.
5. For **Unlock Device**, select the desired doors (or use the search icon to find a specific door) and click the right arrow to move the doors to the field on the right.

Click **Add** to create the unlock schedule.

Editing an Unlock Schedule



Schedule > Unlock Schedule

Basic

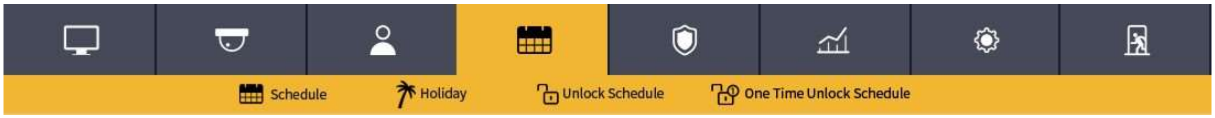
Unlock Schedule Name	: Unlock01
Schedule	: Always
Unlock Device	: Door 1

No	Unlock Schedule Name	Schedule	Unlock Device
1	Unlock01	Always	Door 1

1. Select the desired Unlock Schedule and click **Edit**.
2. Edit the Unlock Schedule **Name, Schedule Type, Unlock Device.**
3. Click **Save**.

Deleting an Unlock Schedule

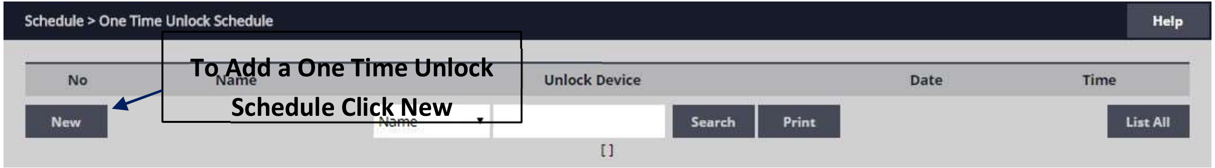
1. Select the Unlock Schedule to be deleted.
2. Click **Delete**. A confirmation box will appear.
3. Click **OK** to confirm.



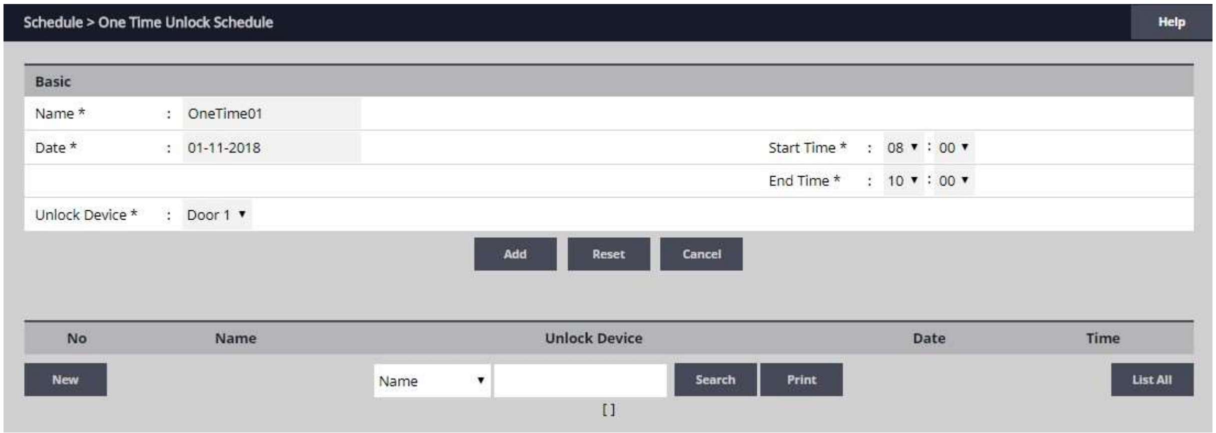
One Time Unlock Schedule

A One Time Unlock Schedule defines one date and time to automatically unlock one selected door.

Adding a One Time Unlock Schedule



To Add a One Time Unlock Schedule Click New

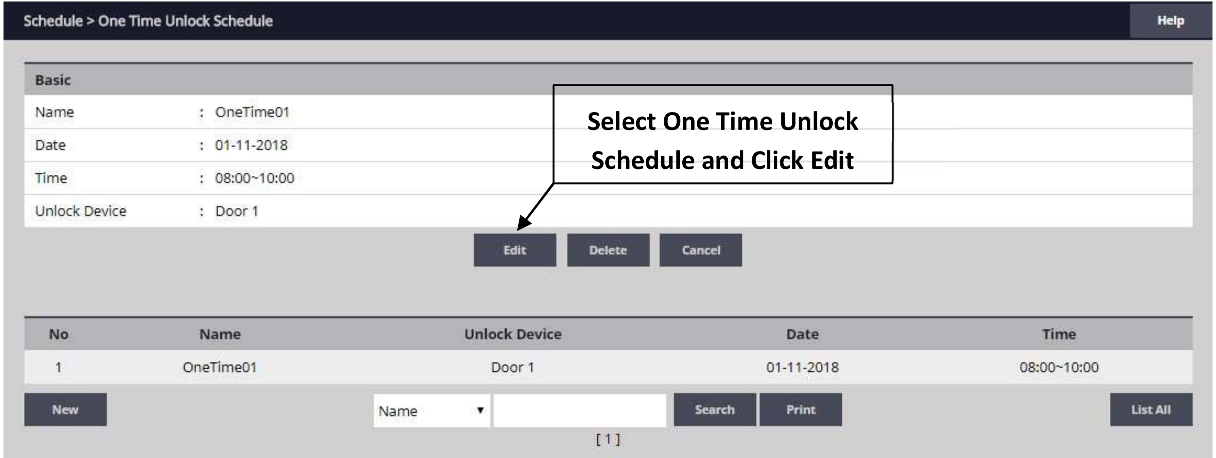


Name *	: OneTime01			
Date *	: 01-11-2018	Start Time *	:	08 : 00
		End Time *	:	10 : 00
Unlock Device *	: Door 1			

1. Click **New**.
2. Enter a **Name** for the One Time Unlock Schedule.
3. Select the **Date** when the door will be unlocked.
4. Select the **Start Time** and **End Time** for the unlock period.
5. Click the drop-down to select a door to unlock.

Click **Add** to create the One Time Unlock Schedule.

Editing a One Time Schedule



Name	: OneTime01
Date	: 01-11-2018
Time	: 08:00~10:00
Unlock Device	: Door 1

Select One Time Unlock Schedule and Click Edit

No	Name	Unlock Device	Date	Time
1	OneTime01	Door 1	01-11-2018	08:00~10:00

1. Select the desired One Time, Unlock Schedule and click **Edit**.
2. Make the changes desired.
3. Click **Save**.

Deleting a One Time Schedule

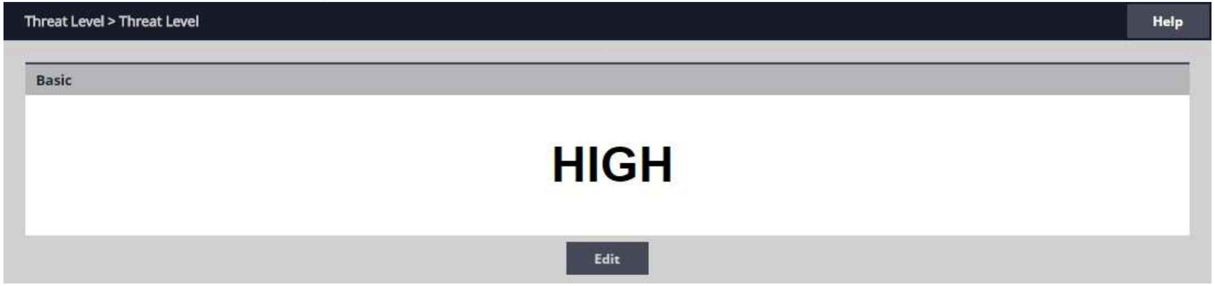
1. Select the desired One Time Unlock Schedule to be deleted.
2. Click **Delete**. A confirmation box will appear.
3. Click **OK** to confirm.

Threat Level

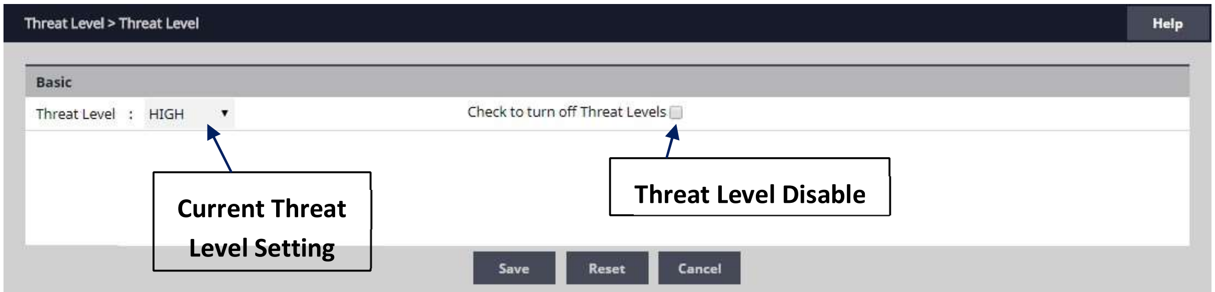
Optional Feature

Threat Levels are used in systems to modify existing unlock schedules and Access Level privileges. The system has five pre-defined Threat Levels. The names of each can be changed to match installation requirements.

Current Threat Level Setting



HIGH

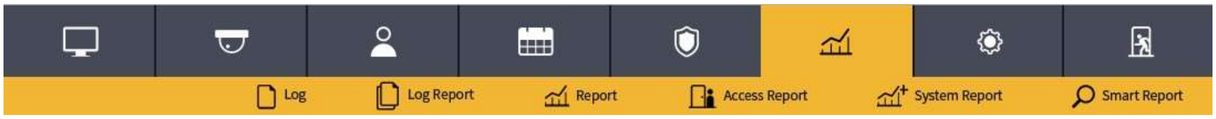


Threat Level : HIGH ▾

Check to turn off Threat Levels □

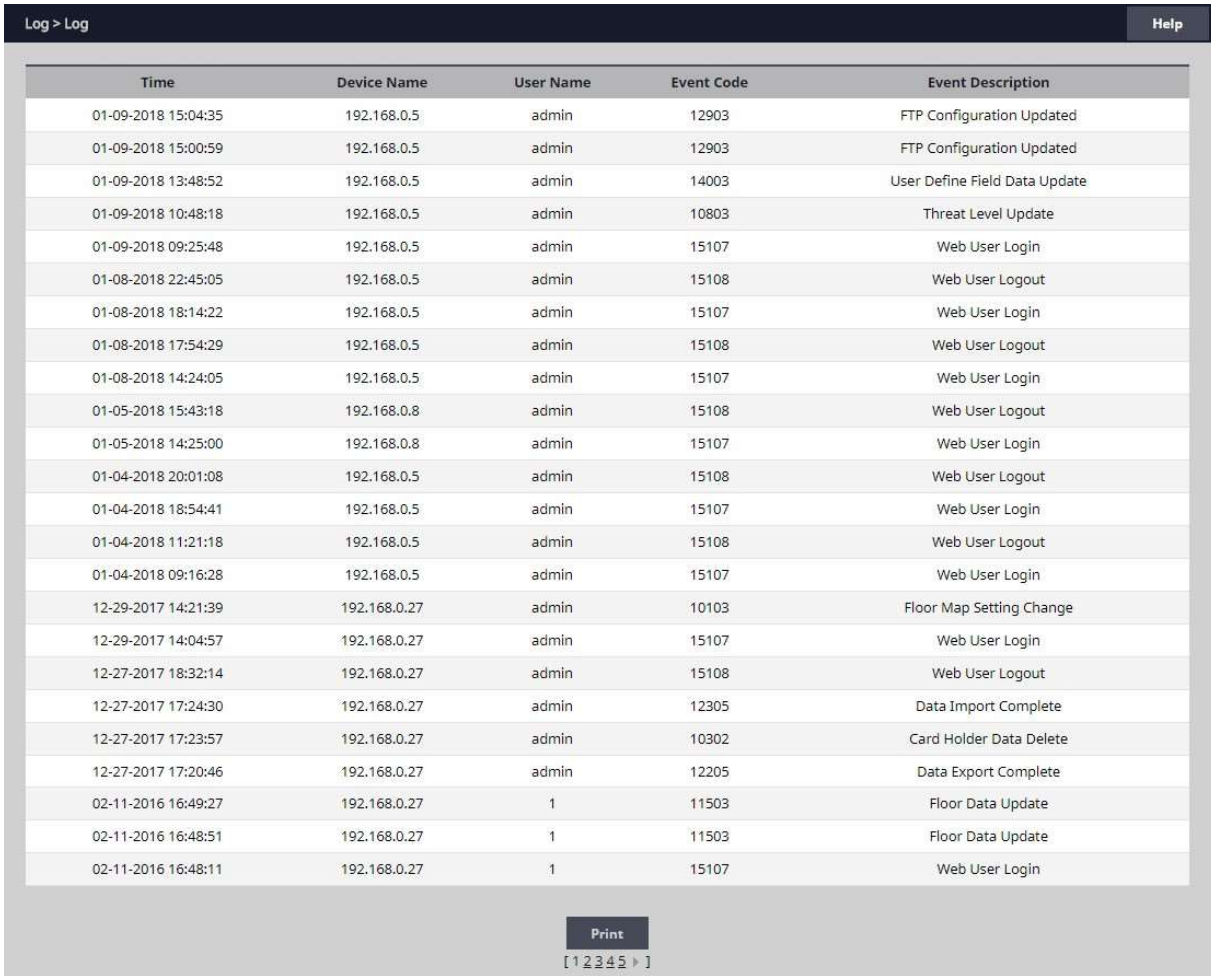
1. Click **Edit** to change or disable the Threat Level.
2. Un-check the **Turn Off Threat Level** checkbox to enable Threat Levels.
3. Use the **Threat Level** dropdown menu to select a Threat Level.
4. Click **Save**.

✓ ***NOTE:*** *When the Threat Level is Off, defined Access Level privileges and unlock schedules operate normally.*



Log

Log displays the most recent events for quick viewing.



Time	Device Name	User Name	Event Code	Event Description
01-09-2018 15:04:35	192.168.0.5	admin	12903	FTP Configuration Updated
01-09-2018 15:00:59	192.168.0.5	admin	12903	FTP Configuration Updated
01-09-2018 13:48:52	192.168.0.5	admin	14003	User Define Field Data Update
01-09-2018 10:48:18	192.168.0.5	admin	10803	Threat Level Update
01-09-2018 09:25:48	192.168.0.5	admin	15107	Web User Login
01-08-2018 22:45:05	192.168.0.5	admin	15108	Web User Logout
01-08-2018 18:14:22	192.168.0.5	admin	15107	Web User Login
01-08-2018 17:54:29	192.168.0.5	admin	15108	Web User Logout
01-08-2018 14:24:05	192.168.0.5	admin	15107	Web User Login
01-05-2018 15:43:18	192.168.0.8	admin	15108	Web User Logout
01-05-2018 14:25:00	192.168.0.8	admin	15107	Web User Login
01-04-2018 20:01:08	192.168.0.5	admin	15108	Web User Logout
01-04-2018 18:54:41	192.168.0.5	admin	15107	Web User Login
01-04-2018 11:21:18	192.168.0.5	admin	15108	Web User Logout
01-04-2018 09:16:28	192.168.0.5	admin	15107	Web User Login
12-29-2017 14:21:39	192.168.0.27	admin	10103	Floor Map Setting Change
12-29-2017 14:04:57	192.168.0.27	admin	15107	Web User Login
12-27-2017 18:32:14	192.168.0.27	admin	15108	Web User Logout
12-27-2017 17:24:30	192.168.0.27	admin	12305	Data Import Complete
12-27-2017 17:23:57	192.168.0.27	admin	10302	Card Holder Data Delete
12-27-2017 17:20:46	192.168.0.27	admin	12205	Data Export Complete
02-11-2016 16:49:27	192.168.0.27	1	11503	Floor Data Update
02-11-2016 16:48:51	192.168.0.27	1	11503	Floor Data Update
02-11-2016 16:48:11	192.168.0.27	1	15107	Web User Login

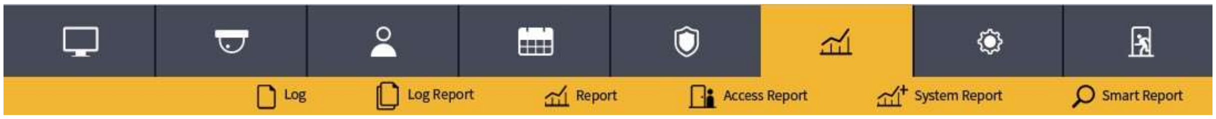
Viewing the Log

1. When **Log** is selected, the log displays on the screen.
2. Click the page number or arrows at the bottom of the screen to display other pages of the log.

Printing the Log

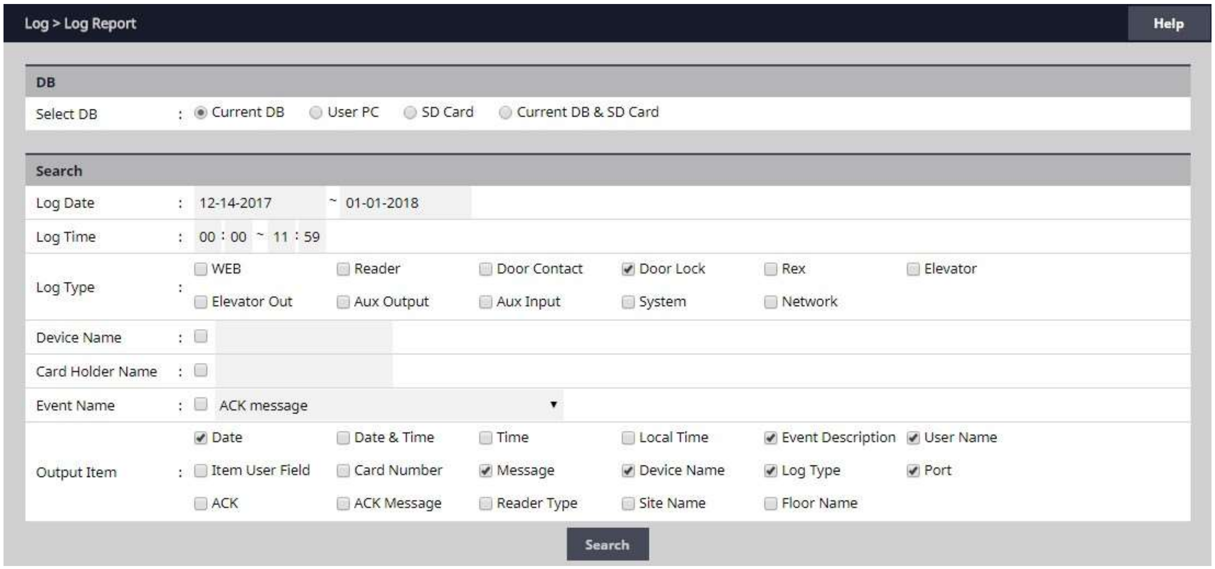
3. To print out the log, click **Print**.

Log Report



The ***Log Report*** allows the operator to create a customized report of system, network and Controller events.

Customizing the Log Report



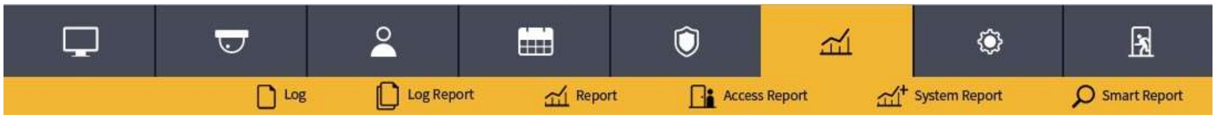
DB

Select DB	:	● Current DB ○ User PC ○ SD Card ○ Current DB & SD Card

Search

Log Date	:	12-14-2017 ~ 01-01-2018
Log Time	:	00 : 00 ~ 11 : 59
Log Type	:	□ WEB □ Reader □ Door Contact ☑ Door Lock □ Rex □ Elevator □ Elevator Out □ Aux Output □ Aux Input □ System □ Network
Device Name	:	□
Card Holder Name	:	□
Event Name	:	□ ACK message ▾
Output Item	:	☑ Date □ Date & Time □ Time □ Local Time ☑ Event Description ☑ User Name □ Item User Field □ Card Number ☑ Message ☑ Device Name ☑ Log Type ☑ Port □ ACK □ ACK Message □ Reader Type □ Site Name □ Floor Name

1. Select the database to search, either **Current DB**, **User PC**, or **SD Card**.
2. Select beginning and ending **Log Date** for the search.
3. Select the general events to search for with the **Log Type** checkboxes.
4. Search for a particular device by checking the **Device Name** checkbox and enter the device name.
5. Search for a particular Card Holder by checking the **Card Holder Name** checkbox and enter the Card Holder name.
6. Select specific system events by checking the **Event Name** checkbox and selecting the specific event in the dropdown list.
7. To create the log report, click **Search**.
8. To print the log report, click **Print**.
9. To save the log report as a text file, click **CSV**. The data will be downloaded through the browser.



Report

Report allows the operator to view and print or save a report of items in the system's memory. The report is created using Filters. Items that match the filters entered will be included in the report.

Running a Report

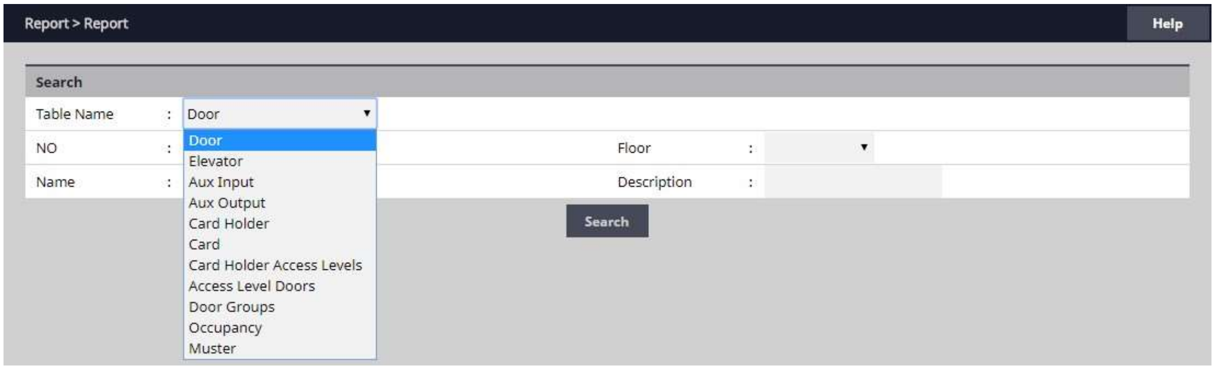


Table Name : Door

NO :

Floor :

Name :

Description :

1. Use the **Table Name** dropdown to select which area of system memory to generate a report from.

✓ ***NOTE:*** *The remaining filter options will vary depending on the Table Name selected.*

Doors, Elevators, Aux In & Out

· Select the filters for the report.

Number (NO), Floor, Name, Description Card Holder

· Select the filters for the report.

Card Holder Number (NO), Last Name, First Name, Card Number, Card Status Card

· Select the filters for the report.

Card Number, Card Status, Card Format, Card Type, Last Name, First Name, Phone Number Card Holder Access Levels

· Select the filters for the report.

Card Holder Number (NO), Last Name, First Name, Card Number, Access Level, Door Number (NO), Door Name Access Level Doors

· Select the filters for the report.

Access Level Number (NO), Access Level, Reader Number (NO), Reader Name, Door Number (NO), Door Name Door Groups

· Select the filters for the report.

Door Group Number (NO), Group Name, Access Level, Door Number (NO), Door Name Occupancy

· Select the filter for the report.

Region Muster

· Select the filter for the report.

Region

2. To generate the report, click **Search**.
3. To print the report, click **Print**.
4. To save the log report as a textfile, click **CSV**. The data will be downloaded through the browser.

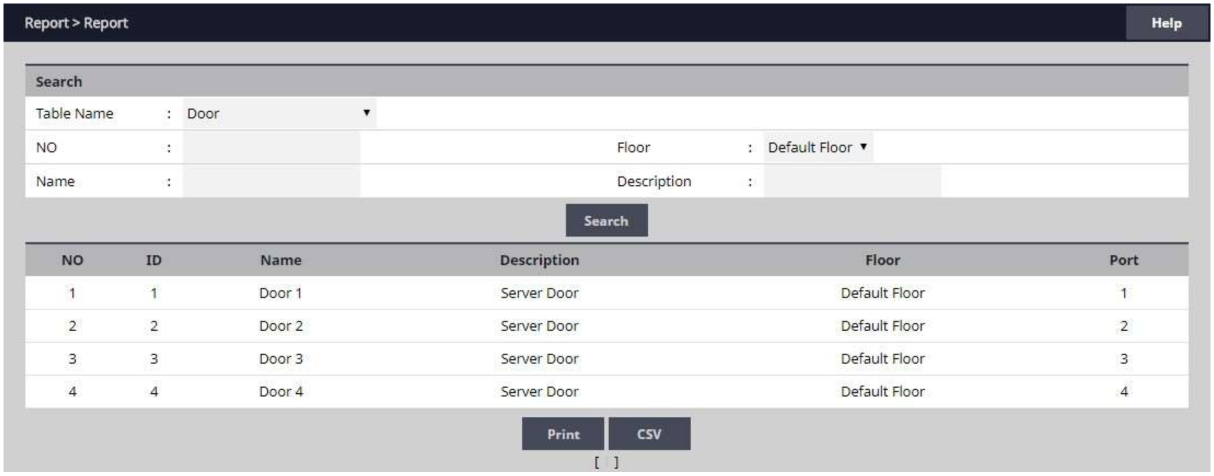


Table Name : Door

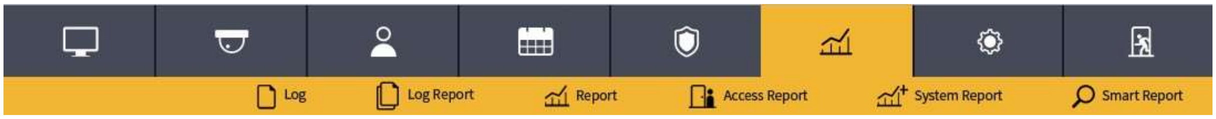
NO :

Floor : Default Floor

Name :

Description :

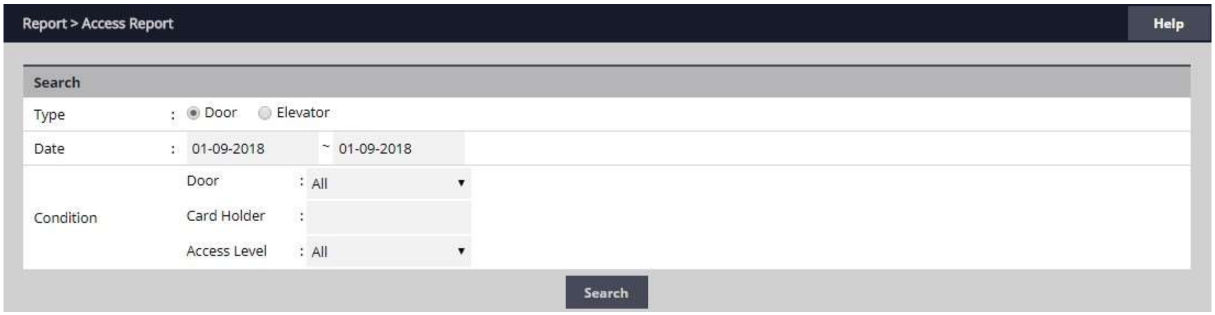
NO	ID	Name	Description	Floor	Port
1	1	Door 1	Server Door	Default Floor	1
2	2	Door 2	Server Door	Default Floor	2
3	3	Door 3	Server Door	Default Floor	3
4	4	Door 4	Server Door	Default Floor	4



Access Report

The ***Access Report*** allows the user to generate reports for all access events that occur at any door or elevator.

Running an Access Report

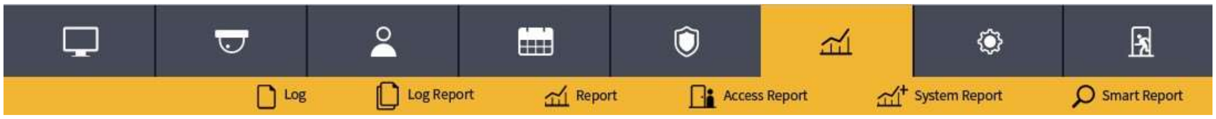


Type : ● Door ○ Elevator

Date : 01-09-2018 ~ 01-09-2018

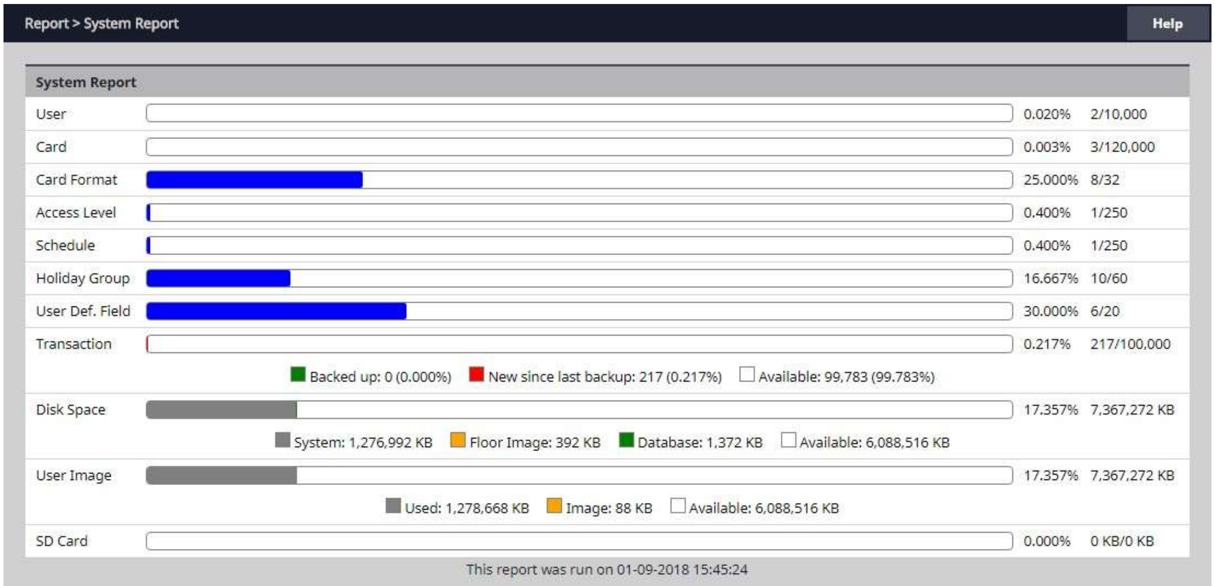
Condition
Door : All
Card Holder :
Access Level : All

1. Select **Door** or **Elevator** for the **Type** to search for.
2. Select the starting and ending date range for the search in the **Date** fields.
3. Select the **Door**, **Card Holder**, and **Access Level** to search for in the Condition fields.
4. To generate the report, click **Search**.
5. To print the report, click **Print**.
6. To export the report as a file, click **CSV**. The data will be downloaded through the browser.



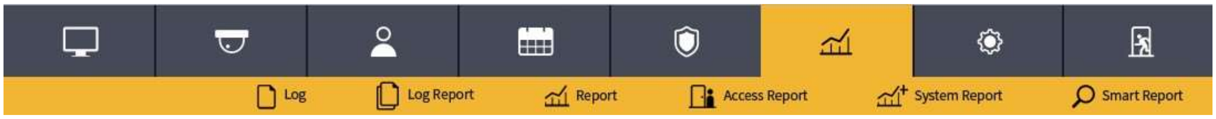
System Report

The ***System Report*** displays the current memory allocation of the database.
The report runs when System Report is selected.



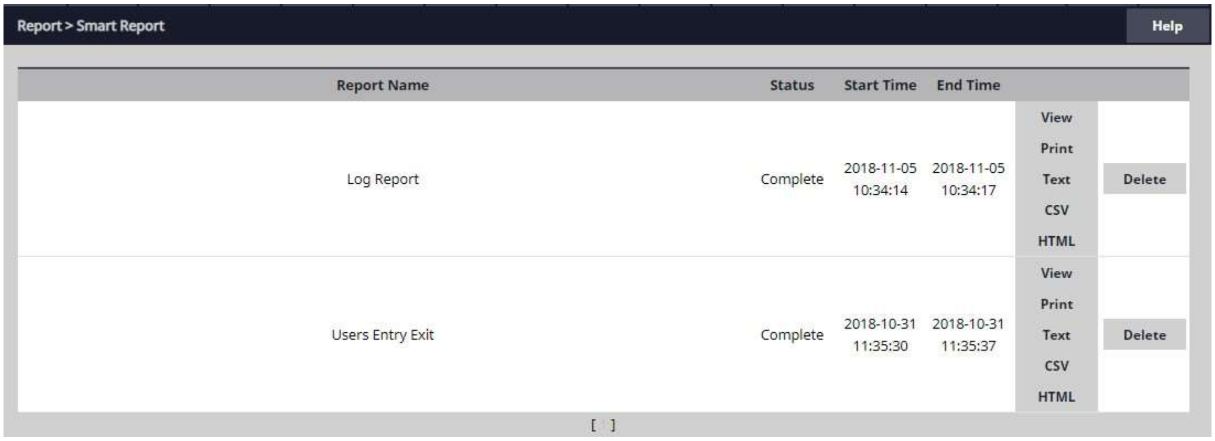
System Report			
User		0.020%	2/10,000
Card		0.003%	3/120,000
Card Format		25.000%	8/32
Access Level		0.400%	1/250
Schedule		0.400%	1/250
Holiday Group		16.667%	10/60
User Def. Field		30.000%	6/20
Transaction		0.217%	217/100,000
	🟩 Backed up: 0 (0.000%) 🟥 New since last backup: 217 (0.217%) □ Available: 99,783 (99.783%)		
Disk Space		17.357%	7,367,272 KB
	▨ System: 1,276,992 KB 🟧 Floor Image: 392 KB 🟩 Database: 1,372 KB □ Available: 6,088,516 KB		
User Image		17.357%	7,367,272 KB
	▨ Used: 1,278,668 KB 🟧 Image: 88 KB □ Available: 6,088,516 KB		
SD Card		0.000%	0 KB/0 KB

This report was run on 01-09-2018 15:45:24



Smart Report

The Smart Report option displays Smart Reports that were generated with the Smart Report Setting. Options are available for viewing, printing, and exporting the Smart Report.



Report > Smart Report

Report Name	Status	Start Time	End Time		
Log Report	Complete	2018-11-05 10:34:14	2018-11-05 10:34:17	View Print Text CSV HTML	Delete
Users Entry Exit	Complete	2018-10-31 11:35:30	2018-10-31 11:35:37	View Print Text CSV HTML	Delete

[ ]

Viewing a Smart Report

1. With the selector buttons for the desired Smart Report, click **View**.
2. A Smart Report Viewer browser window will open displaying the Smart Report.
3. Use the page numbers at the bottom to navigate to other pages of the Smart Report.

Printing a Smart Report

1. With the selector buttons for the desired Smart Report, click **Print**.
2. A Smart Report Viewer browser window will open displaying the Smart Report.
3. Click the **Print** button in the upper right corner to send the Smart Report to the system's printer.

Exporting to a Text File

1. With the selector buttons for the desired Smart Report, click **Text**.
2. The browser will prompt for saving or viewing. Select your choice.
3. A basic text file will be created.

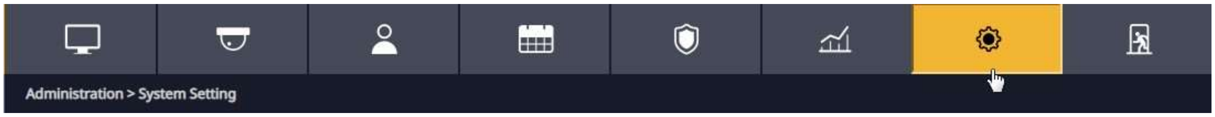
Exporting to a CSV File

1. With the selector buttons for the desired Smart Report, click **CSV**.
2. The browser will prompt for saving or viewing. Select your choice.
3. A comma separated value file for use in spreadsheets will be created.

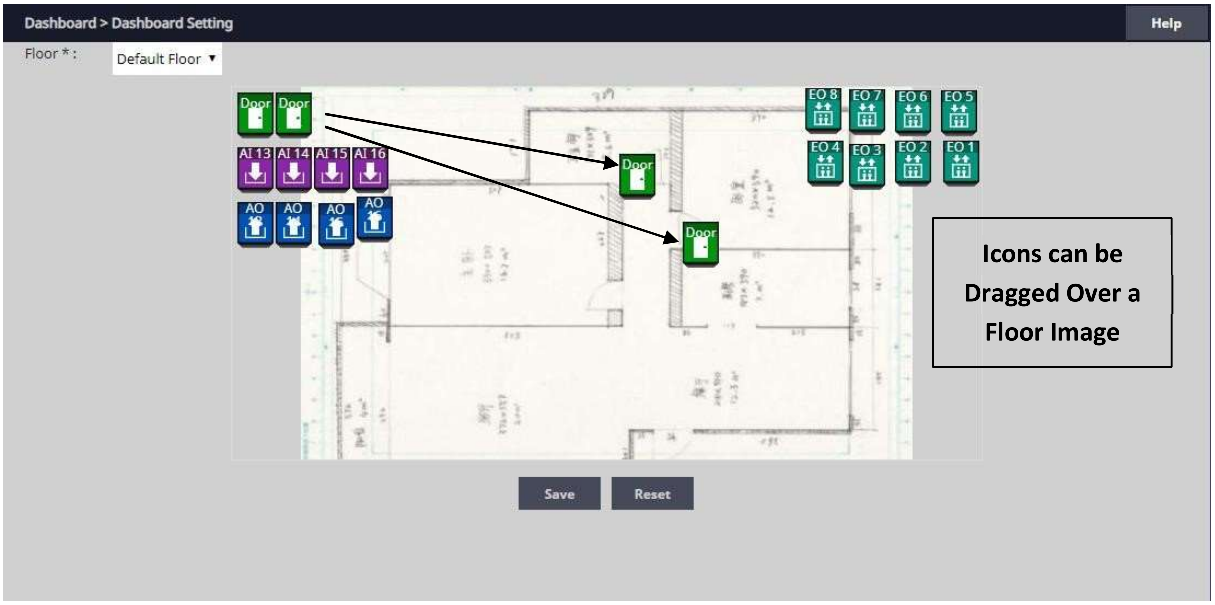
Exporting to a HTML File

1. With the selector buttons for the desired Smart Report, click **HTML**.
2. The browser will prompt for saving or viewing. Select your choice.
3. An HTML file for viewing in a browser will be created.

Dashboard Setting



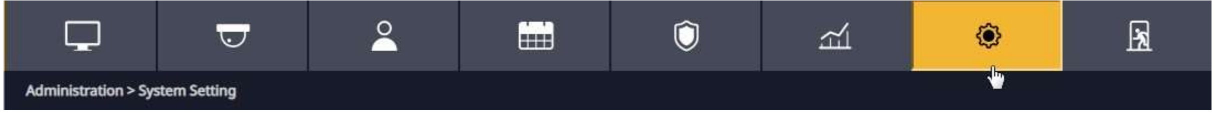
The ***Dashboard Setting*** dialog provides default icons for each door, input and output. Customize the visual layout of the system by dragging the icons to the floor image (see ***Floor Setting*** to add an image of the floor).



Floor * : Default Floor

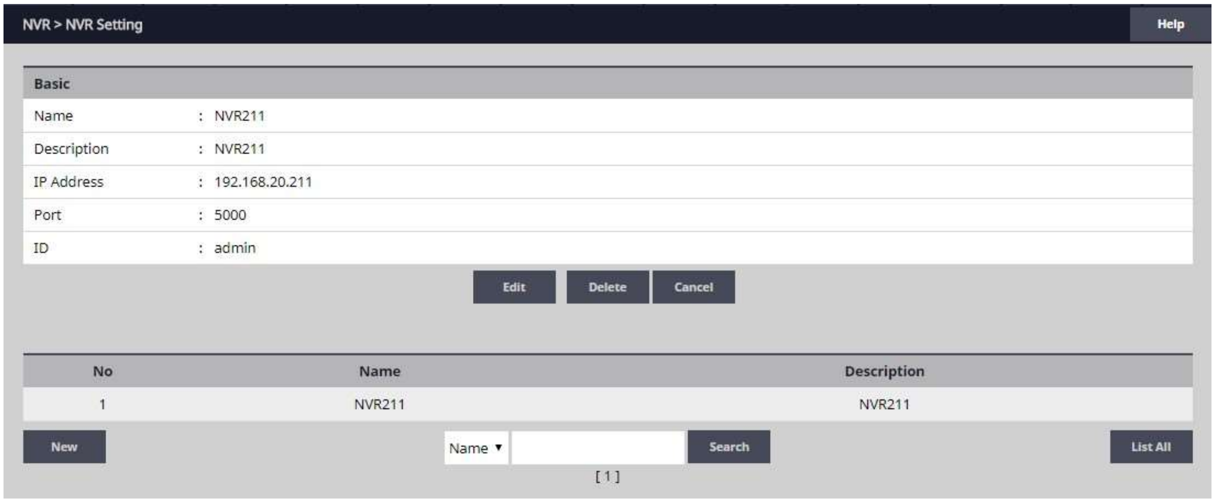
Icons can be Dragged Over a Floor Image

NVR Setting



Optional Feature

NVR Setting allows configuration of network video recorders.



NVR > NVR Setting

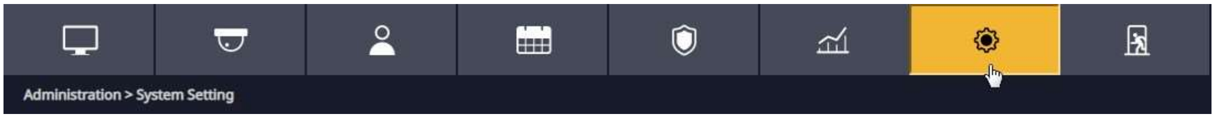
Basic

Name	:	NVR211
Description	:	NVR211
IP Address	:	192.168.20.211
Port	:	5000
ID	:	admin

No	Name	Description
1	NVR211	NVR211

Adding a NVR

1. Click **New** and enter the information for the NVR.
2. Click **Add**.

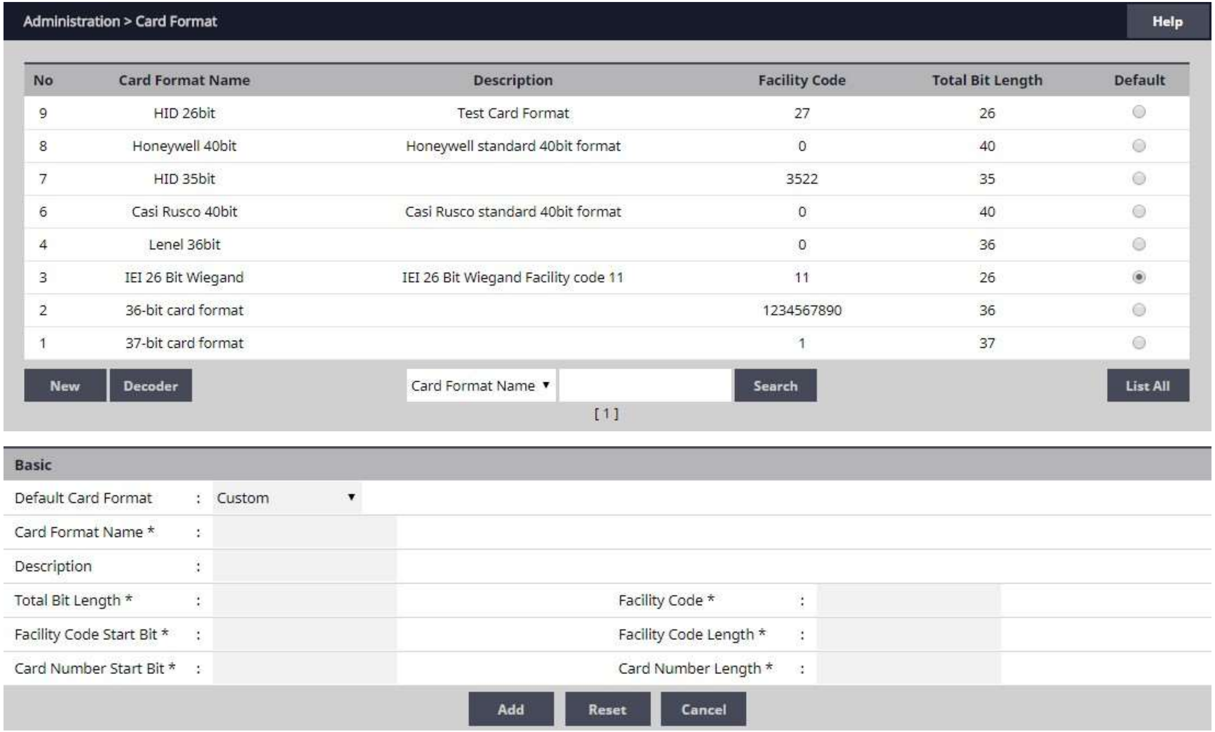


Administration > System Setting

Card Format

Card Format displays the default card formats of the system. The system has several pre-configured card formats. If the desired card format is not listed, a custom format may be added.

Adding a Card Format



Administration > Card Format

No	Card Format Name	Description	Facility Code	Total Bit Length	Default
9	HID 26bit	Test Card Format	27	26	○
8	Honeywell 40bit	Honeywell standard 40bit format	0	40	○
7	HID 35bit		3522	35	○
6	Casi Rusco 40bit	Casi Rusco standard 40bit format	0	40	○
4	Lenel 36bit		0	36	○
3	IEI 26 Bit Wiegand	IEI 26 Bit Wiegand Facility code 11	11	26	●
2	36-bit card format		1234567890	36	○
1	37-bit card format		1	37	○

Basic

Default Card Format :	Custom ▾		
Card Format Name * :			
Description :			
Total Bit Length * :		Facility Code * :	
Facility Code Start Bit * :		Facility Code Length * :	
Card Number Start Bit * :		Card Number Length * :	

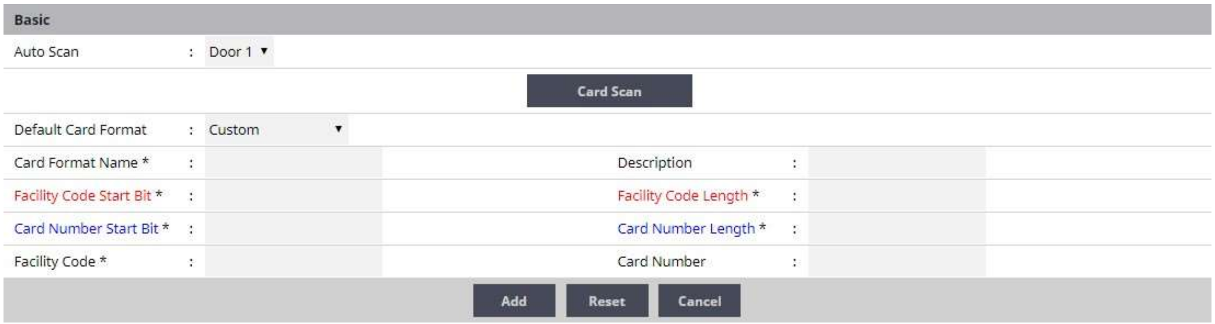
1. Click **New**.
2. Enter a name and description (optional) for the card format.
3. Enter the facility code bit/length, card number bit/length and parity information as provided by the card manufacturer.
4. Click **Add** to save the changes.

✓ ***NOTE:*** *It is recommended to delete card formats that are not in use.*

Using the Decoder

If the desired card format is not listed as a default format, the Decoder can be utilized to auto scan and detect the card format.

1. Click **Decoder**.

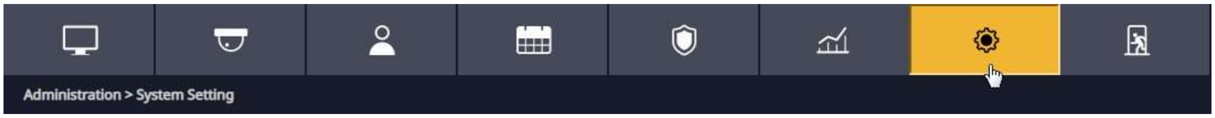


Basic

Auto Scan	: Door 1 ▾		
Default Card Format	: Custom ▾		
Card Format Name *	:	Description	:
Facility Code Start Bit *	:	Facility Code Length *	:
Card Number Start Bit *	:	Card Number Length *	:
Facility Code *	:	Card Number	:

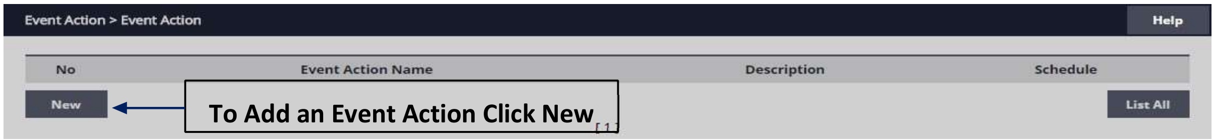
2. Select the door where the card will be auto scanned.
3. Click **Card Scan** and present the card (or multiple cards) to the reader.
4. The new card format will populate the data fields.
5. Click **Add** to save the new format.

✓ ***NOTE:*** *The decoder takes a "best guess" based on existing card formats. Without knowledge of the card's start bits and length, it cannot guarantee proper decoding.*

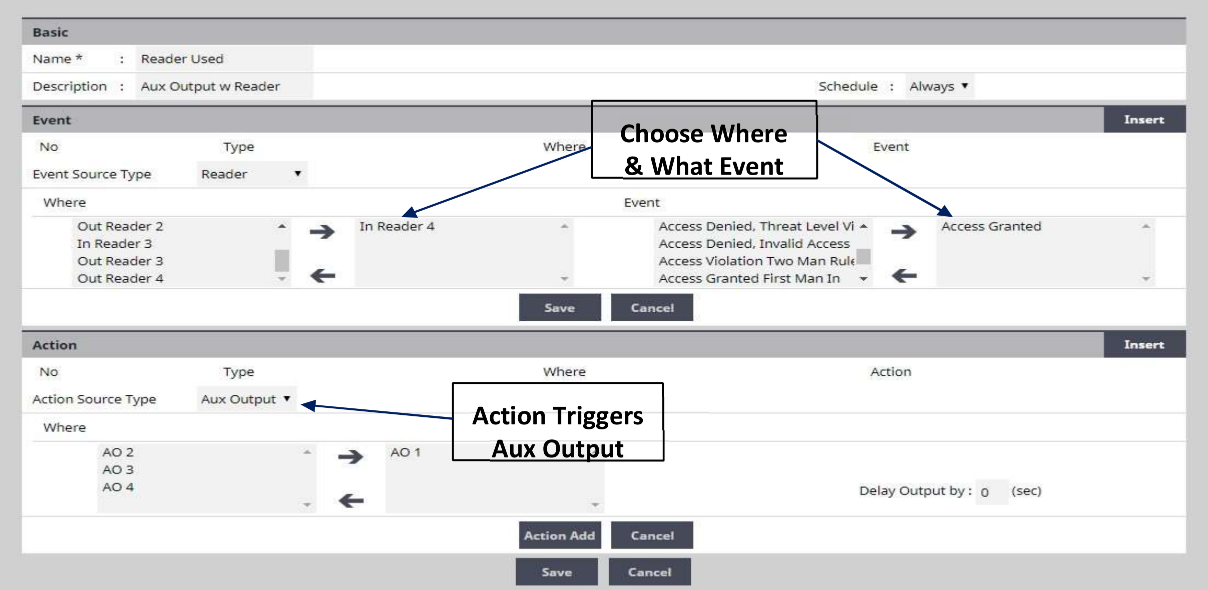


Event Action

Event Action allows the operator to create events that are assigned to actions. For example, the operator may assign a time schedule to an auxiliary output.



To Add an Event Action Click New



Name * : Reader Used

Description : Aux Output w Reader

Schedule : Always ▾

Event Source Type Reader ▾

Where: Out Reader 2, In Reader 3, Out Reader 3, Out Reader 4 → In Reader 4

Event: Access Denied, Threat Level Vi, Access Denied, Invalid Access, Access Violation Two Man Rule, Access Granted First Man In → Access Granted

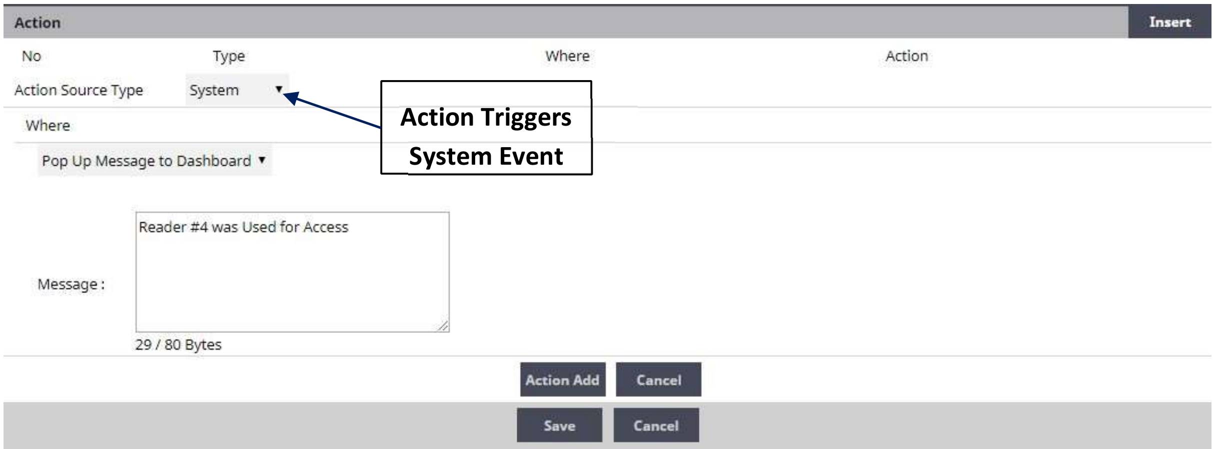
Choose Where & What Event

Action Source Type Aux Output ▾

Where: AO 2, AO 3, AO 4 → AO 1

Delay Output by : 0 (sec)

Action Triggers Aux Output



Action Source Type System ▾

Where

Pop Up Message to Dashboard ▾

Message : Reader #4 was Used for Access

29 / 80 Bytes

Action Triggers System Event

Adding an Event Action

1. Click **New** and enter a name and description.

2. In the **Basic** section, name the event, fill in a **Description**, and select a **Schedule** for the time the Event Action will be active.

Event

3. In the **Event** section, click **Insert** to add a new event.

4. Choose the type of equipment that can trigger the event action in the **Event Source Type** dropdown.

5. Under **Where**, choose the event source location(s) by selecting the location(s) and clicking the right arrow to move it to the field on the right.

6. Under **Event**, choose the event(s) to monitor by selecting the event(s) and clicking the right arrow to move it to the field on the right. This is the event(s) that will ***trigger*** the action.

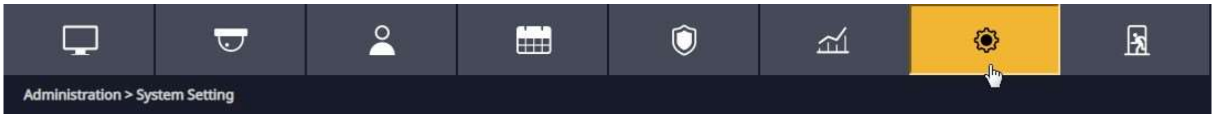
Action

7. In the **Action** section, click Insert.

8. Choose either **Aux Output** or **System** for the **Action Source Type. Aux Output**

· This is the auxiliary relay(s) that will respond to the event. Select them and move it to the right by clicking the right arrow. **System**

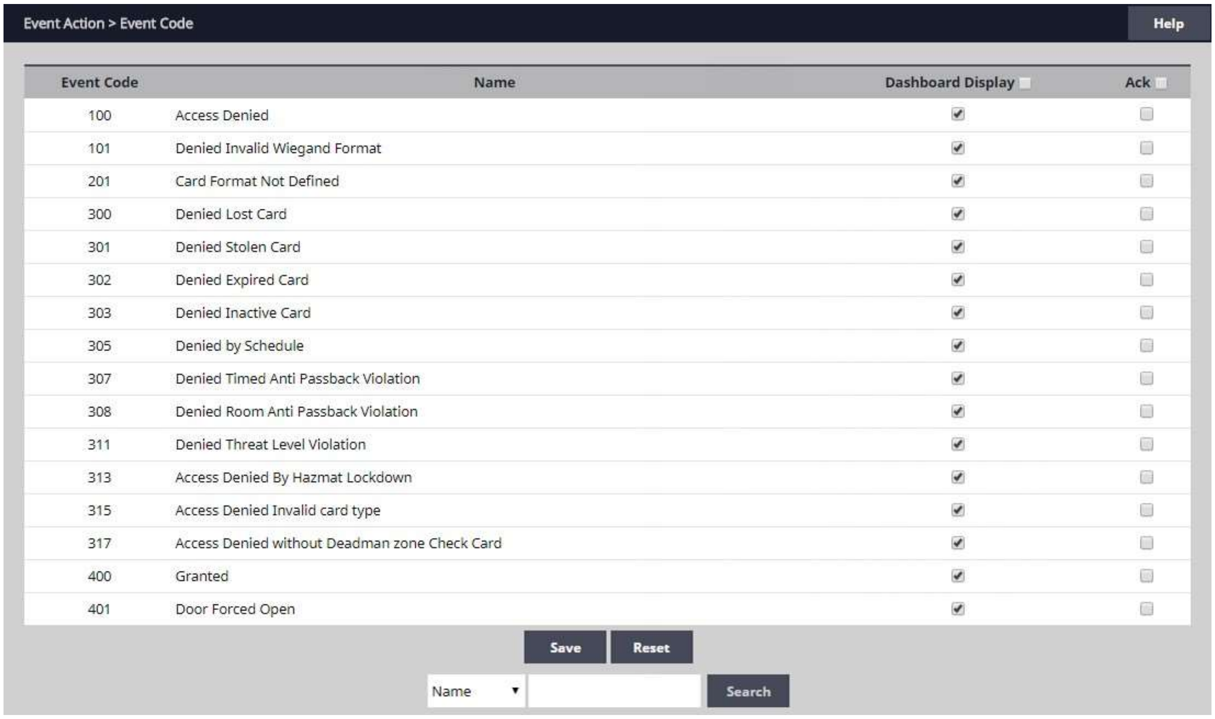
· These are various messages and operations that the system can perform if the Event Action triggers. ✓
NOTE: *To have the system send an e-mail for an event, use the* ***Where*** *dropdown and select* ***Send E-Mail.***
9. Click **Action Save** and **Save** in each section to save the settings.



Event Code

Event Code lists the events that are available to the operator. The user can configure the event to display in the Dashboard and/or require the operator to acknowledge the event.

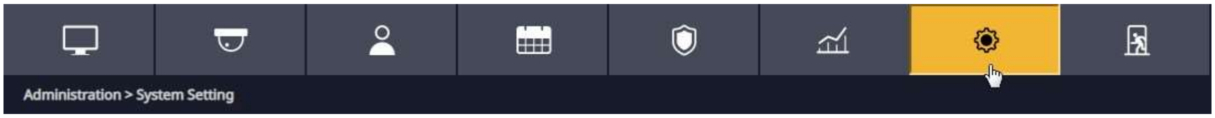
Selecting Event Codes



Event Code	Name	Dashboard Display ☐	Ack ☐
100	Access Denied	☑	☐
101	Denied Invalid Wiegand Format	☑	☐
201	Card Format Not Defined	☑	☐
300	Denied Lost Card	☑	☐
301	Denied Stolen Card	☑	☐
302	Denied Expired Card	☑	☐
303	Denied Inactive Card	☑	☐
305	Denied by Schedule	☑	☐
307	Denied Timed Anti Passback Violation	☑	☐
308	Denied Room Anti Passback Violation	☑	☐
311	Denied Threat Level Violation	☑	☐
313	Access Denied By Hazmat Lockdown	☑	☐
315	Access Denied Invalid card type	☑	☐
317	Access Denied without Deadman zone Check Card	☑	☐
400	Granted	☑	☐
401	Door Forced Open	☑	☐

1. On the **Event Code** list, edit the check boxes for the events codes that will display on the dashboard if they occur.
2. On the **Event Code** list, edit the checkboxes for the events codes that will require operator acknowledgment if they occur.

Use the **Search** button to find specific event codes or event code names.

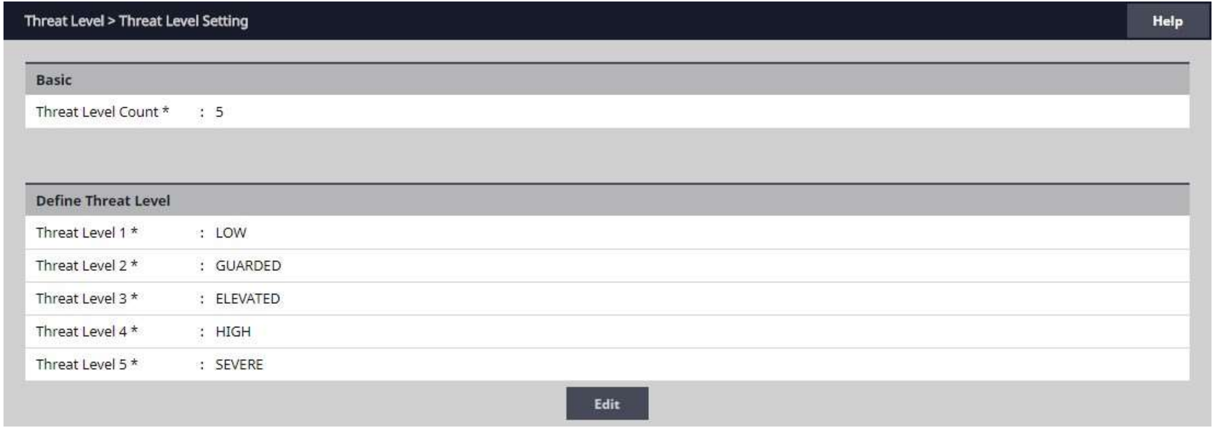


Threat Level Setting

Optional Feature

There is a three tier hierarchy of Threat Levels to consider when configuring an system. First the ***System*** Threat Level, second the ***Door*** Threat Level and third the ***Card Holder*** Threat Level. See the Door and Card Holder sections for details on setting the Door and Card Holder Threat Levels.

System Threat Level Setup

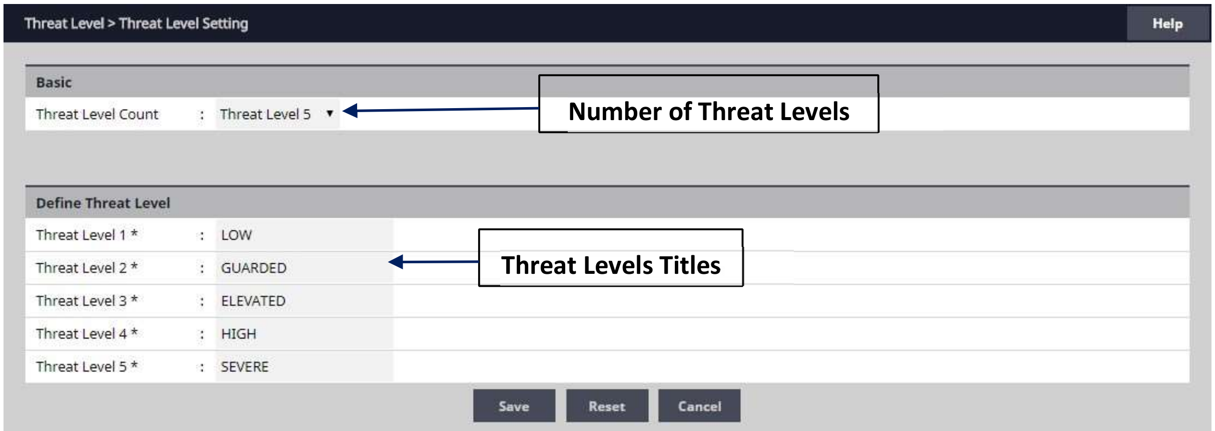


Basic

Threat Level Count * : 5

Define Threat Level

Threat Level 1 *	LOW
Threat Level 2 *	GUARDED
Threat Level 3 *	ELEVATED
Threat Level 4 *	HIGH
Threat Level 5 *	SEVERE



Basic

Threat Level Count : Threat Level 5 ▾

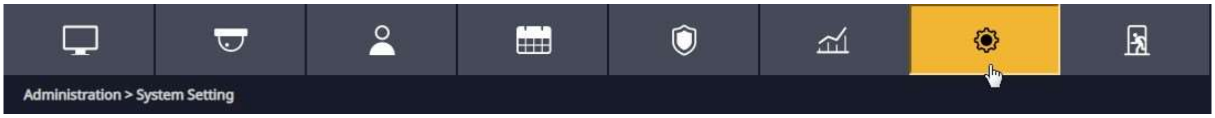
Number of Threat Levels

Define Threat Level

Threat Level 1 *	LOW
Threat Level 2 *	GUARDED
Threat Level 3 *	ELEVATED
Threat Level 4 *	HIGH
Threat Level 5 *	SEVERE

Threat Levels Titles

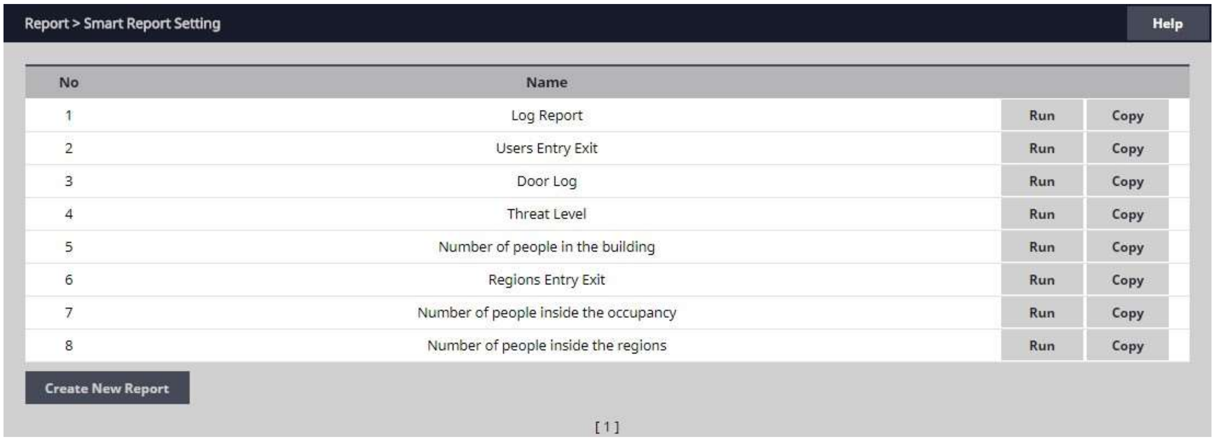
1. Click **Edit** to change the number or title of the Threat Levels.
2. Select the number of Threat Levels available for the system with the **Threat Level Count** dropdown. Up to 25 Threat Levels can be defined.
3. The titles of each Threat Level can be customized to suit the installation.
4. Click **Save** when finished.



Smart Report Setting

Smart Report Setting is a function that allows creating and saving custom designed system reports with interactive features. Each element of the report can be customized to suit the installation or management of the installation.

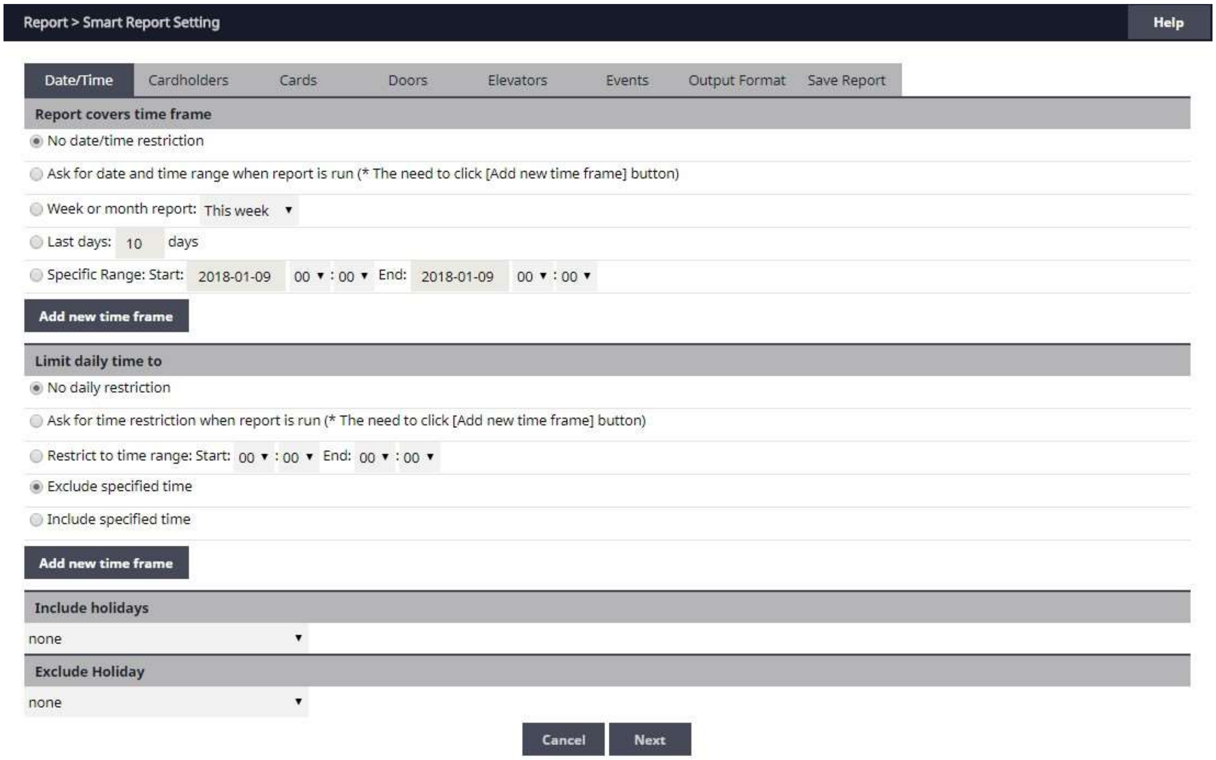
Creating a Smart Report



No	Name		
1	Log Report	Run	Copy
2	Users Entry Exit	Run	Copy
3	Door Log	Run	Copy
4	Threat Level	Run	Copy
5	Number of people in the building	Run	Copy
6	Regions Entry Exit	Run	Copy
7	Number of people inside the occupancy	Run	Copy
8	Number of people inside the regions	Run	Copy

1. Click **Create New Report** to begin setting up a smart report template.

Date / Time



Report > Smart Report Setting

Report covers time frame

● No date/time restriction

○ Ask for date and time range when report is run (* The need to click [Add new time frame] button)

○ Week or month report: This week ▾

○ Last days: 10 days

○ Specific Range: Start: 2018-01-09 00 ▾ : 00 ▾ End: 2018-01-09 00 ▾ : 00 ▾

Limit daily time to

● No daily restriction

○ Ask for time restriction when report is run (* The need to click [Add new time frame] button)

○ Restrict to time range: Start: 00 ▾ : 00 ▾ End: 00 ▾ : 00 ▾

● Exclude specified time

○ Include specified time

Include holidays

none ▾

Exclude Holiday

none ▾

Report Covers Time Frame

· Select one of the time frame options, enter any variable data, then click **Add New Time Frame** to add the filter to the Smart Report.

Limit Daily Time To

· Select one of the daily time limit options, enter any variable data, choose to include or exclude these times, then click Add New Time Frame to add the filter to the Smart Report.

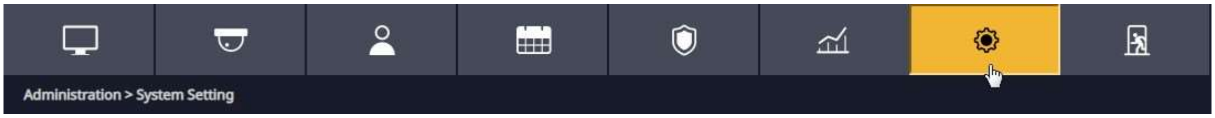
Include Holidays

· Choose holidays to include in the report with the dropdown selector.

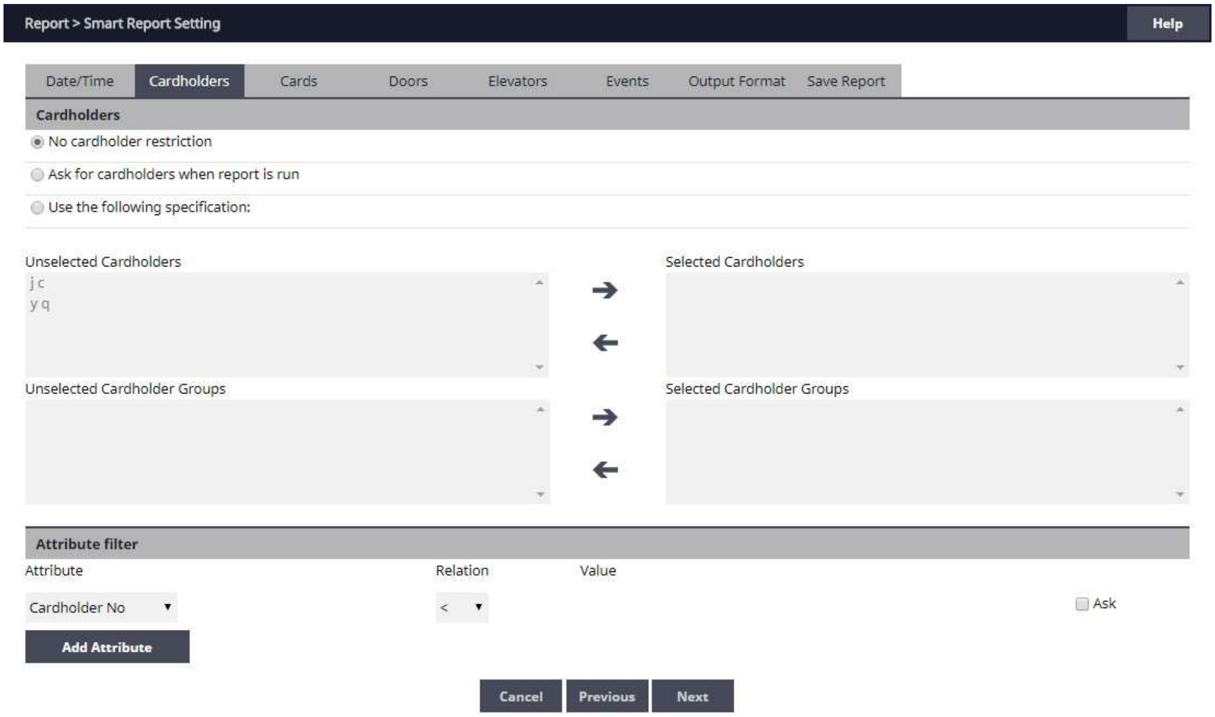
Exclude Holidays

· Choose holidays to exclude in the report with the dropdown selector.

2. Click **Next** to setup the Card Holder filter.



Cardholders



Report > Smart Report Setting

Cardholders

● No cardholder restriction

○ Ask for cardholders when report is run

○ Use the following specification:

Unselected Cardholders		Selected Cardholders
j c y q	→ ←	

Unselected Cardholder Groups		Selected Cardholder Groups
	→ ←	

Attribute filter

Attribute	Relation	Value	
Cardholder No ▾	< ▾		□ Ask

Cardholder Filters

· Select one of the Card Holder filter options for no restriction, ask when report is run, or use manual Card Holder selection with Card Holders or Card Holder groups.

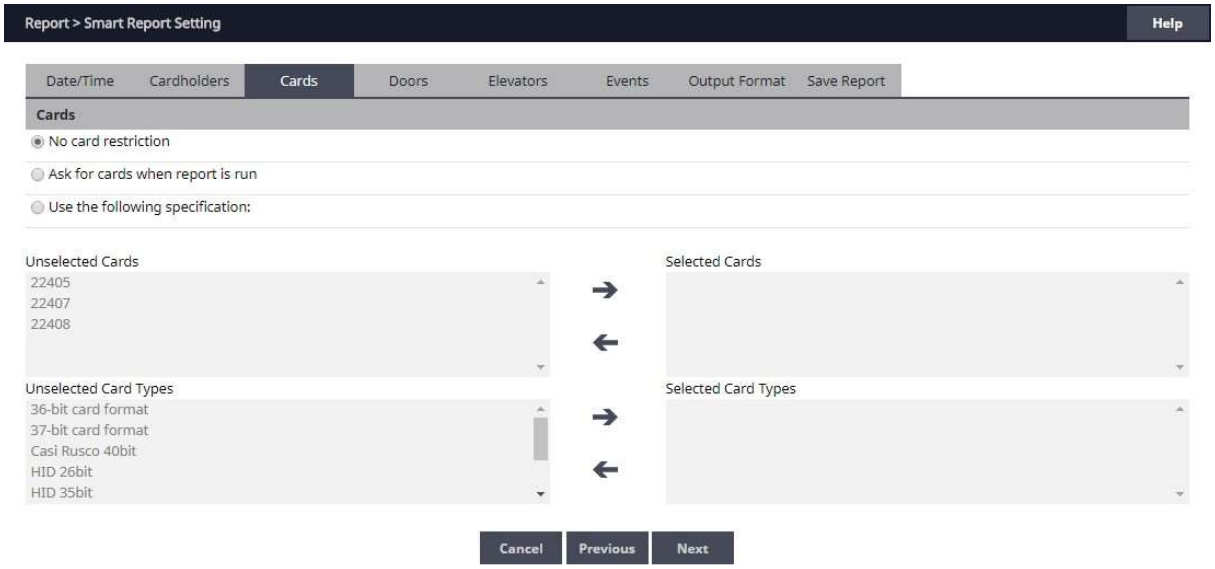
Attribute Filter

· Select a Card Holder **Attribute**, then choose a logical **Relation** and **Value** for the filter. Check the Ask checkbox for a prompt at run time.

· Click **Add Attribute** to add the filter to the Smart Report.

3. Click **Next** to setup the Card filter.

Cards



Cards

● No card restriction

○ Ask for cards when report is run

○ Use the following specification:

Unselected Cards: 22405, 22407, 22408

Selected Cards:

Unselected Card Types: 36-bit card format, 37-bit card format, Casi Rusco 40bit, HID 26bit, HID 35bit

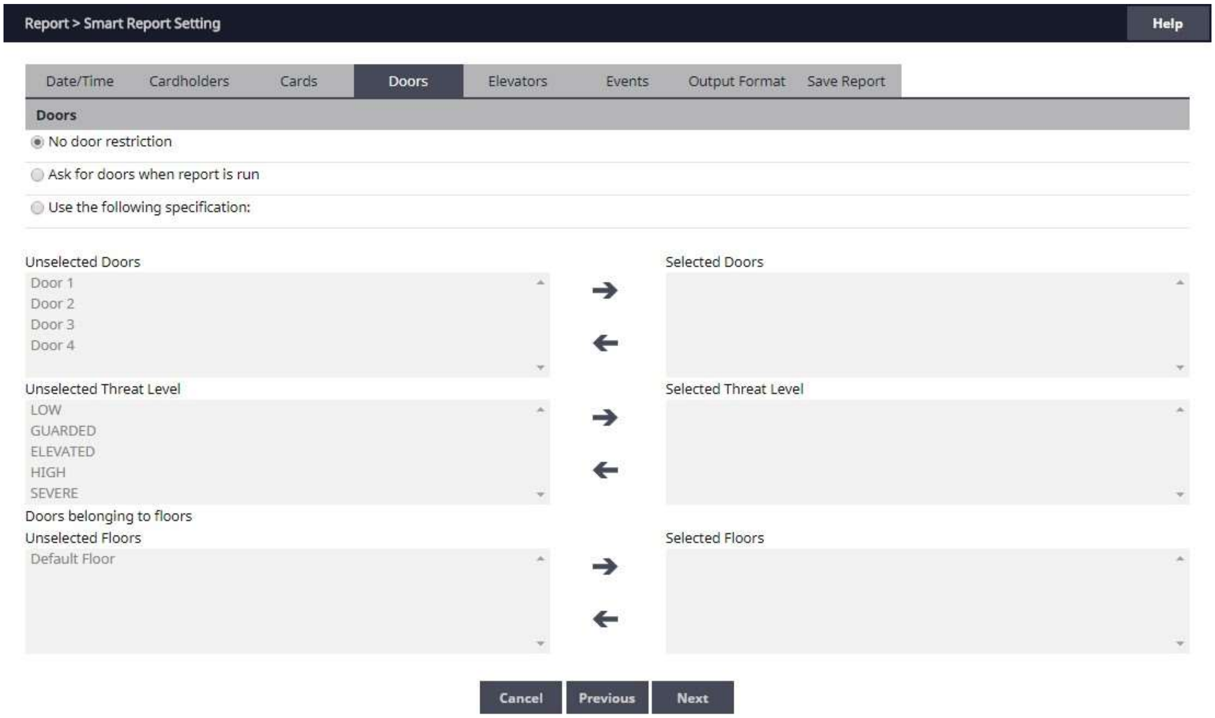
Selected Card Types:

Card Filters

· Select one of the Card Holder Filter options for no restriction, ask when report is run, or use manual Card Holder selection with cards or card types.

4. Click **Next** to setup the Doors filter.

Doors



Doors

● No door restriction

○ Ask for doors when report is run

○ Use the following specification:

Unselected Doors: Door 1, Door 2, Door 3, Door 4

Selected Doors:

Unselected Threat Level: LOW, GUARDED, ELEVATED, HIGH, SEVERE

Selected Threat Level:

Doors belonging to floors

Unselected Floors: Default Floor

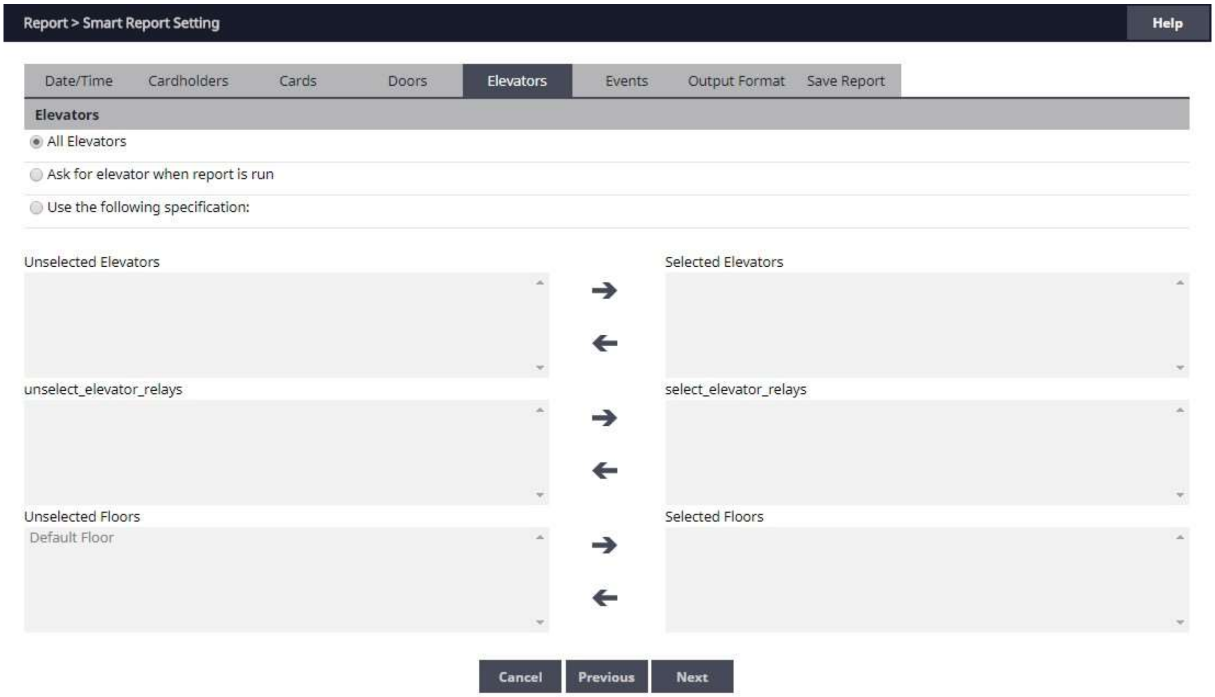
Selected Floors:

Door Filters

· Select one of the door filter options for no restriction, ask when report is run, or use manual door selection, Threat Level selection, or doors on selected floors.

5. Click **Next** to setup the Elevators filters.

Elevators



Report > Smart Report Setting

Elevators

● All Elevators

○ Ask for elevator when report is run

○ Use the following specification:

Unselected Elevators

Selected Elevators

unselect_elevator_relays

select_elevator_relays

Unselected Floors

Default Floor

Selected Floors

Elevator Filters

· Select one of the elevator filter options for all elevators, ask when report is run, or use manual elevator selection, elevator relays, or elevators on selected floors.

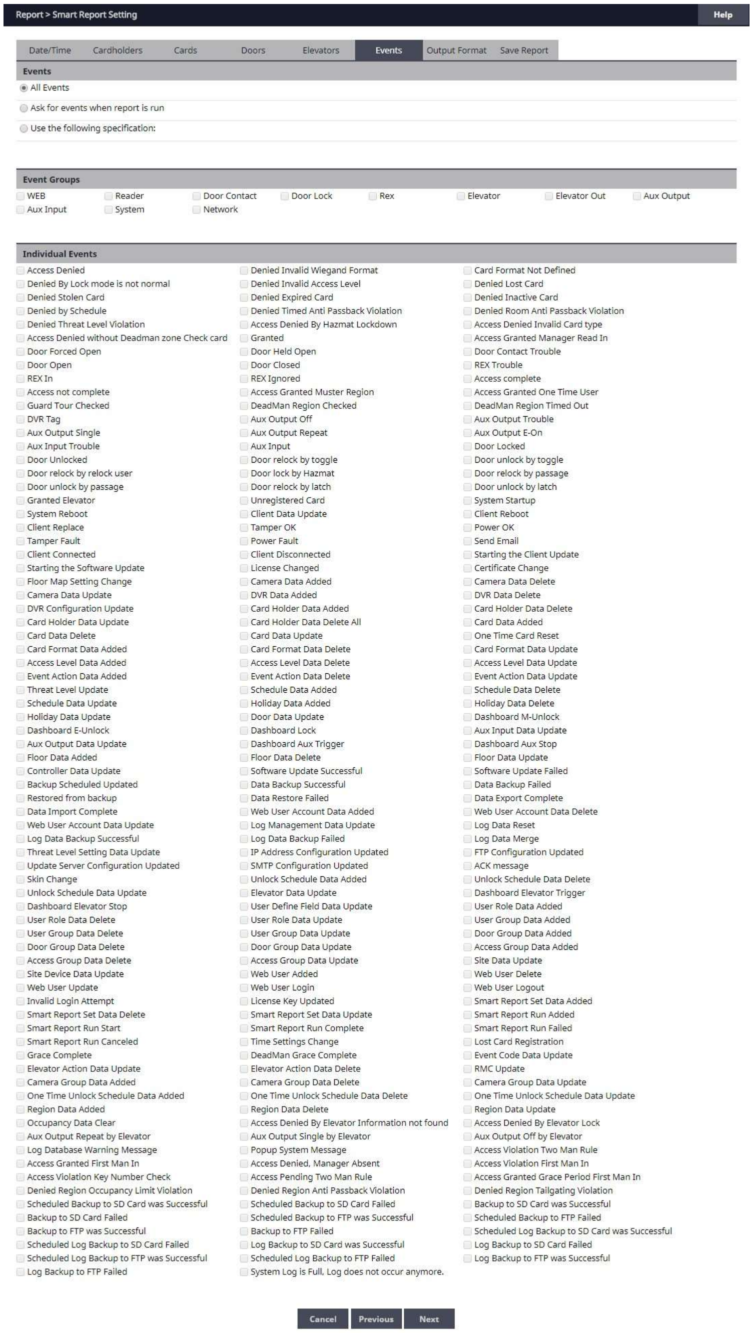
6. Click Next to setup the Events filters.

Events Event Filters

·Select one of the event filter options for all events, ask when report is run, or use the event filter checkboxes. **Event Groups** · Use the checkboxes to select Event Group filters for the Smart Report.

Individual Events · Use the checkboxes to select Individual Event filters for the Smart Report.

7. Click **Next** to setup the Output Format for the Smart Report.



Events

● All Events

○ Ask for events when report is run

○ Use the following specification:

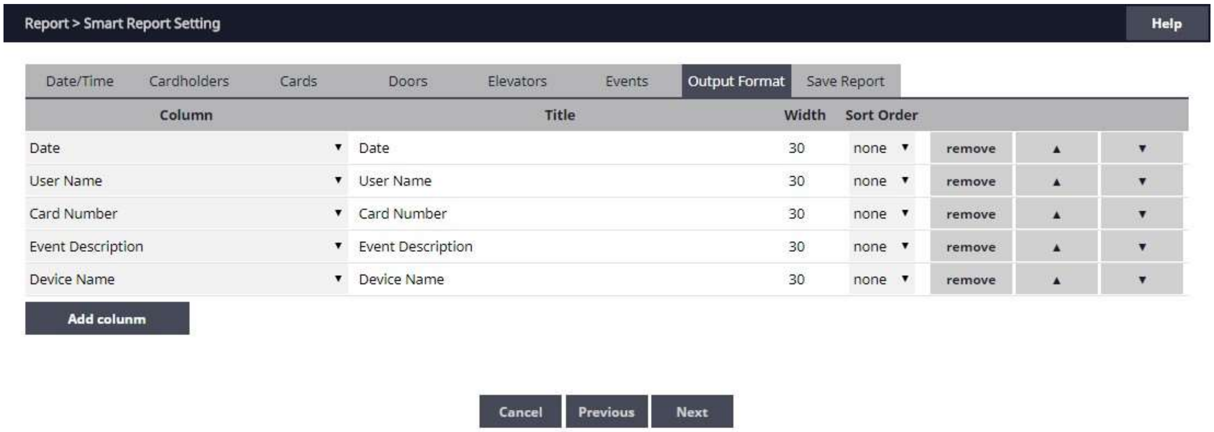
Event Groups

☐ WEB	☐ Reader	☐ Door Contact	☐ Door Lock	☐ Rex	☐ Elevator	☐ Elevator Out	☐ Aux Output
☐ Aux Input	☐ System	☐ Network					

Individual Events

☐ Access Denied	☐ Denied Invalid Wiegand Format	☐ Card Format Not Defined
☐ Denied By Lock mode is not normal	☐ Denied Invalid Access Level	☐ Denied Lost Card
☐ Denied Stolen Card	☐ Denied Expired Card	☐ Denied Inactive Card
☐ Denied by Schedule	☐ Denied Timed Anti Passback Violation	☐ Denied Room Anti Passback Violation
☐ Denied Threat Level Violation	☐ Access Denied By Hazmat Lockdown	☐ Access Denied Invalid Card type
☐ Access Denied without Deadman zone Check card	☐ Granted	☐ Access Granted Manager Read In
☐ Door Forced Open	☐ Door Held Open	☐ Door Contact Trouble
☐ Door Open	☐ Door Closed	☐ REX Trouble
☐ REX In	☐ REX Ignored	☐ Access complete
☐ Access not complete	☐ Access Granted Muster Region	☐ Access Granted One Time User
☐ Guard Tour Checked	☐ DeadMan Region Checked	☐ DeadMan Region Timed Out
☐ DVR Tag	☐ Aux Output Off	☐ Aux Output Trouble
☐ Aux Output Single	☐ Aux Output Repeat	☐ Aux Output E-On
☐ Aux Input Trouble	☐ Aux Input	☐ Door Locked
☐ Door Unlocked	☐ Door relock by toggle	☐ Door unlock by toggle
☐ Door relock by relock user	☐ Door lock by Hazmat	☐ Door relock by passage
☐ Door unlock by passage	☐ Door relock by latch	☐ Door unlock by latch
☐ Granted Elevator	☐ Unregistered Card	☐ System Startup
☐ System Reboot	☐ Client Data Update	☐ Client Reboot
☐ Client Replace	☐ Tamper OK	☐ Power OK
☐ Tamper Fault	☐ Power Fault	☐ Send Email
☐ Client Connected	☐ Client Disconnected	☐ Starting the Client Update
☐ Starting the Software Update	☐ License Changed	☐ Certificate Change
☐ Floor Map Setting Change	☐ Camera Data Added	☐ Camera Data Delete
☐ Camera Data Update	☐ DVR Data Added	☐ DVR Data Delete
☐ DVR Configuration Update	☐ Card Holder Data Added	☐ Card Holder Data Delete
☐ Card Holder Data Update	☐ Card Holder Data Delete All	☐ Card Data Added
☐ Card Data Delete	☐ Card Data Update	☐ One Time Card Reset
☐ Card Format Data Added	☐ Card Format Data Delete	☐ Card Format Data Update
☐ Access Level Data Added	☐ Access Level Data Delete	☐ Access Level Data Update
☐ Event Action Data Added	☐ Event Action Data Delete	☐ Event Action Data Update
☐ Threat Level Update	☐ Schedule Data Added	☐ Schedule Data Delete
☐ Schedule Data Update	☐ Holiday Data Added	☐ Holiday Data Delete
☐ Holiday Data Update	☐ Door Data Update	☐ Dashboard M-Unlock
☐ Dashboard E-Unlock	☐ Dashboard Lock	☐ Aux Input Data Update
☐ Aux Output Data Update	☐ Dashboard Aux Trigger	☐ Dashboard Aux Stop
☐ Floor Data Added	☐ Floor Data Delete	☐ Floor Data Update
☐ Controller Data Update	☐ Software Update Successful	☐ Software Update Failed
☐ Backup Scheduled Updated	☐ Data Backup Successful	☐ Data Backup Failed
☐ Restored from backup	☐ Data Restore Failed	☐ Data Export Complete
☐ Data Import Complete	☐ Web User Account Data Added	☐ Web User Account Data Delete
☐ Web User Account Data Update	☐ Log Management Data Update	☐ Log Data Reset
☐ Log Data Backup Successful	☐ Log Data Backup Failed	☐ Log Data Merge
☐ Threat Level Setting Data Update	☐ IP Address Configuration Updated	☐ FTP Configuration Updated
☐ Update Server Configuration Updated	☐ SMTP Configuration Updated	☐ ACK message
☐ Skin Change	☐ Unlock Schedule Data Added	☐ Unlock Schedule Data Delete
☐ Unlock Schedule Data Update	☐ Elevator Data Update	☐ Dashboard Elevator Trigger
☐ Dashboard Elevator Stop	☐ User Define Field Data Update	☐ User Role Data Added
☐ User Role Data Delete	☐ User Role Data Update	☐ User Group Data Added
☐ User Group Data Delete	☐ User Group Data Update	☐ Door Group Data Added
☐ Door Group Data Delete	☐ Door Group Data Update	☐ Access Group Data Added
☐ Access Group Data Delete	☐ Access Group Data Update	☐ Site Data Update
☐ Site Device Data Update	☐ Web User Added	☐ Web User Delete
☐ Web User Update	☐ Web User Login	☐ Web User Logout
☐ Invalid Login Attempt	☐ License Key Updated	☐ Smart Report Set Data Added
☐ Smart Report Set Data Delete	☐ Smart Report Set Data Update	☐ Smart Report Run Added
☐ Smart Report Run Start	☐ Smart Report Run Complete	☐ Smart Report Run Failed
☐ Smart Report Run Canceled	☐ Time Settings Change	☐ Lost Card Registration
☐ Grace Complete	☐ DeadMan Grace Complete	☐ Event Code Data Update
☐ Elevator Action Data Update	☐ Elevator Action Data Delete	☐ RMC Update
☐ Camera Group Data Added	☐ Camera Group Data Delete	☐ Camera Group Data Update
☐ One Time Unlock Schedule Data Added	☐ One Time Unlock Schedule Data Delete	☐ One Time Unlock Schedule Data Update
☐ Region Data Added	☐ Region Data Delete	☐ Region Data Update
☐ Occupancy Data Clear	☐ Access Denied By Elevator Information not found	☐ Access Denied By Elevator Lock
☐ Aux Output Repeat by Elevator	☐ Aux Output Single by Elevator	☐ Aux Output Off by Elevator
☐ Log Database Warning Message	☐ Popup System Message	☐ Access Violation Two Man Rule
☐ Access Granted First Man In	☐ Access Denied, Manager Absent	☐ Access Violation First Man In
☐ Access Violation Key Number Check	☐ Access Pending Two Man Rule	☐ Access Granted Grace Period First Man In
☐ Denied Region Occupancy Limit Violation	☐ Denied Region Anti Passback Violation	☐ Denied Region Tailgating Violation
☐ Scheduled Backup to SD Card was Successful	☐ Scheduled Backup to SD Card Failed	☐ Backup to SD Card was Successful
☐ Backup to SD Card Failed	☐ Scheduled Backup to FTP was Successful	☐ Scheduled Backup to FTP Failed
☐ Backup to FTP was Successful	☐ Backup to FTP Failed	☐ Scheduled Log Backup to SD Card was Successful
☐ Scheduled Log Backup to SD Card Failed	☐ Log Backup to SD Card was Successful	☐ Log Backup to SD Card Failed
☐ Scheduled Log Backup to FTP was Successful	☐ Scheduled Log Backup to FTP Failed	☐ Log Backup to FTP was Successful
☐ Log Backup to FTP Failed	☐ System Log is Full, Log does not occur anymore.	

Output Format



Column	Title	Width	Sort Order
Date ▾	Date	30	none ▾
User Name ▾	User Name	30	none ▾
Card Number ▾	Card Number	30	none ▾
Event Description ▾	Event Description	30	none ▾
Device Name ▾	Device Name	30	none ▾

The Output Format settings control the resulting look of a Smart Report when it is run. The columns, column titles, column widths and sort orders can be customized and saved for a Smart Report.

8. For each column of the Smart Report, choose the column details.

Column

· Use the dropdown selectors to choose the data field to place in the column.

Title

· Enter the title to place above the column.

Width

· Choose the number of characters wide for the column. **Sort**

Order

·Select a number for the sort order, the lower the number, the higher output will be in the sort results (or select None for no sort priority for the column).

Column Order

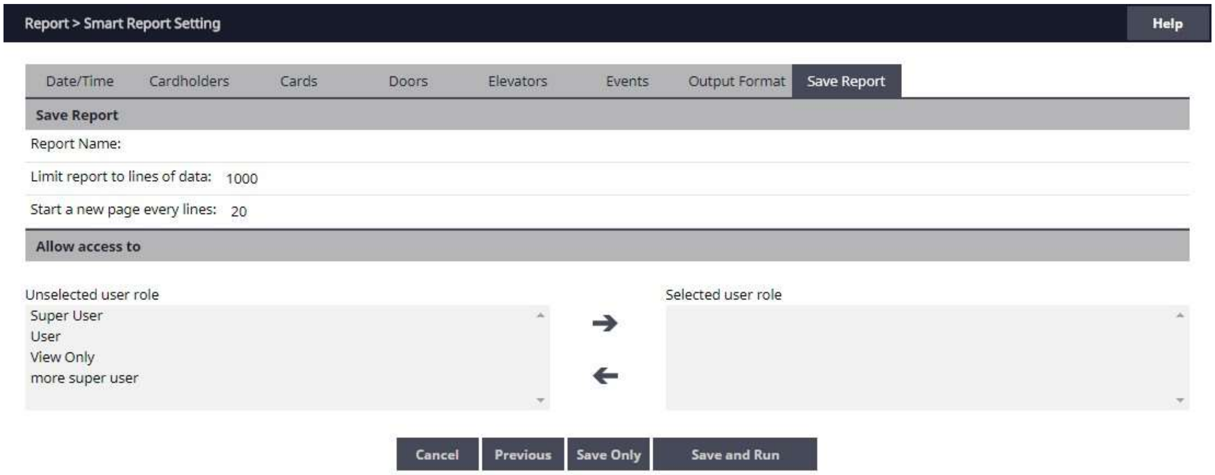
· Use the arrow buttons to rearrange the column order of the Smart Report.

· Click **Remove** to delete a column from the Smart Report.

9. Click **Add Column** to add a column to the Output Format configuration window.

10. Click Next to finish setting up the Smart Report.

Save Report



Save Report

Report Name:

Limit report to lines of data: 1000

Start a new page every lines: 20

Allow access to

Unselected user role

Super User
User
View Only
more super user

Selected user role

Saving the report saves all the filter and column options from the other Smart Report Setting tabs.

Save Report

· Enter a Report Name for the customized Smart Report.

· Enter the maximum number of lines to limit the report length.

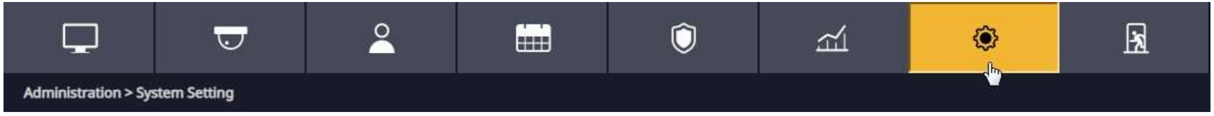
· Enter the number of lines allowed for each page of the report. A form feed will occur when this line count is reached.

Allow Access To

·Choose which User Roles will be allowed to run the Smart Report.

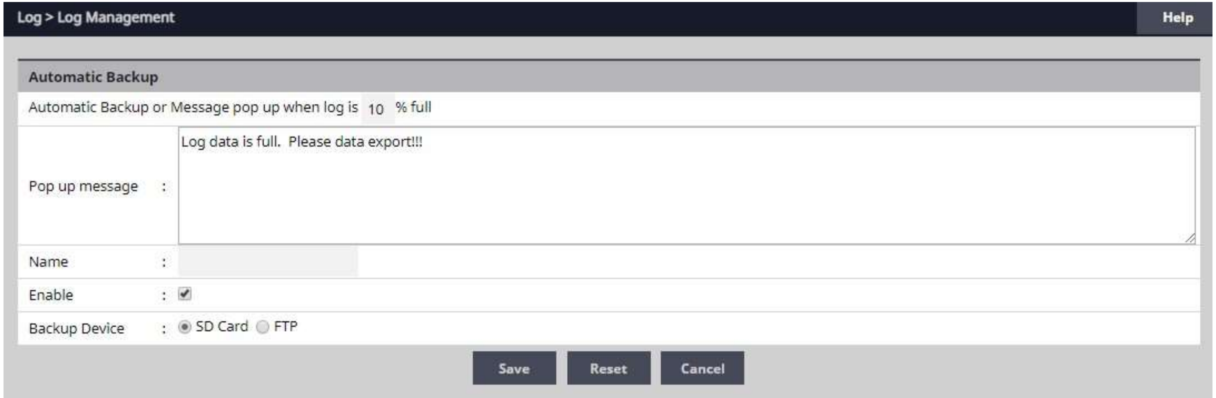
11. Select **Save Only** to save the customized Smart Report without running the report. Select **Save and Run** to save the customized Smart Report and run the report.

Log Management



Log Management allows the operator to create a backup of all log events. The backup can be scheduled and directed to the
SD card on the Controller or an FTP location. The backup can also be manually generated to a CSV or DB file.

Automatic Log Backup



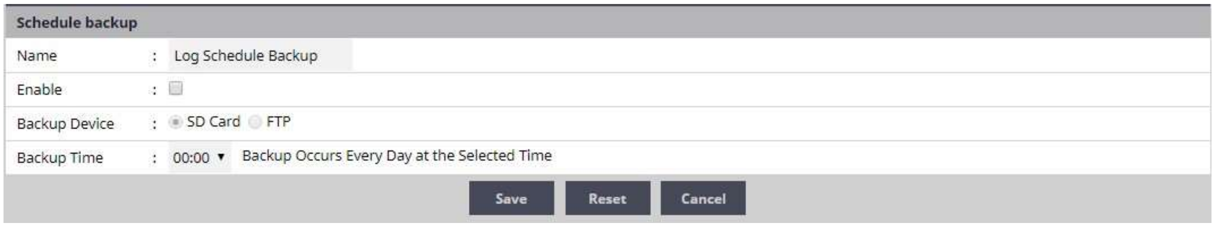
Automatic Backup

Automatic Backup or Message pop up when log is 10 % full

Pop up message :	Log data is full. Please data export!!!
Name :	
Enable :	☑
Backup Device :	● SD Card ○ FTP

1. Enter the percentage of log fullness to trigger a pop up message or automatic log backup.
2. The message displayed can be edited in the **Pop Up Message** field.
3. Enter a name for the backup in the **Name** field.
4. To enable the automatic log backup check the **Enable** checkbox.
5. Select either **SD Card** or **FTP** for the **Backup Device**.
6. Click **Save**.

Schedule Log Backup



Schedule backup

Name :	Log Schedule Backup
Enable :	□
Backup Device :	● SD Card ○ FTP
Backup Time :	00:00 ▾ Backup Occurs Every Day at the Selected Time

1. Enter a name for the backup in the **Name** field.
2. To enable the scheduled log backup check the **Enable** checkbox.
3. Select either **SD Card** or **FTP** for the **Backup Device**.
4. Select the daily time for the scheduled log backup from the **Backup Time** dropdown.

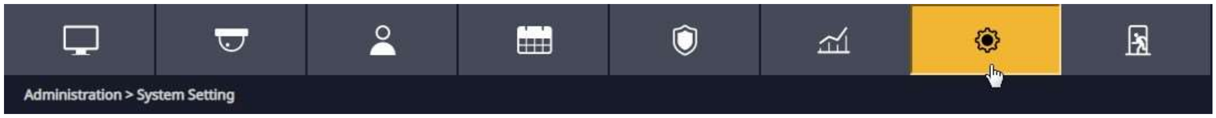
Log Reset

1. To delete all log data in memory, click **Reset**
2. Enter an administrator password to confirm the log reset.
3. Click **OK**.

Manual Log Backup

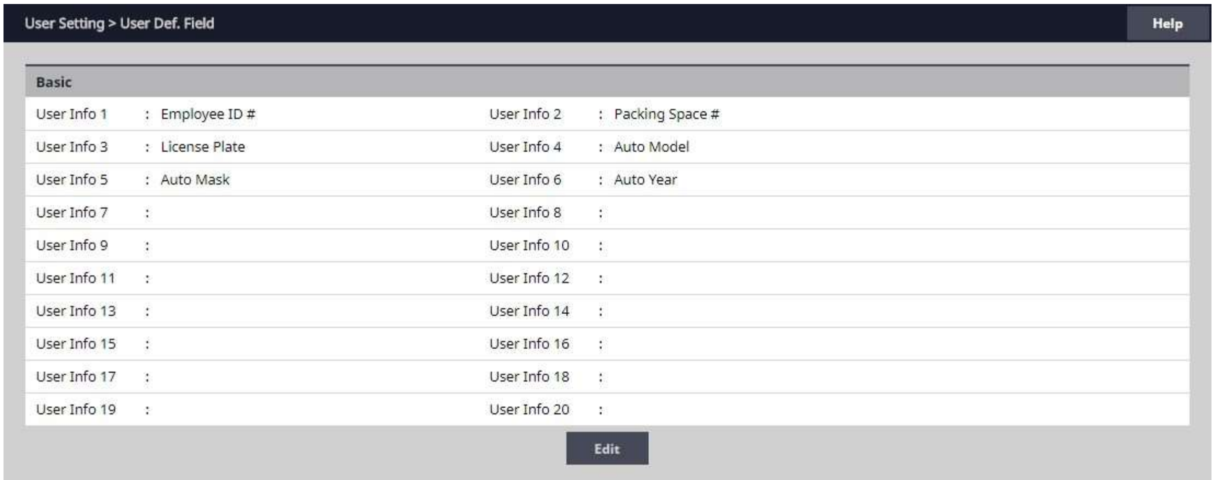
1. Select the backup type, either **CSV** or **Database** format. Click **Backup**.

User Defined Field



Administration > System Setting

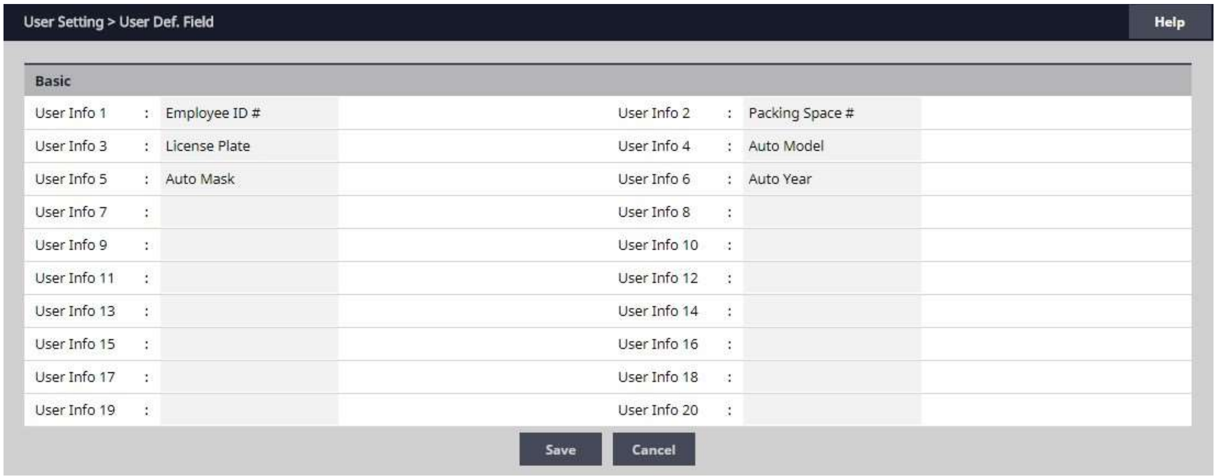
User Defined Fields are 20 custom data fields that can be assigned to a Card Holder profile. This field can be used for employee ID or other specific information unique to a Card Holder.



User Setting > User Def. Field

Basic

User Info 1	: Employee ID #	User Info 2	: Packing Space #
User Info 3	: License Plate	User Info 4	: Auto Model
User Info 5	: Auto Mask	User Info 6	: Auto Year
User Info 7	:	User Info 8	:
User Info 9	:	User Info 10	:
User Info 11	:	User Info 12	:
User Info 13	:	User Info 14	:
User Info 15	:	User Info 16	:
User Info 17	:	User Info 18	:
User Info 19	:	User Info 20	:



User Setting > User Def. Field

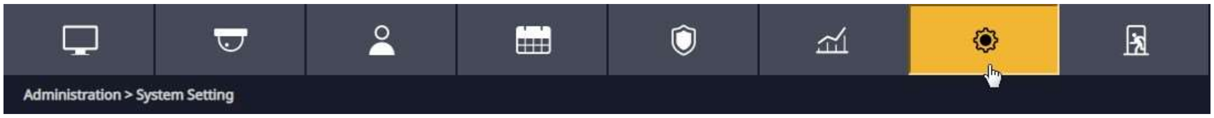
Basic

User Info 1	: Employee ID #	User Info 2	: Packing Space #
User Info 3	: License Plate	User Info 4	: Auto Model
User Info 5	: Auto Mask	User Info 6	: Auto Year
User Info 7	:	User Info 8	:
User Info 9	:	User Info 10	:
User Info 11	:	User Info 12	:
User Info 13	:	User Info 14	:
User Info 15	:	User Info 16	:
User Info 17	:	User Info 18	:
User Info 19	:	User Info 20	:

Editing User Defined Fields

1. Click **Edit** to enter user defined fields.
2. Enter any custom data in the 20 **User Info** fields.
3. Click **Save** when finished.

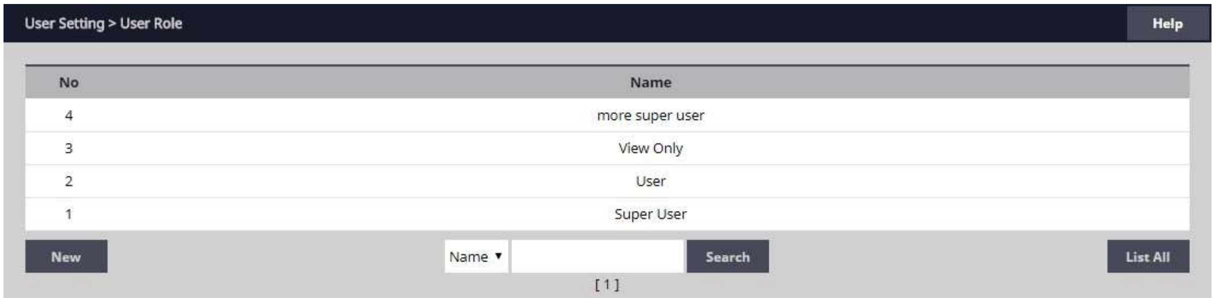
User Role



Administration > System Setting

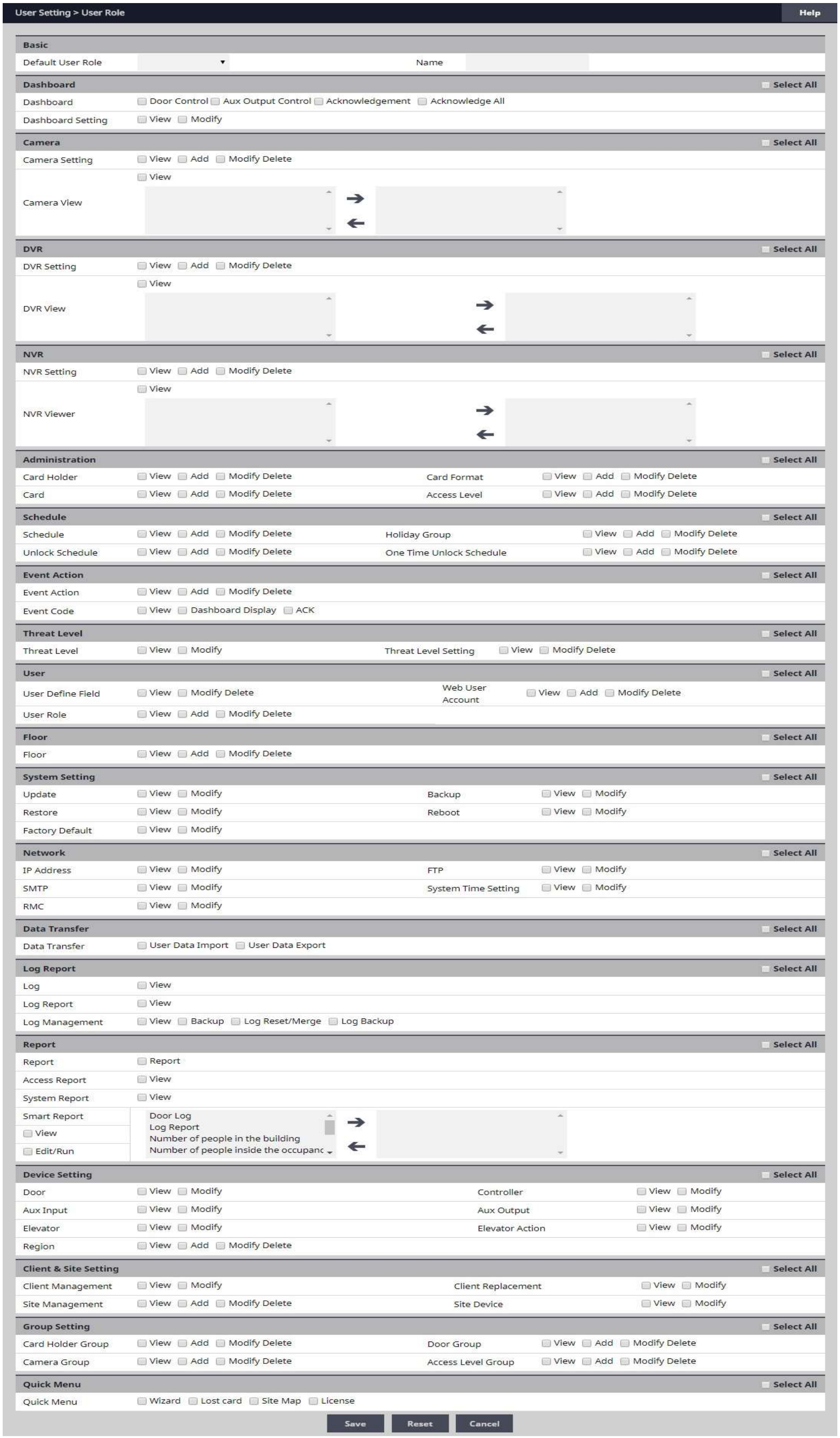
User Roles define the access privilege of the operators. A ***User ID*** is assigned to each person who will work with the Controller. Each ***User ID*** can be configured to have different system privileges. System privileges determine the options the user has available in the Controller browser interface.

Setting User Roles



No	Name
4	more super user
3	View Only
2	User
1	Super User

1. Select the user role to edit and click **Edit**.
2. Enter the options and name for the **Basic** settings.
3. Select the **Dashboard** options that will be available for the user.
4. Select the **Camera** options that will be available for the user.
5. Select the **DVR** options that will be available for the user.
6. Select the N**VR** options that will be available for the user.
7. Select the **Administration** options that will be available for the user.
8. Select the **Schedule** options that will be available for the user.
9. Select the **Event Action** options that will be available for the user.
10. Select the **Threat Level** options that will be available for the user.
11. Select the **User** options that will be available for the user.
12. Select the **Floor** options that will be available for the user.
13. Select the **System Setting** options that will be available for the user.
14. Select the **Network** options that will be available for the user.
15. Select the **Data Transfer** options that will be available for the user.
16. Select the **Log Report** options that will be available for the user.
17. Select the **Report** options that will be available for the user。
18. Select the **Device Setting** options that will be available for the user.
19. Select the **Client & Site Setting** options that will be available for the user.
20. Select the **Group Setting** options that will be available for the user.
21. Select the **Quick Menu** options that will be available for the user.
22. Click **Save**.



User Setting > User Role

Help

Basic

Default User Role	▾	Name	

Dashboard □ Select All

Dashboard	□ Door Control □ Aux Output Control □ Acknowledgement □ Acknowledge All
Dashboard Setting	□ View □ Modify

Camera □ Select All

Camera Setting	□ View □ Add □ Modify Delete
Camera View	□ View

DVR □ Select All

DVR Setting	□ View □ Add □ Modify Delete
DVR View	□ View

NVR □ Select All

NVR Setting	□ View □ Add □ Modify Delete
NVR Viewer	□ View

Administration □ Select All

Card Holder	□ View □ Add □ Modify Delete	Card Format	□ View □ Add □ Modify Delete
Card	□ View □ Add □ Modify Delete	Access Level	□ View □ Add □ Modify Delete

Schedule □ Select All

Schedule	□ View □ Add □ Modify Delete	Holiday Group	□ View □ Add □ Modify Delete
Unlock Schedule	□ View □ Add □ Modify Delete	One Time Unlock Schedule	□ View □ Add □ Modify Delete

Event Action □ Select All

Event Action	□ View □ Add □ Modify Delete
Event Code	□ View □ Dashboard Display □ ACK

Threat Level □ Select All

Threat Level	□ View □ Modify	Threat Level Setting	□ View □ Modify Delete

User □ Select All

User Define Field	□ View □ Modify Delete	Web User Account	□ View □ Add □ Modify Delete
User Role	□ View □ Add □ Modify Delete		

Floor □ Select All

Floor	□ View □ Add □ Modify Delete

System Setting □ Select All

Update	□ View □ Modify	Backup	□ View □ Modify
Restore	□ View □ Modify	Reboot	□ View □ Modify
Factory Default	□ View □ Modify		

Network □ Select All

IP Address	□ View □ Modify	FTP	□ View □ Modify
SMTP	□ View □ Modify	System Time Setting	□ View □ Modify
RMC	□ View □ Modify		

Data Transfer □ Select All

Data Transfer	□ User Data Import □ User Data Export

Log Report □ Select All

Log	□ View
Log Report	□ View
Log Management	□ View □ Backup □ Log Reset/Merge □ Log Backup

Report □ Select All

Report	□ Report
Access Report	□ View
System Report	□ View
Smart Report □ View □ Edit/Run	Door Log Log Report Number of people in the building Number of people inside the occupanc

Device Setting □ Select All

Door	□ View □ Modify	Controller	□ View □ Modify
Aux Input	□ View □ Modify	Aux Output	□ View □ Modify
Elevator	□ View □ Modify	Elevator Action	□ View □ Modify
Region	□ View □ Add □ Modify Delete		

Client & Site Setting □ Select All

Client Management	□ View □ Modify	Client Replacement	□ View □ Modify
Site Management	□ View □ Add □ Modify Delete	Site Device	□ View □ Modify

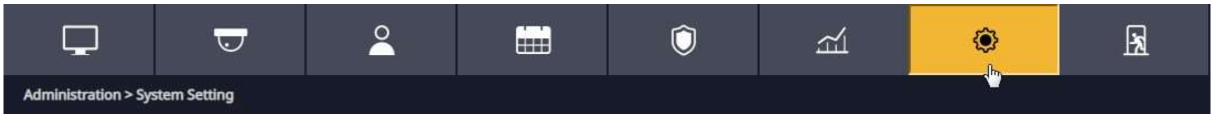
Group Setting □ Select All

Card Holder Group	□ View □ Add □ Modify Delete	Door Group	□ View □ Add □ Modify Delete
Camera Group	□ View □ Add □ Modify Delete	Access Level Group	□ View □ Add □ Modify Delete

Quick Menu □ Select All

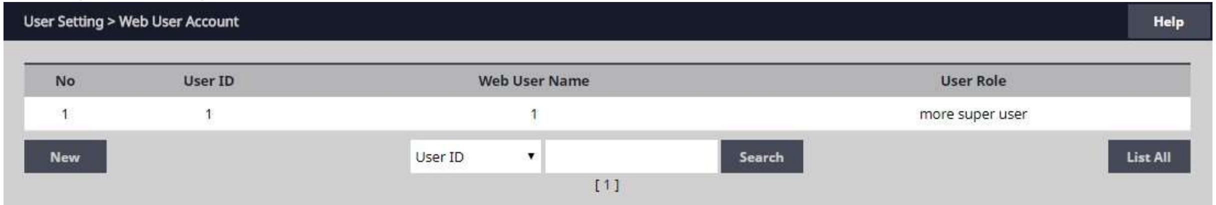
Quick Menu	□ Wizard □ Lost card □ Site Map □ License

Web User Account

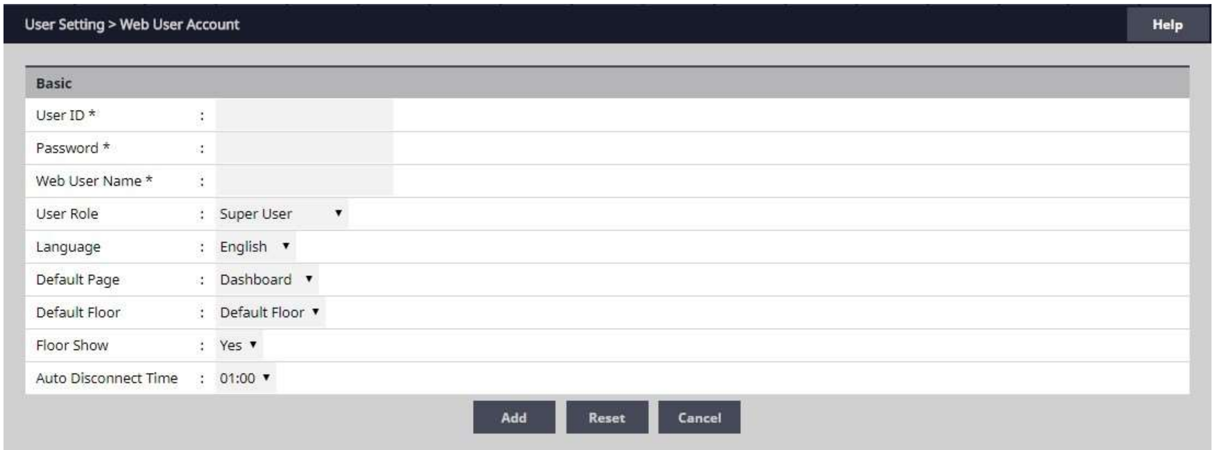


Create or edit the ***Web User Accounts*** that are used to log into to the Controller.

Adding or Editing a Web User

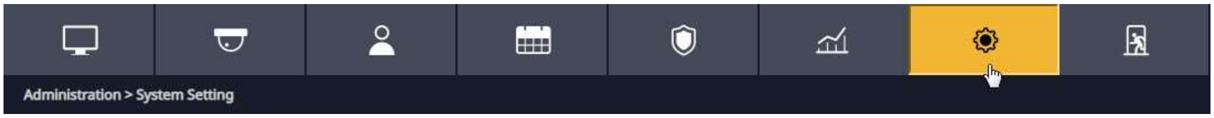


No	User ID	Web User Name	User Role
1	1	1	more super user



Basic		
User ID *	:	
Password *	:	
Web User Name *	:	
User Role	:	Super User ▾
Language	:	English ▾
Default Page	:	Dashboard ▾
Default Floor	:	Default Floor ▾
Floor Show	:	Yes ▾
Auto Disconnect Time	:	01:00 ▾

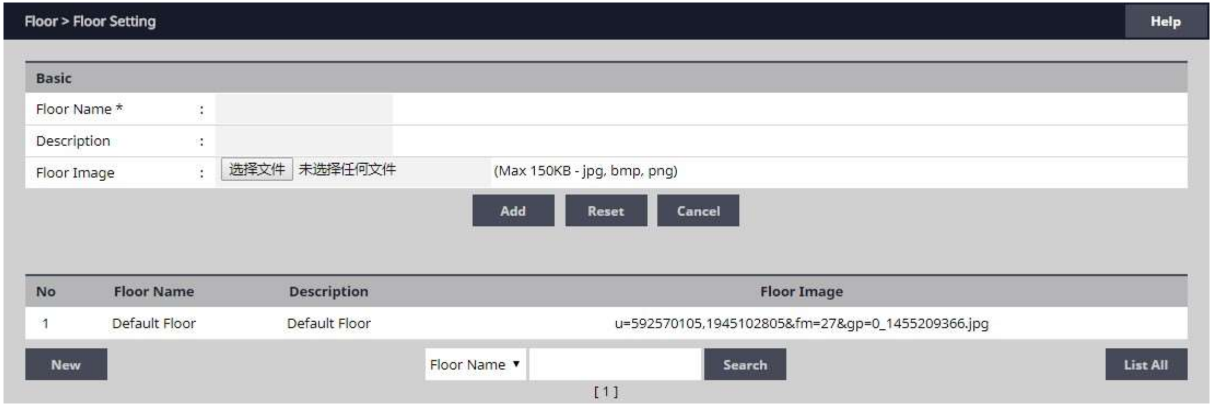
1. To add a new Web User, click New. To edit an existing Web User, click **Edit**.
2. Enter the **User ID**, **Password** and **Web User Name** of the new user.
3. Assign a **User Role**, which defines the privilege level of the user account.
4. Enter the **Language** and **Default Page** for the user.
5. Assign the **Default Floor** and enable **Floor Show** if the floor graphic will display to the user.
6. Enter the **Auto Disconnect Time**, which is the amount of time, in hours, before the Controller will automatically log out the user.
7. Click **Add** or **Save** to save the settings.



Floor Setting

Floor Setting allows the operator to load and view floor plan graphics which will be displayed on the Dashboard.

Adding a Graphic



Basic		
Floor Name *	:	
Description	:	
Floor Image	:	选择文件 未选择任何文件 (Max 150KB - jpg, bmp, png)

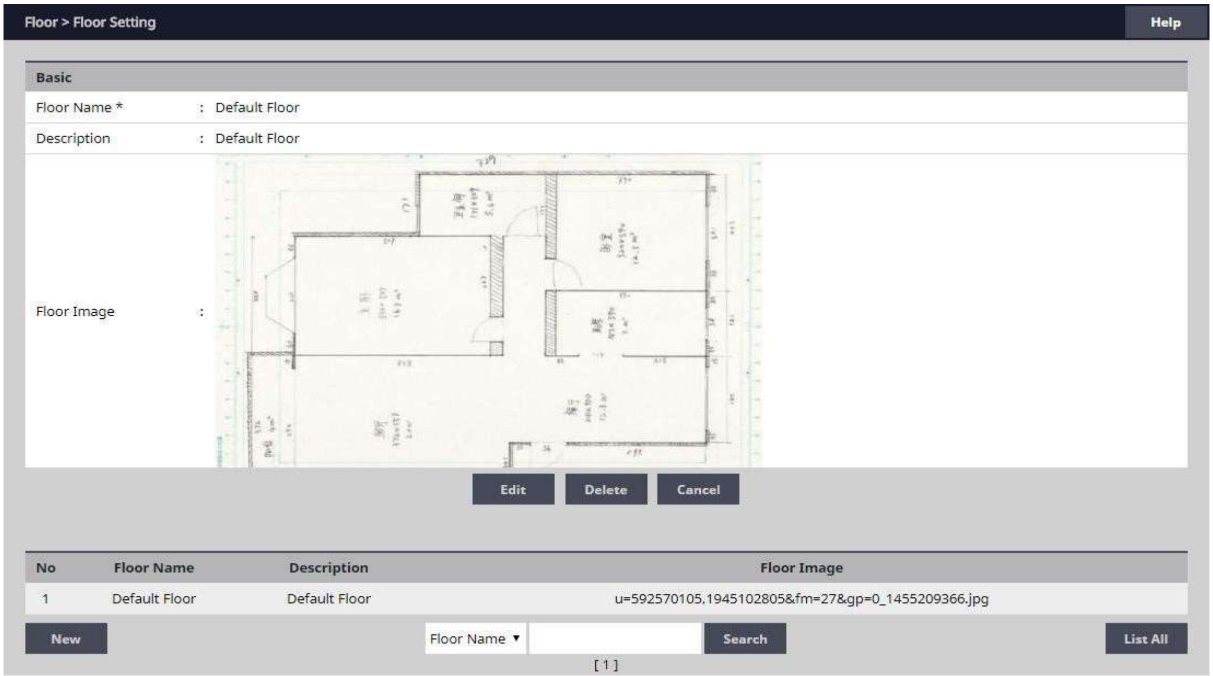
No	Floor Name	Description	Floor Image
1	Default Floor	Default Floor	u=592570105,1945102805&fm=27&gp=0_1455209366.jpg

1. To add a new floor plan graphic, click **New**.
2. Enter a name for the floor in the **Floor Name** field.
3. Enter a description for the floor graphic in the **Description** field.
4. To add a new image, click **Choose File** and select the graphics file.

✓ ***NOTE:*** *The maximum JPG, BMP, or PNG image size is 685 pixels wide by 340 pixels high and the maximum file size is 150KB*

5. To save the graphic, click **Add**.

Viewing a Graphic



Floor > Floor Setting

Basic

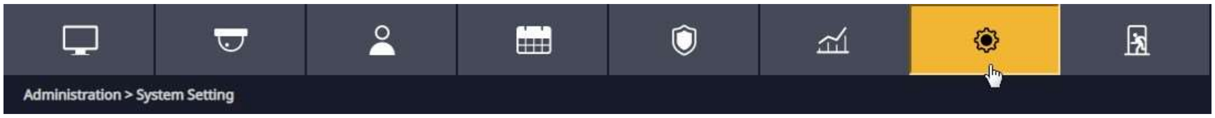
Floor Name *	: Default Floor
Description	: Default Floor
Floor Image	:

No	Floor Name	Description	Floor Image
1	Default Floor	Default Floor	u=592570105,1945102805&fm=27&gp=0_1455209366.jpg

1. Click on a floor graphic in the table.
2. The floor graphic will be previewed on the screen.

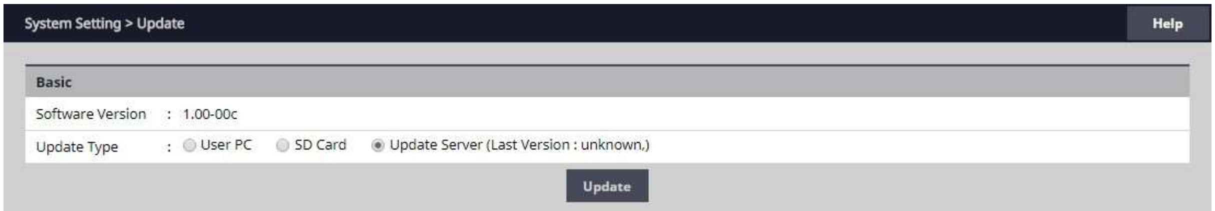
Deleting a Graphic

1. Click on a floor graphic in the table.
2. Click Delete to remove the entire floor graphic record, or click Edit then Delete Image File to just delete the graphic and leave the floor name and description.


Administration > System Setting

Update

Update allows the user to update the firmware of the Controller.


System Setting > Update

Basic

Software Version : 1.00-00c

Update Type : ○ User PC ○ SD Card ● Update Server (Last Version : unknown,)

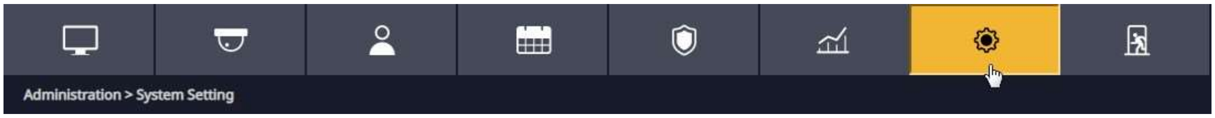
Updating the Firmware

1. Select the location of the firmware file. **User PC**, **SD Card**, or **Update Server**.
2. Click **Update**.

✓ ***NOTE:*** *This function only updates the firmware of the Controller. To update the client firmware refer to Client Management.*

◆ ***WARNING:*** *Servers and Clients MUST be using the same firmware version!*

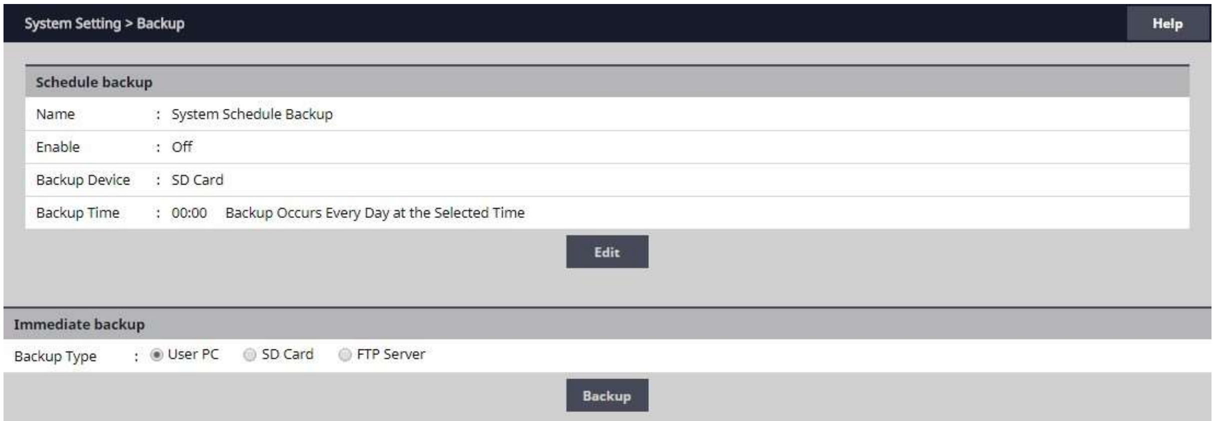
✓ ***NOTE:*** *Gateway and DNS IP addresses must be configured to access the update server. Refer to IP Address to configure these settings.*



Administration > System Setting

Backup

Backup enables the system backup and defines the backup device, time and location of the backup.



System Setting > Backup

Schedule backup

Name	:	System Schedule Backup
Enable	:	Off
Backup Device	:	SD Card
Backup Time	:	00:00 Backup Occurs Every Day at the Selected Time

Immediate backup

Backup Type : ● User PC ○ SD Card ○ FTP Server

The system automatically assigns a name to the backup at the time of the backup with the following format:

·**YYYYMMDDHHMMSS**

·**YYYY** = 4-digit year

·**MM** = 2-digit month

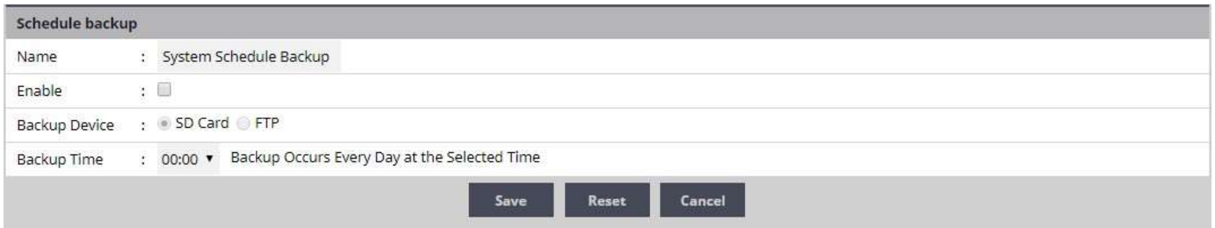
·**DD** = 2-digit day

·**HH** = 2-digit hour

·**MM** = 2-digit minutes

·**SS** = 2-digit seconds

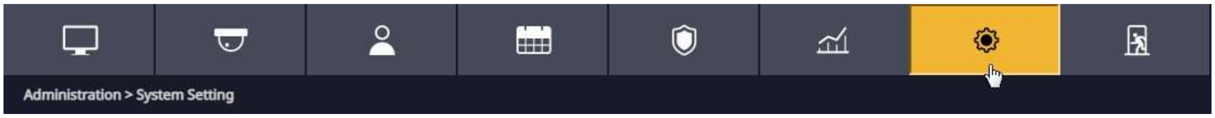
Scheduled Backup



Schedule backup

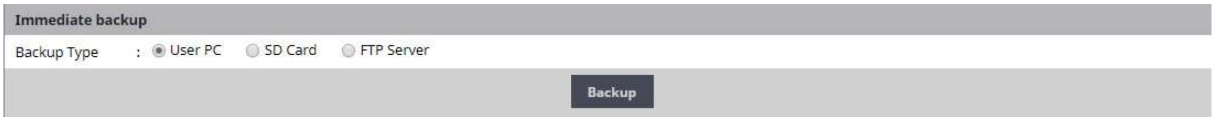
Name	:	System Schedule Backup
Enable	:	□
Backup Device	:	● SD Card ○ FTP
Backup Time	:	00:00 ▾ Backup Occurs Every Day at the Selected Time

1. To change the backup settings, click **Edit**.
2. Set a log name for the backup in the **Name** field.



3. For automatically scheduled daily backup check the **Enable** checkbox.
4. Select **SD Card** or **FTP** for the backup device.
5. Choose a time for the daily backup with the **Backup Time** selector.
6. Click **Save**.

Immediate Backup



Immediate backup

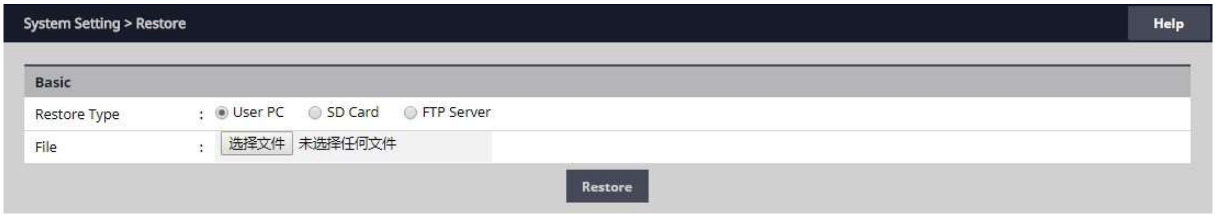
Backup Type : ● User PC ○ SD Card ○ FTP Server

Backup

1. Select **User PC**, **SD Card** or **FTP Server** for the backup device.
2. To run an immediate backup, click **Backup**

Restore

Restore allows the operator to restore the system from a backup.



System Setting > Restore

Help

Basic

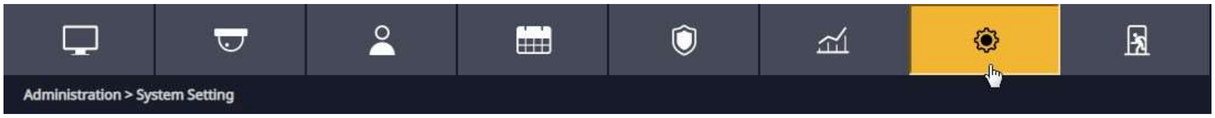
Restore Type : ● User PC ○ SD Card ○ FTP Server

File : 选择文件 未选择任何文件

Restore

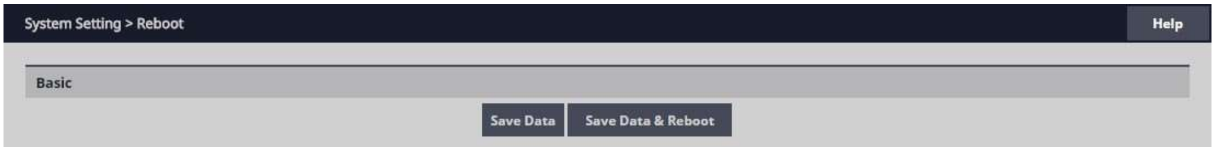
Restoring the System

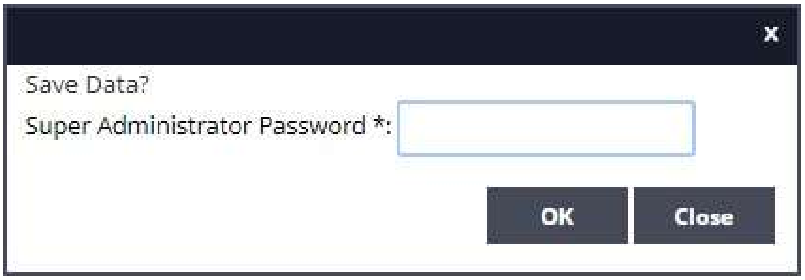
1. Select the location of the restore file. **User PC**, **SD Card**, or **FTP Server**.
2. Enter a file name and path or click **Browse** to choose the file to restore from.
3. Click **Restore**.



Reboot

Save and Reboot can save the Controller data only, or save the Controller data and reboot the Controller.

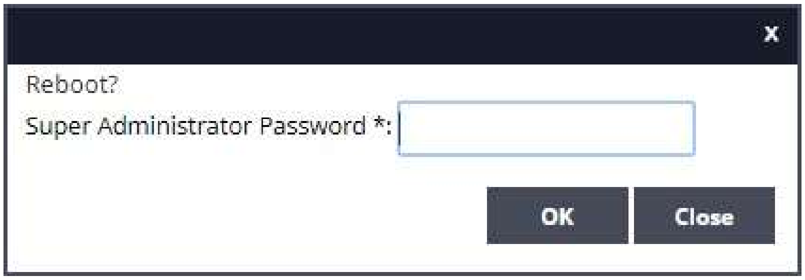



Save Data?

Super Administrator Password *:

Saving Data

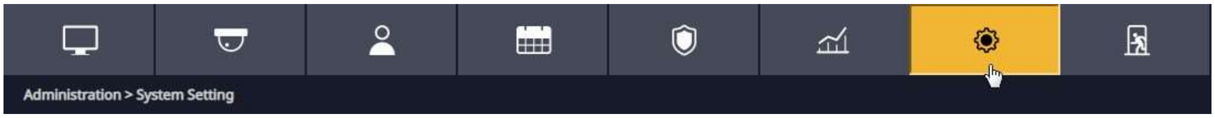
1. Click **Save Data** to force a data save on the Controller.
2. Enter a super administrator password and click **OK**.


Reboot?

Super Administrator Password *:

Saving Data and Rebooting

1. Click **Save Data & Reboot** to force a data save on the Controller and restart the system.
2. Enter an super administrator password and click **OK**.

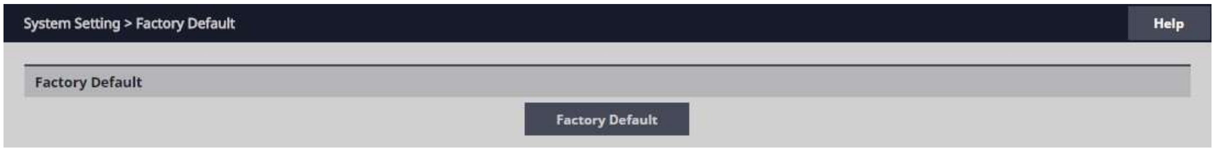


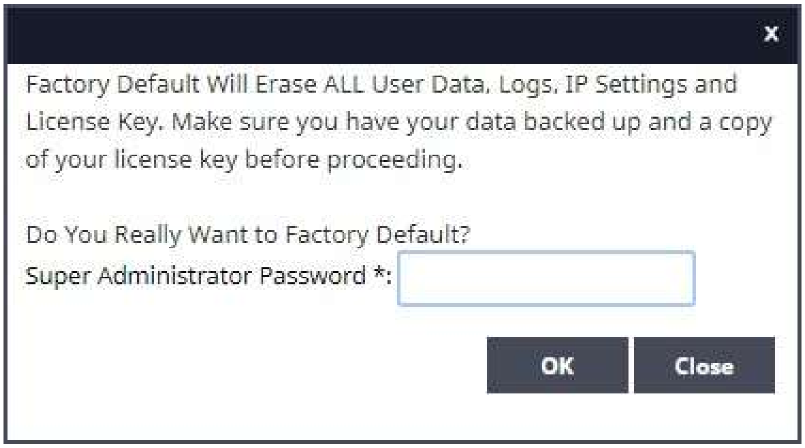
Factory Default

Factory Default will erase **ALL** Card Holder data, logs, IP settings and license key.

◆ ***!! IMPORTANT !!:*** *Write down the license key prior to performing a factory default.*

◆ ***WARNING:*** *It will take 3-5 minutes to factory default a system. DO NOT power down when performing a factory default. Make sure the electrical power source is reliable when performing a factory default. Any loss of power during a factory default can damage your system.*





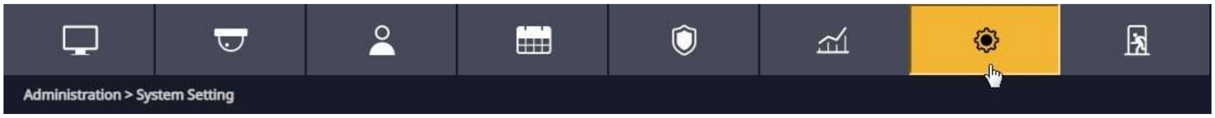
Factory Default Will Erase ALL User Data, Logs, IP Settings and License Key. Make sure you have your data backed up and a copy of your license key before proceeding.

Do You Really Want to Factory Default?

Super Administrator Password *:

Resetting to Factory Defaults

1. After heeding the above warnings, click **Factory Default**.
2. Enter an **Super Administrator Password** and click **OK**.
3. Wait 3-5 minutes for the system to reset and reboot.
4. Enter the license key when the system restarts.



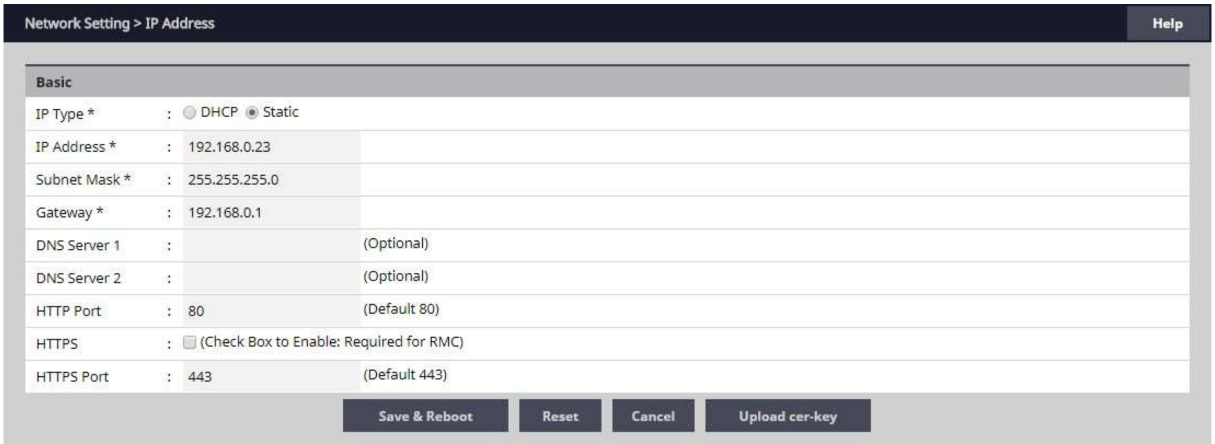
Administration > System Setting

IP Address

The ***Internet Protocol (IP) Address*** area sets all of the network settings including the IP Address, Subnet Mask, Gateway Address, DNS Server 1, DNS Server 2, and HTTP Port.

DHCP assigns an IP address to the Controller automatically on a network containing a DHCP Server (a router will typically have a built-in DHCP Server). When Static is selected, options IP Address, Subnet Mask, Gateway must be entered.

DNS is an Internet service that translates domain names into IP addresses. The IP address of a DNS is required if using NTP time server or SMTP e-mail.



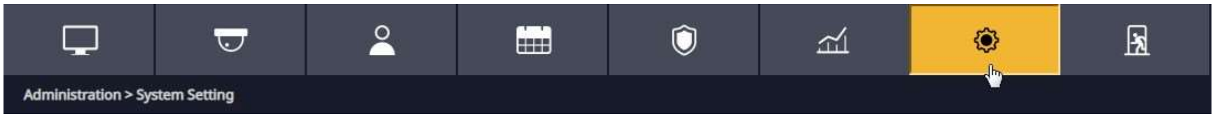
Network Setting > IP Address

Basic

IP Type *	:	○ DHCP ● Static	
IP Address *	:	192.168.0.23	
Subnet Mask *	:	255.255.255.0	
Gateway *	:	192.168.0.1	
DNS Server 1	:		(Optional)
DNS Server 2	:		(Optional)
HTTP Port	:	80	(Default 80)
HTTPS	:	□ (Check Box to Enable: Required for RMC)	
HTTPS Port	:	443	(Default 443)

Editing Network Settings

1. Select **DHCP** or Static. (Skip to Step 5 if using DHCP).
2. Enter a static **IP Address** for the Controller to use on the LAN. The first three values must match other devices on the network (e.g.,192.1.0.x).
3. Enter the **Subnet Mask** address. The Subnet Mask determines the manual address mask used by the Controller (typically255.255.255.0).
4. Set the **Gateway** Address to match the address of the router that connects the LAN to the Internet.
5. Enter the IP address of the **DNS Server 1** (optional, use for NTP time server access or SMTP e-mail connection).

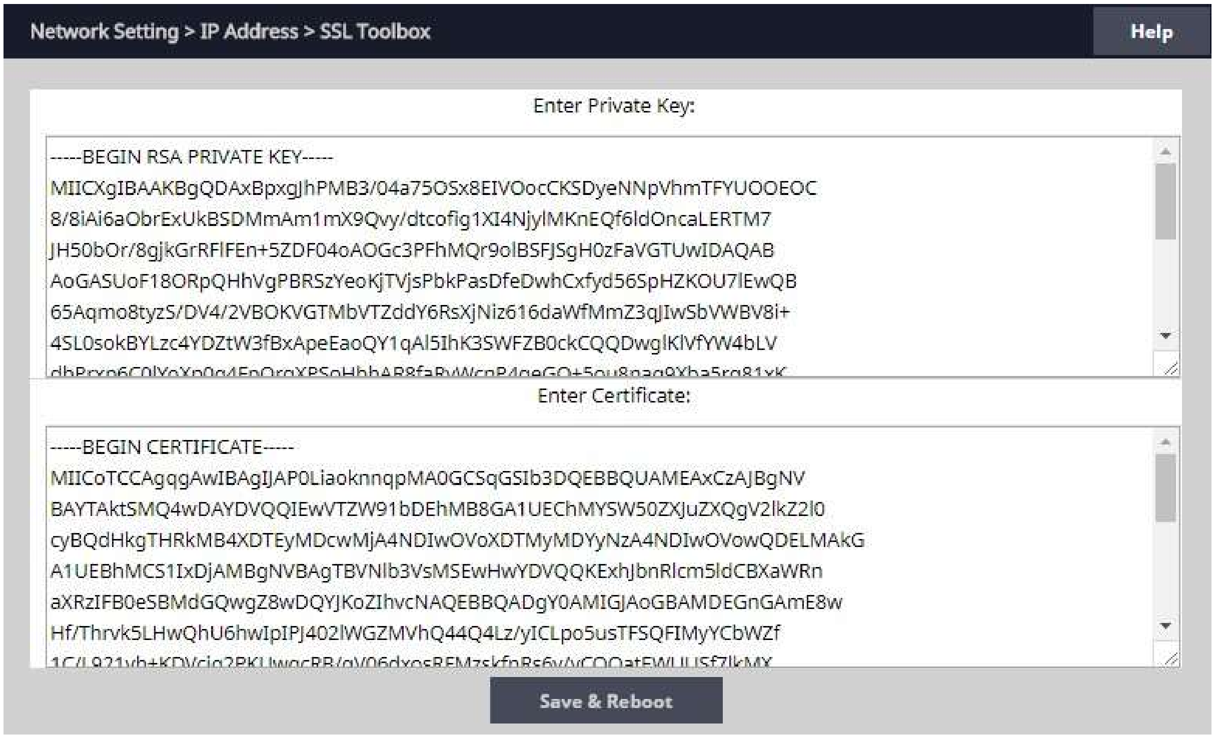


6. Enter the IP address of the **DNS Server 2** (optional, use for NTP time server access or SMTP e-mail connection).
7. Enter the **HTTP Port** number for remote Web browser connection (typically 80).
8. Check the **HTTPS** checkbox if RMC is being used.
9. If using HTTPS, edit the **HTTPS Port** number if required (default is 443).
10. When finished entering the network settings, click **Save & Reboot**.

Upload cer-key

For installations using Hyper Text Transport Protocol Secure (HTTPS) communications, the NanoAccess system uses a default security key and certificate. If the installations network requires a different specific security key and certificate, edit the two items.

1. Click **Upload cer-key**.
2. Enter the **Private Key** into the SSL Toolbox.
3. Enter the **Certificate** into the SSL Toolbox.
4. Click **Save & Reboot**.



Enter Private Key:

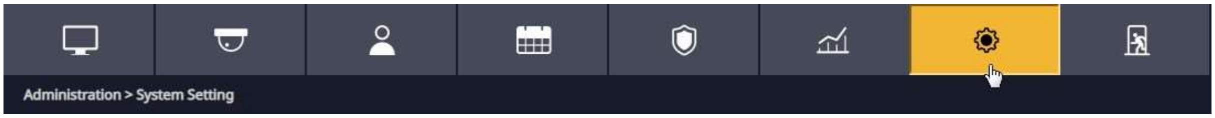
```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDAxBpxgJhPMB3/04a75OSx8EIVOocCKSDyeNNpVhmTFYUOOEOC
8/8iAi6aObrExUkBSDMmAm1mX9Qvy/dtcofig1XI4NjylMKnEQf6ldOncaLERTM7
JH50bOr/8gjkGrRFlFEn+5ZDF04oAOGc3PFhMQr9olBSFJSgH0zFaVGTUwIDAQAB
AoGASUoF18ORpQHhVgPBRSzYeoKjTVjsPbkPasDfeDwhCxfyd56SpHZKOU7lEwQB
65Aqmo8tyzS/DV4/2VBOKVGTMbVTZddY6RsXjNiz616daWfMmZ3qJIwSbVWBV8i+
4SL0sokBYLzc4YDZtW3fBxApeEaoQY1qAl5IhK3SWFZB0ckCQQDwglKlVfYW4bLV
dhPrxp6C0lYoXp0q4FpOrqXPSoHbbAR8faRyWcpP4qeGO+5ou8paq9Xba5rg81xK
```

Enter Certificate:

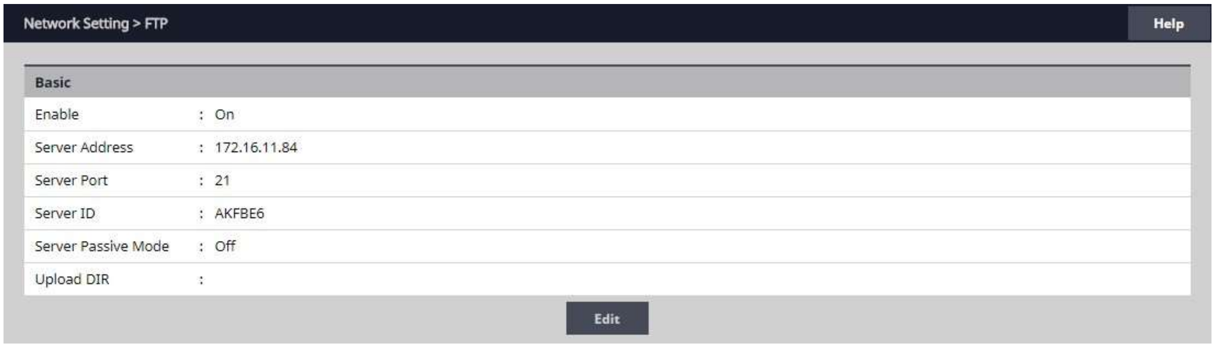
```
-----BEGIN CERTIFICATE-----
MIICoTCCAgqgAwIBAgIJAP0LiaoknnqpMA0GCSqGSIb3DQEBBQUAMEAxCzAJBgNV
BAYTAktSMQ4wDAYDVQQIEwVTZW91bDEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0
cyBQdHkgTHRkMB4XDTEyMDcwMjA4NDIwOVoXDTMyMDYyNzA4NDIwOVowQDELMAkG
A1UEBhMCS1IxDjAMBgNVBAgTBVNlb3VsMSEwHwYDVQQKExhJbnRlcm5ldCBXaWRn
aXRzIFB0eSBMdGQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMDEGnGAmE8w
Hf/Thrvk5LHwQhU6hwIpIPJ402lWGZMVhQ44Q4Lz/yICLpo5usTFSQFIMyYCbWZf
1C/L921vh+KDVcig2PKUwqcRB/qV06dxosREMzskfpRs6v/vCOOatEWUUSf7lkMX
```

FTP

File Transfer Protocol (FTP) enables and configures the system to backup to an FTP location. Enter FTP information as provided by your web host.

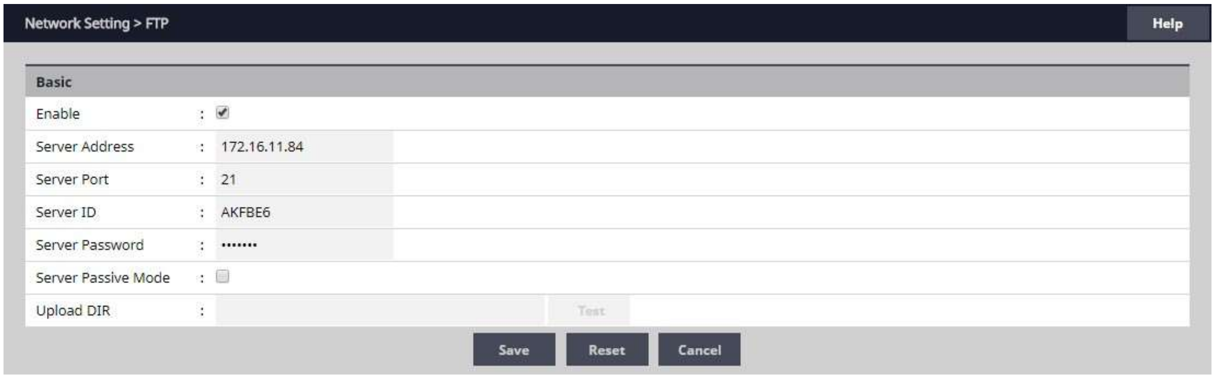


Administration > System Setting



Network Setting > FTP

Basic	
Enable	: On
Server Address	: 172.16.11.84
Server Port	: 21
Server ID	: AKFBE6
Server Passive Mode	: Off
Upload DIR	:



Network Setting > FTP

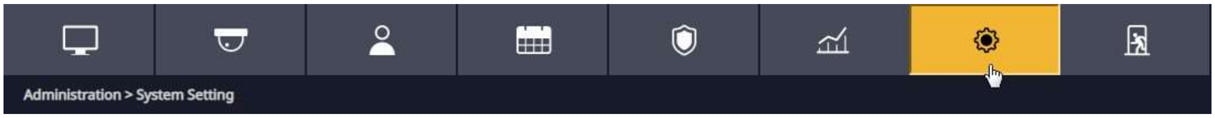
Basic	
Enable	: ☑
Server Address	: 172.16.11.84
Server Port	: 21
Server ID	: AKFBE6
Server Password	: •••••••
Server Passive Mode	: □
Upload DIR	:

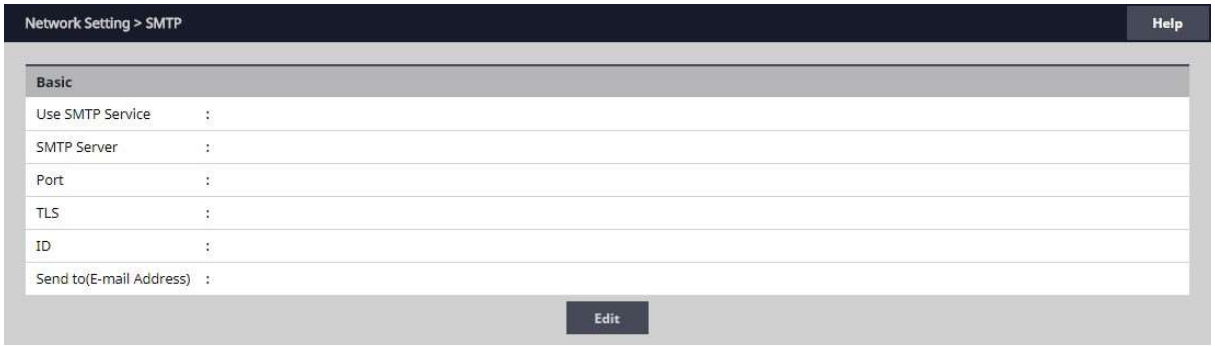
Editing FTP Settings

1. Check the **Enable** checkbox to enable an FTP server connection.
2. Enter the IP address of the FTP server in the **Server Address** field.
3. Enter the communications port number into the **Server Port** field.
4. Enter the FTP server user name into the **Server ID** field.
5. Enter the FTP server password into the **Server Password** field.
6. Check the **Server Passive Mode** checkbox if required by the FTP server.
7. Enter the upload directory path used on the FTP server in the **Upload DIR** field.
8. Click **Save** to save the changes.

SMTP

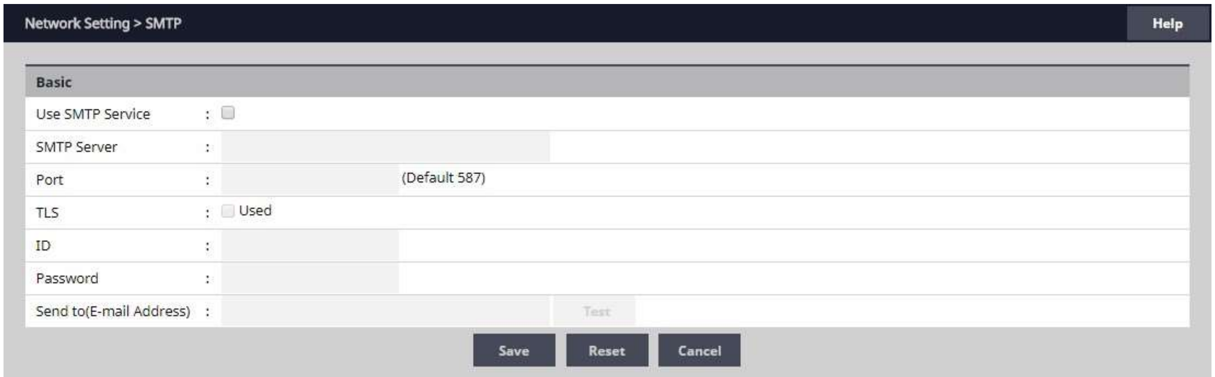
Simple Mail Transfer Protocol (SMTP) provides the ability to send email to specified email addresses.





Basic

Use SMTP Service	:
SMTP Server	:
Port	:
TLS	:
ID	:
Send to(E-mail Address)	:



Basic

Use SMTP Service	: □
SMTP Server	:
Port	: (Default 587)
TLS	: □ Used
ID	:
Password	:
Send to(E-mail Address)	:

Editing SMTP Settings

1. To allow the Controller to send SMTP e-mail messages, check the **Use SMTP Service** checkbox. 2. Enter the SMTP mail server URL (typically “mail. your email domain.com”) the **SMTP Server** field.

3. Enter the incoming port number of the SMTP mail server in the **Port** field.

4. Enable TLS if your mail server uses secure server communication (this is common). Check the **TLS Used** checkbox to enable TLS.

5. Enter your SMTP mail server user ID (your email address) in the **ID** field.

6. Enter your SMTP mail server Password in the **Password** field.

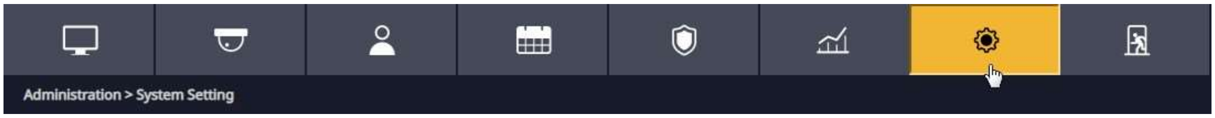
7. Test the system by entering an email address in the **Send to (E-mail Address)** field and click **Test**.

8. Click **Save** to save the changes.

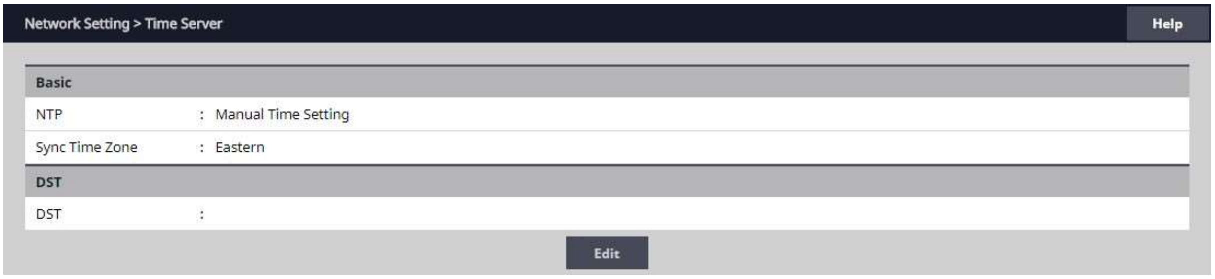
✓ ***NOTE:*** *The Controller’s Gateway IP address and DNS address must be properly configured to be able to send email. Refer to IP Address to configure these settings.*

Time Server

Time Server provides the ability to sync the system to a time server or manually set the time.

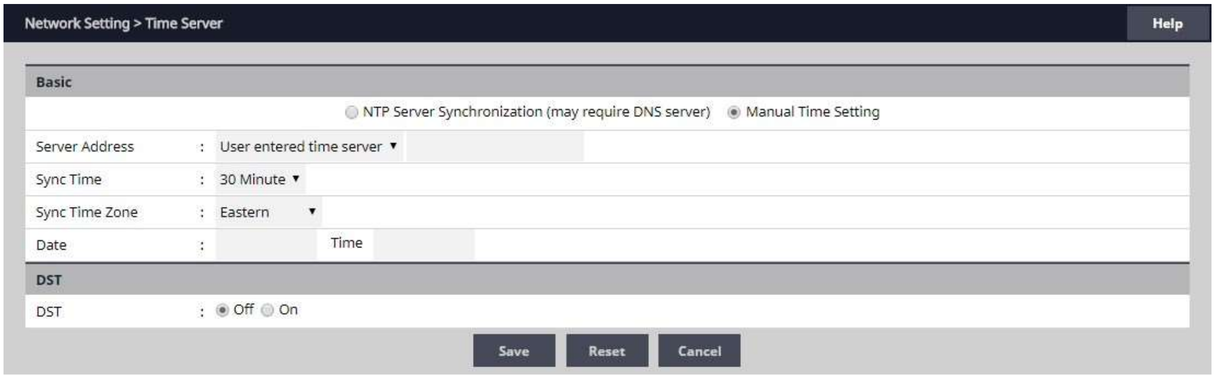


✓ ***NOTE:*** *Gateway IP and DNS IP addresses must be configured to access public time servers. Refer to IP Address to configure these settings.*



Network Setting > Time Server

Basic	
NTP	: Manual Time Setting
Sync Time Zone	: Eastern
DST	
DST	:



Network Setting > Time Server

Basic	
	○ NTP Server Synchronization (may require DNS server) ● Manual Time Setting
Server Address	: User entered time server ▾
Sync Time	: 30 Minute ▾
Sync Time Zone	: Eastern ▾
Date	: Time
DST	
DST	: ● Off ○ On

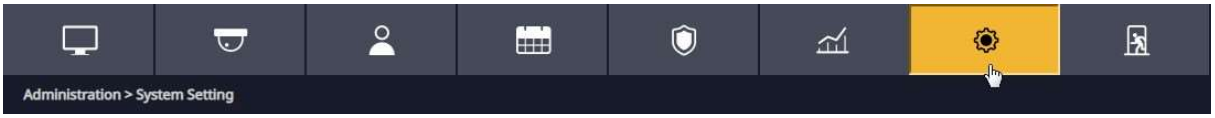
Editing Time Server Settings

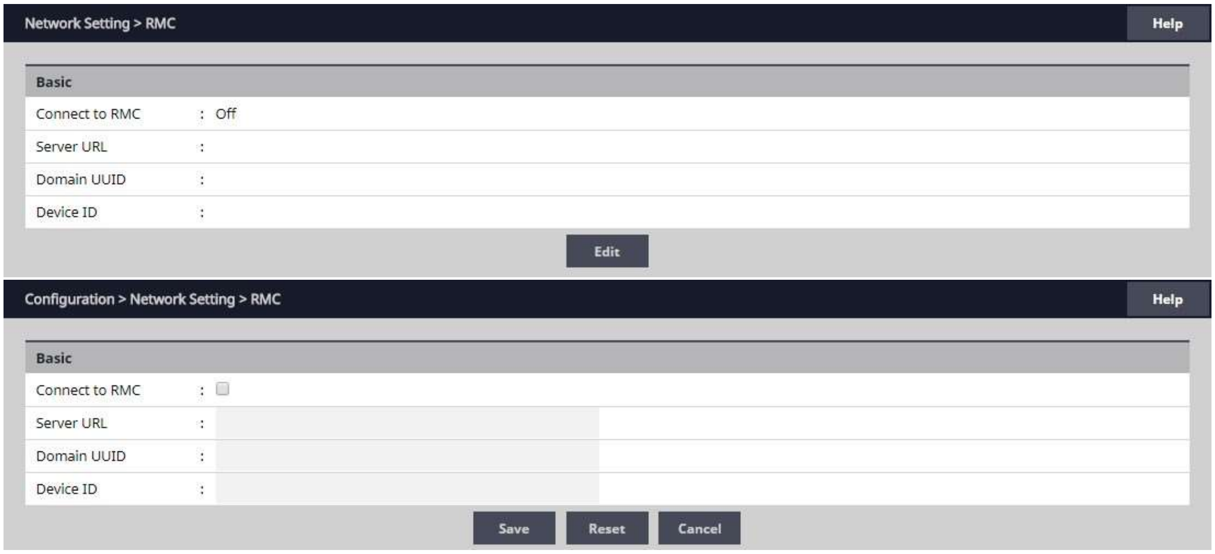
1. To manually set the system time select **Manual Time Setting**. Skip to Step 6.
2. To use a time server, select **NTP Server Synchronization**.
3. Select one of the time servers from the **Server Address** drop box.
4. Select the time period for the timeserver synchronization from the **Sync Time** dropdown. Skip to Step7.
5. Select the time zone at the Controller's installation location from the **Sync Time Zone** dropdown.
6. For manual date and time setting, enter the current date and time in the **Date** and **Time** fields.
7. To enable Daylight Saving Time (DST) select **ON**. Enter the DST start and end dates in the two fields.
8. Click **Save**.

RMC

The ***Remote Management Console*** (RMC) server is used to manage multiple Controllers, usually from a remote location.

If using RMC, the settings for the RMC server's URL, Domain UUID, and Device ID will need to be edited in the Controller.





Network Setting > RMC

Basic

Connect to RMC : Off
Server URL :
Domain UUID :
Device ID :

Configuration > Network Setting > RMC

Basic

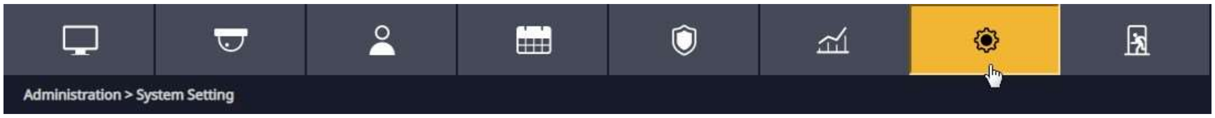
Connect to RMC : □
Server URL :
Domain UUID :
Device ID :

Editing RMC Settings

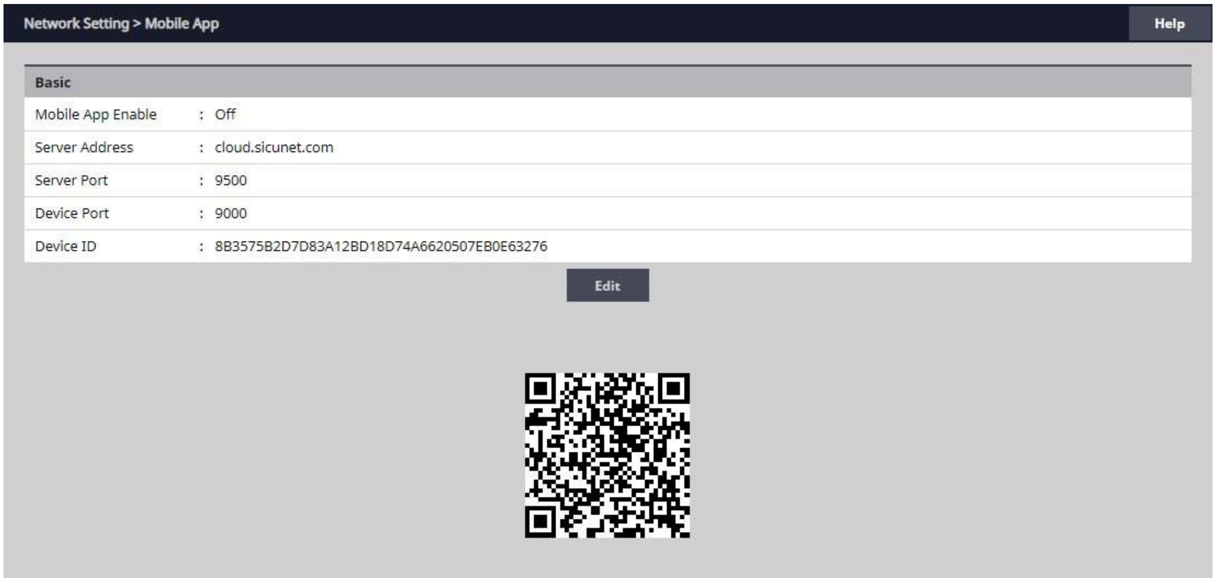
1. Click **Edit** button
2. Tick Connect to RMC.
3. Default Server IP is rmc.EyeLock.com and Default Server Port is 9900, if you need you can change.
4. Click **Save** to keep the changes. Refer to the RMC User Guide for details on RMC setup and operation.

Mobile App

We can access system from iPhone, iPad and Android devices by ***Mobile App.*** If using Mobile App. We need to connect server.

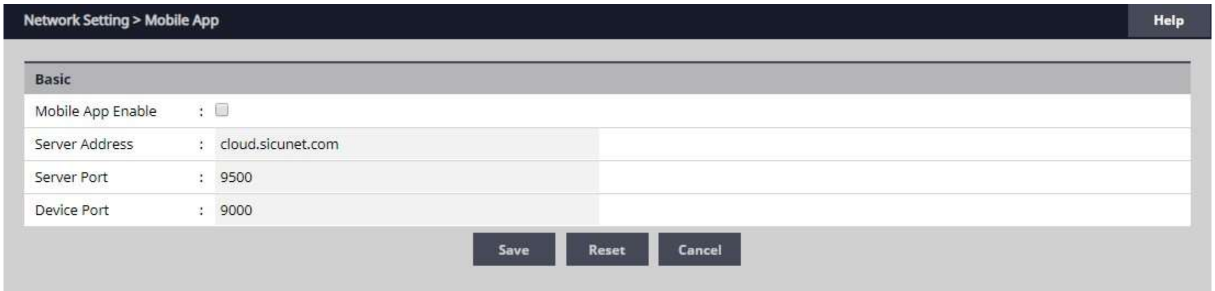


Administration > System Setting



Network Setting > Mobile App

Basic	
Mobile App Enable	: Off
Server Address	: cloud.sicunet.com
Server Port	: 9500
Device Port	: 9000
Device ID	: 8B3575B2D7D83A12BD18D74A6620507EB0E63276



Network Setting > Mobile App

Basic	
Mobile App Enable	: □
Server Address	: cloud.sicunet.com
Server Port	: 9500
Device Port	: 9000

Editing Mobile App 1.
Click **Edit** button.

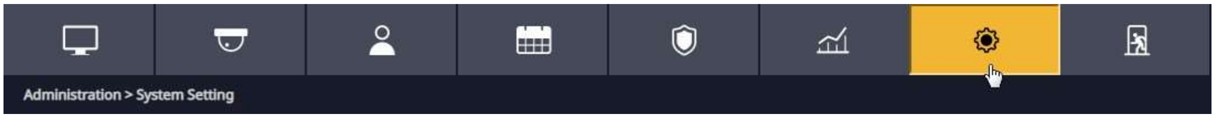
2. Tick Mobile App Enable.

3. Server Address, Server Port and Device port have default value, if you need, you can change.

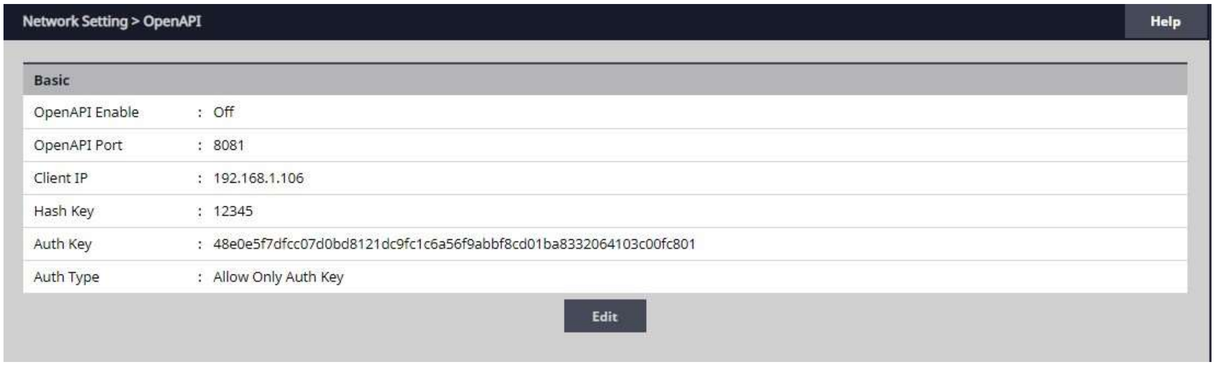
4. Click **Save** to keep the changes. Refer to the **NanoAccess Mobile User Guide** for details on Mobile setup and operation.

Open API

The ***Open API*** is used to access program interface.



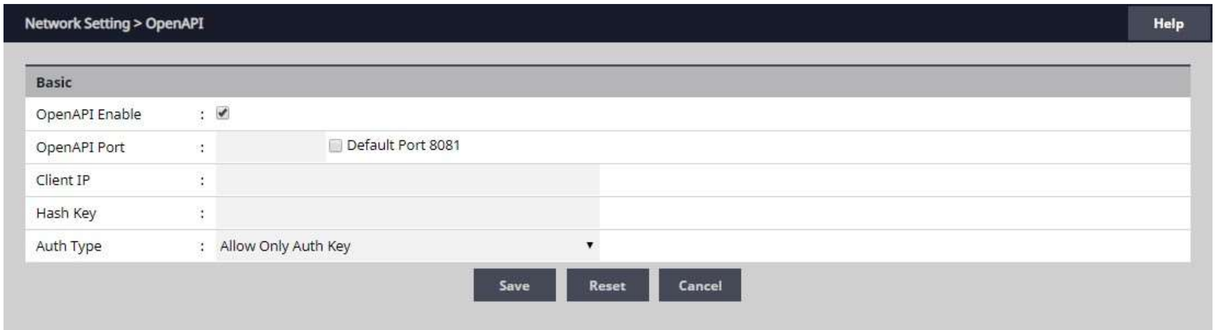
Administration > System Setting



Network Setting > OpenAPI

Basic

OpenAPI Enable	:	Off
OpenAPI Port	:	8081
Client IP	:	192.168.1.106
Hash Key	:	12345
Auth Key	:	48e0e5f7dfcc07d0bd8121dc9fc1c6a56f9abbf8cd01ba8332064103c00fc801
Auth Type	:	Allow Only Auth Key



Network Setting > OpenAPI

Basic

OpenAPI Enable	:	☑
OpenAPI Port	:	□ Default Port 8081
Client IP	:	
Hash Key	:	
Auth Type	:	Allow Only Auth Key ▾

Editing Open API

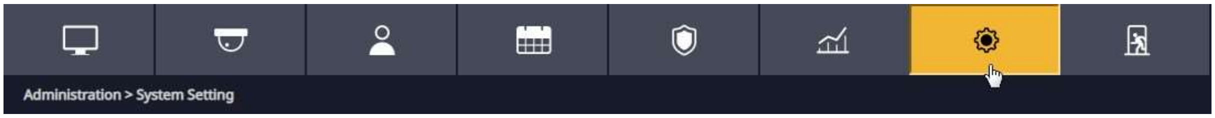
1. Click **Edit** button.
2. Tick OpenAPI Enable.
3. Enter the OpenAPI Port, Client IP and Hash Key, select Auth Type.
4. Click **Save** to keep the changes. Refer to the Open API User Guide for details on API setup and operation.

Door

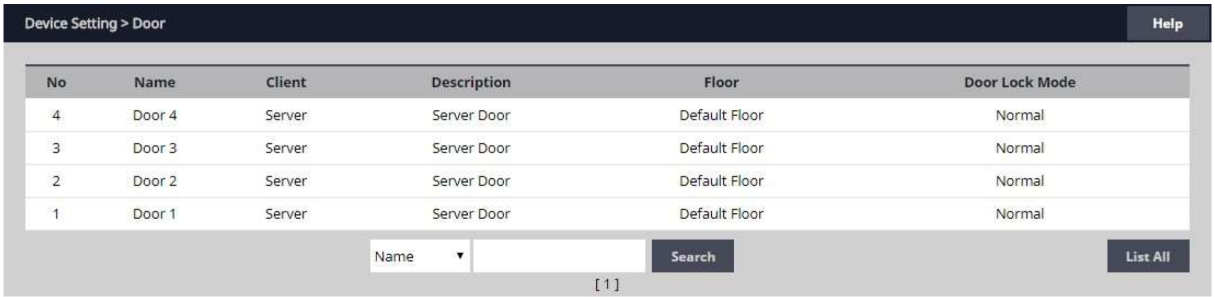
Door displays the doors that are assigned to the system. Click on the door name for additional information pertaining to each door.

✓ ***NOTE:*** *When programming various elements of the system, do not use the same name for multiple items (e.g., use Door 1, Door 2, etc.).*

✓ ***NOTE:*** *Do not use special characters (<>?{})(*&%#@^{ \|/).*



Editing a Door


Device Setting > Door

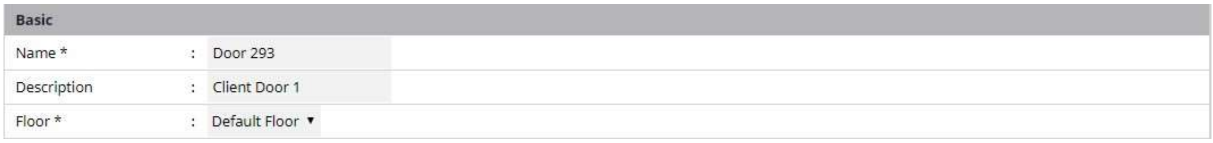
Help

No	Name	Client	Description	Floor	Door Lock Mode
4	Door 4	Server	Server Door	Default Floor	Normal
3	Door 3	Server	Server Door	Default Floor	Normal
2	Door 2	Server	Server Door	Default Floor	Normal
1	Door 1	Server	Server Door	Default Floor	Normal

Select the desired door. Scroll to the bottom of the page and click **Edit**.

After making any edits, be sure to click Save at the bottom of the page.

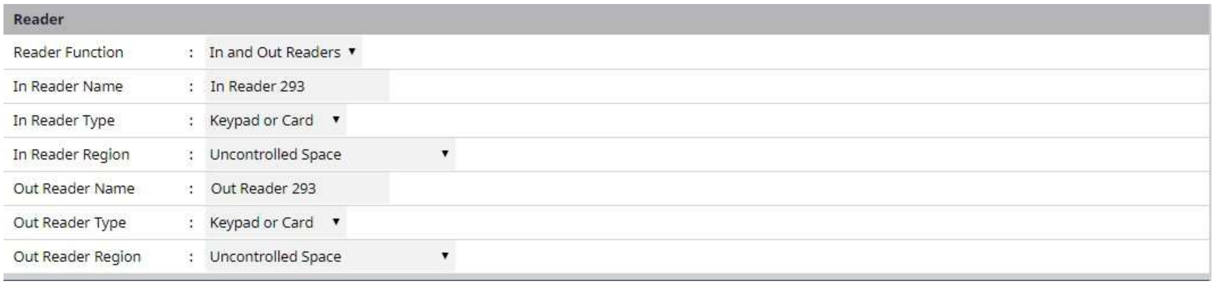
Basic


Basic

Name *	:	Door 293
Description	:	Client Door 1
Floor *	:	Default Floor ▼

1. Enter the desired **Name** and **Description** (optional) for the door.
2. For multi-floor installations, select the **Floor**.

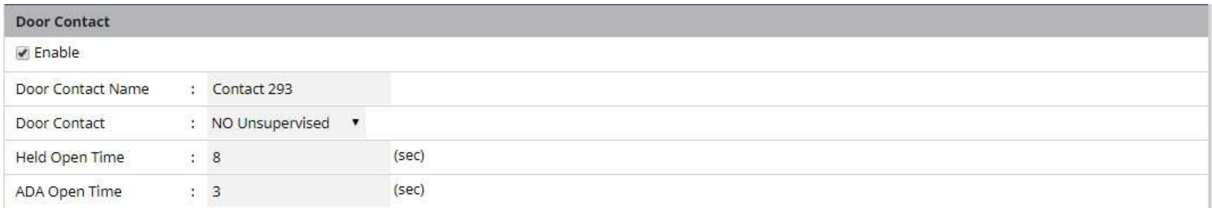
Reader


Reader

Reader Function	:	In and Out Readers ▼
In Reader Name	:	In Reader 293
In Reader Type	:	Keypad or Card ▼
In Reader Region	:	Uncontrolled Space ▼
Out Reader Name	:	Out Reader 293
Out Reader Type	:	Keypad or Card ▼
Out Reader Region	:	Uncontrolled Space ▼

1. In the **Reader** section, select the settings for the door's reader.

Door Contact



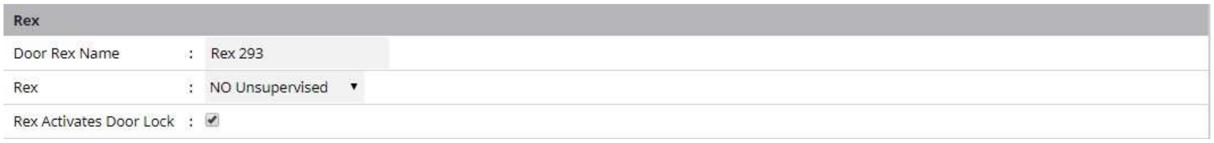
Door Contact

☑ Enable

Door Contact Name	:	Contact 293	
Door Contact	:	NO Unsupervised ▼	
Held Open Time	:	8	(sec)
ADA Open Time	:	3	(sec)

1. In the **Door Contact** section, check the Enable checkbox if a door contact is used.
2. **Name** the door contact and select its type.
3. Adjust the **Held Open Time**, which is the length of time the door can be open following a valid access request.
4. The **ADA Open Time** is an additional time added to the Held Open Time.

Rex

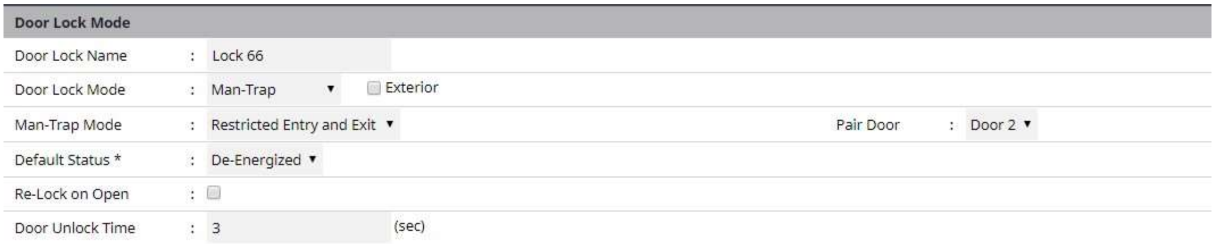


Rex

Door Rex Name	:	Rex 293
Rex	:	NO Unsupervised ▼
Rex Activates Door Lock	:	☑

1. Enter the **Door Rex Name** for the door's request to exit switch.
2. Select the type of **Rex** switch.
3. Check the **Rex Activates Door Lock** checkbox to have the Rex activate the door's lock.

Door Lock Mode



Door Lock Mode

Door Lock Name	:	Lock 66			
Door Lock Mode	:	Man-Trap ▼ ☐ Exterior			
Man-Trap Mode	:	Restricted Entry and Exit ▼	Pair Door	:	Door 2 ▼
Default Status *	:	De-Energized ▼			
Re-Lock on Open	:	☐			
Door Unlock Time	:	3 (sec)			

1. Choose a **Door Lock Name** to name the lock for logging.

2. Configure **Door Lock Mode** as follows:

· **Normal:** Lock activates in response to a valid access request and REX unlocks door for exit.

· **Locked:** Does NOT grant access in response to REX, card or code.

· **Locked w/REX:** Remains in locked mode, ONLY REX will activate lock.

· **Unlocked:** Door will remain unlocked at ALL times.

· **Man-Trap:** Sets the door lock for use in conjunction with another door to create a man-trap passage. A Man-Trap will only allow one door to be opened if the other door is locked. When Man-Trap is selected, **Man-Trap Mode** options appear:

· **Unlock:** No security on Entry or Exit.

· **Secure Entry/Free Egress:** Two options, both options use card access to enter the Exterior Door. Option 1 allows free exit through the exterior door; Option 2 requires card access to exit through the exterior door.

· **Restricted Entry and Exit:** Four options, all options use card access to enter the Exterior Door. Option 1 allows free exit through the exterior door; Option 2 requires card access to exit through the interior door, Option 3requires card access to exit through the exterior door. Option 4 requires card access to exit through either door.

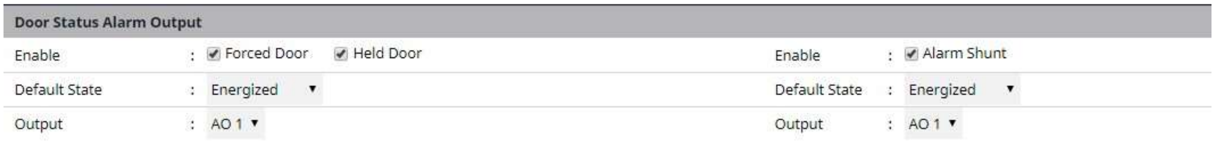
· **Pair Door:** Select the second Man-Trap door that is closest to the secured area.

3. Select the Door's **Default Status**. This setting will be determined by the lock type (energized or de-energized).

4. Assign **Re-Lock on Open** if desired. This will re-lock the door immediately upon opening the door.

5. Adjust **Door Unlock Time** if desired. This is the length of time the door relay is active after a valid access request.

Door Status Alarm Output



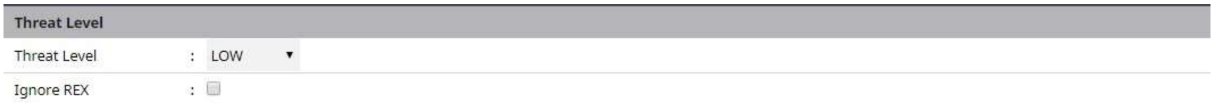
Door Status Alarm Output

Enable	:	☑ Forced Door ☑ Held Door	Enable	:	☑ Alarm Shunt
Default State	:	Energized ▾	Default State	:	Energized ▾
Output	:	AO 1 ▾	Output	:	AO 1 ▾

Sets the actions of a door contact on the door. The door contact must be enabled to use these functions.

1. Check **Forced Door** to trigger the door alarm output if the door opens, but no access was granted.
2. Check **Held Door** to trigger the door alarm output if the door is held open longer than the **Held Open Time**.
3. Select Energized or De-energized for the **Default State** of the Door Status Alarm Output.
4. Select an **Output** to use for the Door Status Alarm Output.
5. Click to enable an **Alarm Shunt** output to operate when access is granted to the secured door.
6. Select Energized or De-energized for the **Default State** of the Alarm Shunt Output.
7. Select an **Output** to use for the Alarm Shunt Output.

Threat Level



Threat Level

Threat Level	:	LOW ▾
Ignore REX	:	□

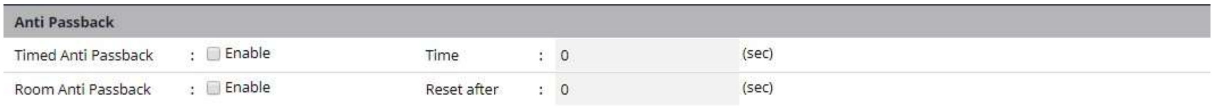
1. Select the highest **Threat Level** allowed before the door will automatically lock.

✓ ***Note:*** *An unlocked door will lock if the System Threat Level is greater than the Door Threat Level; including doors that are unlocked by schedule.*

✓ ***Note:*** *The Dashboard M-Unlock and E-Unlock may be used to unlock a door that has been locked due to elevated system Threat Level.*

2. Check **Ignore REX** to ignore input from a Rex button if the current System Threat Level is higher than the Door Threat Level.

Anti-Passback



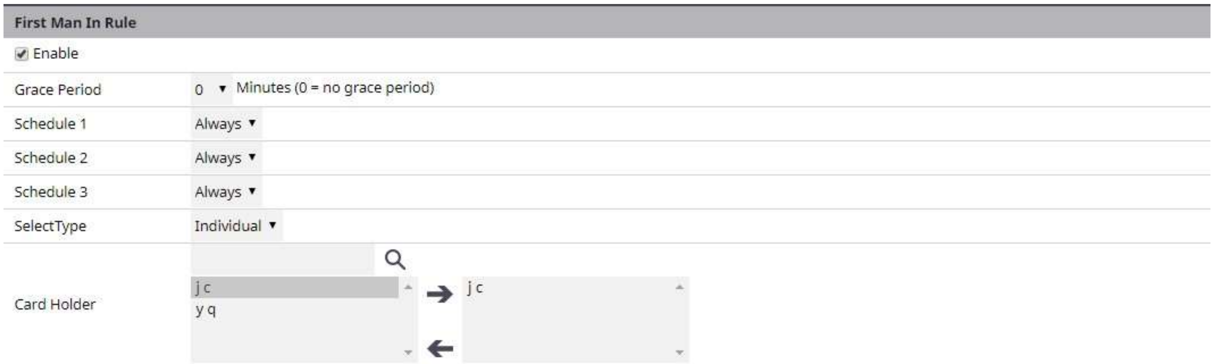
Anti Passback

Timed Anti Passback	:	□ Enable	Time	:	0	(sec)
Room Anti Passback	:	□ Enable	Reset after	:	0	(sec)

1. Check to enable **Timed Anti Passback**. Select a time in seconds to disable a credential after it has been used to grant access.

2. Check to enable **Room Anti Passback**. Select a time in seconds to disable access to a room after access has been granted to the room.

First Man In Rule



First Man In Rule

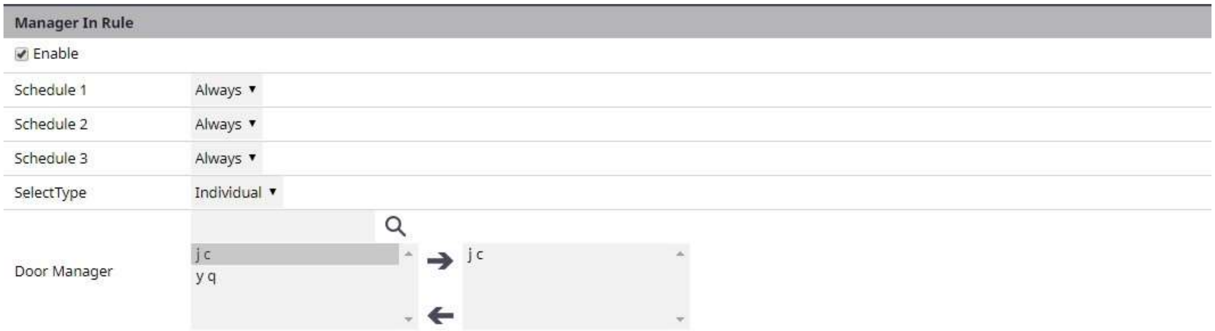
☑ Enable

Grace Period	0 ▾ Minutes (0 = no grace period)
Schedule 1	Always ▾
Schedule 2	Always ▾
Schedule 3	Always ▾
SelectType	Individual ▾
Card Holder	j c y q → j c

First Man in Rule unlocks a door when first Card Holder enters.

1. Check **Enable** to use a First Man In Rule.
2. Select a **Grace Period** to allow the selected first man Card Holder(s) access minutes before a scheduled start time.
3. Select up to three time **Schedules** for the rule to be active.
4. Select the **Type** of Card Holders (individual or group).
5. Search or choose **Card Holder**(s) or **Groups** for the rule. Use the arrows to move the name(s) in and out.

Manager In Rule



Manager In Rule

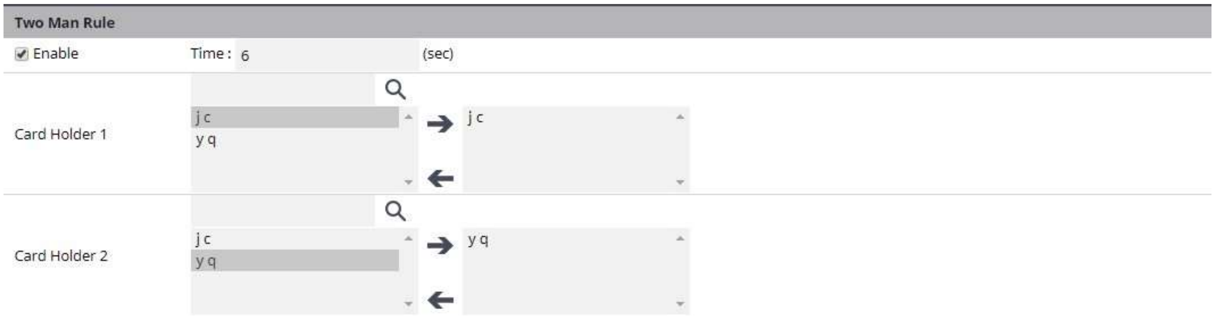
☑ Enable

Schedule 1	Always ▾
Schedule 2	Always ▾
Schedule 3	Always ▾
SelectType	Individual ▾
Door Manager	j c y q → j c

With Manager in Rule enabled, if a Card Holder designated as a Door Manager has not entered the system within a specific time period, the door will not unlock.

1. Check **Enable** to use the Manager In Rule.
2. Select up to three time **Schedules** for the rule to be active.
3. Select the **Type** of Card Holders (individual or group).
4. Search or choose **Card Holder**(s) or **Groups** for the rule. Use the arrows to move the name(s) in and out.

Two Man Rule



Two Man Rule

☑ Enable Time : 6 (sec)

Card Holder 1: j c, y q → j c

Card Holder 2: j c, y q → y q

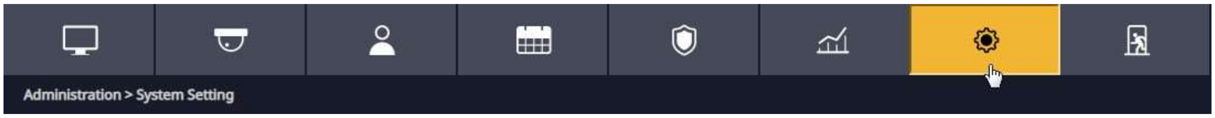
With Two Man Rule enabled, two Card Holders must present credentials at the same time in order to unlock the door. Credentials must be presented in the proper sequence (Card Holder 1 then Card Holder 2), or access will be denied.

1. Check **Enable** to use the Two Man Rule.
2. Enter a **Time** in seconds allowed for the second Card Holder to present their credentials.
3. Search or choose **Card Holder 1** for the rule. Use the arrows to move the name(s) in and out.
4. Search or choose **Card Holder 2** for the rule. Use the arrows to move the name(s) in and out.

Saving Changes

After making any edits, be sure to click **Save** at the bottom of the page.

Elevator

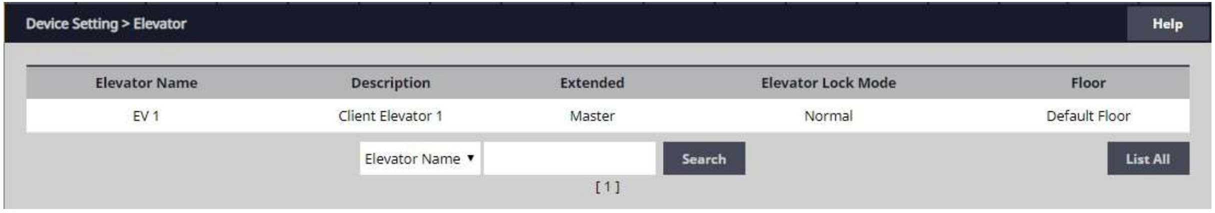


Administration > System Setting

Optional Feature

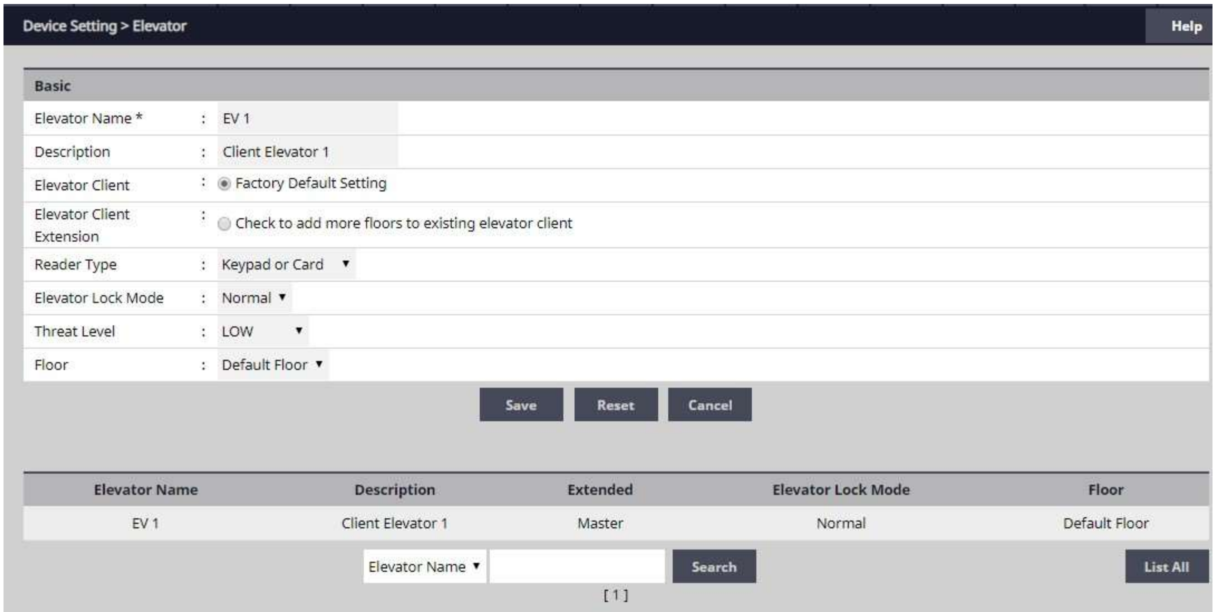
Elevator displays the elevators that are assigned to the system. Click on the elevator name to view or edit the settings of the elevator. Each elevator cab requires an elevator module, which activates up to 8 outputs for controlling access to floors. Access to more than 8 floors requires additional elevator modules.

Editing an Elevator



Device Setting > Elevator

Elevator Name	Description	Extended	Elevator Lock Mode	Floor
EV 1	Client Elevator 1	Master	Normal	Default Floor



Device Setting > Elevator

Basic		
Elevator Name *	:	EV 1
Description	:	Client Elevator 1
Elevator Client	:	● Factory Default Setting
Elevator Client Extension	:	○ Check to add more floors to existing elevator client
Reader Type	:	Keypad or Card ▾
Elevator Lock Mode	:	Normal ▾
Threat Level	:	LOW ▾
Floor	:	Default Floor ▾

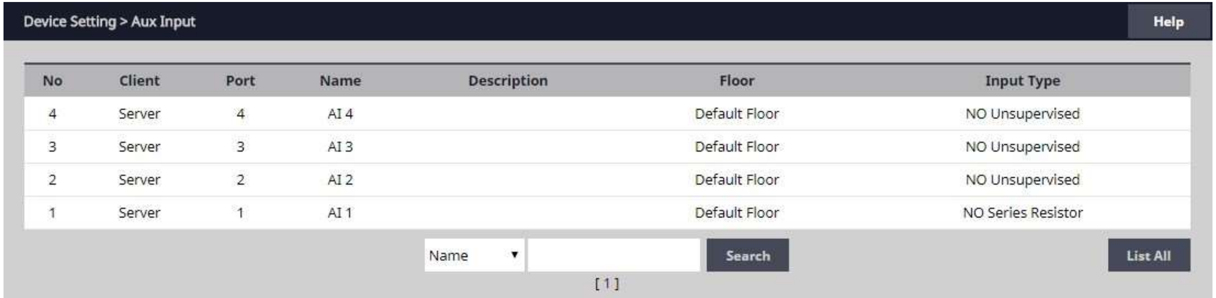
Elevator Name	Description	Extended	Elevator Lock Mode	Floor
EV 1	Client Elevator 1	Master	Normal	Default Floor

1. Click the desired elevator from the list and click **Edit**.
2. For **Elevator Name**, enter a name for the elevator.
3. For **Description**, enter a description for the elevator.
4. Select **Elevator Client** for the factory default setting for the client, or **Elevator Client Extension** to add more floors to an existing elevator client.
5. Select the **Reader Type** that matches the elevator reader from the dropdown list.
6. Select the **Elevator Lock Mode** from the dropdown list.
7. Select the **Threat Level** from the dropdown list.
8. Select the **Floor** from the dropdown list.
9. Click **Save**.

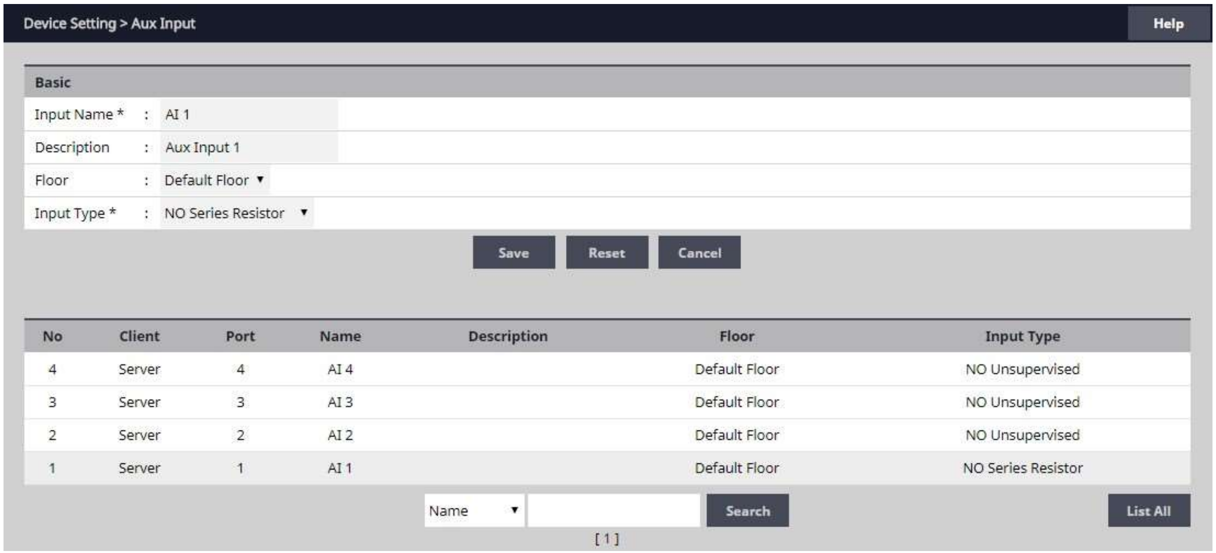
Aux Input

Aux Input displays the inputs that are assigned to the system. Click on the input name to view or edit the settings of the input.

Editing an Input



No	Client	Port	Name	Description	Floor	Input Type
4	Server	4	AI 4		Default Floor	NO Unsupervised
3	Server	3	AI 3		Default Floor	NO Unsupervised
2	Server	2	AI 2		Default Floor	NO Unsupervised
1	Server	1	AI 1		Default Floor	NO Series Resistor



Basic

Input Name *	:	AI 1
Description	:	Aux Input 1
Floor	:	Default Floor ▼
Input Type *	:	NO Series Resistor ▼

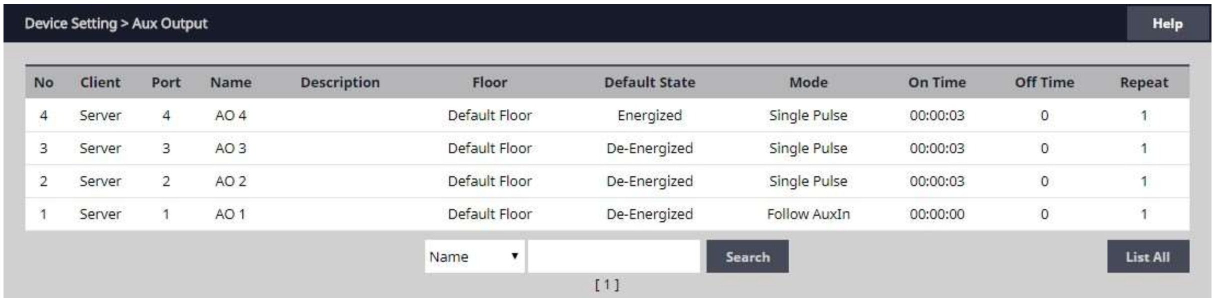
No	Client	Port	Name	Description	Floor	Input Type
4	Server	4	AI 4		Default Floor	NO Unsupervised
3	Server	3	AI 3		Default Floor	NO Unsupervised
2	Server	2	AI 2		Default Floor	NO Unsupervised
1	Server	1	AI 1		Default Floor	NO Series Resistor

1. Select the desired input and click **Edit**.
2. Enter a desired **Name** and **Description** (optional) for the input.
3. Assign the input to a **Floor** for viewing on the Dashboard.
4. Select the appropriate **Input Type** for the input. This setting will be determined by the wiring and type of switch connected to the input (NC or NO, supervised or unsupervised).
5. Click **Save**.

Aux Output

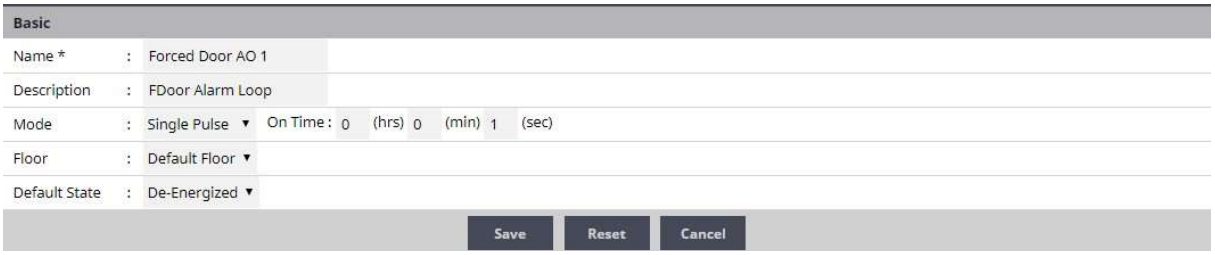
Aux Output displays the outputs that are assigned to the system. Click on the output name to view or edit the settings of the output.

Editing an Output



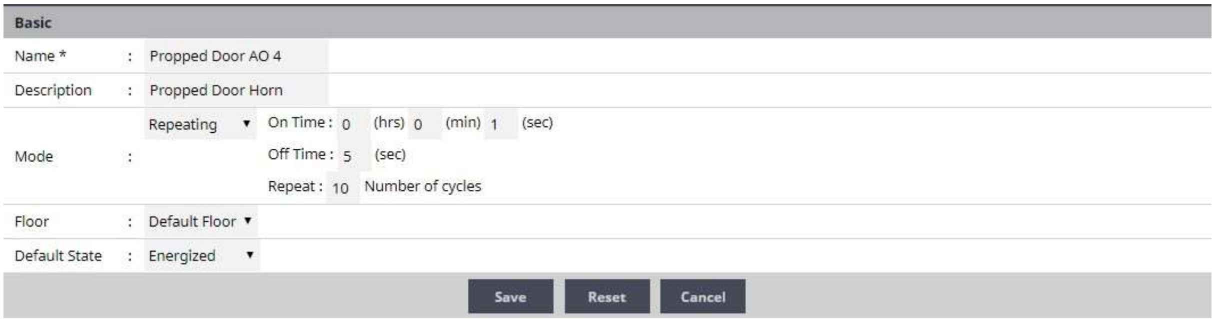
Device Setting > Aux Output

No	Client	Port	Name	Description	Floor	Default State	Mode	On Time	Off Time	Repeat
4	Server	4	AO 4		Default Floor	Energized	Single Pulse	00:00:03	0	1
3	Server	3	AO 3		Default Floor	De-Energized	Single Pulse	00:00:03	0	1
2	Server	2	AO 2		Default Floor	De-Energized	Single Pulse	00:00:03	0	1
1	Server	1	AO 1		Default Floor	De-Energized	Follow AuxIn	00:00:00	0	1



Basic

Name *	:	Forced Door AO 1
Description	:	FDoor Alarm Loop
Mode	:	Single Pulse ▾ On Time : 0 (hrs) 0 (min) 1 (sec)
Floor	:	Default Floor ▾
Default State	:	De-Energized ▾



Basic

Name *	:	Propped Door AO 4
Description	:	Propped Door Horn
Mode	:	Repeating ▾ On Time : 0 (hrs) 0 (min) 1 (sec) Off Time : 5 (sec) Repeat : 10 Number of cycles
Floor	:	Default Floor ▾
Default State	:	Energized ▾

1. Select the desired output and click **Edit**.
2. Enter a desired **Name** and **Description** (optional) for the output.
3. Configure the **Mode** of the output:

· **Single Pulse:** Output latches in response to a valid event for the time entered.

· **Repeating:** Output opens and closes in a cycle for the time entered.

· **E-On:** Will latch the output ON when activated from the dashboard. Press Stop on dashboard turn output OFF. · **E-Off:** Will latch the output OFF when activated from the dashboard. Press Stop on dashboard to turn output back ON.

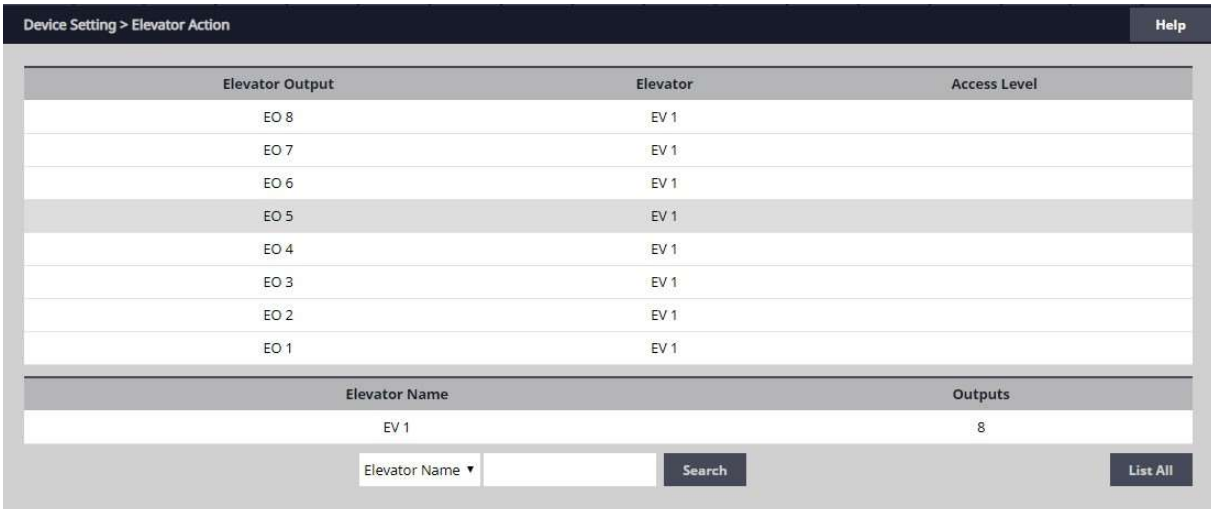
4. Assign the output to a **Floor** for viewing on the Dashboard.
5. Select the **Default State** of the output (energized or de-energized).
6. Click **Save**.

Elevator Action

Optional Feature

Elevator Action allows the operator to assign the elevator outputs to Access Levels.

Adding an Elevator Action



Elevator Output	Elevator	Access Level
EO 8	EV 1	
EO 7	EV 1	
EO 6	EV 1	
EO 5	EV 1	
EO 4	EV 1	
EO 3	EV 1	
EO 2	EV 1	
EO 1	EV 1	

Elevator Name	Outputs
EV 1	8

1. Select an elevator output from the list and click **Edit**.
2. Enter a name and additional information as required.

✓ ***NOTE:*** *In order to activate floors, first assign an access level to doors.*

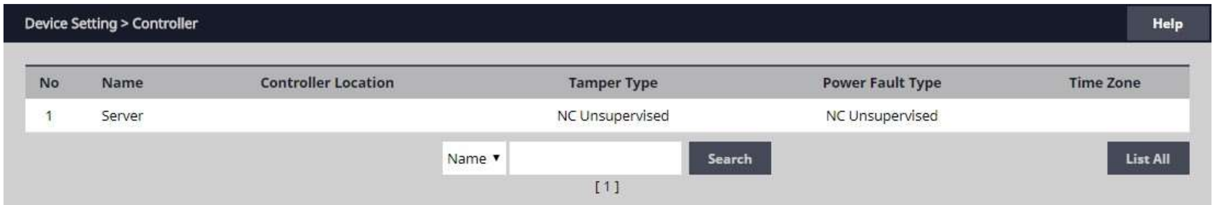
3. Select the Access Level that will be used to grant access to the floor(s). (Doors must be assigned to the Access Level for the Access Level to be active).
4. Click **Save** to save the changes.

✓ ***NOTE:*** *When a valid credential is presented to the reader, the elevator outputs will be activated as configured in the Elevator Action. For example, if Elevator outputs EO 1, EO 2, EO 3 and EO 4 are assigned to Floors 1-4 Access Level, all four outputs will activate when the valid credential is presented. This allows the Card Holder to select floors 1-4 in the elevator cab.*

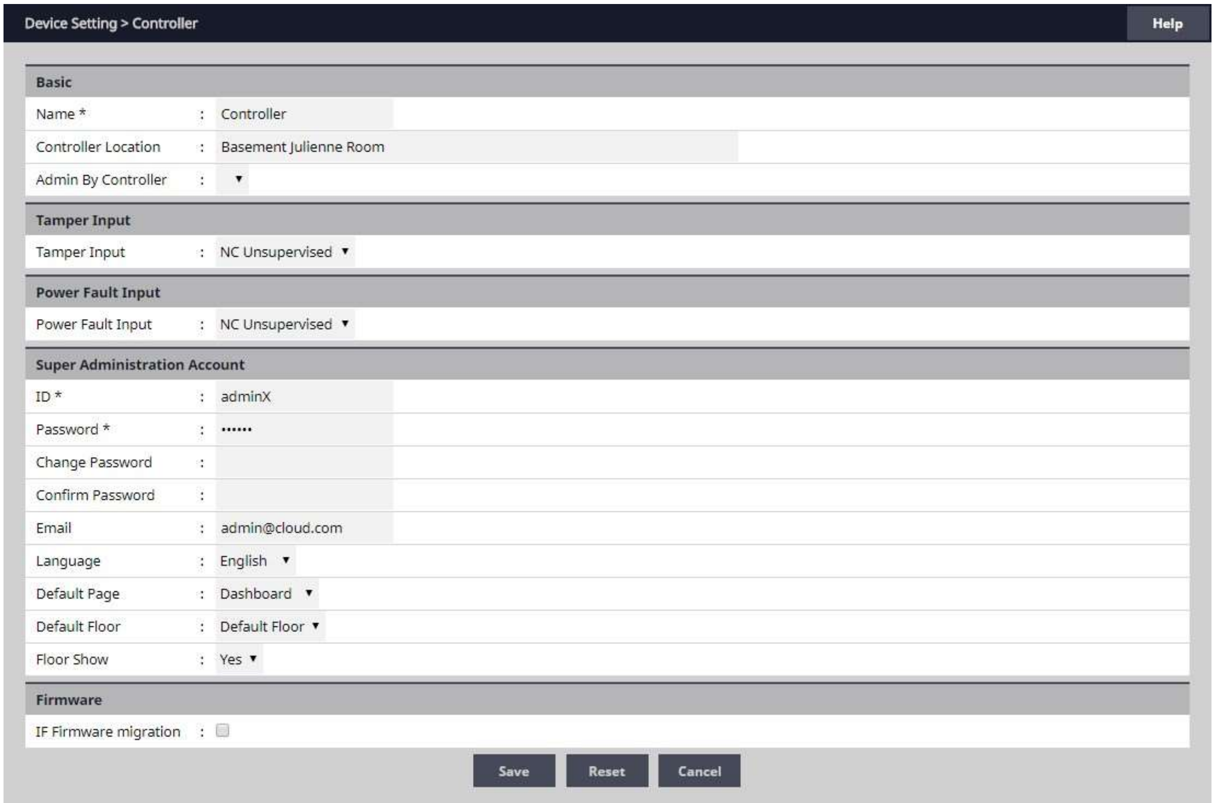
Controller

Controller displays information pertaining to each system Controller. Click on the Controller name on the list to view or edit information.

Editing the Controller Info



No	Name	Controller Location	Tamper Type	Power Fault Type	Time Zone
1	Server		NC Unsupervised	NC Unsupervised	



Basic		
Name *	:	Controller
Controller Location	:	Basement Julienne Room
Admin By Controller	:	▾
Tamper Input		
Tamper Input	:	NC Unsupervised ▾
Power Fault Input		
Power Fault Input	:	NC Unsupervised ▾
Super Administration Account		
ID *	:	adminX
Password *	:	••••••
Change Password	:	
Confirm Password	:	
Email	:	admin@cloud.com
Language	:	English ▾
Default Page	:	Dashboard ▾
Default Floor	:	Default Floor ▾
Floor Show	:	Yes ▾
Firmware		
IF Firmware migration	:	□

1. Select the Controller and click **Edit**.

2. Enter a desired name and location (optional).

3. Select the appropriate **Tamper Input** value. This will be determined by the wiring configuration of the input. 4. Select the appropriate **Power Fault Input** value. This will be determined by the wiring configuration of the input.

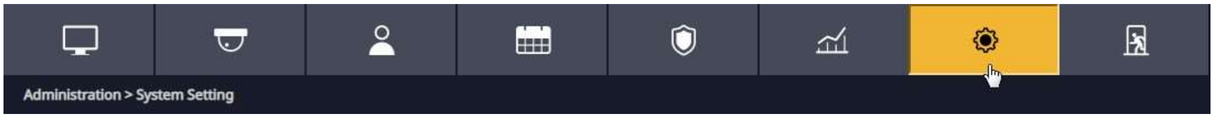
5. Enter the **ID** and **Password** of the **Super Administration Account**. This is the top-level administration account for the Controller.

6. Set the default language, page and floor for the account.

7. Click **Save**.

✓ ***IMPORTANT!*** *It is highly advised to change the Super Administrator password. Keep it in a safe place. This password cannot be recovered if it is lost or forgotten.*

Region

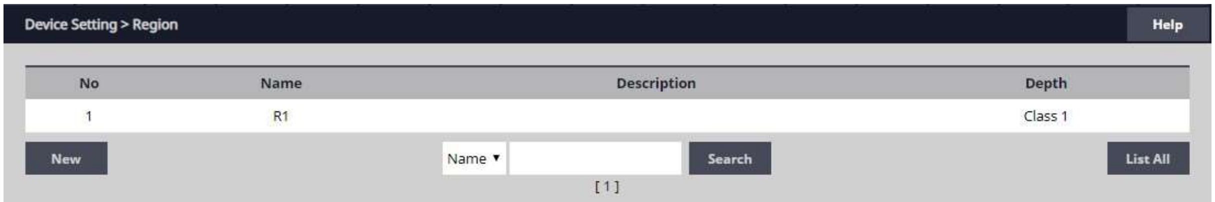


Administration > System Setting

A ***Region*** is an area (a “zone”) you want to limit security into and/or out of. Entering or exiting a Region occurs through controlled door access. The In Reader and Out Reader (if used) for a door can each be assigned a Region.

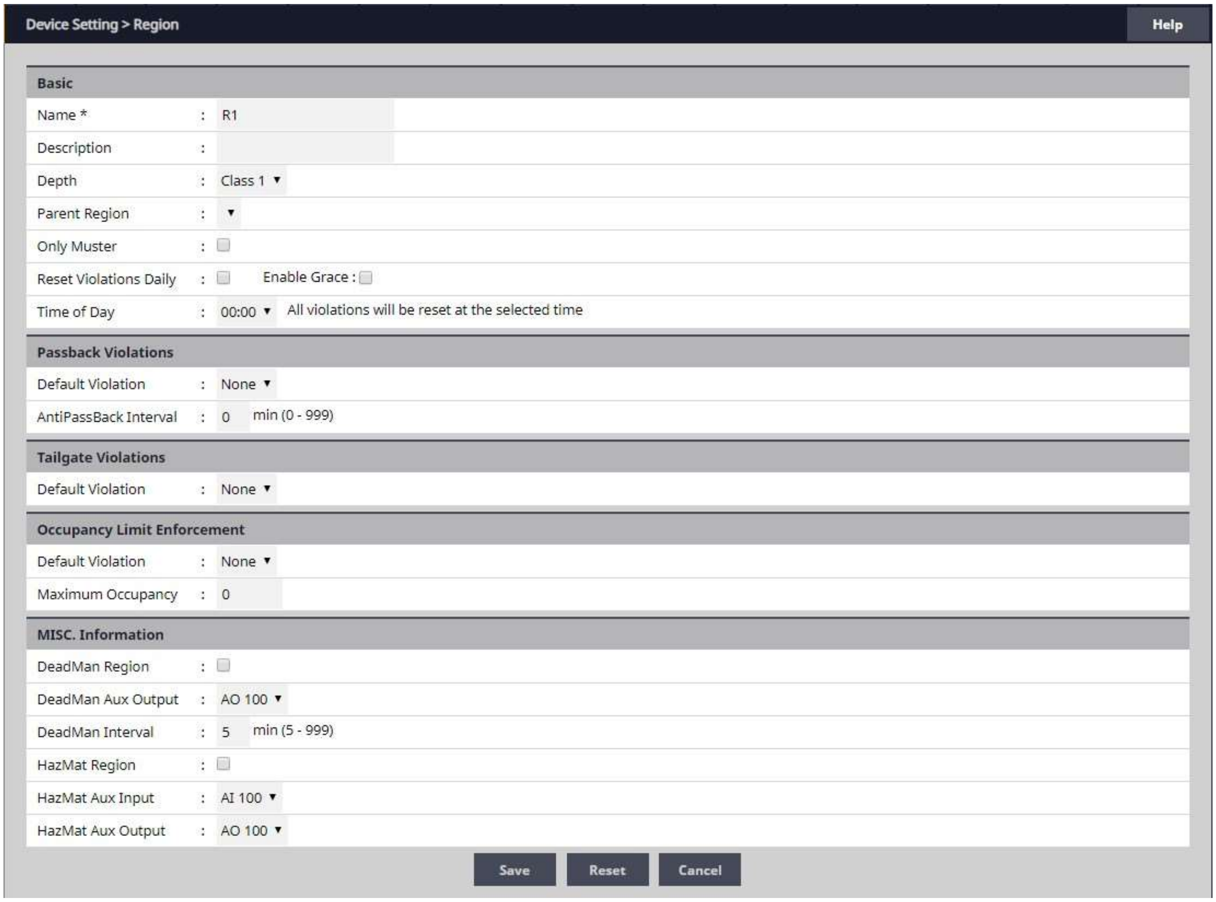
The primary usage for Regions is to count or control occupancy and implement door access sequence rules to prevent or track access to areas if the correct door access sequence is not met.

A Region can contain up to five nested partitions called “Sub Regions” and “Child Regions”, each controlling access to a sub-section of the “Parent” Region.



Device Setting > Region

No	Name	Description	Depth
1	R1		Class 1



Device Setting > Region

Basic

Name *	:	R1
Description	:	
Depth	:	Class 1 ▾
Parent Region	:	▾
Only Muster	:	□
Reset Violations Daily	:	□ Enable Grace : □
Time of Day	:	00:00 ▾ All violations will be reset at the selected time

Passback Violations

Default Violation	:	None ▾
AntiPassBack Interval	:	0 min (0 - 999)

Tailgate Violations

Default Violation	:	None ▾

Occupancy Limit Enforcement

Default Violation	:	None ▾
Maximum Occupancy	:	0

MISC. Information

DeadMan Region	:	□
DeadMan Aux Output	:	AO 100 ▾
DeadMan Interval	:	5 min (5 - 999)
HazMat Region	:	□
HazMat Aux Input	:	AI 100 ▾
HazMat Aux Output	:	AO 100 ▾

Region Rules Overview

· Regions contain Credentials that are owned by Card Holders. Because Card Holders can have multiple

Credentials, a Card Holder could exist in multiple Regions at the same time but a Credential can only exist in one Region at a time.

· Once the Card Holder enters a Region, they remain in the Region for occupancy until they enter another Region or exit the Region by presenting a Credential on the out reader.

· A Region can contain Sub Regions and Child Regions that are contained inside the main Region.

· Anti Passback and Tailgating rules are applied to Regions.

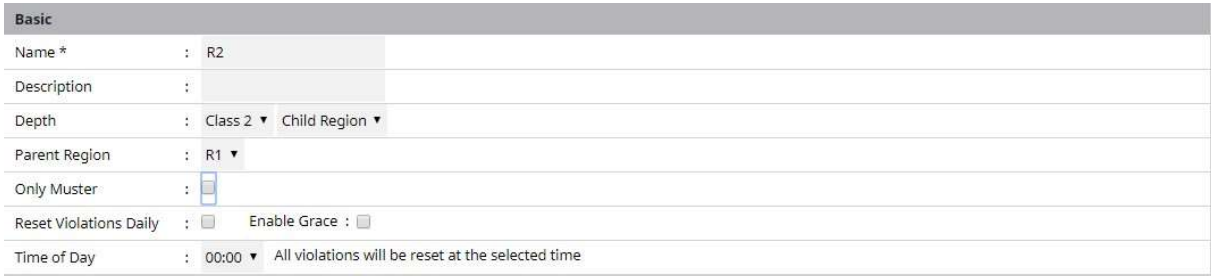
· A maximum of 125 Regions are supported on a system.

Examples of Regions

Regions should be programmed to suit the controlled access requirements and the expected Card Holder locations as they move about the installation.

· Example 1: A company has a room with its building that is used to store hazardous chemicals. That room can become a Hazardous Region within the Building Region and restrict access to a limited number of Card Holders. · Example 2: A company has four buildings at its facility. By making each a Region and using occupancy, an administrator can locate what building a Card Holder is in if there is an emergency.

Child Regions



Basic		
Name *	:	R2
Description	:	
Depth	:	Class 2 ▼ Child Region ▼
Parent Region	:	R1 ▼
Only Muster	:	□
Reset Violations Daily	:	□ Enable Grace : □
Time of Day	:	00:00 ▼ All violations will be reset at the selected time

A Child Region follows the definition of a Region with these exceptions:

· A Child Region cannot have an occupancy limit, only a Parent or Sub Region can have an occupancy limit. · The Card Holder does appear in the Child Region on the Occupancy Report. See Occupancy for more information.

· Normally, a Child Region will be fully contained within the Parent Region but the rules do not restrict this · A Child Region is logically contained inside of it Parent Region. This means if the Card Holder in the Child Region, they are, for occupancy, in the Parent Region.

· Anti Pass Back and Tail Gating rules can be applied to Child Regions · There is a maximum of 20 Child Regions per Region.

· There is a maximum of 250 total Child Regions per system.

Child Region Notes

·Under the Region setting for the Door - A Child of a Parent would be a Class 2. A Child of a Child would be Class3.etc. When a Class other than Class 1 is selected, the Parent Region option will turn into a drop down list.

· Specify the Parent Region for this Child Region from the drop down list

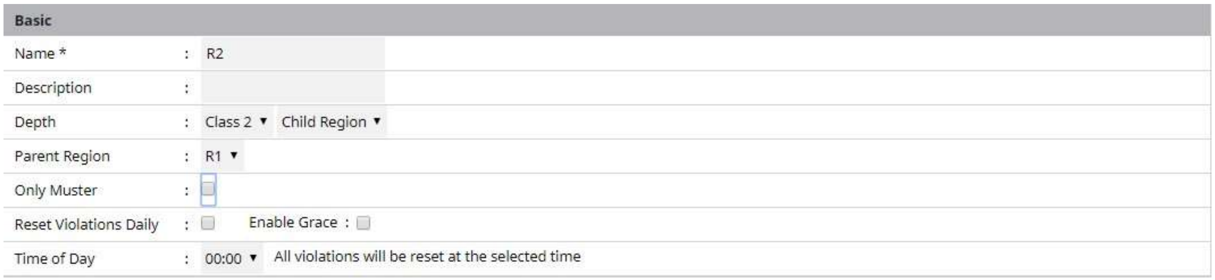
Sub Regions

Sub Regions function the same as Child Regions, except for occupancy counting. Sub Regions can report occupancy counts of the Sub Region as well as contribute to the occupancy count of the Parent Region.

Adding or Editing a Region

1. Click New to add a region or click Edit to modify a region.

Basic



Basic

Name *	:	R2
Description	:	
Depth	:	Class 2 ▾ Child Region ▾
Parent Region	:	R1 ▾
Only Muster	:	□
Reset Violations Daily	:	□ Enable Grace : □
Time of Day	:	00:00 ▾ All violations will be reset at the selected time

2. For the Region's **Name**, enter up to 30characters.

3. In the **Description** field, enter a short description of the Region.

4. Select the **Depth** for the Region. Class1 is the highest. Class 2 through Class5 are Sub Regions or Child Regions, each sub Class must physically reside inside the next lower number Class number around it.

5. If **Parent Region** is left empty (the default) the Region becomes the Parent Region. If the Region is Class2-5, select Sub Region or Child Region's the **Parent Region**.

6. If the Region is used only for Muster Station personnel assembly, check **Only Muster**. The remaining Region options are not used or available when Only Muster is selected.

Muster Region Notes

· A Muster Region is a Region used as a centralized place to do a roll call.

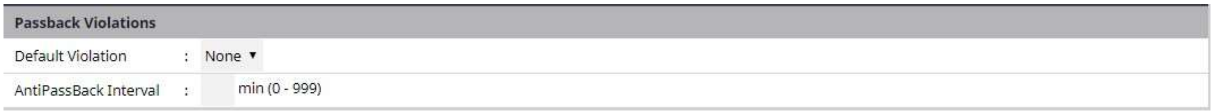
· A Muster Region will remove Card Holders from their currently occupied Region and place them in the Muster Region where the reader is at.

· Maximum number of Muster Regions 125.

· A Muster Region is attached to an In/Out set of readers for a door (both readers must be defined to the Region). · A Muster Region is valid for the entire site. It is possible to have multiple Muster Regions but they all serve in parallel for the entire site. For instance, each building of a site could have its own Muster Reader but a Card Holder could go to any of the Muster stations to check in.

· A Muster Region cannot contain another Muster Region.

Passback Violations



Passback Violations

Default Violation	:	None ▾
AntiPassBack Interval	:	min (0 - 999)

Anti Pass Back is intended to prevent Card Holders from sharing credentials to gain access. With timed anti passback, a ***Passback Violation*** event occurs when the same credential is used to request access to the same door or region more than once during a set period of time.

1. Select the level for the **Default Violation**.

· **None:** Timed Anti Passback is not in use (default setting).

· **Soft:** Triggers an alarm then grants access if the Anti Passback time interval has not expired before the credential was used at the same reader again.

· **Hard:** Triggers an alarm and prevents access if the Anti Passback time interval has not expired before the credential was used at the same reader again.

2. Enter the number of minutes (0-999) for **Anti Passback** Interval. This is the length of time that presenting the same credential again will cause an anti passback violation. Check the **Enable Grace** checkbox to allow the administrator to permit grace for the Card Holder in case of an anti passback violation.

✓ ***NOTE:*** *Selecting 0 minutes for the Anti Passback Interval allows no time and effectively disables the Passback Violation for the region. Don't set it to 0 and expect Anti Passback to function properly.*

3. To minimize clutter on the Grace Screen, check the **Reset Violations Daily** checkbox to clear all Passback Violations for the Region once a day.

4. When Reset Violations Daily is enabled, select the **Time of Day** for the reset to occur.

Passback Violation Operation Notes

·Presenting a credential again before the timer has expired will restart the timer.

·Timed Anti Passback is for In Readers only, it has no effect on Out Readers.

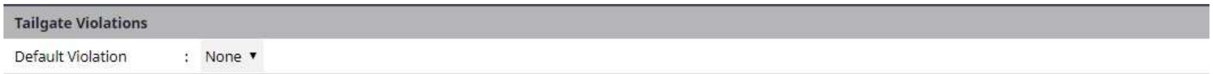
·If the Card Holder exits the Region through an Out Reader, the timer is reset and stopped.

·When Enable Grace is set, Card Holders can only re-enter the Region by properly exiting the Region first or by beingGraced in.

·The log message for a Passback Violation is "Denied Region Anti Passback Violation".

·Anti Passback can also be set for a door not assigned to a Region using the Door setup menu, but if the door is later assigned to a Region, the Region Anti Passback setting will override the door setting.

Tailgate Violations



Tailgate Violations

Default Violation : None ▾

A ***Tailgate Violation*** occurs when an authorized Card Holder is granted access and one or more persons pass through the open controlled access point in addition to the authorized Card Holder. Tailgating is detected when a Card Holder tries to exit a Region, or enter another Region, from a Region which they were never granted access to enter.

1. Select the level for the **Default Violation**.

· **None:** Tailgating feature is turned off (default setting).

· **Soft:** Triggers an alarm then grants access.

· **Hard:** Triggers an alarm and prevents access through the Out Reader and/or the In Reader of a sub Region.

Tailgate Violation Operation Notes

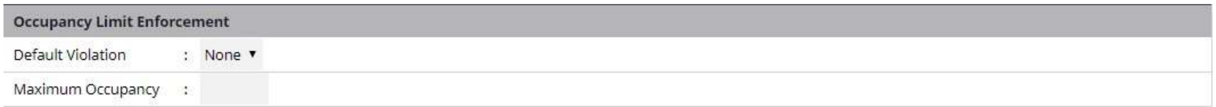
· In the Door setup menu, the Out Reader Region must be set to the Region with the Tailgate Default Violation turned ON.

· Hard Tailgating is only for the most secure facilities and requires In Readers and Out Readers at all doors.

· With Hard Tailgating, if a Card Holder leaves a Region by any other means than authorized controlled exiting, a Tailgate Violation will occur at any other door until either (1) the Card Holder presents their credential to a Muster Reader (this removes the Tailgate Violation and adds the Card Holder to the Muster Region), or (2) the Card Holder is Graced by the system administrator using the Grace Tab on the Dashboard (they will be placed in the Region where they swiped their card to enter), or (3) the Card Holder can somehow get back into the Region the system thinks they Occupy and then exit that Region correctly.

· Hard Tailgating applies to the Region the system thinks the Card Holder is in and will deny access to any other non-connected Region. For example, suppose there are two separate buildings, Bldg1 is Region 1 with Hard Tailgating, Bldg2 is Region 2 with Soft Tailgating. If the Card Holder enters Bldg 1 and occupies Region 1, then leaves Bldg 1 without being granted exit access, the Card Holder will be denied access to any other door (trying to re-enter Bldg1, entering or exiting Bldg 2). However, if the Card Holder enters Bldg 2 first and Occupies Region 2, then leaves Bldg 2 without being granted exit access, the Card Holder will create a warning but will be allowed access into either building.

Occupancy Limit Enforcement



Occupancy Limit Enforcement

Default Violation : None ▾

Maximum Occupancy :

Occupancy Limit Enforcement counts and/or limits (restricts) the number of Card Holder credentials that can occupy a given Region at the same time.

The log message for an Occupancy Limit violation is “Access Denied Occupancy Limit Violation”.

1. Select the level for the **Default Violation**.

· **None:** The Controller counts occupancy, but no action results (default setting).

· **Soft:** When a Card Holder presents credentials to enter the Region and the occupancy limit has been reached, an alarm activates and the Card Holder is granted access. An alarm will continue to activate for each new Card Holder that presents credentials until the occupancy count falls under the Maximum Occupancy number. · **Hard:** When a Card Holder presents credentials to enter the Region and the occupancy limit has been reached, an alarm activates and the Card Holder is denied access.

2. Enter the **Maximum Occupancy** number (0-99999) allowed in the Region. (Entering 0 results in no occupancy limit, the Controller just counts occupancy.)

Occupancy Rules

·When a Card Holder presents a credential to a reader and is granted access, the Card Holder credential enters into the Region specified by the In Reader and exits the Card Holder credential from all other Regions.

·A Card Holder credential can only exist in one Region at a time.

·A Card Holder may occupy multiple regions if they are assigned multiple credentials.

·A Child Region cannot have an Occupancy Limit because its occupancy count is included as part of its Parent Region.

Region Occupancy Counting

·The occupancy count for a Region is the sum of the occupancy count for the Region plus any Child Regions or Sub Regions, which in turn may have Children or Sub Regions of their own.

·When a Card Holder credential enters a Region, the occupancy count for that Region increases by 1.

·When a Card Holder credential exits a Region, the occupancy count for that Region decreases by 1.

·The Occupancy count can never go below 0.

Occupancy Limit Enforcement Notes

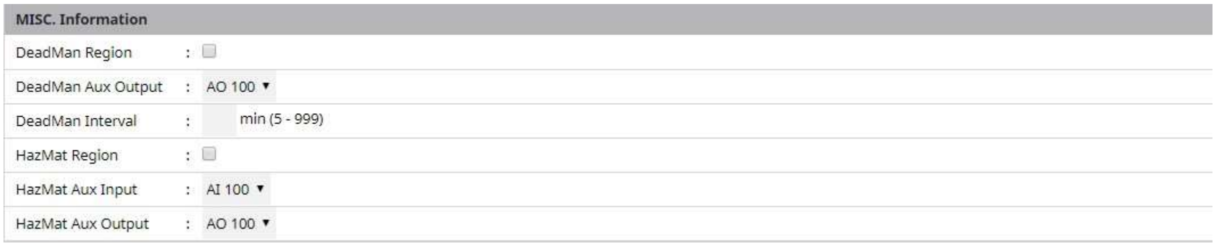
· For occupancy counting to work effectively, both In Readers and Out Readers must be used.

· An Out Reader cannot be in an uncontrolled space (no Region assigned) unless the In Reader is also in an uncontrolled space (means it is not connected to a Region).

· The In Reader and Out Reader cannot be the same device unless they are both setup as in an uncontrolled space or a Muster Region.

· Card Holders with the Exempt option enabled still obey the occupancy limit enforcement rules.

· A denied access attempt at an occupied Region does not restrict the Card Holder from entering other Regions with normal access.



MISC. Information		
DeadMan Region	:	☐
DeadMan Aux Output	:	AO 100 ▾
DeadMan Interval	:	min (5 - 999)
HazMat Region	:	☐
HazMat Aux Input	:	AI 100 ▾
HazMat Aux Output	:	AO 100 ▾

Deadman Region

A ***Dead Man*** region requires each Card Holder, after entering the region to periodically check in for safety reasons. Card Holders are issued a normal card to enter and exit the region and a special "Dead Man Card" to indicate activity An alarm will activate after the Card Holder's DeadMan Interval has expired unless they have:

✓Swiped their Dead Man Card a tone of the Dead Man Regions Out Readers. This will reset the timer to the DeadMan Interval for that Card Holder.

✓Exited the Region using their normal card. This will cancel the timer for that Card Holder.

✓Swiped their normal card at a Muster station. This will cancel the timer for that Card Holder.

Once the alarm has been activated, the alarm may be deactivated by:

✓Card Holder swiping their Dead Man Card at one of the Dead Man Regions Out Readers. This will reset the timer to DeadMan Interval for that Card Holder. It may or may not turn off the alarm.

✓Card Holder exiting using their normal card. This will cancel the timer for that Card Holder. It may or may not turn off the alarm.

✓Card Holder swiping their normal card at a Muster station. This will cancel the timer for that Card Holder. It may or may not turn off the alarm.

✓System Administrator Acknowledges the alarm. This will deactivate the alarm even if all Card Holder alarm triggers have not been cleared.

If multiple Card Holder have triggered the Dead Man Alarm, then only when the last Card Holder has been cleared will the alarm be deactivated.

Creating a Dead Man Region

1. Check the DeadMan Region checkbox to create a Dead Man Region.
2. Enter a time in minutes (5-60) for the DeadMan Interval. The default is 5 minutes.

Dead Man Region Notes

· In the Door setting for the reader in the Dead Man Region, the Out Reader Region must be set to the Region defined as a Dead Man region.

A ***HazMat Region*** can be locked down to prevent entry and exit in case of hazardous materials emergency. When the selected AUX input is triggered, all doors associated with the HazMat Region will be locked and all access in and out of the HazMat Region will be denied until the selected AUX input has returned to normal. After a HazMat alarm has been triggered, a HazMat Unlock Card is required to cancel the alarm.

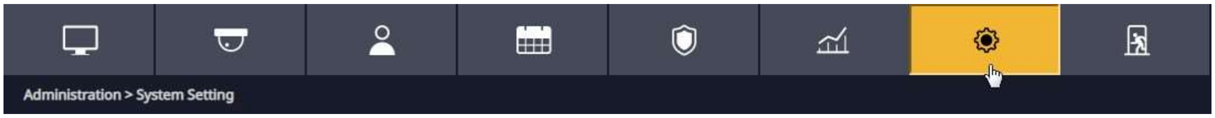
Creating a HazMat Region

1. Check the **HazMat Region** checkbox to create a HazMat Region.
2. For the HazMat Input, select the Auxiliary Input (1-4) that the trigger device is connected to.

HazMat Region Notes

· The log message for a hazardous materials alarm is: "Hazmat Region Lockdown [Region Name]".

· For a HazMat Unlock Card, in the Card setting for a Card Holder select HazMat Unlock for the Card Type.



Client Management

Optional Feature

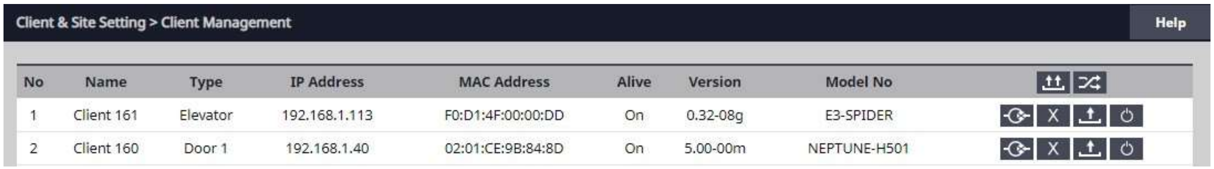
Client Management allows the user to enable/disable, connect/disconnect, and update client Controllers associated to the main Controller's server database.

Client Management allows user to update the firmware of the clients. The firmware for an individual Controller may be updated by clicking the **Update Client** button for the Controller. If multiple Controllers are connected to a main Controller, the **Update All** will update all the clients.

✓ ***NOTE:*** *It will take 2-5 minutes to update each client. During that time the clients will be off-line.*

✓ ***NOTE****: Gateway and DNS IP addresses must be configured to access the Update Server. Refer to IP Address to configure these settings.*

✓ ***WARNING:*** *All Controllers in a system MUST be using the same firmware version.*



No	Name	Type	IP Address	MAC Address	Alive	Version	Model No
1	Client 161	Elevator	192.168.1.113	F0:D1:4F:00:00:DD	On	0.32-08g	E3-SPIDER
2	Client 160	Door 1	192.168.1.40	02:01:CE:9B:84:8D	On	5.00-00m	NEPTUNE-H501

Managing Clients

1. The installed client(s) will be listed in the Client Management section.
2. Use the ***Client Management*** buttons to manage the system clients.

Global Commands

Update All

· Updates all connected Clients

Data Sync

· Re-sends Server Database to all Clients

Client Specific Commands

Client Disconnect

· Disables a client in the Server Database

Client Connect

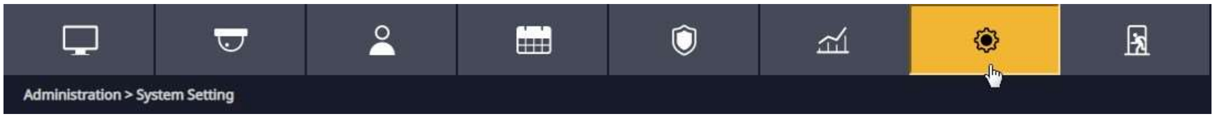
· Enables a client in the Server Database

Delete Client

· Permanently removes Client from Server Database

Update Client

· Updates the selected Client firmware to the latest version



Client Reboot

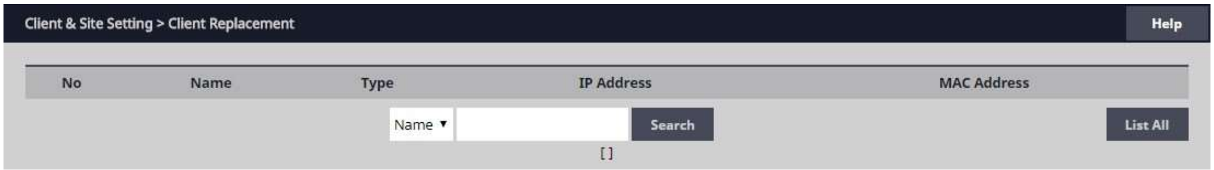
· Reboots selected Client

Client Replacement

Optional Feature

Client Replacement is used when an existing client Controller is replaced with a new client Controller.

Replace a Client



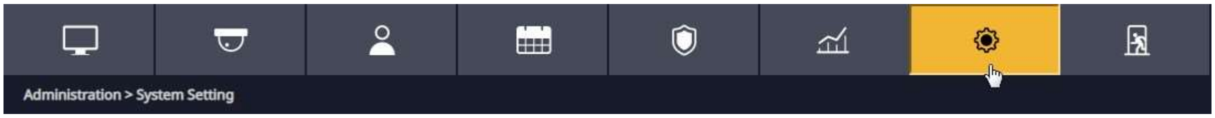
No	Name	Type	IP Address	MAC Address

1. Power off bad Client board and disconnect from network. At the Dashboard the Door and Aux icons are grayed out.
2. Install replacement Client board on the network and set the IP to the same address as the bad client.
3. Save the MAC address of the new client. ✓ ***NOTE:*** *Leave the Server address set to 0.0.0.0*
4. On the Controller, go to Site ***Management*** **>** ***Client Replacement***. Select the IP/MAC of the bad client and click **Edit** button.
5. Change the MAC address to the replacement client
6. Login to the replacement client and set the server IP and click **Save**.
7. After the replacement client connects, the dashboard icons will change from gray to color.

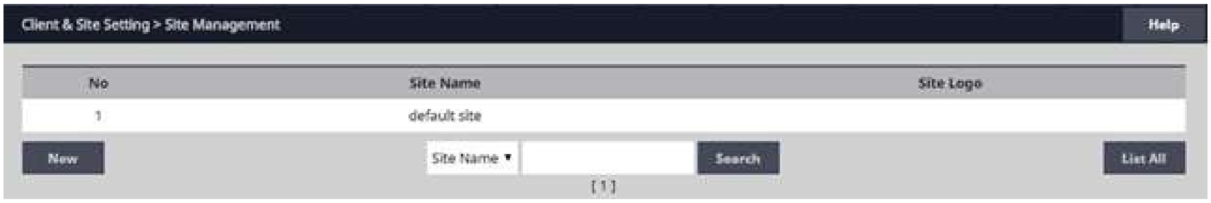
Site Management

Optional Feature

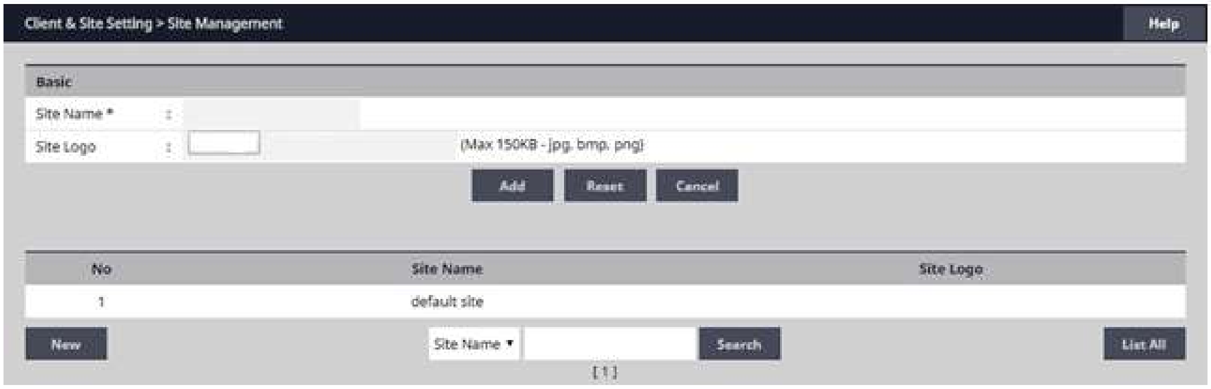
Site Management provides the ability to modify site.



Adding a Site



No	Site Name	Site Logo
1	default site	



Basic

Site Name *	:	
Site Logo	:	(Max 150KB - jpg, bmp, png)

No	Site Name	Site Logo
1	default site	

1. Click **New**.
2. Enter the desired name for the site.
3. To add a logo, click **Choose File** and select the logo file.

✓ ***NOTE:*** *The maximum JPG, BMP, or PNG image size is 685 pixels wide by 340pixels high and the maximum file size is 150KB.*

4. Click **Add** to save the new site.

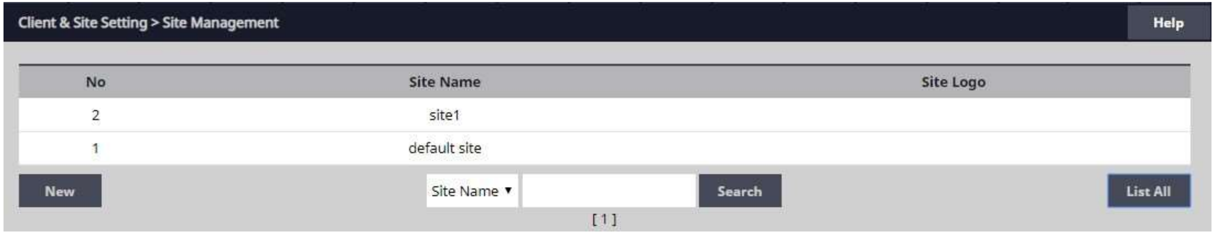
Deleting a Site

1. Select the site to be deleted.

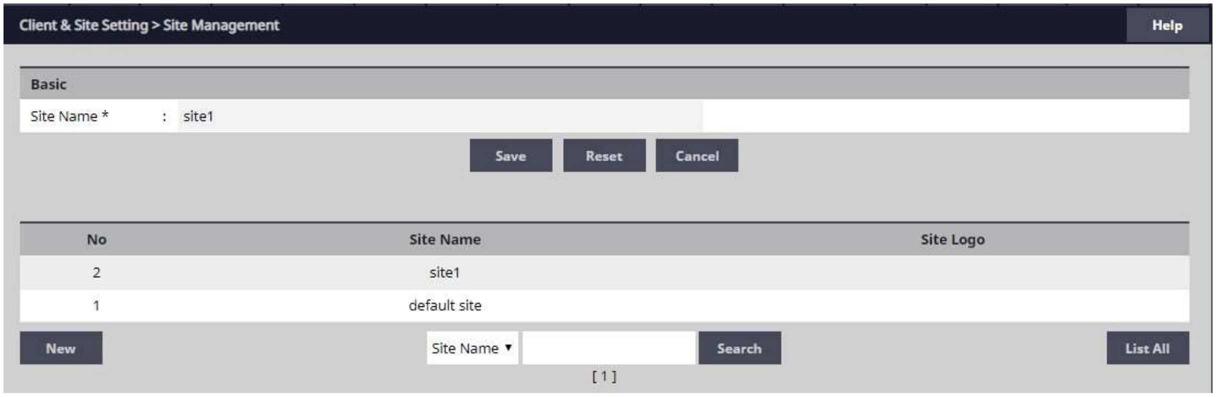
   ✓ ***NOTE:*** *default site cannot be deleted.*

2. The site will appear, click **Delete**.
3. Click **OK** to confirm the deletion.

Editing a Site



No	Site Name	Site Logo
2	site1	
1	default site	



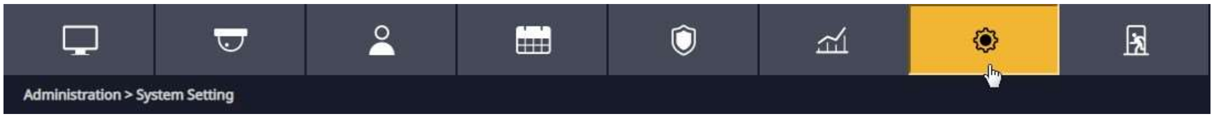
Basic

Site Name * : site1

No	Site Name	Site Logo
2	site1	
1	default site	

1. Select the site to be edited and click **Edit**.
2. Perform the desired changes to the **Site name**.
3. click **Save** to save the changes.

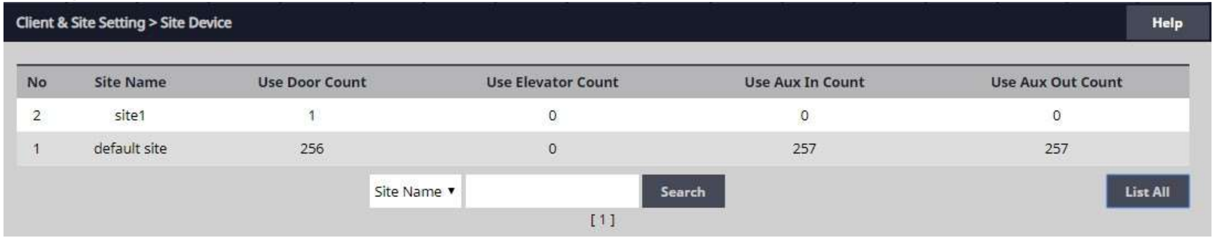
Site Device



Administration > System Setting

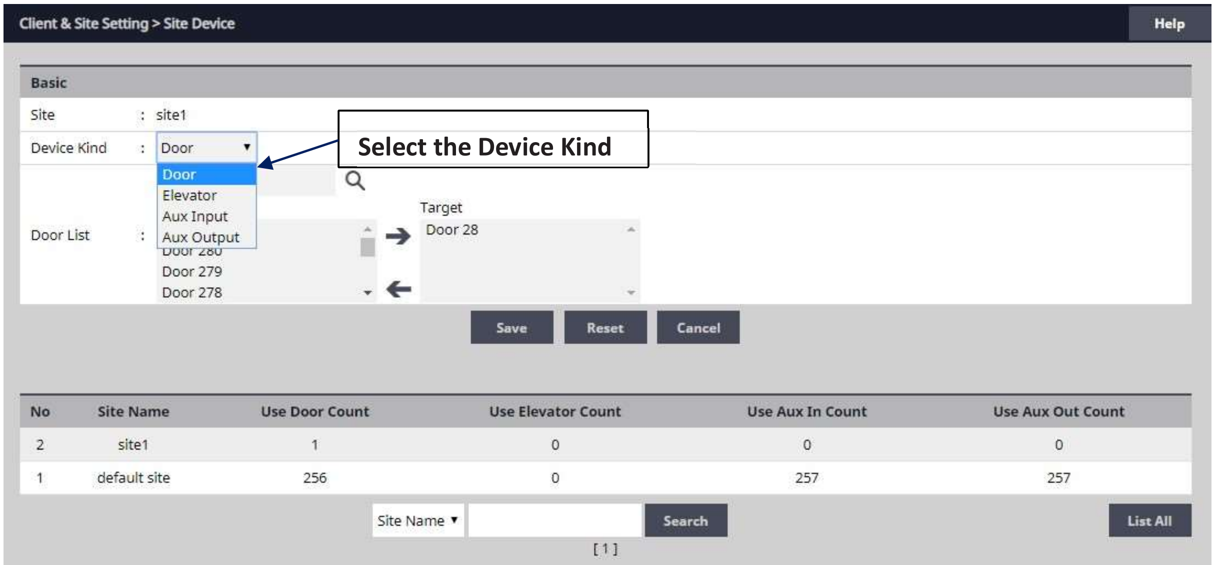
Site device is used to assigns system resources (Doors, AUX Inputs, AUX Outputs, Entire Clients, Access Levels) to sites.

Editing Site Device



Client & Site Setting > Site Device

No	Site Name	Use Door Count	Use Elevator Count	Use Aux In Count	Use Aux Out Count
2	site1	1	0	0	0
1	default site	256	0	257	257



Client & Site Setting > Site Device

Site : site1

Device Kind : Door

Select the Device Kind

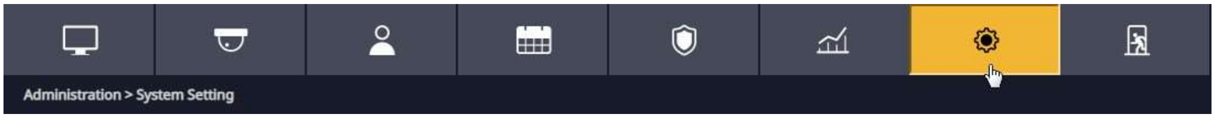
Door List :

No	Site Name	Use Door Count	Use Elevator Count	Use Aux In Count	Use Aux Out Count
2	site1	1	0	0	0
1	default site	256	0	257	257

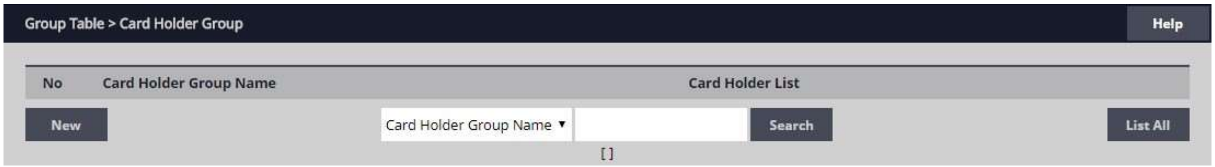
1. Select the site to be edited and click **Edit**.
2. Select the device kind on the Device Kind dropdown.
3. For the Door List, select the desired device.
4. click **Save** to save the changes.

Card Holder Group

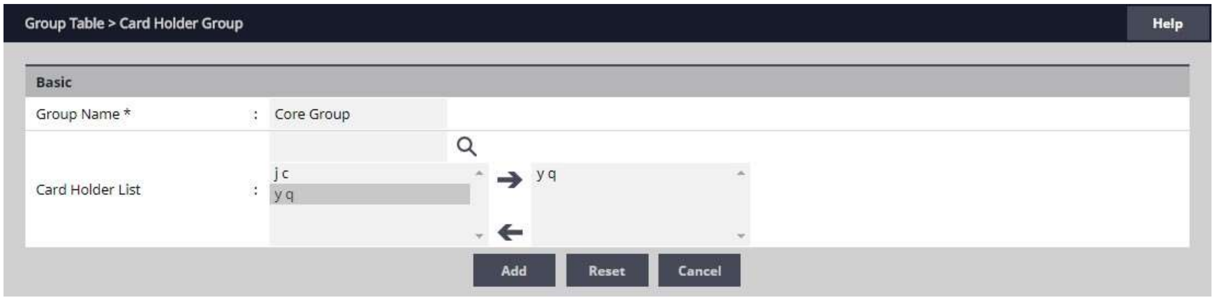
A ***Card Holder Group*** contains individual Card Holders for the purposes of common access and reporting.


Administration > System Setting

Adding a Card Holder Group


Group Table > Card Holder Group

No	Card Holder Group Name	Card Holder List


Group Table > Card Holder Group

Basic

Group Name * : Core Group

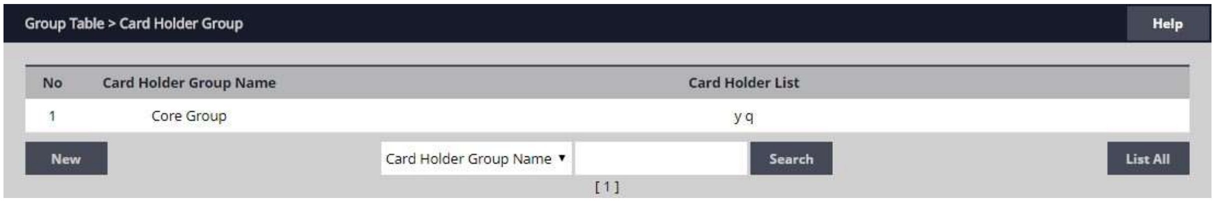
Card Holder List : j c, y q → y q

1. Click **New**.
2. Enter the Card Holder **Group Name**.
3. For **Card Holder List**, select the desired card holders (or use the search icon to find a specific cardholder) and click the right arrow to move them to the field on the right.

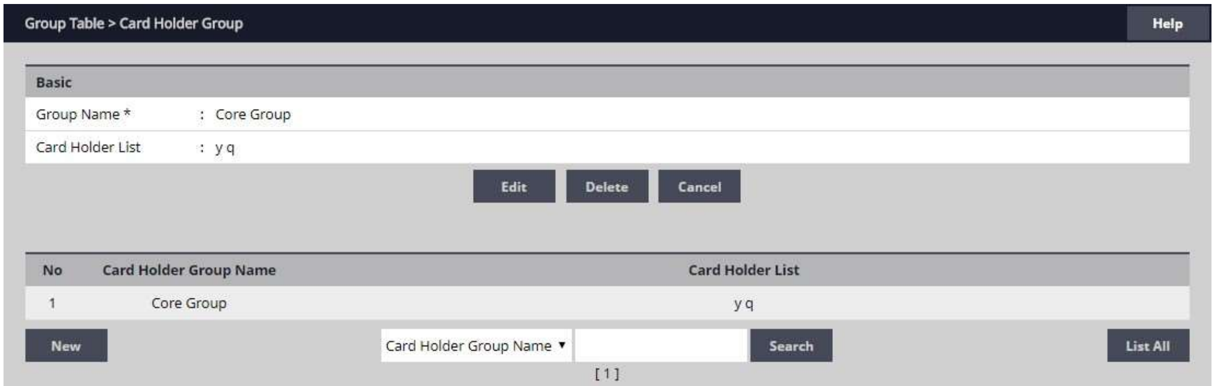
✓ ***NOTE:*** *Ctrl-click or shift-click will select multiple Card Holders.*

4. Click **Add** to save the changes.

Editing a Card Holder Group


Group Table > Card Holder Group

No	Card Holder Group Name	Card Holder List
1	Core Group	y q

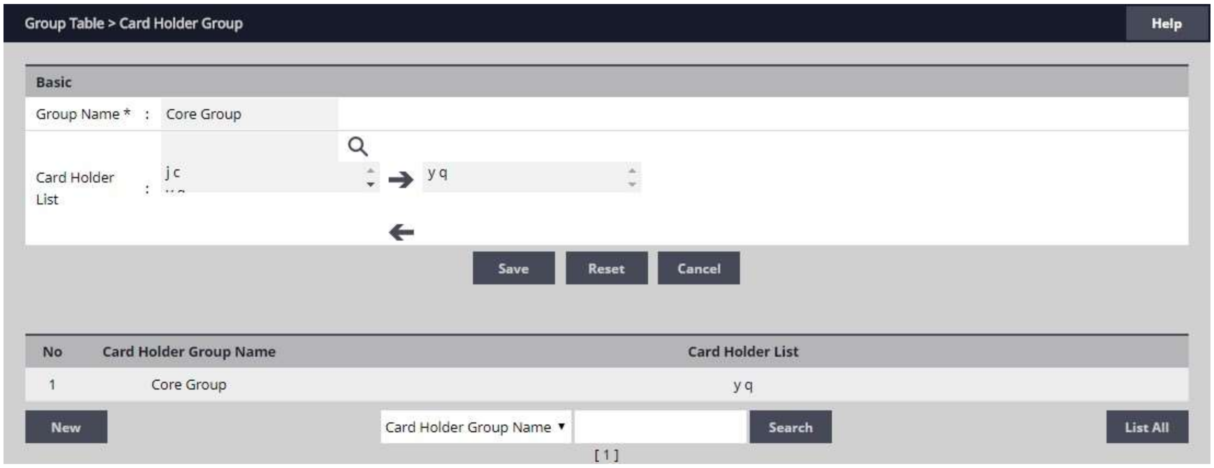

Group Table > Card Holder Group

Basic

Group Name * : Core Group

Card Holder List : y q

No	Card Holder Group Name	Card Holder List
1	Core Group	y q



Basic

Group Name * : Core Group

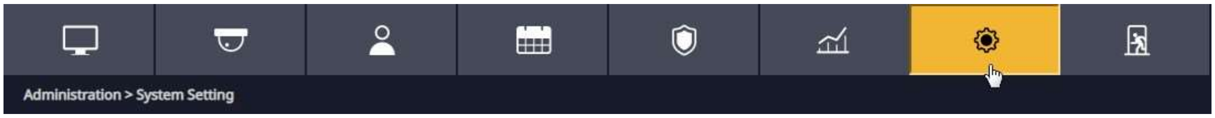
Card Holder List : j c → y q

No	Card Holder Group Name	Card Holder List
1	Core Group	y q

1. Click on the Card Holder Group name to edit.
2. Click **Edit**.
3. The Card Holder Group name can be edited.
4. Card holders can be added or removed from the group.
5. Click **Save**.

Deleting a Card Holder Group

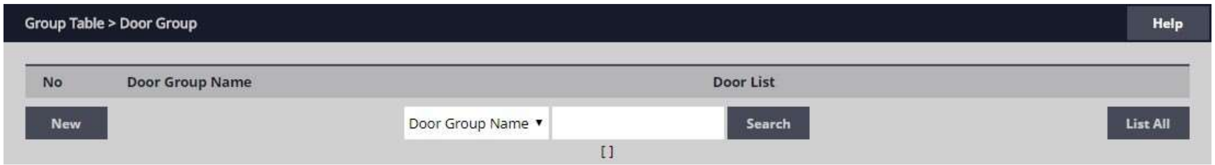
1. Click on the Card Holder Group name to delete.
2. Click **Delete**.

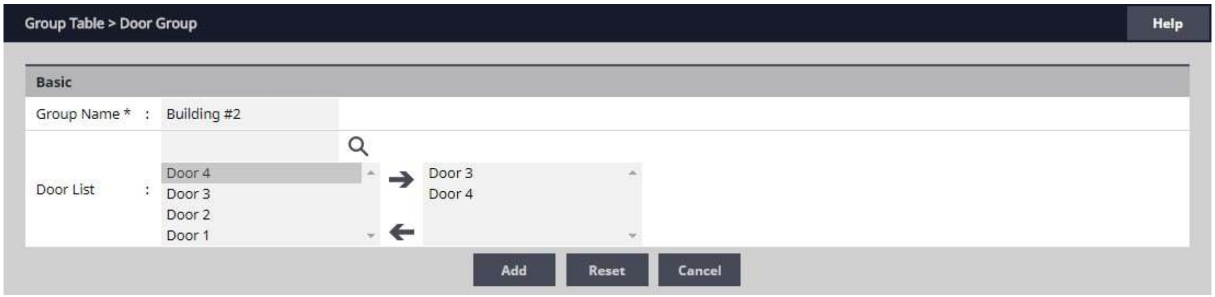


Door Group

The ***Door Group*** allows individual doors to be combined in groups. The group can then be added to an Access Level for simpler management.

Adding a Door Group





Group Name * : Building #2

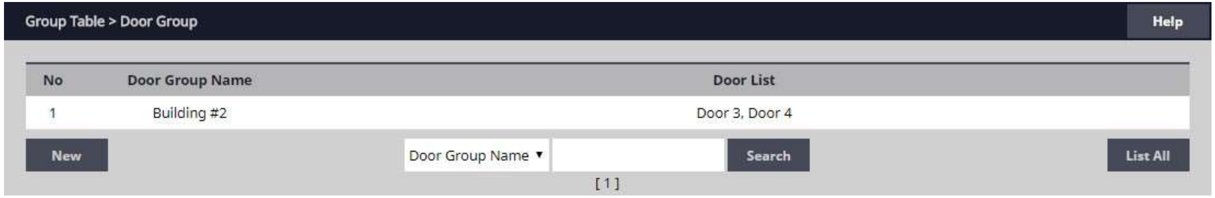
Door List : Door 4, Door 3, Door 2, Door 1 → Door 3, Door 4

1. Click **New**.
2. Enter the desired door **Group Name**.
3. For **Door List**, select the desired doors (or use the search icon to find a specific door) and click the right arrow to move the doors to the field on the right.

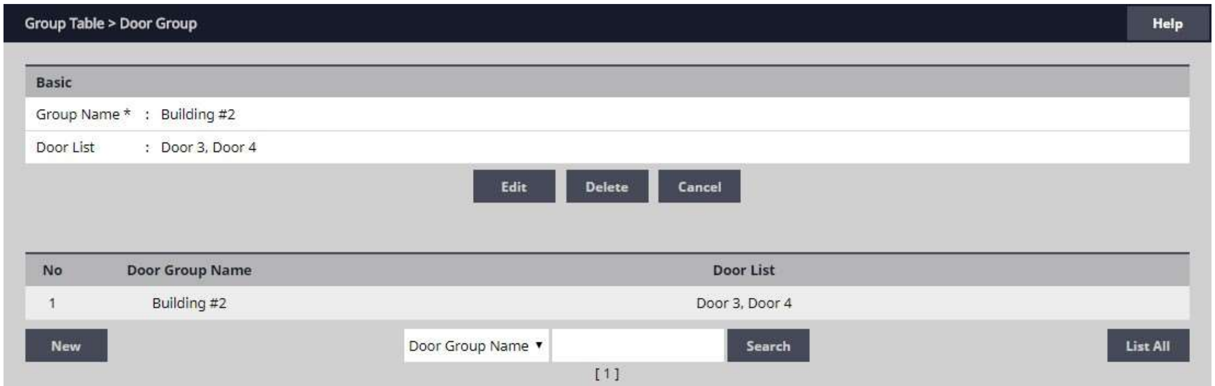
✓ ***NOTE:*** *Ctrl-click or shift-click will select multiple doors.*

4. Click **Add** to save the changes.

Editing a Door Group


Group Table > Door Group

No	Door Group Name	Door List
1	Building #2	Door 3, Door 4

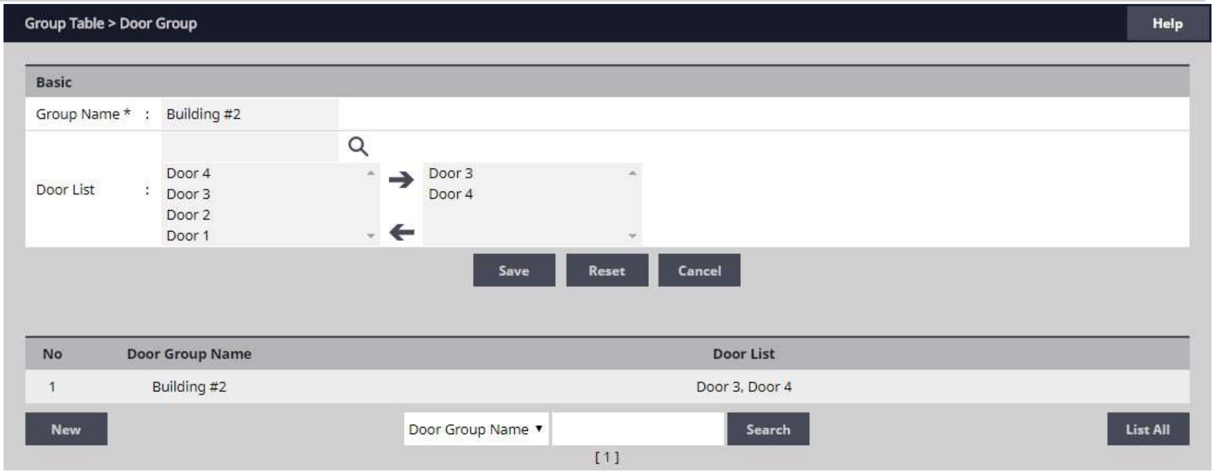

Group Table > Door Group

Basic

Group Name * : Building #2

Door List : Door 3, Door 4

No	Door Group Name	Door List
1	Building #2	Door 3, Door 4


Group Table > Door Group

Basic

Group Name * : Building #2

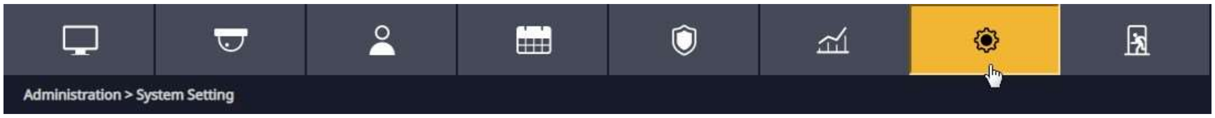
Door List : Door 4, Door 3, Door 2, Door 1 → Door 3, Door 4

No	Door Group Name	Door List
1	Building #2	Door 3, Door 4

1. Click on the Door Group name to edit.
2. Click **Edit**.
3. The Door Group name can be edited.
4. Doors can be added or removed from the group.
5. Click **Save**.

Deleting a Door Group

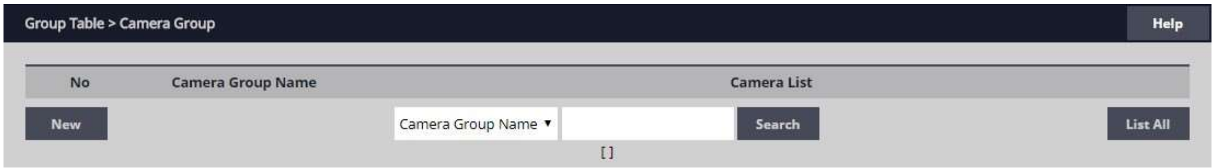
1. Click on the Door Group name to delete.
2. Click **Delete**.

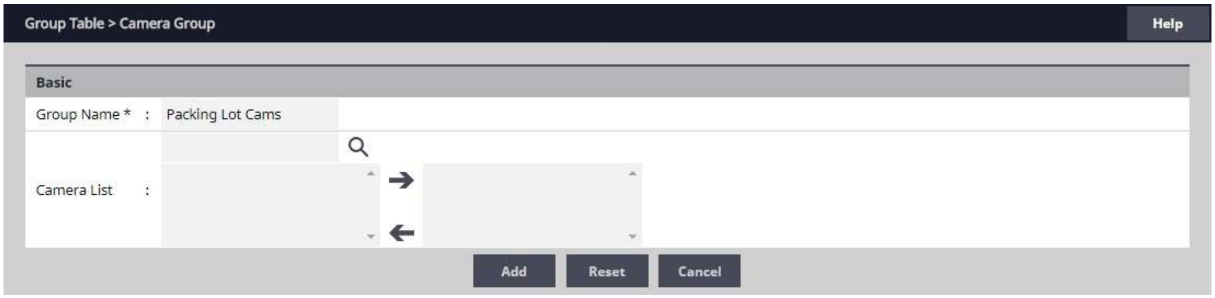


Camera Group

The ***Camera Group*** allows individual cameras to be combined in groups.

Adding a Camera Group





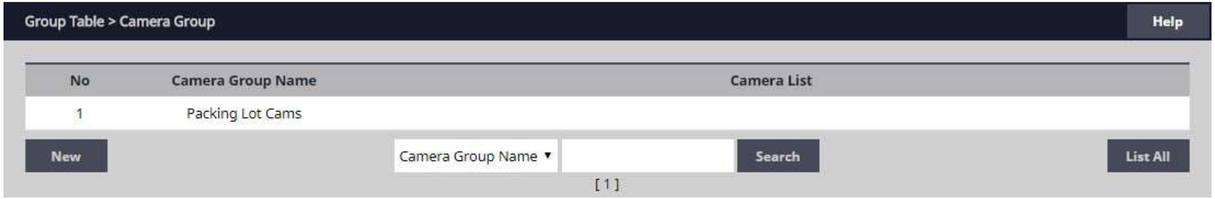
Group Name * : Packing Lot Cams

1. Click **New**.
2. Enter the desired camera **Group Name**.
3. For **Camera List**, select the desired cameras (or use the search icon to find a specific camera) and click the right arrow to move the cameras to the field on the right.

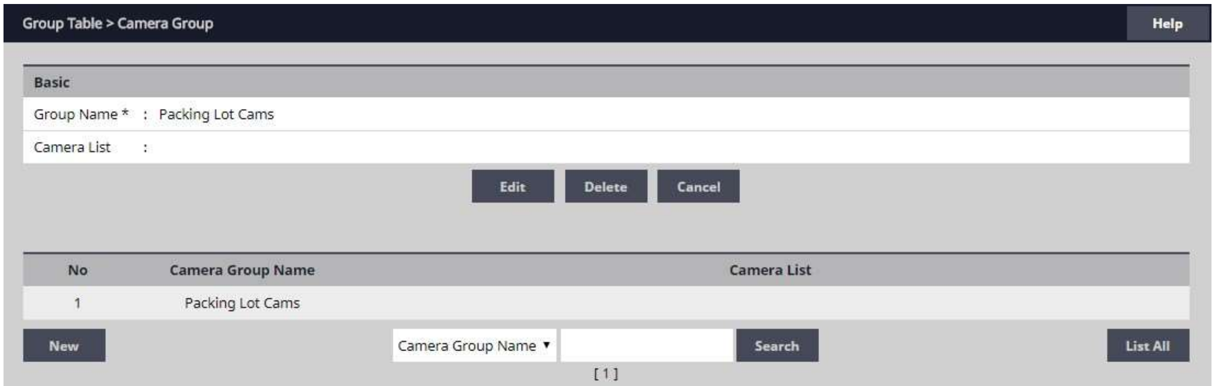
✓ ***NOTE:*** *Ctrl-click or shift-click will select multiple cameras.*

4. Click **Add** to save the changes.

Editing a Camera Group



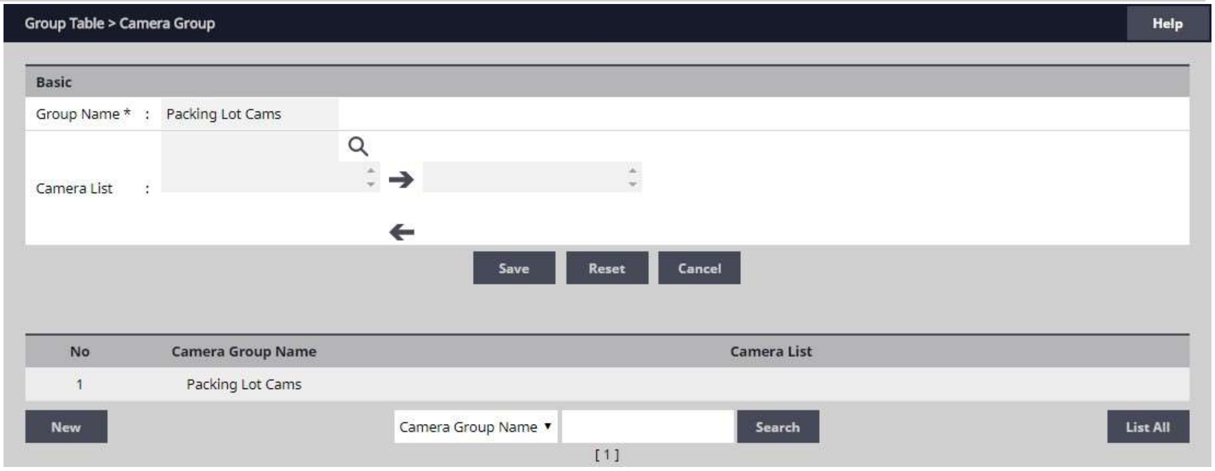
No	Camera Group Name	Camera List
1	Packing Lot Cams	



Group Name * : Packing Lot Cams

Camera List :

No	Camera Group Name	Camera List
1	Packing Lot Cams	



Group Name * : Packing Lot Cams

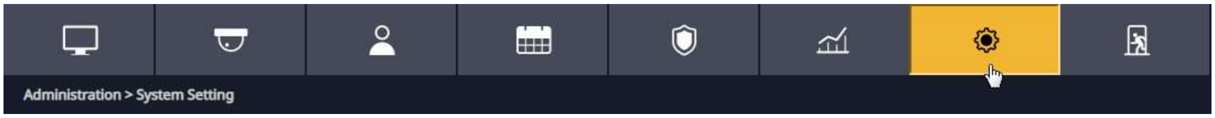
Camera List :

No	Camera Group Name	Camera List
1	Packing Lot Cams	

1. Click on the Camera Group name to edit.
2. Click **Edit**.
3. The Camera Group name can be edited.
4. Cameras can be added or removed from the group.
5. Click Save.

Deleting a Camera Group

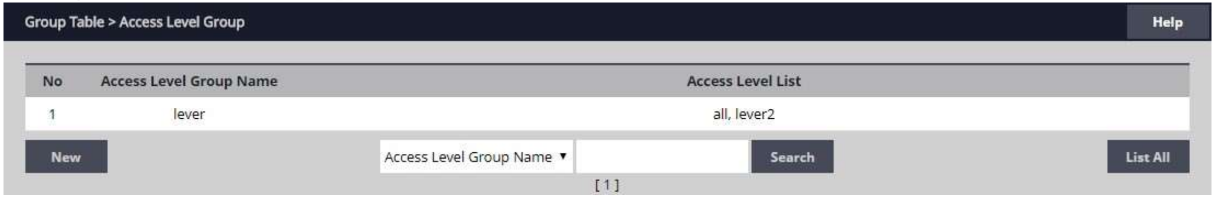
1. Click on the Camera Group name to delete.
2. Click **Delete**.


Administration > System Setting

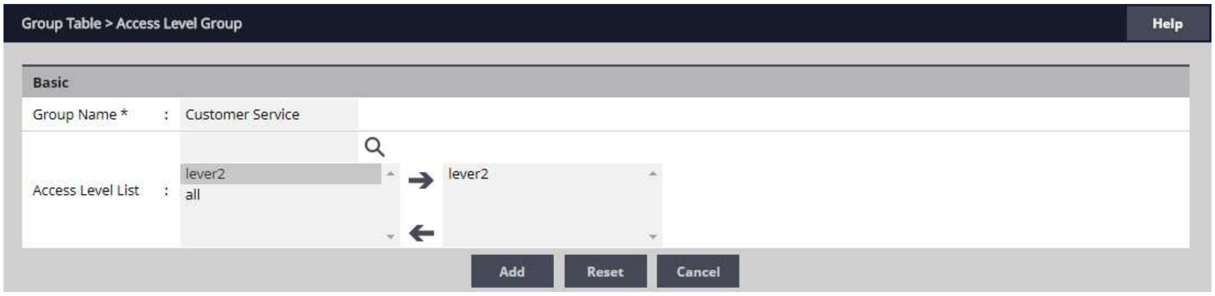
Access level Group

Add individual Access Levels to ***Access Level Groups***. These groups can then be assigned to cards in the Card Holder section.

Adding an Access Level Group


Group Table > Access Level Group

No	Access Level Group Name	Access Level List
1	lever	all, lever2


Group Table > Access Level Group

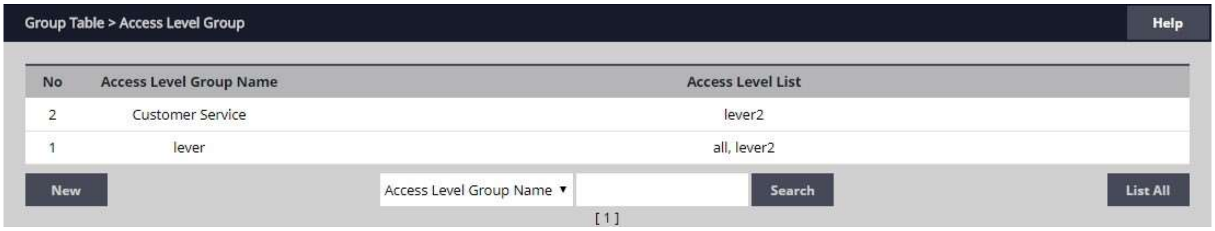
Basic

Group Name * : Customer Service

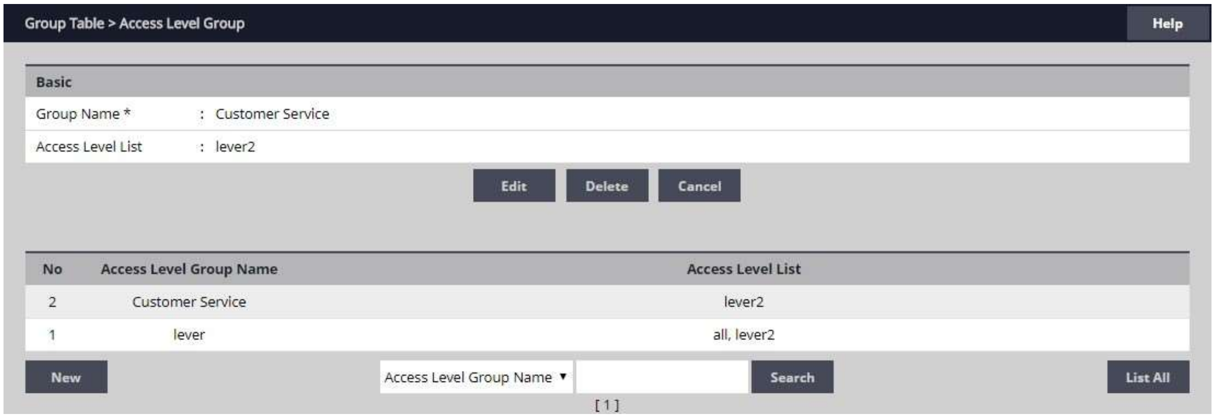
Access Level List : lever2, all → lever2

1. Click **New**.
2. Enter the desired **Group Name**.
3. For **Access Level List**, select the desired access level (or use the search icon to find an access level) and click the right arrow to move the access levels to the field on the right. ✓ ***NOTE:*** *Ctrl-click or shift-click will select multiple Access Levels.*
4. Click **Add** to save the changes.

Editing a Access Level Group


Group Table > Access Level Group

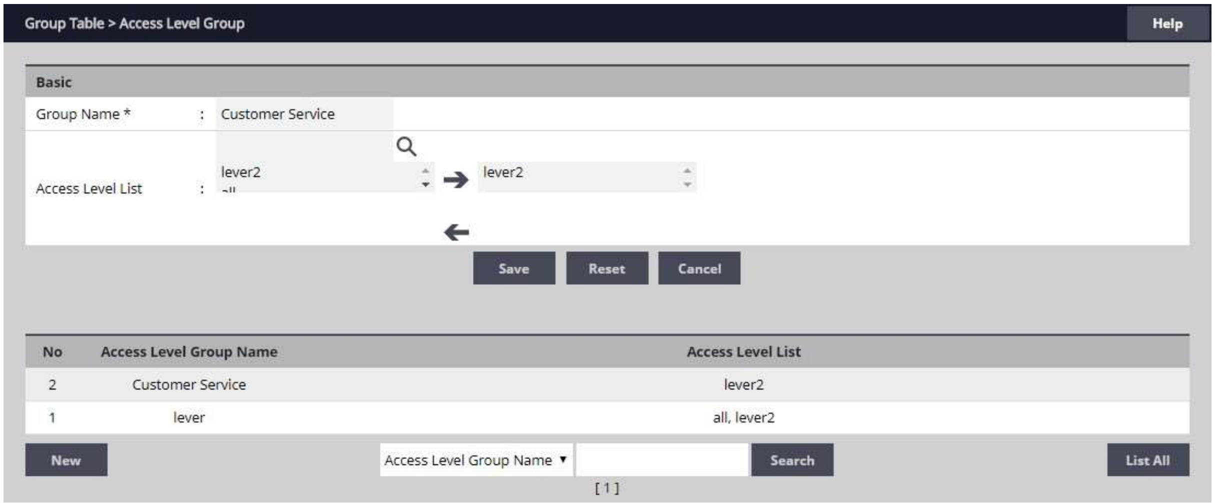
No	Access Level Group Name	Access Level List
2	Customer Service	lever2
1	lever	all, lever2



Basic

Group Name *	:	Customer Service
Access Level List	:	lever2

No	Access Level Group Name	Access Level List
2	Customer Service	lever2
1	lever	all, lever2



Basic

Group Name *	:	Customer Service
Access Level List	:	lever2 all → lever2

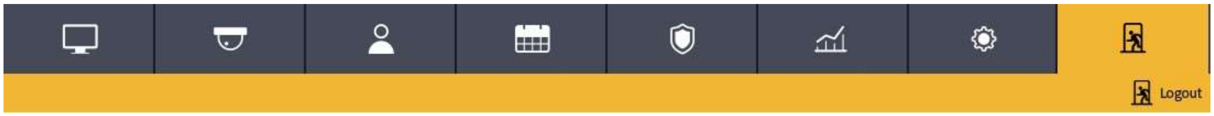
No	Access Level Group Name	Access Level List
2	Customer Service	lever2
1	lever	all, lever2

1. Click on the Access Level Group name to edit.
2. Click **Edit**.
3. The Access Level Group name can be edited.
4. Access Levels can be added or removed from the group.
5. Click **Save**.

Deleting an Access Level Group

1. Click on the Access Level Group name to delete.
2. Click **Delete**.

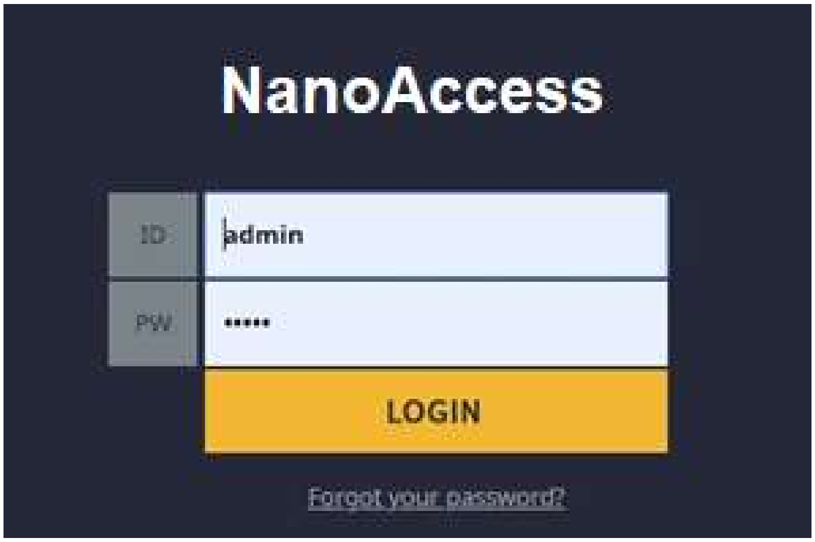
Logout



Logout prevents unauthorized persons from working in the system but still allows all access control operations to continue. **To secure the system, be sure to logout when finished.**

Logging Out of the Controller

1. When ready to exit, click **Logout**.



NanoAccess

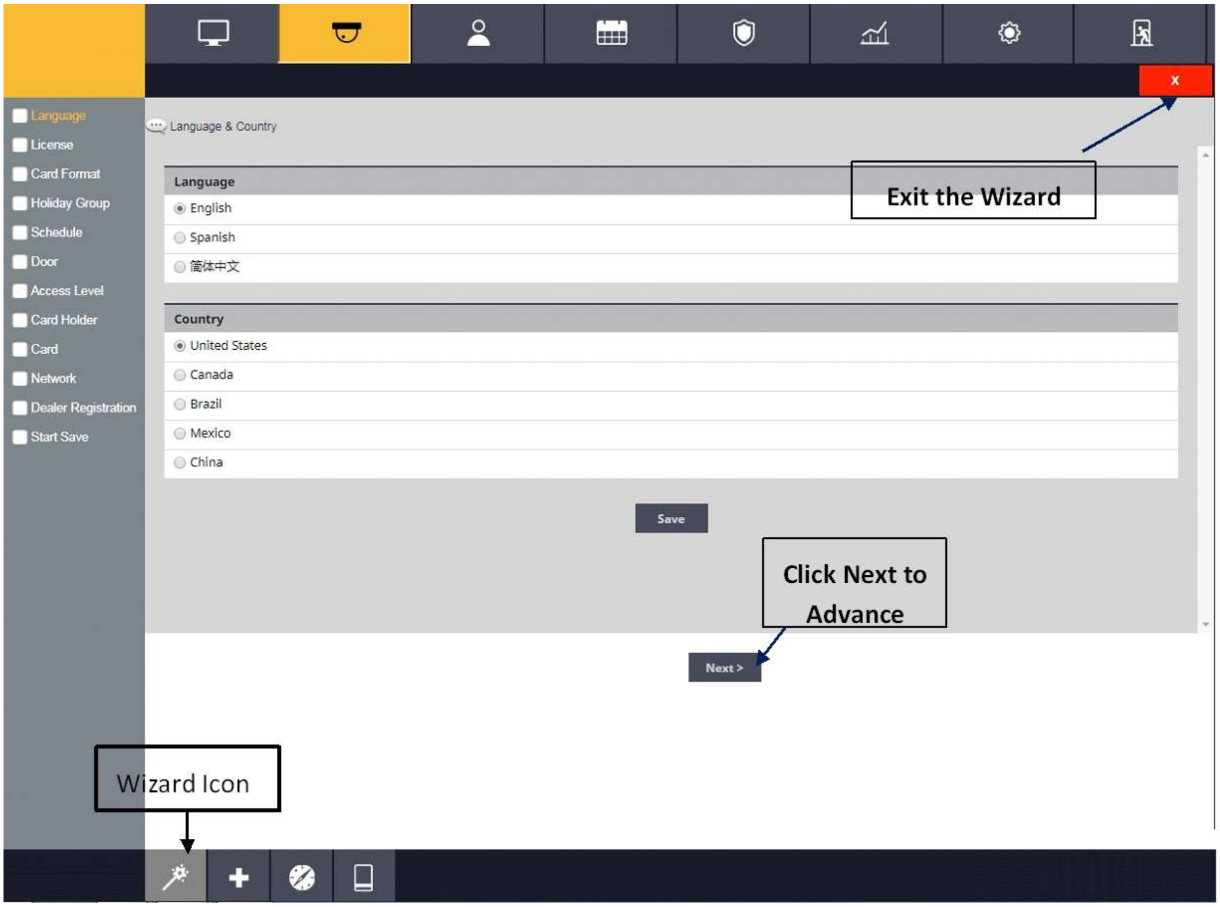
ID admin

PW •••••

2. The Controller will logout the user and return to the Login screen.

4. Using the Wizard

The ***Wizard*** allows the user to configure the basic settings of the system. Advance through each setting by clicking the **Next** button. The Wizard will launch automatically the first time the system is run. Visit the Wizard at any time by clicking the icon in the lower left corner of the window.



Language

● English
○ Spanish
○ 简体中文

Country

● United States
○ Canada
○ Brazil
○ Mexico
○ China

Exit the Wizard

Click Next to Advance

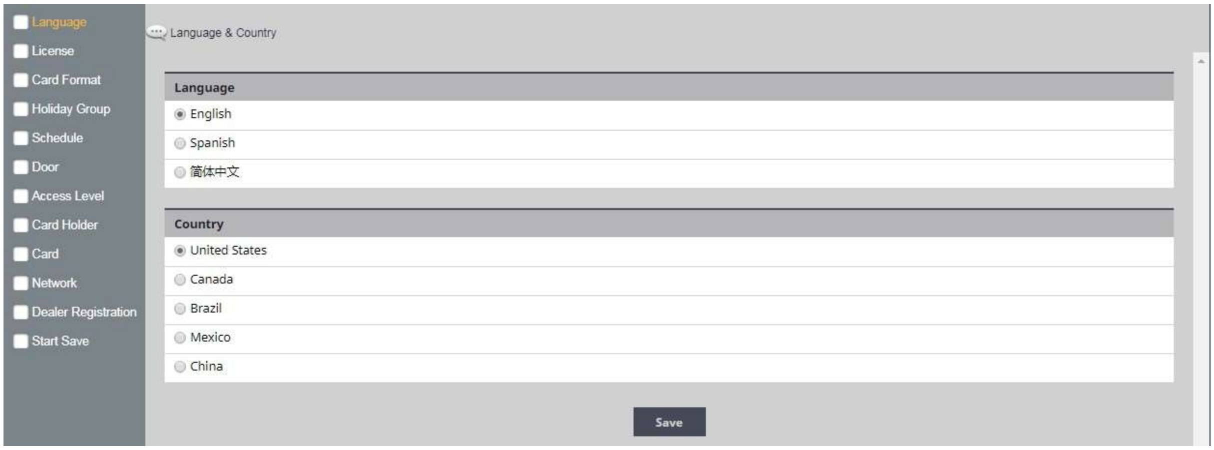
Wizard Icon

✓ ***NOTE:*** *When programming various elements of the system, do not use the same name for multiple items (e.g., use Door 1, Door 2, etc.).*

✓ ***NOTE:*** *Do not use special characters (<>?{})(*&%#@^{ \|/).*

Language

Use ***Language*** to select the country and language where the system will be located. Click **Next** to advance.



Language

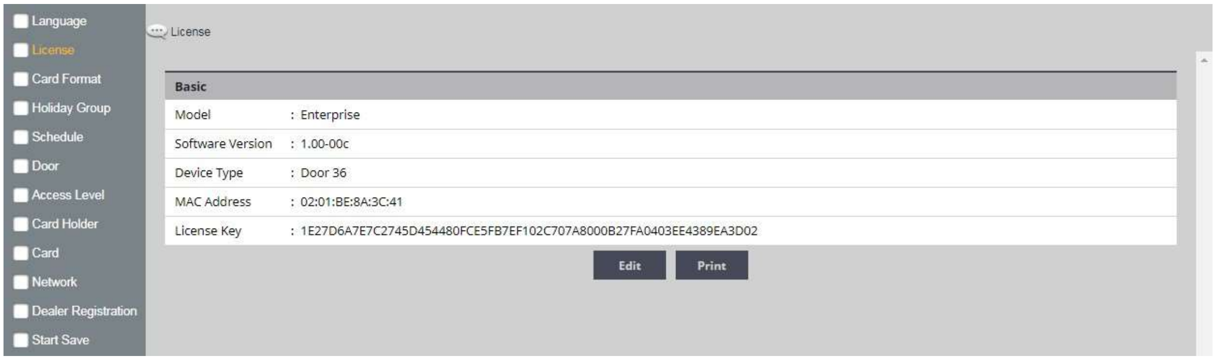
● English
○ Spanish
○ 简体中文

Country

● United States
○ Canada
○ Brazil
○ Mexico
○ China

License

License displays the basic system information of the Controller. Please print the **License Key** for future needs or in case of a factory default. Click **Next**.



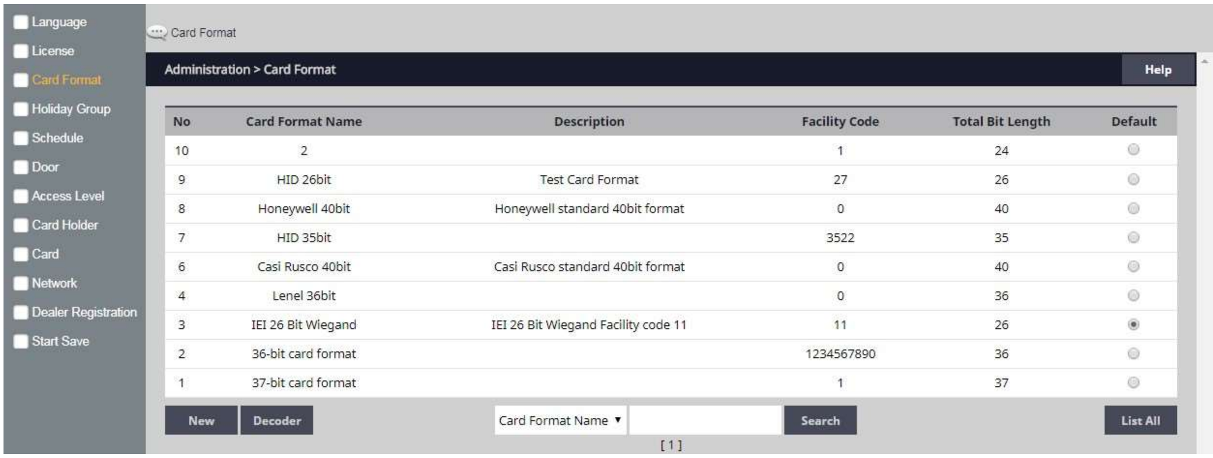
Basic

Model	: Enterprise
Software Version	: 1.00-00c
Device Type	: Door 36
MAC Address	: 02:01:BE:8A:3C:41
License Key	: 1E27D6A7E7C2745D454480FCE5FB7EF102C707A8000B27FA0403EE4389EA3D02

Card Format

Card Format displays the default card formats of the system. The system includes several pre-configured card formats. If the desired card format is listed, click **Next** to advance to the next Wizard item. If the desired card format is not listed, click **New** to enter the format information and click **Add**.

✓ ***NOTE:*** *It is recommended to delete card formats that are not in use.*

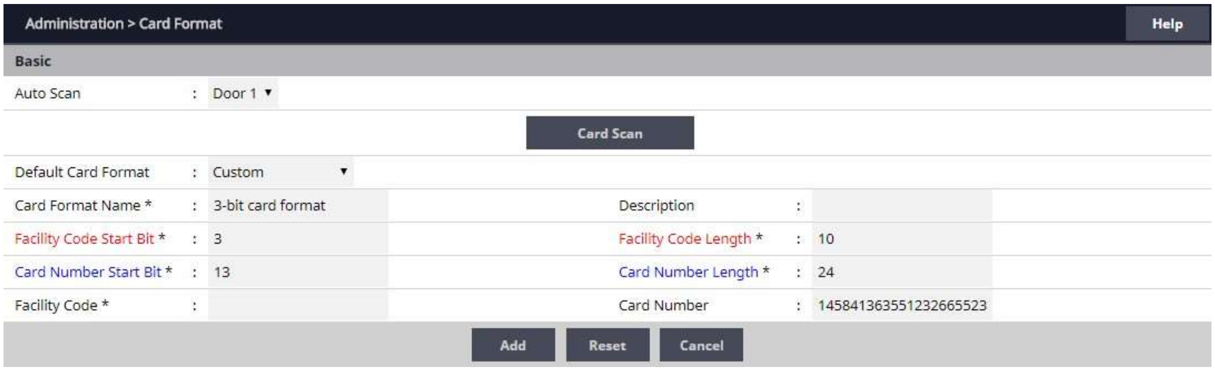


No	Card Format Name	Description	Facility Code	Total Bit Length	Default
10	2		1	24	○
9	HID 26bit	Test Card Format	27	26	○
8	Honeywell 40bit	Honeywell standard 40bit format	0	40	○
7	HID 35bit		3522	35	○
6	Casi Rusco 40bit	Casi Rusco standard 40bit format	0	40	○
4	Lenel 36bit		0	36	○
3	IEI 26 Bit Wiegand	IEI 26 Bit Wiegand Facility code 11	11	26	●
2	36-bit card format		1234567890	36	○
1	37-bit card format		1	37	○

Using the Decoder

If the desired card format is not listed as a default format, the Decoder can be utilized to auto scan and detect the card format.

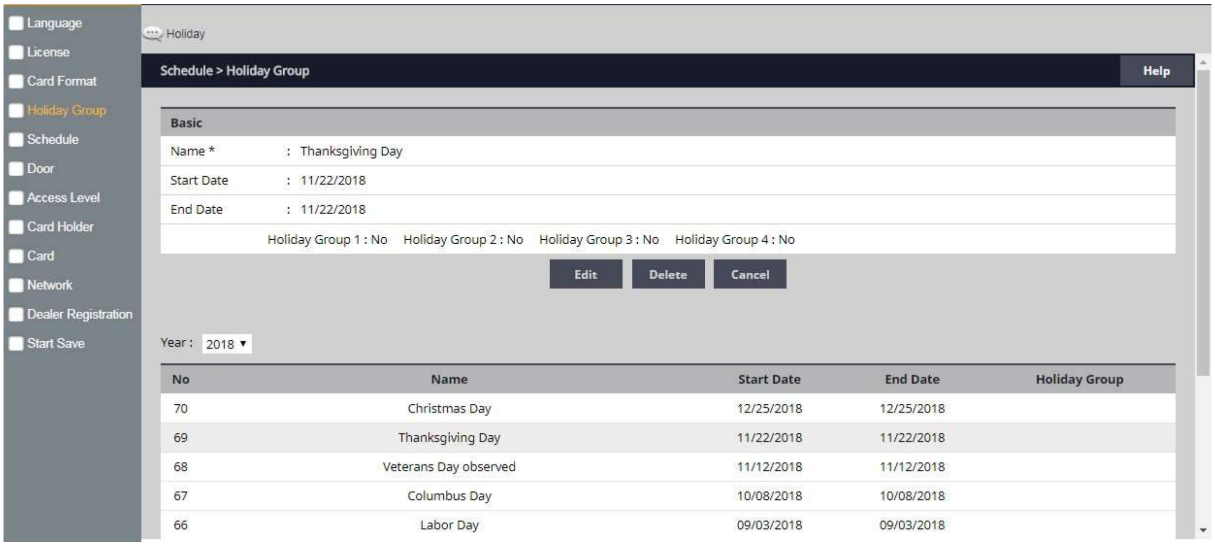
1. Click **Decoder**.
2. Select the door where the card will be auto scanned.
3. Click **Card Scan** and present the card (or multiple cards) to the reader.
4. The new card format will populate the data fields.
5. Click **Add** to save the new format.



Auto Scan	:	Door 1 ▾			
Default Card Format	:	Custom ▾			
Card Format Name *	:	3-bit card format	Description	:	
Facility Code Start Bit *	:	3	Facility Code Length *	:	10
Card Number Start Bit *	:	13	Card Number Length *	:	24
Facility Code *	:		Card Number	:	145841363551232665523

Holiday Group

Use ***Holiday Groups*** to define days and times during the year when holiday hours are used. When the holiday starts, the Controller switches from regular hours to holiday hours. When the holiday ends, the regular hours resume. You can assign four holiday groups with up to 30 holidays total among the groups. A holiday can include any number of consecutive days within the same calendar year. The Controller has pre-configured holiday groups based upon the country you selected in the ***Language*** section of the Wizard. The holiday groups are pre-configured through 2021 for quick set-up.



Basic

Name * : Thanksgiving Day

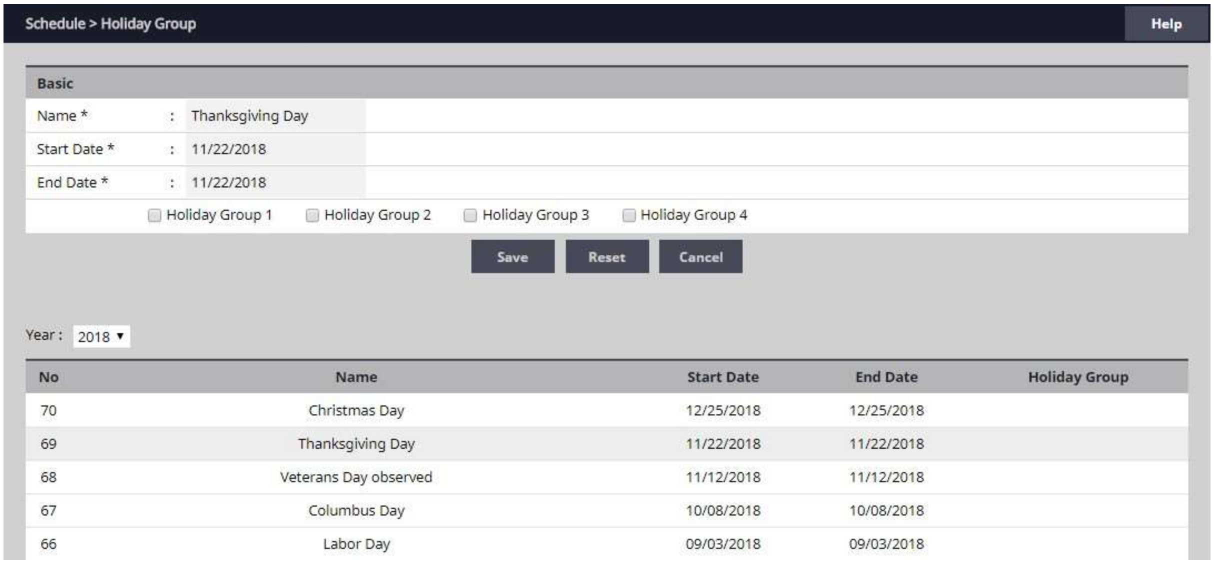
Start Date : 11/22/2018

End Date : 11/22/2018

Holiday Group 1 : No Holiday Group 2 : No Holiday Group 3 : No Holiday Group 4 : No

Year : 2018 ▾

No	Name	Start Date	End Date	Holiday Group
70	Christmas Day	12/25/2018	12/25/2018	
69	Thanksgiving Day	11/22/2018	11/22/2018	
68	Veterans Day observed	11/12/2018	11/12/2018	
67	Columbus Day	10/08/2018	10/08/2018	
66	Labor Day	09/03/2018	09/03/2018	



Basic

Name * : Thanksgiving Day

Start Date * : 11/22/2018

End Date * : 11/22/2018

□ Holiday Group 1 □ Holiday Group 2 □ Holiday Group 3 □ Holiday Group 4

Year : 2018 ▾

No	Name	Start Date	End Date	Holiday Group
70	Christmas Day	12/25/2018	12/25/2018	
69	Thanksgiving Day	11/22/2018	11/22/2018	
68	Veterans Day observed	11/12/2018	11/12/2018	
67	Columbus Day	10/08/2018	10/08/2018	
66	Labor Day	09/03/2018	09/03/2018	

Editing a Holiday

1. Select the desired holiday and click **Edit**.
2. Change the start date and end date to the desired date.
3. Rename the holiday (it is recommended that pre-configured holidays be renamed when edited).
4. Click **Save**.

Deleting a Holiday

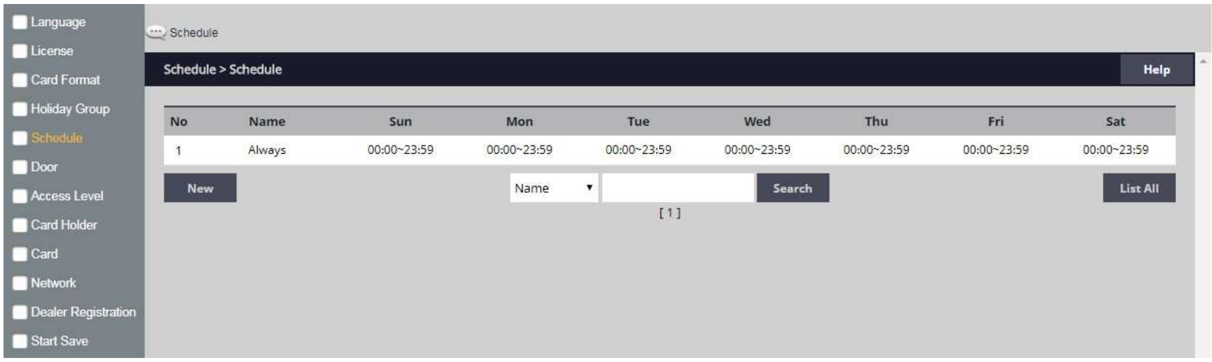
1. Highlight the holiday to be deleted.
2. Click **Delete**. A confirmation box will appear.
3. Click **OK** to confirm.

Adding a Holiday

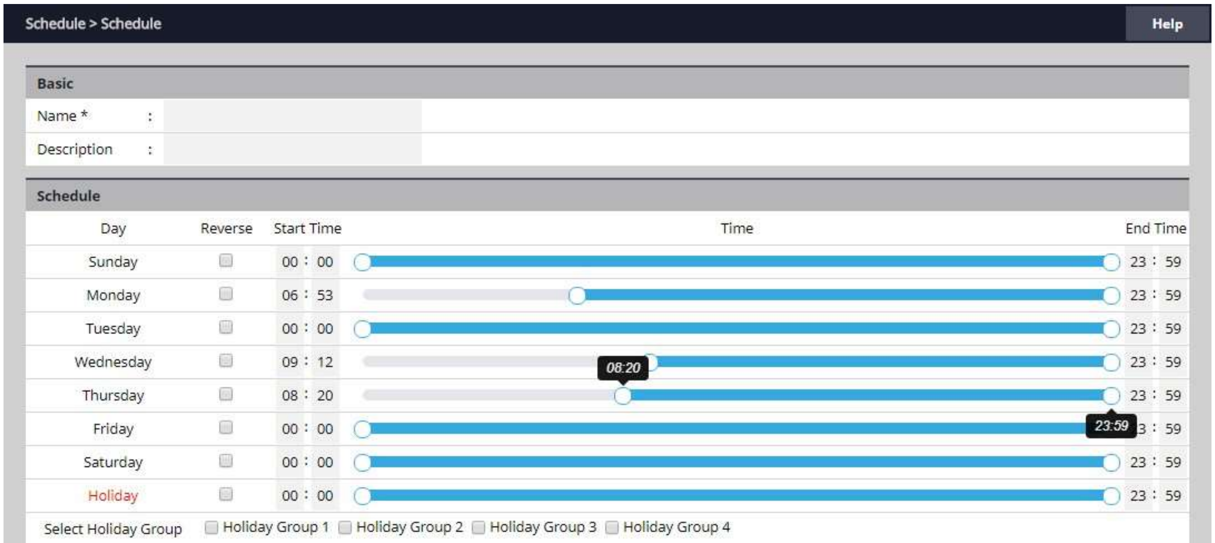
1. Click **New** and enter the desired name, start date and end date.
2. Select the desired holiday group for the new holiday.
3. Click **Add** to save the new holiday.

Schedule

A ***Schedule*** is a combination of a time interval and one or more days of the week. Use schedules to identify the hours and days when inputs, outputs or door access are in operation. Assign holiday groups to the schedule to control when operations occur on holidays. There is one default time schedule of ***Always***, which is defined as 00:00-23:59, seven days per week.



No	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	Always	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59	00:00~23:59



Basic

Name *	:	
Description	:	

Schedule

Day	Reverse	Start Time	Time	End Time
Sunday	□	00 : 00		23 : 59
Monday	□	06 : 53		23 : 59
Tuesday	□	00 : 00		23 : 59
Wednesday	□	09 : 12		23 : 59
Thursday	□	08 : 20	08:20	23 : 59
Friday	□	00 : 00	23:59	23 : 59
Saturday	□	00 : 00		23 : 59
Holiday	□	00 : 00		23 : 59

Select Holiday Group □ Holiday Group 1 □ Holiday Group 2 □ Holiday Group 3 □ Holiday Group 4

Adding a Schedule 1.
Click **New**.

2. Enter the desired name and description (optional) for the schedule.

3. Adjust the sliders for the **Start Time** and **End Time** on days when the schedule is to be active.(Collapse slider for no access on that day.)

4. (Optional) Select a holiday group to allow access on the holidays in the group. If a holiday group is selected, identify a start and end time for holiday access.

5. Click **Add** to save the new schedule.

✓ ***Note:*** *To create a schedule with a "Midnight Crossing" (e.g., 16:00 to00:30) click Reverse.*

Deleting a Schedule

1. Select the schedule to be deleted.
2. The schedule will appear. Scroll to the bottom of the page and click **Delete**.
3. Click **OK** to confirm the deletion.

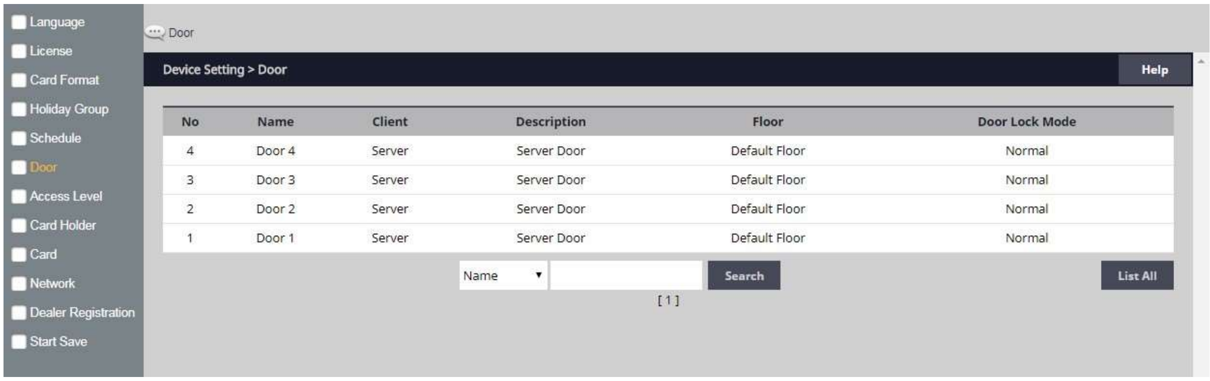
Editing a Schedule

1. Select the schedule to be edited and click **Edit**.

2. Perform the desired changes to the name, description and time intervals.
3. Scroll down and click **Save** to save the changes.

Door

Displays the ***Doors*** that are assigned to the system. Click on the door name to view or edit each door.



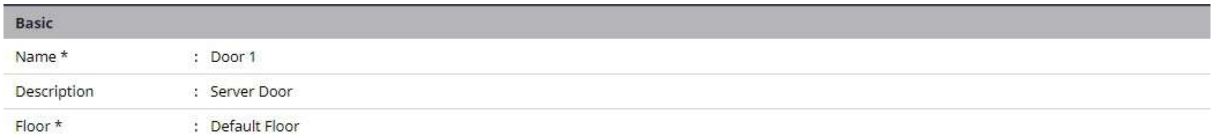
No	Name	Client	Description	Floor	Door Lock Mode
4	Door 4	Server	Server Door	Default Floor	Normal
3	Door 3	Server	Server Door	Default Floor	Normal
2	Door 2	Server	Server Door	Default Floor	Normal
1	Door 1	Server	Server Door	Default Floor	Normal

Editing a Door

Select the desired door. Scroll to the bottom of the page and click **Edit**.

After making any edits, be sure to click Save at the bottom of the page.

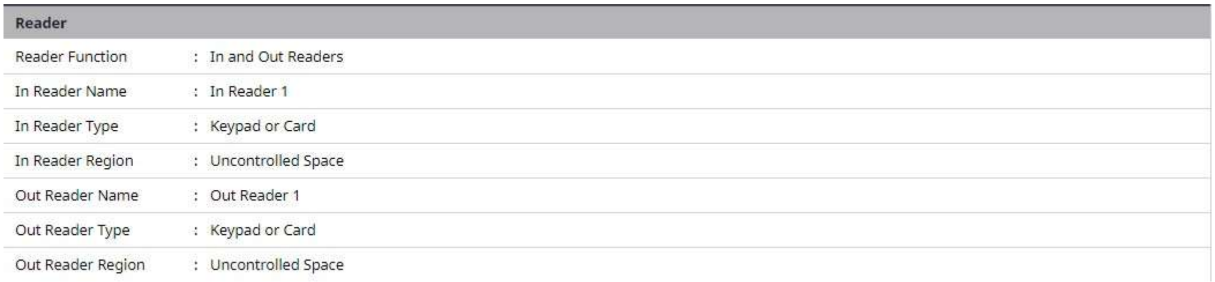
Basic



Basic		
Name *	:	Door 1
Description	:	Server Door
Floor *	:	Default Floor

1. Enter the desired **Name** and **Description** (optional) for the door.
2. For multi-floor installations, select the **Floor**.

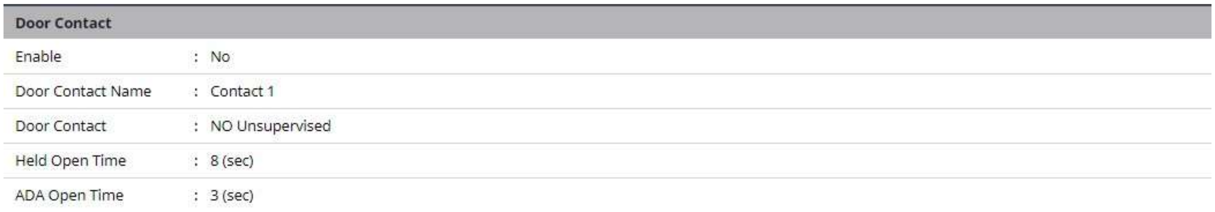
Reader



Reader		
Reader Function	:	In and Out Readers
In Reader Name	:	In Reader 1
In Reader Type	:	Keypad or Card
In Reader Region	:	Uncontrolled Space
Out Reader Name	:	Out Reader 1
Out Reader Type	:	Keypad or Card
Out Reader Region	:	Uncontrolled Space

1. In the **Reader** section, select the settings for the door's reader.

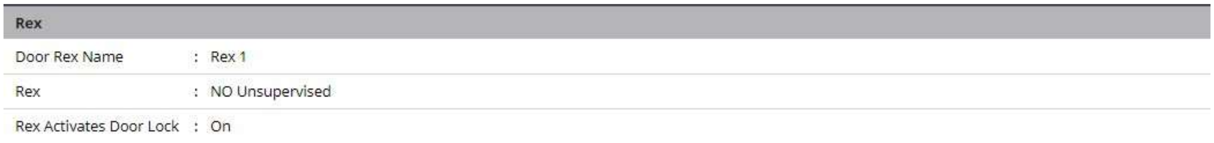
Door Contact



Door Contact		
Enable	:	No
Door Contact Name	:	Contact 1
Door Contact	:	NO Unsupervised
Held Open Time	:	8 (sec)
ADA Open Time	:	3 (sec)

1. In the **Door Contact** section, check the Enable checkbox if a door contact is used.
2. **Name** the door contact and select its type.
3. Adjust the **Held Open Time**, which is the length of time the door can be open following a valid access request.
4. The **ADA Open Time** is an additional time added to the Held Open Time.

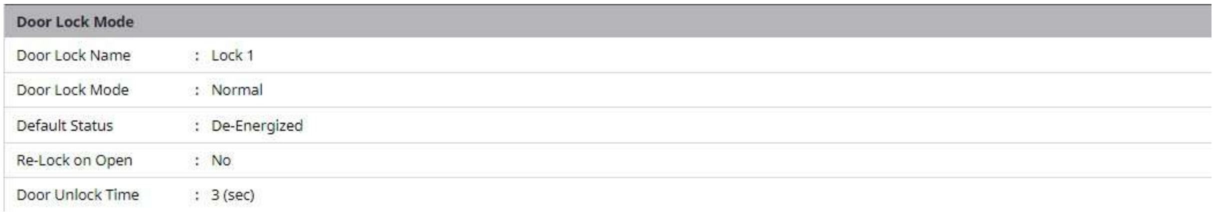
Rex



Rex		
Door Rex Name	:	Rex 1
Rex	:	NO Unsupervised
Rex Activates Door Lock	:	On

1. Enter the **Door Rex Name** for the door's request to exit switch.
2. Select the type of **Rex** switch.
3. Check the **Rex Activates Door Lock** checkbox to have the Rex activate the door's lock.

Door Lock Mode



Door Lock Mode		
Door Lock Name	:	Lock 1
Door Lock Mode	:	Normal
Default Status	:	De-Energized
Re-Lock on Open	:	No
Door Unlock Time	:	3 (sec)

1. Choose a **Door Lock Name** to name the lock for logging.
2. Configure **Door Lock Mode** as follows:

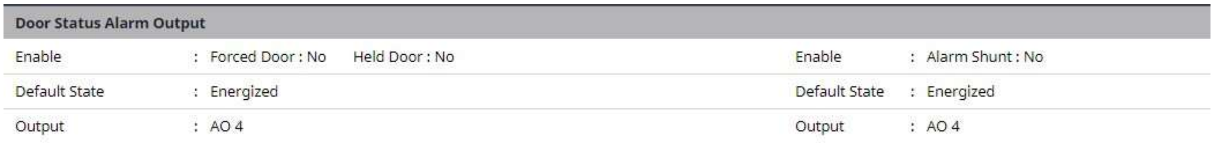
- · **Normal:** Lock activates in response to a valid access request and REX unlocks door for exit.
- · **Locked:** Does NOT grant access in response to REX, card or code.
- · **Locked w/REX:** Remains in locked mode, ONLY REX will activate lock.
- · **Unlocked:** Door will remain unlocked at ALL times.
- · **Man-Trap:** Sets the door lock for use in conjunction with another door to create a man-trap passage. A Man-Trap will only allow one door to be opened if the other door is locked. When Man-Trap is selected, **Man-Trap Mode** options appear:
- · **Unlock:** No security on Entry or Exit.
- · **Secure Entry/Free Egress:** Two options, both options use card access to enter the Exterior Door. Option 1 allows free exit through the exterior door; Option 2 requires card access to exit through the exterior door.
- · **Restricted Entry and Exit:** Four options, all options use card access to enter the Exterior Door. Option 1 allows free exit through the exterior door; Option 2 requires card access to exit through the interior door, Option 3requires card access to exit through the exterior door. Option 4 requires card access to exit through either door.
- · **Pair Door:** Select the second Man-Trap door that is closest to the secured area.

3. Select the Door's **Default Status**. This setting will be determined by the lock type (energized or de-energized).

4. Assign **Re-Lock on Open** if desired. This will re-lock the door immediately upon opening the door.

5. Adjust **Door Unlock Time** if desired. This is the length of time the door relay is active after a valid access request.

Door Status Alarm Output

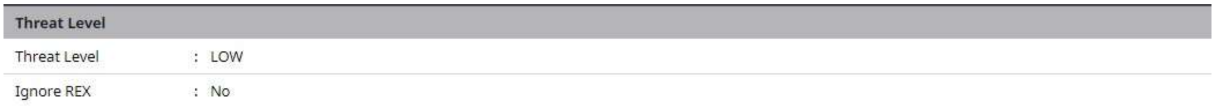


Door Status Alarm Output					
Enable	:	Forced Door : No Held Door : No	Enable	:	Alarm Shunt : No
Default State	:	Energized	Default State	:	Energized
Output	:	AO 4	Output	:	AO 4

Sets the actions of a door contact on the door. The door contact must be enabled to use these functions.

1. Check **Forced Door** to trigger the door alarm output if the door opens, but no access was granted.
2. Check **Held Door** to trigger the door alarm output if the door is held open longer than the **Held Open Time**.
3. Select Energized or De-energized for the **Default State** of the Door Status Alarm Output.
4. Select an **Output** to use for the Door Status Alarm Output.
5. Click to enable an **Alarm Shunt** output to operate when access is granted to the secured door.
6. Select Energized or De-energized for the **Default State** of the Alarm Shunt Output.
7. Select an **Output** to use for the Alarm Shunt Output.

Threat Level



Threat Level		
Threat Level	:	LOW
Ignore REX	:	No

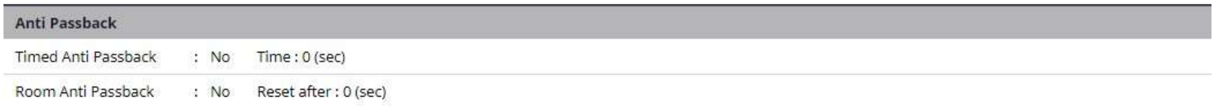
1. Select the highest **Threat Level** allowed before the door will automatically lock.

✓ ***Note:*** *An unlocked door will lock if the System Threat Level is greater than the Door Threat Level; including doors that are unlocked by schedule.*

✓ ***Note:*** *The Dashboard M-Unlock and E-Unlock may be used to unlock a door that has been locked due to elevated system Threat Level.*

2. Check **Ignore REX** to ignore input from a Rex button if the current System Threat Level is higher than the Door Threat Level.

Anti-Passback

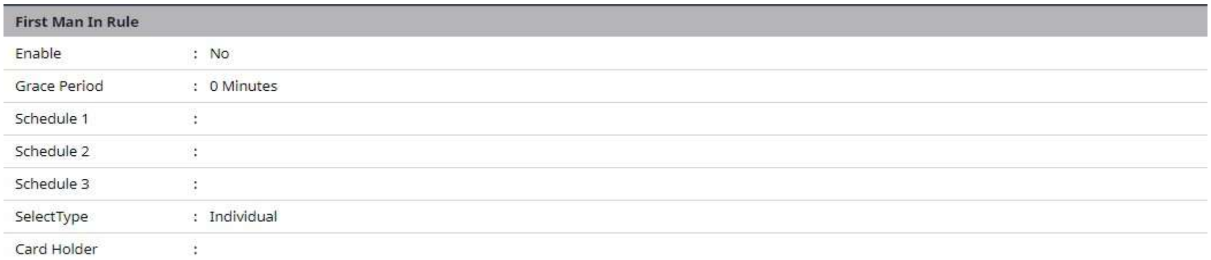


Anti Passback			
Timed Anti Passback	:	No	Time : 0 (sec)
Room Anti Passback	:	No	Reset after : 0 (sec)

1. Check to enable **Timed AntiPassback**. Select a time in seconds to disable a credential after it has been used to grant access.

2. Check to enable **Room Anti Passback**. Select a time in seconds to disable access to a room after access has been granted to the room.

First Man In Rule

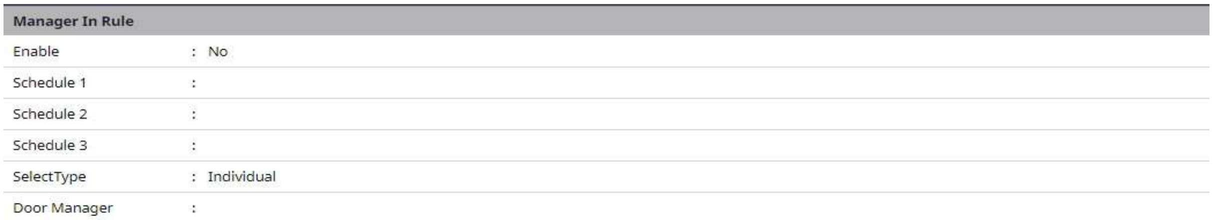


First Man In Rule	
Enable	: No
Grace Period	: 0 Minutes
Schedule 1	:
Schedule 2	:
Schedule 3	:
SelectType	: Individual
Card Holder	:

First Man in Rule unlocks a door when first Card Holder enters.

1. Check **Enable** to use a First Man In Rule.
2. Select a **Grace Period** to allow the selected first man Card Holder(s) access minutes before a scheduled start time.
3. Select up to three time **Schedules** for the rule to be active.
4. Select the **Type** of Card Holders (individual or group).
5. Search or choose **Card Holder**(s) or **Groups** for the rule. Use the arrows to move the name(s) in and out.

Manager In Rule

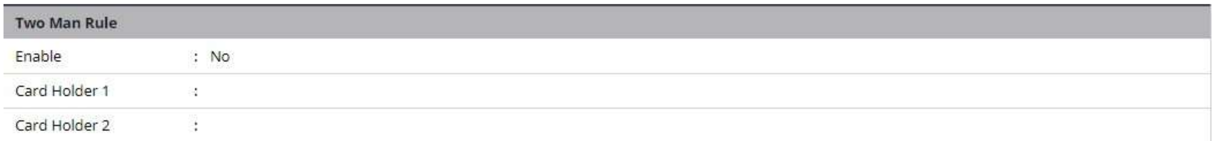


Manager In Rule	
Enable	: No
Schedule 1	:
Schedule 2	:
Schedule 3	:
SelectType	: Individual
Door Manager	:

With Manager in Rule enabled, if a Card Holder designated as a Door Manager has not entered the system within a specific time period, the door will not unlock.

1. Check **Enable** to use the Manager In Rule.
2. Select up to three time **Schedules** for the rule to be active.
3. Select the **Type** of Card Holders (individual or group).
4. Search or choose Card **Holder**(s) or **Groups** for the rule. Use the arrows to move the name(s) in and out.

Two Man Rule



Two Man Rule	
Enable	: No
Card Holder 1	:
Card Holder 2	:

With Two Man Rule enabled, two Card Holders must present credentials at the same time in order to unlock the door. Credentials must be presented in the proper sequence (Card Holder 1 then Card Holder 2), or access will be denied.

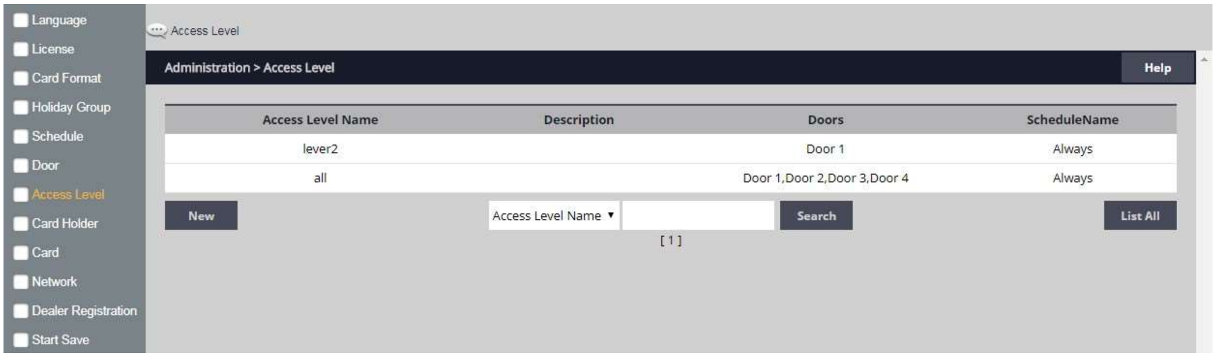
1. Check **Enable** to use the Two Man Rule.
2. Enter a **Time** in seconds allowed for the second Card Holder to present their credentials.
3. Search or choose **Card Holder 1** for the rule. Use the arrows to move the name(s) in and out.
4. Search or choose **Card Holder 2** for the rule. Use the arrows to move the name(s) in and out.

Saving Changes

After making any edits, be sure to click **Save** at the bottom of the page.

Access Levels

An Access Level establishes which doors the Card Holder can access and when they are allowed to access them. Access Levels are comprised of a time schedule and door(s).

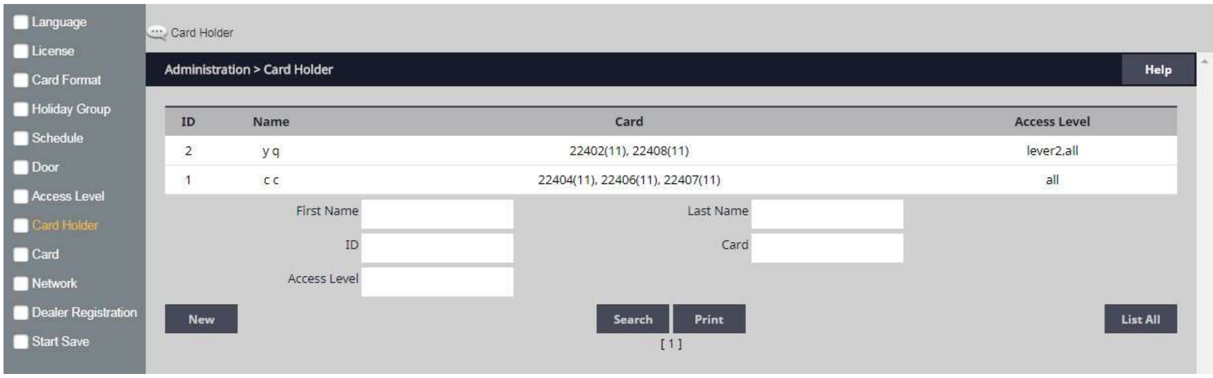


Access Level Name	Description	Doors	ScheduleName
lever2		Door 1	Always
all		Door 1,Door 2,Door 3,Door 4	Always

Adding an Access Level 1.
Click **New**.

2. Enter the Access Level name.
3. Assign a time schedule to the Access Level by choosing it from the drop-down menu.
4. For **Door List** select the desired doors (or use the search icon to find a specific door) and click the right arrow to move the doors to the field on the right.
5. Click **Add** to save the changes.

Card Holder



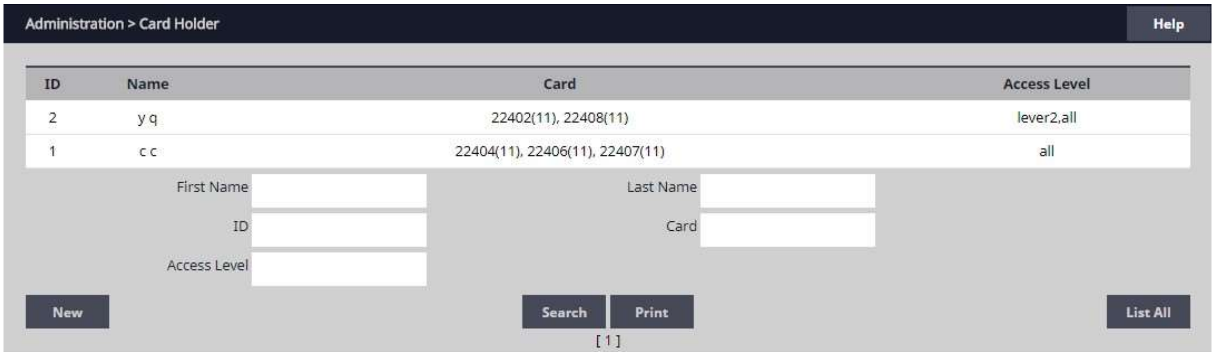
ID	Name	Card	Access Level
2	y q	22402(11), 22408(11)	lever2,all
1	c c	22404(11), 22406(11), 22407(11)	all

First Name
Last Name
ID
Card
Access Level

To Add a Card Holder

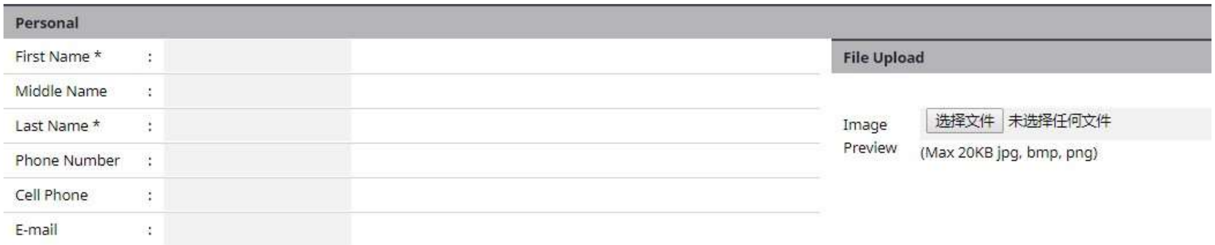
Individuals who enter the facility are entered in the system as ***Card Holders***.

Creating a Card Holder



ID	Name	Card	Access Level
2	y q	22402(11), 22408(11)	lever2,all
1	c c	22404(11), 22406(11), 22407(11)	all

First Name
Last Name
ID
Card
Access Level



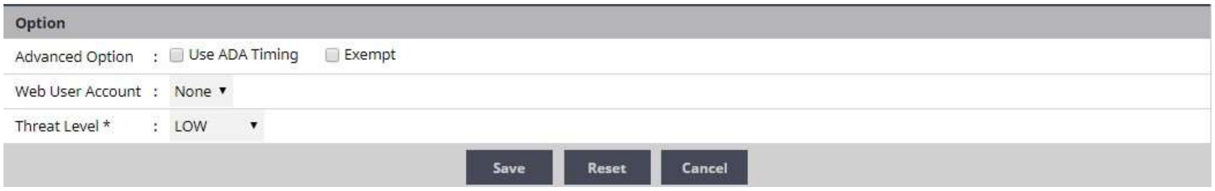
First Name * :
Middle Name :
Last Name * :
Phone Number :
Cell Phone :
E-mail :

Image 选择文件 未选择任何文件
Preview (Max 20KB jpg, bmp, png)

1. Click **New**.
2. Enter the name and contact information of the Card Holder.
3. Under **File Upload**, click **Snapshot** to take a picture from an attached USB camera or click **Browse** to select a file to assign an image to the Card Holder for identification purposes.

✓ ***NOTE:*** *Picture files can be 20 Kb maximum. JPG, BMP, or PNG formats.*

Card Holder Options



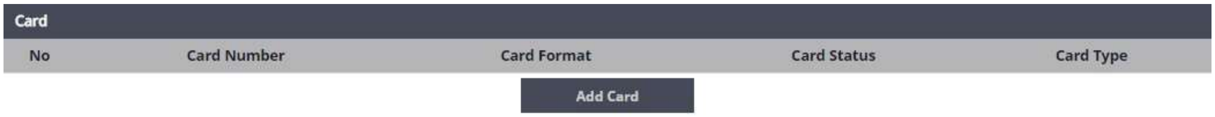
Advanced Option : □ Use ADA Timing □ Exempt
Web User Account : None ▾
Threat Level * : LOW ▾

1. Select **ADA Timing** for extended timing for the door relay.
2. Select **Exempt** to allow the Card Holder to bypass Anti-Passback rules (except occupancy rules) if the Card Holder is allowed access to the region.
3. Select a **Web User Account** to give the Card Holder operator privileges to the server software.
4. Choose the highest **Threat Level** that the Card Holder will be allowed access.

✓ ***NOTE:*** *A Card Holder cannot access a door if either the Door Threat Level or the System Threat Level is greater than the Card Holder Threat Level.*

5. Click **Save**.

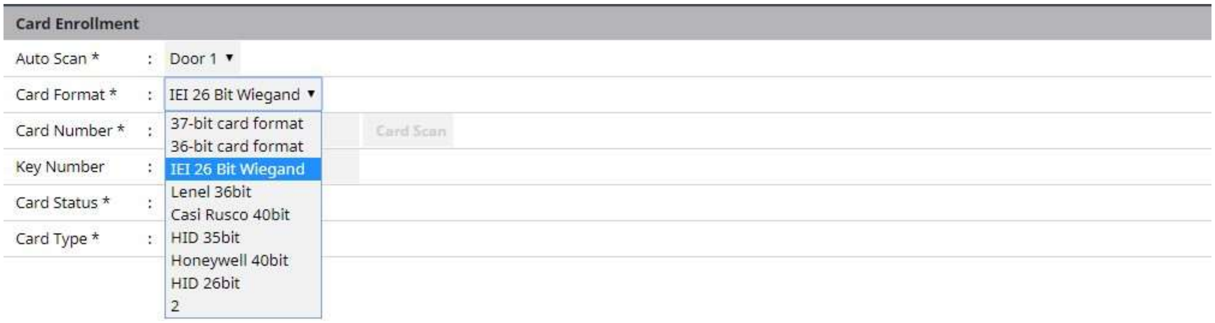
Assigning a Card to an Existing Card Holder



No	Card Number	Card Format	Card Status	Card Type

1. Select the Card Holder from the main window.
2. Click **Add Card**.

Card Format

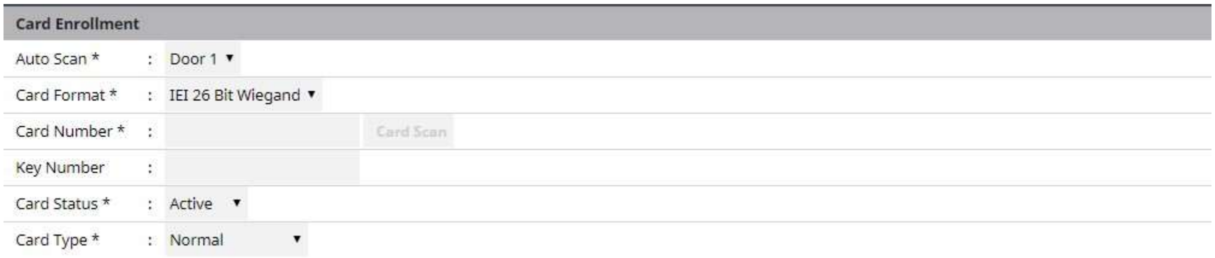


Card Enrollment

Auto Scan *	:	Door 1 ▼
Card Format *	:	IEI 26 Bit Wiegand ▼
Card Number *	:	Card Scan
Key Number	:	
Card Status *	:	
Card Type *	:	

3. Select the appropriate card format from the drop-down field.

Card Number



Card Enrollment

Auto Scan *	:	Door 1 ▼
Card Format *	:	IEI 26 Bit Wiegand ▼
Card Number *	:	Card Scan
Key Number	:	
Card Status *	:	Active ▼
Card Type *	:	Normal ▼

4. Enter the **Card Number**, or use the Auto Scan feature.

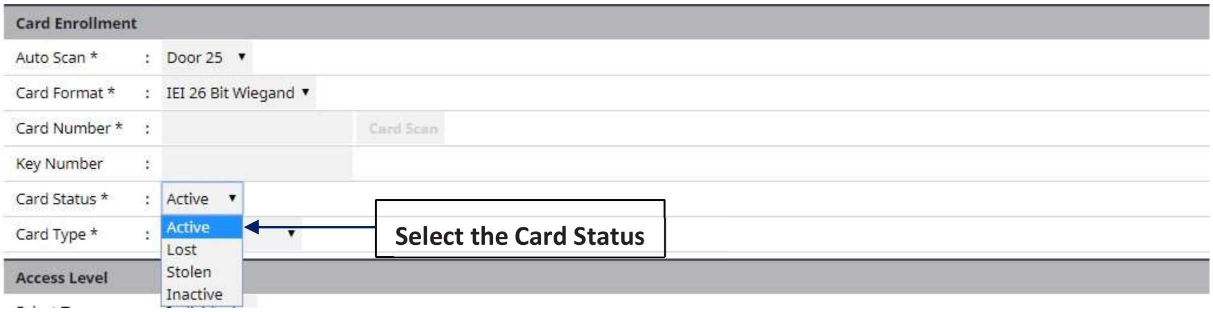
Auto Scan

5. Choose the **Auto Scan** door reader where the card will be presented.

✓ ***NOTE:*** *Card scanner can only be used with doors 1 - 4.*

6. Click **Card Scan** and present the card to the reader. The new card number will populate the data field.

Card Status



Card Enrollment

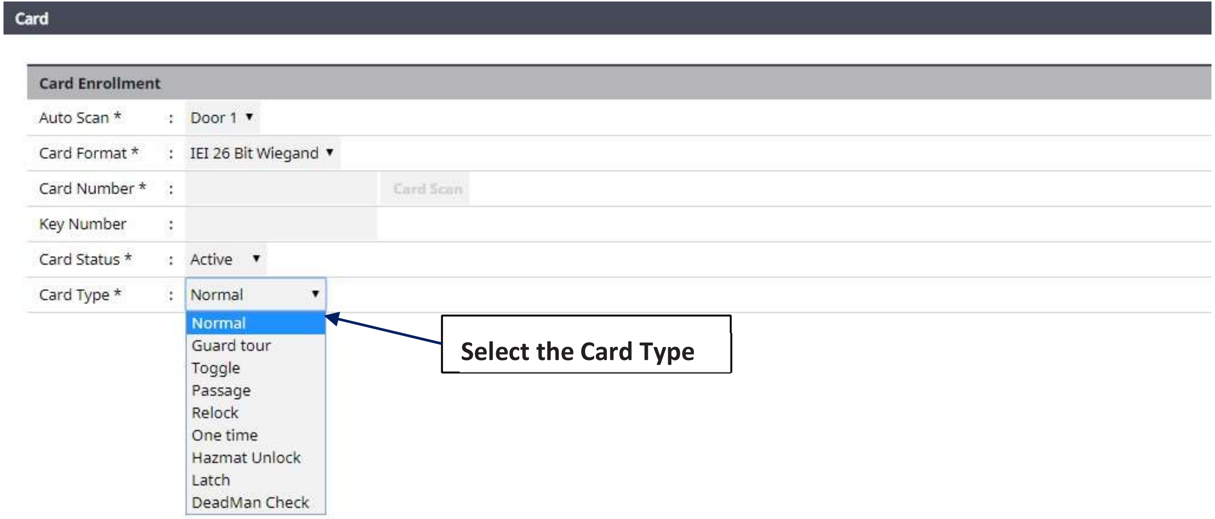
Auto Scan *	:	Door 25 ▼
Card Format *	:	IEI 26 Bit Wiegand ▼
Card Number *	:	Card Scan
Key Number	:	
Card Status *	:	Active ▼
Card Type *	:	▼

Access Level

Select the Card Status

7. Select the card's current status.

Card Type



Card

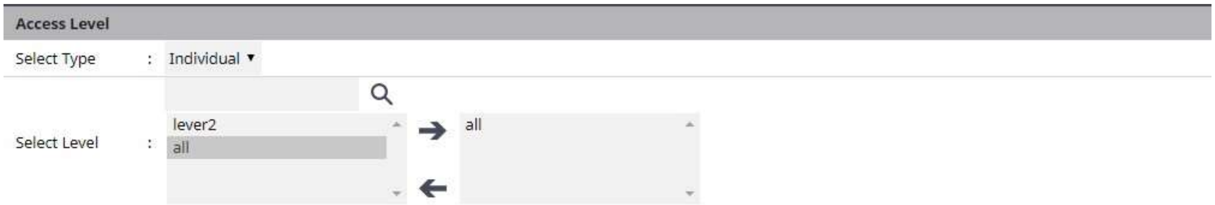
Card Enrollment

Auto Scan *	:	Door 1 ▾
Card Format *	:	IEI 26 Bit Wiegand ▾
Card Number *	:	Card Scan
Key Number	:	
Card Status *	:	Active ▾
Card Type *	:	Normal ▾

Select the Card Type

8. Select the function for the card with card type dropdown.

Access Level



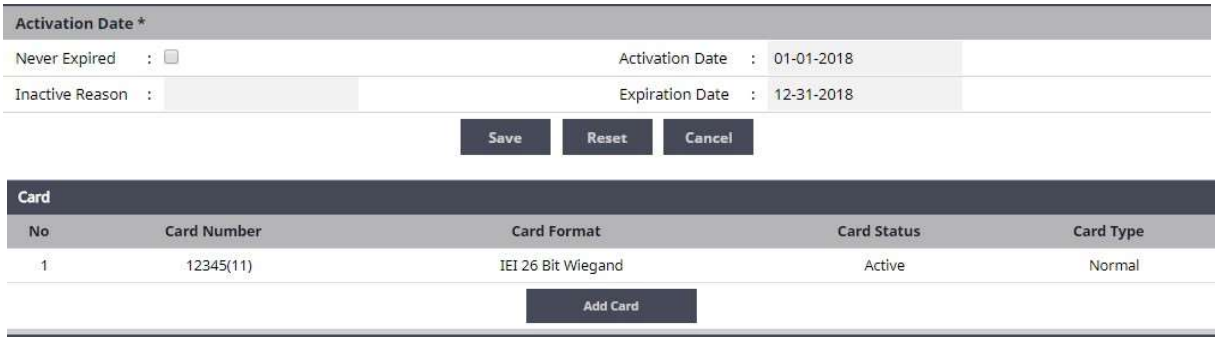
Access Level

Select Type	:	Individual ▾
Select Level	:	lever2 all

9. For **Select Type** select Individual or Group access level.

10. For **Select Level** select the desired access levels (or use the search icon to find a specific access level) and click the right arrow to move the access level to the field on the right.

Activation Date



Activation Date *

Never Expired	:	□	Activation Date	:	01-01-2018
Inactive Reason	:		Expiration Date	:	12-31-2018

Card

No	Card Number	Card Format	Card Status	Card Type
1	12345(11)	IEI 26 Bit Wiegand	Active	Normal

11. Choose an optional activation and expiration date for the card.

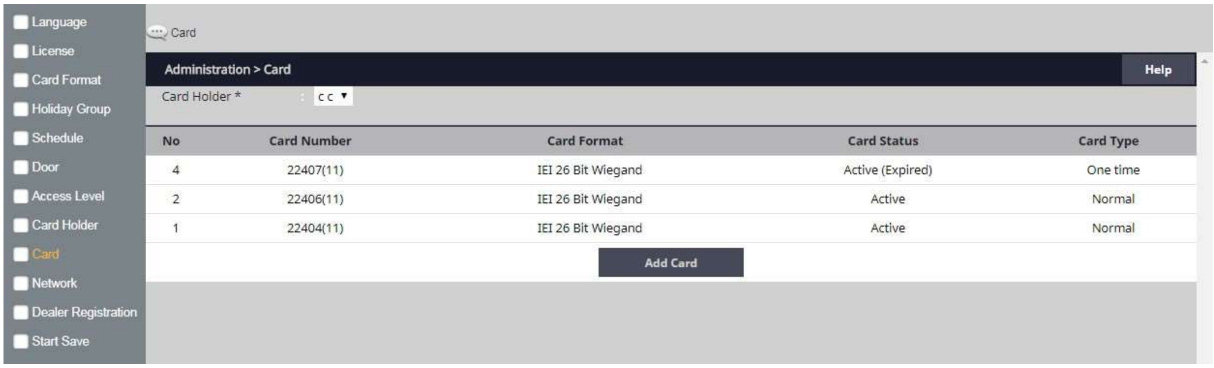
12. Click **Save** to assign the card to the Card Holder.

The added card will show on the card list for the Card Holder.

Click **Add Card** to add additional cards for the selected Card Holder.

Card

Use ***Card*** to enter card numbers in the database and assign the card to a Card Holder

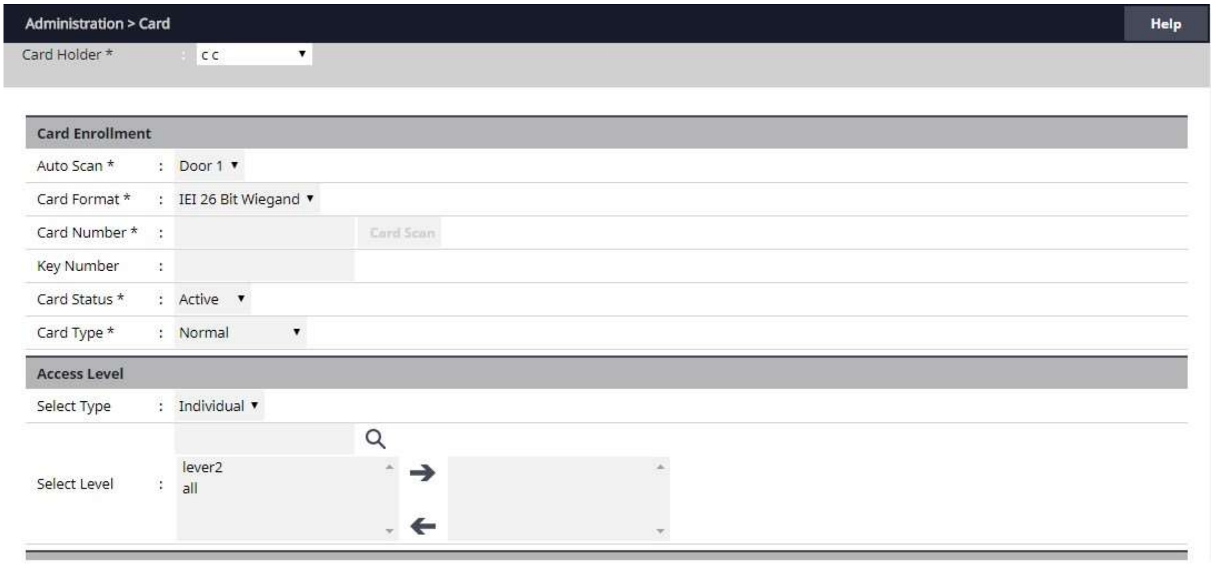


Administration > Card

Card Holder * : c c

No	Card Number	Card Format	Card Status	Card Type
4	22407(11)	IEI 26 Bit Wiegand	Active (Expired)	One time
2	22406(11)	IEI 26 Bit Wiegand	Active	Normal
1	22404(11)	IEI 26 Bit Wiegand	Active	Normal

Assigning a Card to a Card Holder



Administration > Card

Card Holder * : c c

Card Enrollment

Auto Scan *	:	Door 1
Card Format *	:	IEI 26 Bit Wiegand
Card Number *	:	
Key Number	:	
Card Status *	:	Active
Card Type *	:	Normal

Access Level

Select Type	:	Individual
Select Level	:	lever2 all

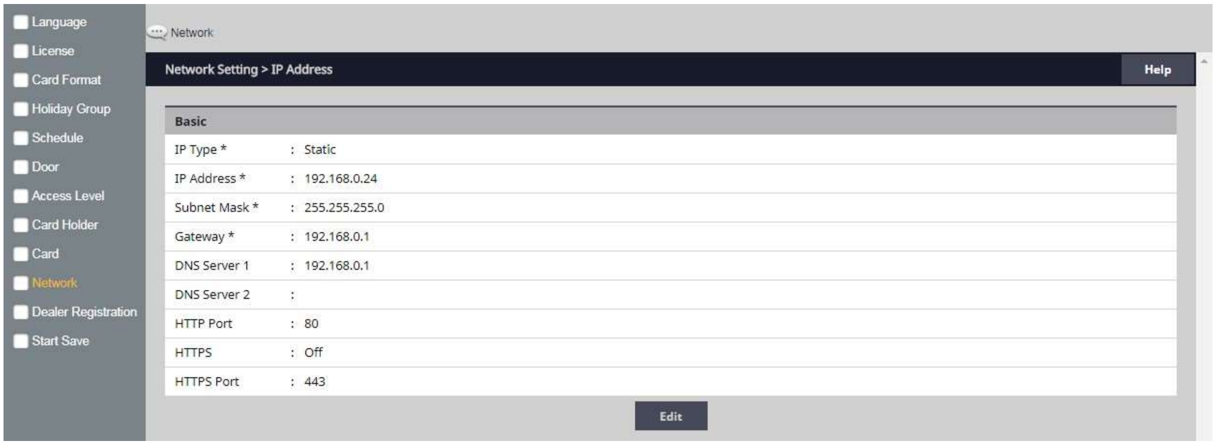
1. Select the Card Holder from the main window.
2. Click **Add Card**.
3. If using **Card Scan**, select the door where the card will be scanned.
4. Select the appropriate **Card Format** from the drop-down.
5. Enter the **Card Number** of the card.
6. If using **Card Scan**, click the button and present the card to the reader.

The card number will populate the Card Number field.

7. For **Select Type** select Individual or Group access level.
8. For **Select Level** select the desired access levels (or use the search icon to find a specific access level) and click the right arrow to move the access level to the field on the right.
9. For **Activation Date**, choose an optional activation and expiration date for the card.
10. Click **Save** to assign the card to the Card Holder.

Network

Enter the ***Network*** configuration information as provided by the IT administrator.



Network Setting > IP Address

Basic

IP Type *	: Static
IP Address *	: 192.168.0.24
Subnet Mask *	: 255.255.255.0
Gateway *	: 192.168.0.1
DNS Server 1	: 192.168.0.1
DNS Server 2	:
HTTP Port	: 80
HTTPS	: Off
HTTPS Port	: 443

DHCP assigns an IP address to the Controller automatically on a network containing a DHCP Server (a router will typically have a built-in DHCP Server). When Static is selected, options IP Address, Subnet Mask, Gateway must be entered.

DNS is an Internet service that translates domain names into IP addresses. The IP address of a DNS is required if using NTP time server or SMTP e-mail.

Editing Network Settings

1. Select **DHCP** or **Static**. (Skip to Step 5 if using DHCP).
2. Enter a static **IP Address** for the Controller to use on the LAN. The first three values must match other devices on the network (e.g., 192.1.0.x).
3. Enter the Subnet Mask address. The Subnet Mask determines the manual address mask used by the Controller (typically 255.255.255.0).
4. Set the Gateway Address to match the address of the router that connects the LAN to the Internet.
5. Enter the IP address of the DNS Server 1 (optional, use for NTP time server access or SMTP e-mail connection).
6. Enter the IP address of the DNS Server 2 (optional, use for NTP time server access or SMTP e-mail connection).
7. Enter the HTTP Port number for remote Web browser connection (typically 80).
8. Check the HTTPS checkbox if RMC is being used.
9. If using HTTPS, edit the port number if required (default is 443).
10. When finished entering the network settings, click **Save & Reboot**.

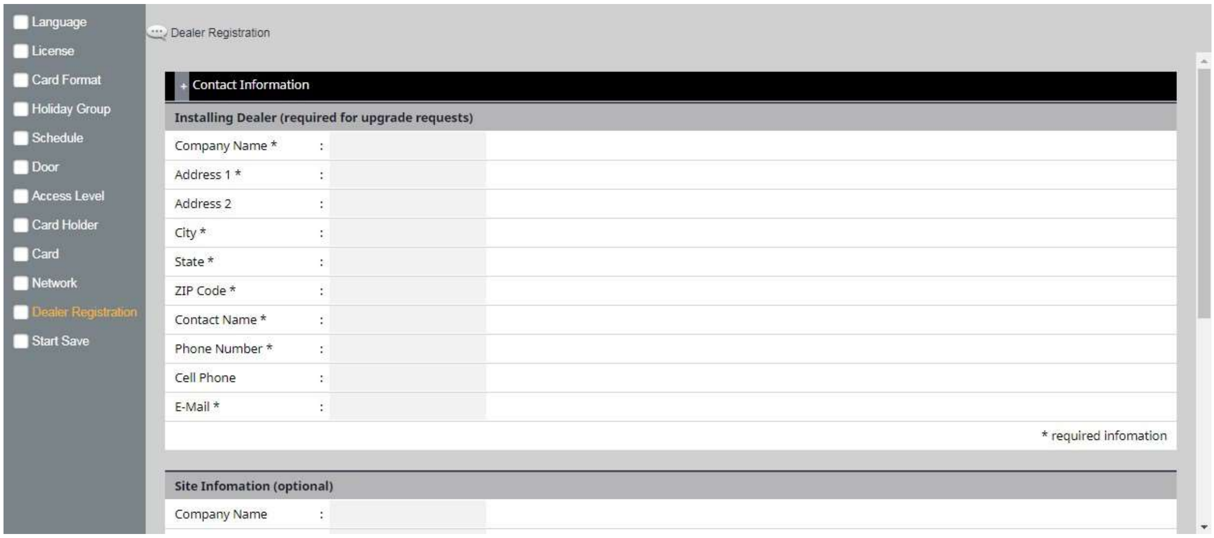
Upload cer-key

For installations using Hyper Text Transport Protocol Secure (HTTPS) communications, the eMerge system uses a default security key and certificate. If the installations network requires a different specific security key and certificate, edit the two items.

1. Click **Upload cer-key**.
2. Enter the **Private Key** into the SSL Toolbox.
3. Enter the **Certificate** into the SSL Toolbox.
4. Click **Save & Reboot**.

Dealer Registration

Dealer Registration is highly recommended for maximum system support. Please fill out the required information.



+ Contact Information

Installing Dealer (required for upgrade requests)

Company Name *	:	
Address 1 *	:	
Address 2	:	
City *	:	
State *	:	
ZIP Code *	:	
Contact Name *	:	
Phone Number *	:	
Cell Phone	:	
E-Mail *	:	

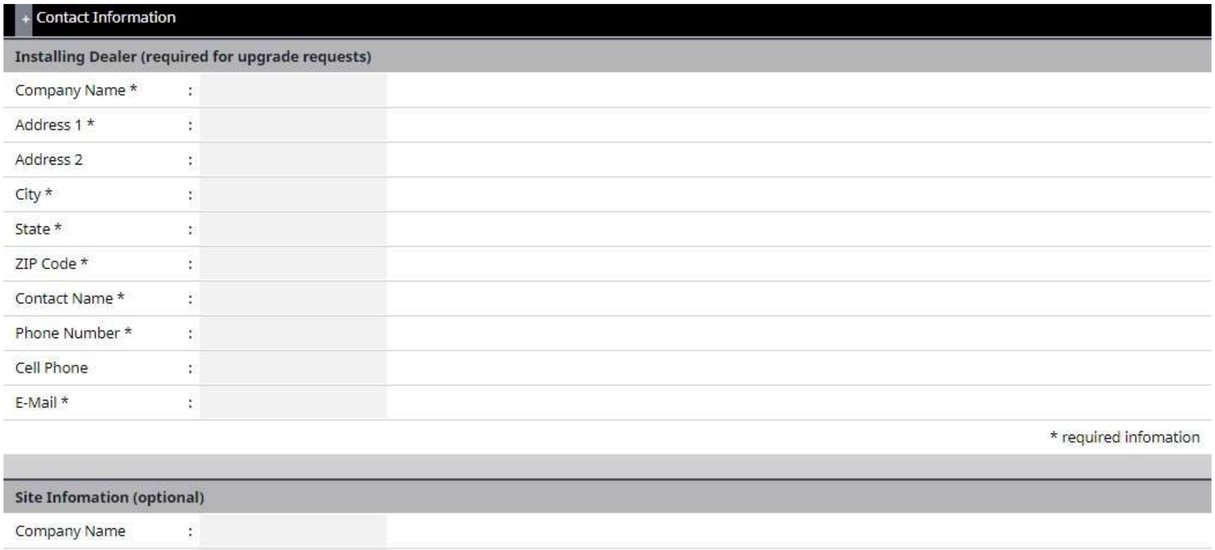
* required infomation

Site Infomation (optional)

Company Name	:	

✓ ***NOTE:*** *Gateway and DNS IP addresses and SMTP must be configured to send the registration email. Refer to IP Address and SMTP to confirm these settings.*

Registering the System



+ Contact Information

Installing Dealer (required for upgrade requests)

Company Name *	:	
Address 1 *	:	
Address 2	:	
City *	:	
State *	:	
ZIP Code *	:	
Contact Name *	:	
Phone Number *	:	
Cell Phone	:	
E-Mail *	:	

* required infomation

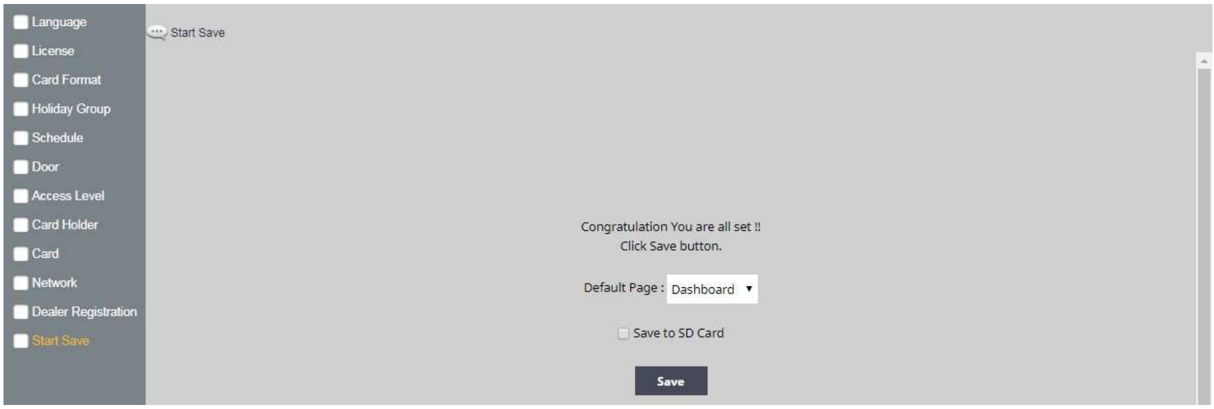
Site Infomation (optional)

Company Name	:	

1. Enter the **Installing Dealer** information (required for upgrade requests).
2. Enter the **Site Information**. This is optional, but recommended to document the site information in the system.
3. When finished editing, click one of the action buttons.
   - The **Register** button will attempt to send an email with the information provided.
   - The **Save** button will save the contact information without sending an email.
   - The **Clear** button will clear the data in the form.

Start Save

Start Save is the command to save the initial settings for the system and select which page appears on logon.



Congratulation You are all set !!
Click Save button.

Default Page : Dashboard ▾

□ Save to SD Card

Save

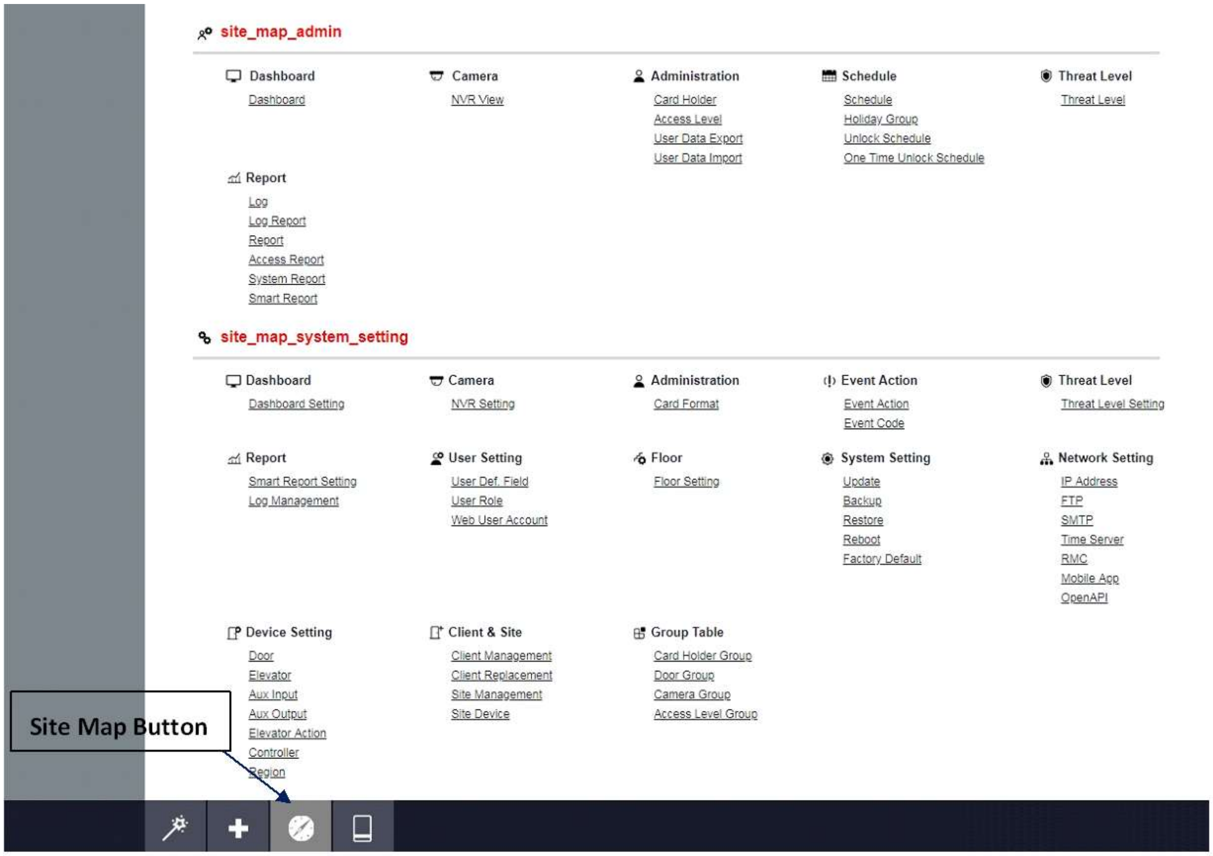
Editing Startup Page

· **Default Page:** Use the dropdown selector to choose the page that the system will display upon logon.

· **Save to SD Card:** Leave this box selected to save the startup information to the SD card. Un-check to save the startup information to the Controller’s memory.

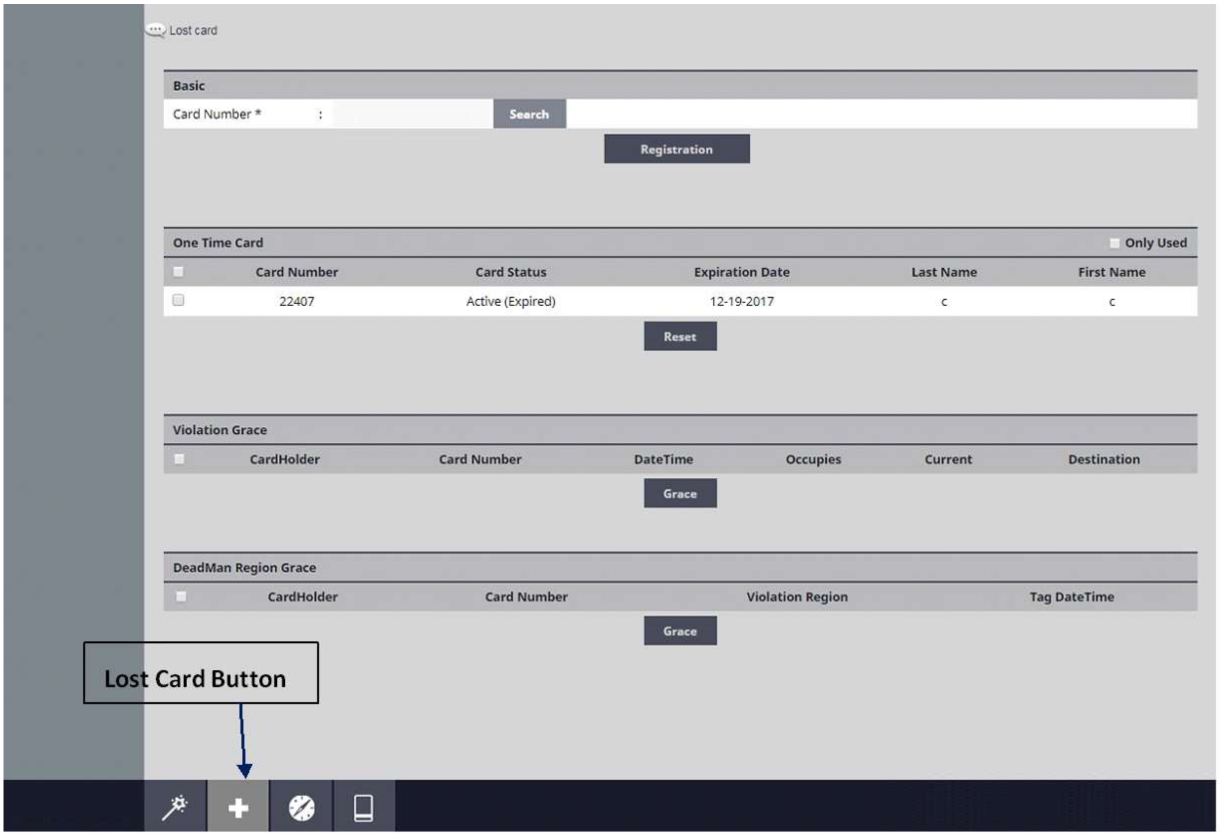
5. Site Map

The ***Site Map*** is an overview of the pages within the Controller interface. Each page listed in the site map is linked to the page it represents. This allows the user to quickly jump to any section listed in the site map.



6. Lost Card

Lost Card is a utility to quickly identify the Card Holder associated with a lost card. The operator may enter any card number to view the Card Holder that is associated with the card, reset a One Time Card, or override a Violation Grace.



Basic

Card Number * :

One Time Card □ Only Used

□	Card Number	Card Status	Expiration Date	Last Name	First Name
□	22407	Active (Expired)	12-19-2017	c	c

Violation Grace

□	CardHolder	Card Number	DateTime	Occupies	Current	Destination

DeadMan Region Grace

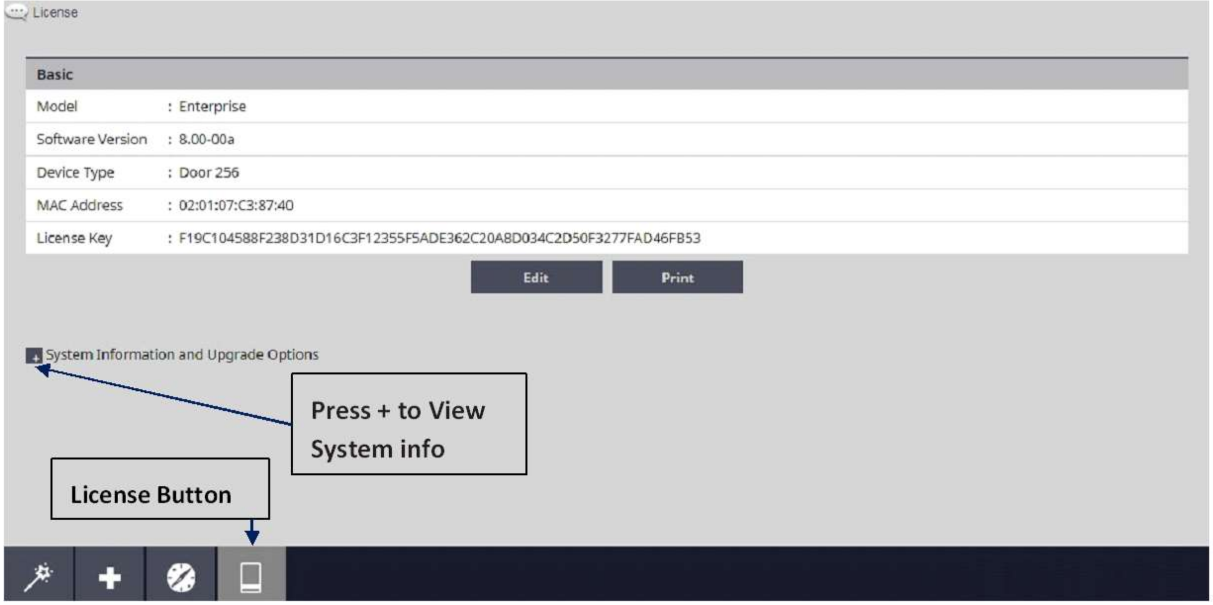
□	CardHolder	Card Number	Violation Region	Tag DateTime

7. License

License display the basic system information of the Controller. Please print the License Key for future needs or in case of a factory default.

✓ ***NOTE:*** *You can use the MAC address to recover the license key for the system.*

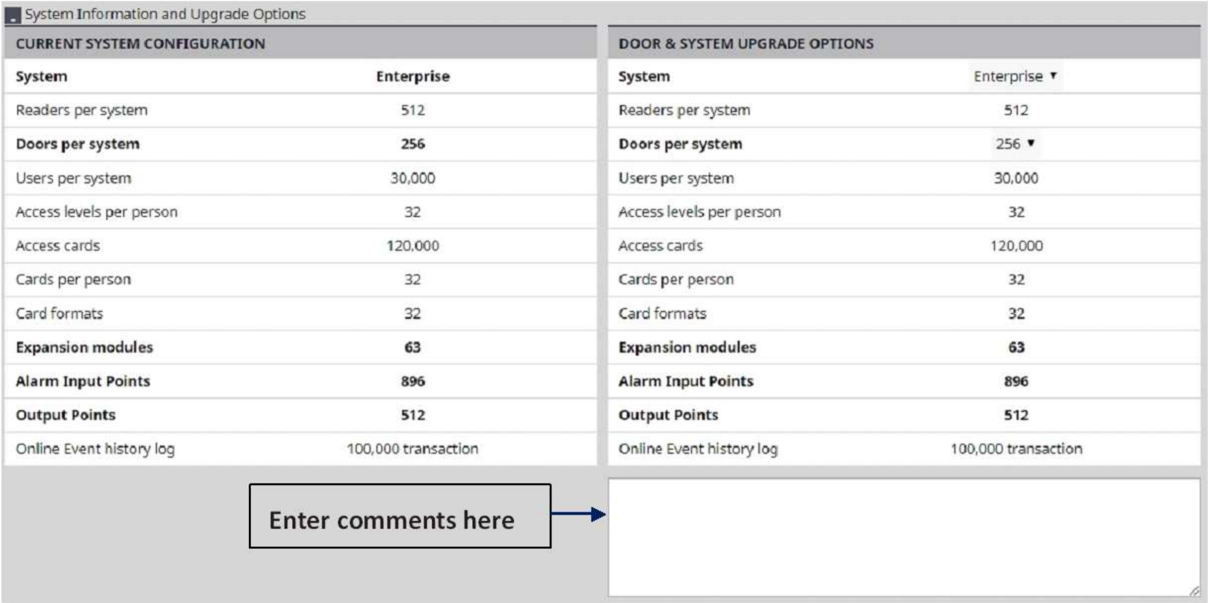
System Information



Basic	
Model	: Enterprise
Software Version	: 8.00-00a
Device Type	: Door 256
MAC Address	: 02:01:07:C3:87:40
License Key	: F19C104588F238D31D16C3F12355F5ADE362C20A8D034C2D50F3277FAD46FB53

Press + to View System info

License Button



CURRENT SYSTEM CONFIGURATION	
System	**Enterprise**
Readers per system	512
Doors per system	**256**
Users per system	30,000
Access levels per person	32
Access cards	120,000
Cards per person	32
Card formats	32
Expansion modules	**63**
Alarm Input Points	**896**
Output Points	**512**
Online Event history log	100,000 transaction

DOOR & SYSTEM UPGRADE OPTIONS	
System	Enterprise ▾
Readers per system	512
Doors per system	256 ▾
Users per system	30,000
Access levels per person	32
Access cards	120,000
Cards per person	32
Card formats	32
Expansion modules	**63**
Alarm Input Points	**896**
Output Points	**512**
Online Event history log	100,000 transaction

Enter comments here

- Press the + sign to display the system configuration information and upgrade options.
- Current system information is shown on the left.
- Upgrade options are shown on the right. Select options from the two dropdown boxes.
- Enter any comments to send with the request in the text box.
- Click **Request Upgrade** to send in an upgrade request.

8. End User License Agreement

IMPORTANT: THIS SOFTWARE END USER LICENSE AGREEMENT (“EULA”) IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR, IF PURCHASED OR OTHERWISE ACQUIRED BY OR FOR AN ENTITY, AN ENTITY) AND EYELOCK, LLC. READ IT CAREFULLY BEFORE USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY USING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS, THEN. DO NOT USE THE SOFTWARE.

1. Definitions

1. “Product” means only the EyeLock NanoAccess system and other EyeLock products.
2. “Software” means only the NanoAccess software program(s) and third party software programs, in each case, provided by EyeLock in connection with the Products, and may include corresponding documentation, associated media, printed materials, and online or electronic documentation, and all updates or upgrades of the above that are provided to you.

2. License Grants

1. You may use the Software on an EyeLock product; provided, however, that, notwithstanding anything contrary contained herein, you may not use the Software on any non- EyeLock product or device, including, but not limited to, mobile devices, internet appliances, set top boxes (STB), home automation systems or any other consumer electronics devices. You may upgrade the Software on an EyeLock NanoAccess product following procedures authorized by EyeLock.
2. You agree that EyeLock may audit your use of the Software for compliance with these terms at any time, upon reasonable notice. In the event that such audit reveals any use of the Software by you other than in full compliance with the terms of this Agreement, you shall reimburse EyeLock for all reasonable expenses related to such audit in addition to any other liabilities you may incur as a result of such non-compliance.
3. Your license rights under this EULA are non-exclusive.

License Restrictions

1. You may not make or distribute copies of the Software, or electronically transfer the Software from a EyeLock product to another EyeLock product, or to a computer or over a network.
2. You may not alter, merge, modify, adapt or translate the Software, or decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form.
3. You may not sell, rent, lease, or sublicense the Software.
4. You may not modify the Software or create derivative works based upon the Software.
5. In the event that you fail to comply with this EULA, EyeLock may terminate the license and you must stop using this Software and stop operating the EyeLock NanoAccess product (with all other rights of both parties and all other provisions of this EULA surviving any such termination).
6. You shall not use the Software to develop any software or other technology having the same primary function as the Software, including but not limited to using the Software in any development or test procedure that seeks to develop like software or other technology, to determine communications protocols used by the EyeLock NanoAccess Product or to determine if such software or other technology performs in a similar manner as the Software.
7. You may not extract any JavaScript from the Software and use it in some other application.

4. Ownership

The foregoing license gives you limited license to use the Software. EyeLock and its licensors and suppliers retain all right, title and interest, including all copyright and intellectual property rights, in and to, the Software and all copies thereof. All rights not specifically granted in this EULA, including Federal and International Copyrights, are reserved by EyeLock and its suppliers.

5. WARRANTY DISCLAIMER

1. THE SOFTWARE IS PROVIDED TO YOU ON AN “AS-IS” BASIS. EYELOCK PROVIDES NO TECHNICAL SUPPORT, WARRANTIES OR REMEDIES FOR THE SOFTWARE.
2. EYELOCK AND ITS LICENSORS AND SUPPLIERS DISCLAIM ALLWARRANTIESAND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING THEWARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE ISNO WARRANTY OF NON-INFRINGEMENT

AND TITLE OR QUIET ENJOYMENT. EYELOCK DOES NOT WARRANT THAT THE SOFTWARE IS ERROR-FREE OR WILL OPERATEWITHOUT INTERRUPTION. NO RIGHTS OR REMEDIES REFERRED TO IN ARTICLE 2A OF THE UCC WILL BE CONFERRED ON YOU UNLESS EXPRESSLY GRANTED HEREIN. THE SOFTWARE IS NOTFAULT TOLERANT, AND IS NOT DESIGNED, INTENDED OR LICENSED FOR SECURITY SYSTEMSUSE OR ANY OTHER USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE CONTROLS, INCLUDING WITHOUT LIMITATION, THE DESIGN, CONSTRUCTION, MAINTENANCE OR OPERATIONOF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFICCONTROL, AND LIFE SUPPORT OR WEAPONS SYSTEMS. EYELOCK SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCHPURPOSES.

3. IF APPLICABLE LAW REQUIRES ANY WARRANTIES WITH RESPECT TO THE SOFTWARE, ALL SUCHWARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY.
4. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY EYELOCK, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES SHALL CREATE A WARRANTY OR IN ANYWAY INCREASE THE SCOPE OF ANY WARRANTY PROVIDED HEREIN.
5. (USA only) SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE.
6. EYELOCK SHALL HAVE NO RESPONSIBILITY IF THE SOFTWARE HAS BEENALTERED IN ANY WAY, OR FOR ANY FAILURE THAT ARISES OUT OF USE OF THE SOFTWARE WITHOTHER THAN A RECOMMENDED HARDWARE CONFIGURATION.

Restrictions. This warranty does not apply to any EyeLock Products that: (a) have been altered, except by EyeLock or with the written permission of EyeLock, (b) have not been installed, operated, repaired, or maintained in accordance with instructions supplied by EyeLock, (c) have been subjected to abnormal physical or electrical stress, misuse, negligence, or accident,(d) are licensed, for beta, evaluation, testing or demonstration purposes; or (e) are systems for which EyeLock has not received a payment of purchase price or license fee.

6. LIMITATION OF LIABILITY

1. NEITHER EYELOCK NOR ITS LICENSORS OR SUPPLIERS SHALL BELIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, COVER OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FORTHE INABILITY TO USE EQUIPMENT OR ACCESS DATA,
LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE), ARISING OUT OF THE USE OF, OR INABILITY TO USE, THE SOFTWARE AND BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF EYELOCK OR ITS REPRESENTATIVES HAVE BEEN ADVISED OFTHE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TOHAVE FAILED OF ITS ESSENTIAL PURPOSE.
2. EYELOCK’S AND ITS LICENSORS AND SUPPLIERS’ TOTAL LIABILITY TO YOUFOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER WILL BE LIMITED TO THE AMOUNT PAIDBY YOU FOR THE SOFTWARE THAT CAUSED SUCH DAMAGE.
3. (USA only) SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OF CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU AND YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATETO STATE.
4. THE FOREGOING LIMITATIONS ON LIABILITY ARE INTENDEDTO APPLYTO ALL ASPECTS OFTHIS EULA.

The Warranty Disclaimer and Limited Liability set forth above inure to the benefit of EyeLock’s licensors and suppliers.

7. Software Transfer Allowed But With Restrictions.

You may permanently transfer rights under this EULA only as part of a permanent sale or transfer of the EyeLock product, and only if the recipient agrees to this EULA. If the Software is an upgrade, any transfer must also include all prior versions of the Software.

8. (Outside of the USA) Consumer End Users Only

The limitations or exclusions of warranties and liability contained in this EULA do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than in the course of a business. The limitations or exclusions of warranties, remedies or liability contained in this EULA shall apply to you only to the extent such limitations or exclusions are permitted under the laws of the jurisdiction where you are located.

9. Third Party Software

The Software may contain third party software which requires notices and/or additional terms and conditions. Such required third party software notices and/or additional terms and conditions are listed below and are made a part of and incorporated by reference into this EULA. By accepting this EULA, you are also accepting the additional terms and conditions, if any, set forth therein.

All questions concerning this EULA shall be directed to: EyeLock, LLC.

NanoAccess® By EyeLock

For further assistance, visit the following online resources:

Technical Support Contact Information:

Phone: 855-EYELOCK

support@eyelock.com

Sales Contact Information:

Phone: 855-EYELOCK

sales@eyelock.com

www.eyelock.com

Visit the NanoAccess™ webpage for more documentation and manuals by scanning the QR code.

eyeLock®

Advanced Biometric Identity Authentication