



EP-4xx / EP-736

EP Series

User Programming Guide

Document Number: 10028379 Rev-A

NORTEK
SECURITY & CONTROL

USA & Canada Toll Free (800) 421-1587
or dial (760) 438-7000
www.nortekcontrol.com

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.

EP Series Telephone Entry & Access System Installation Contact Information

Contents

1. Introduction	2
General Features	2
System Information	2
2. Software Layout	3
System Server Software	3
Toolbar Menu	4
4. Using the Wizard	5
Language	6
License	6
Card Format	7
Using the Decoder	7
Holiday Group	8
Schedules	9
Doors	10
Access Levels	14
Resident	15
Card	18
Network	19
Start Save	20
3. System Programming	21
Connect to the Controller	21
Card Holder	22
Card Holder (Cont.)	23
Card Format	26
Access Level	27
Schedule	28
Holiday	29
Unlock Schedule	30
One Time Unlock Schedule	31
Event Action	32
Event Code	33
Threat Level	34
Threat Level Setting	35
Door	36
Aux Input	40
Aux Output	41
Controller	42
User Defined Field	43
User Role	44
Web User Account	45
Update	45
Backup	46
Restore	46
Save & Reboot	47
Factory Default	47
IP Address	48
FTP	49
SMTP	50
Time Server	51
User Data Export	51
User Data Import	52
Log	53
Log Management	55
Report	56
Access Report	57
System Report	58
Card Holder Group	59
Door Group	60
Access Level Group	61
Client Management	62
Client Replacement	63
Logout	64
5. Site Map	65
6. Lost Card	66
7. License	67
8. End User License Agreement	68
Appendix A:	70
Directory Segmentation	70

1. Introduction

This manual contains information regarding the programming and configuration of the EP Series access control system. The 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 smart phone and tablet.
- 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 about each Card Holder such as phone number or employee ID.
- Define up to 30 holidays for use 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.

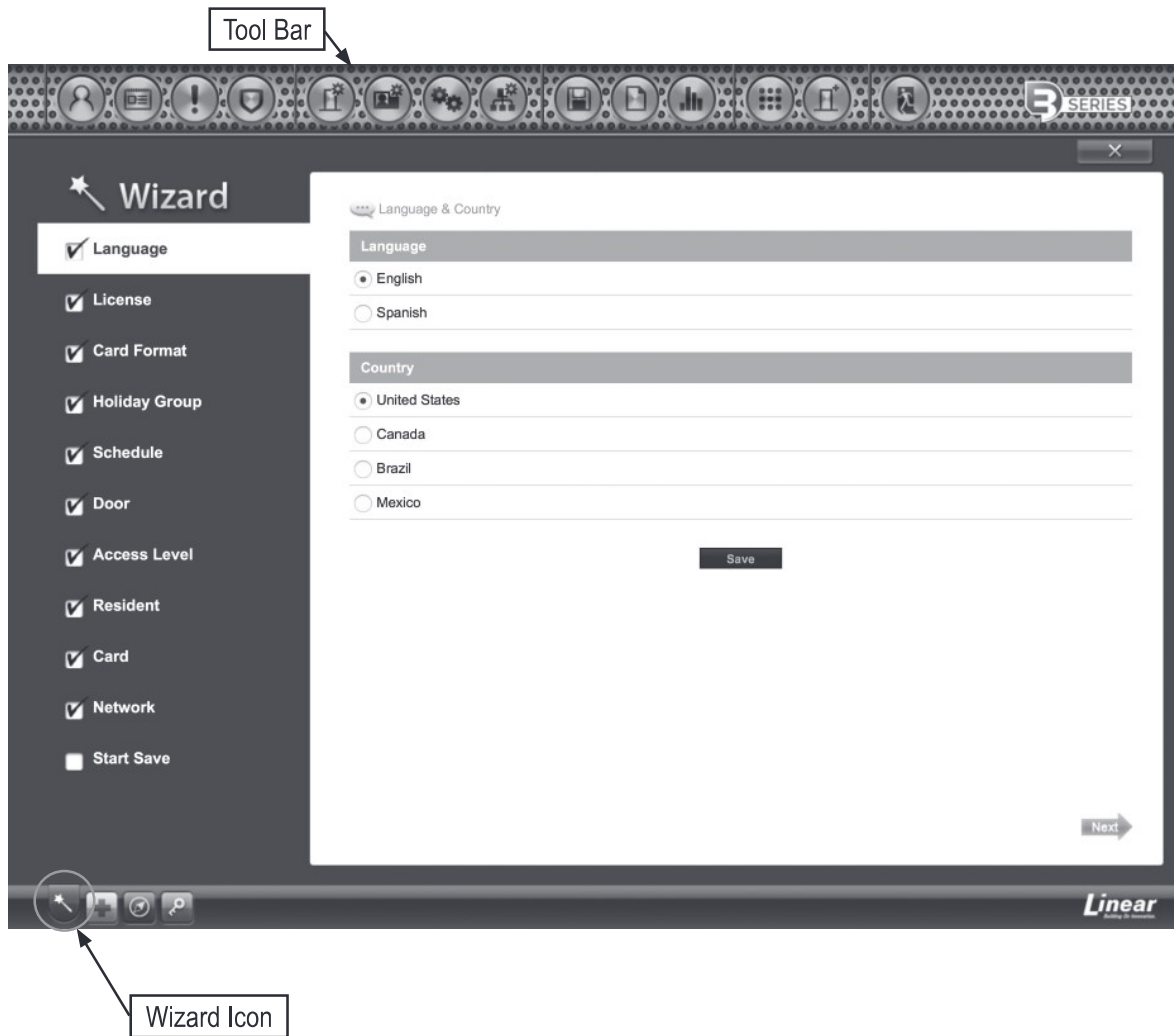
System Information

Feature	System Capacities	
	EP-402	EP-436/736
Model Readers per	4	72
System Doors	2	36
System users per	2	36
System Access Levels	1000	10000
Per person access	32	32
Card	5000	120000
Person Card	32	32
Formats Expansion	32	32
Modules Alarm Input	0	8
Points output	8	126
Points Online event	4	72
History log access level	10000	50000
Per system schedule	250	250
Per system web user role	250	250
Per system one time unlock	32	32
Schedule per system concurrent	150	150
User per system phone	32	32
Number	3000	30000

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.



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
- Network Setup
- System Startup Screen Selection

Toolbar Menu

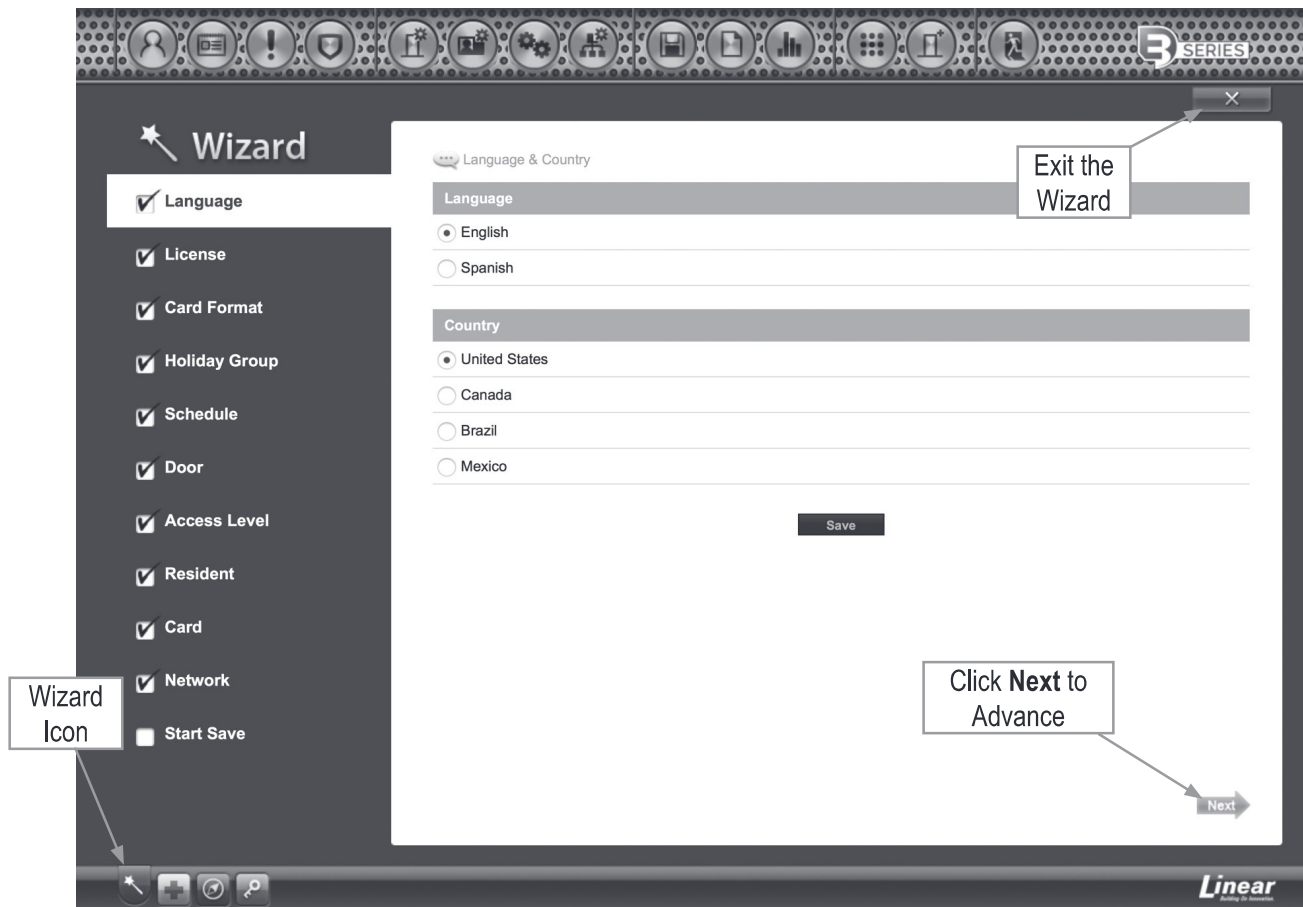
The Toolbar provides access to all setup, programming, management, and reporting options of the Controller.



-  **Administration:** Add, edit, or delete Card Holders, card formats and Access Levels, badge layouts and templates.
-  **Schedule:** Add and edit time schedules, holidays, and unlock schedules.
-  **Events:** Create events that are assigned to actions. For example, a time schedule can be assigned to an auxiliary output.
-  **Threat Level:** Enable and configure Threat Level settings, if Threat Levels are enabled.
-  **Device Setting:** Configure the doors, elevators, inputs and outputs that are licensed and available within the system. Edit Controller locations and region.
-  **User Setting:** Set user fields, define the operators that can login and select their level of system access.
-  **System Setting:** Update, backup, restore or reset the Controller.
-  **Network Setting:** Configure the IP address, FTP, update server, SMTP, time server, and RMC.
-  **Data Transfer:** Export or import data using a CSV file.
-  **Log:** Opens the log database allowing the user to generate, view, and print log reports.
-  **Report:** Provides system and event reporting, smart reports feature customizable report formats.
-  **Group Table:** Enter cards, door and camera groups as well as configure Access Level groups.
-  **Logout:** Logs the operator out of the system.

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.



- » **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.

The screenshot shows the 'Language & Country' configuration screen. On the left, a 'Wizard' sidebar lists several options with checkboxes: Language (checked), License, Card Format, Holiday Group, Schedule, Door, and Access Level. The main area is titled 'Language & Country' and contains two sections. The 'Language' section has two radio buttons: 'English' (selected) and 'Spanish'. The 'Country' section has four radio buttons: 'United States' (selected), 'Canada', 'Brazil', and 'Mexico'. A 'Save' button is located at the bottom right of the main area.



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**.

The screenshot shows the 'License' configuration screen. On the left, the 'Wizard' sidebar lists options with checkboxes: Language, License (checked), Card Format, Holiday Group, and Schedule. The main area is titled 'License' and contains a table with system information. The table has a 'Basic' header and the following rows: Model (TE Server), Software Version (1.00.06 (335ca26782/r23A)), Device Type (Door 36), MAC Address (F0:D1:4F:80:14:D1), and License Key (8DE9B36DF22E85808566EA66BBD805D3331D63FC90C554770A4662C2872E857F). Below the table, there are 'Edit' and 'Print' buttons.

Basic	
Model	: TE Server
Software Version	: 1.00.06 (335ca26782/r23A)
Device Type	: Door 36
MAC Address	: F0:D1:4F:80:14:D1
License Key	: 8DE9B36DF22E85808566EA66BBD805D3331D63FC90C554770A4662C2872E857F



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.*

The screenshot shows the 'Wizard' menu on the left with options: Language, License, Card Format (selected), Holiday Group, Schedule, Door, and Access Level. The main window displays the 'Card Format' table with the following data:

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

At the bottom of the table, there are buttons for 'New', 'Decoder', a search field labeled 'Card Format Name', a 'Search' button, and a 'List All' button. A status bar at the bottom right shows '[1]'.

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.

The screenshot shows the 'Administration > Card Format' window with the 'Basic' tab selected. The 'Auto Scan' dropdown is set to 'Door 1'. Below it is a 'Card Scan' button. The form contains the following fields:

- Default Card Format: Custom (dropdown)
- Card Format Name *: 3-bit card format
- Description: (empty field)
- Facility Code Start Bit *: 3
- Facility Code Length *: 10
- Card Number Start Bit *: 13
- Card Number Length *: 24
- Facility Code *: 12345
- Card Number: 14587946254123585445

At the bottom are buttons for 'Add', 'Reset', and 'Cancel'.



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.

No	Name	Start Date	End Date	Holiday Group
80	Christmas Day	12/25/2019	12/25/2019	
79	Thanksgiving Day	11/28/2019	11/28/2019	
78	Veterans Day	11/11/2019	11/11/2019	
77	Columbus Day	10/14/2019	10/14/2019	
76	Labor Day	09/02/2019	09/02/2019	
75	Independence Day	07/04/2019	07/04/2019	
74	Memorial Day	05/27/2019	05/27/2019	
73	Presidents' Day (Washington's Birthday)	02/18/2019	02/18/2019	
72	Martin Luther King Day	01/21/2019	01/21/2019	

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). It is required to select a Holiday Group to make Holiday active.
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

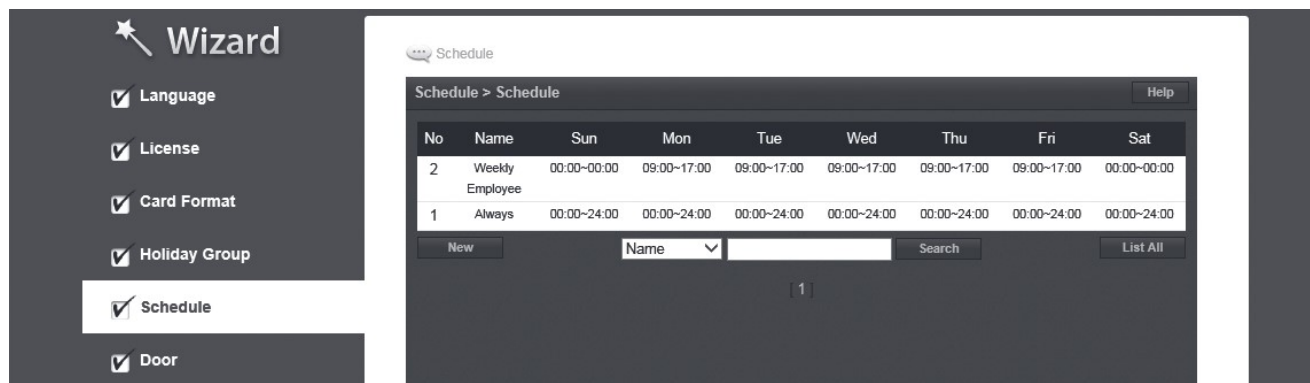
1. Click **New** and enter the desired name, start date and end date.
2. Select the desired holiday group for the new holiday.
3. Click **Add** to save the new holiday.

No	Name	Start Date	End Date	Holiday Group
80	Christmas Day	12/25/2019	12/25/2019	
79	Thanksgiving Day	11/28/2019	11/28/2019	
78	Veterans Day	11/11/2019	11/11/2019	
77	Columbus Day	10/14/2019	10/14/2019	
76	Labor Day	09/02/2019	09/02/2019	



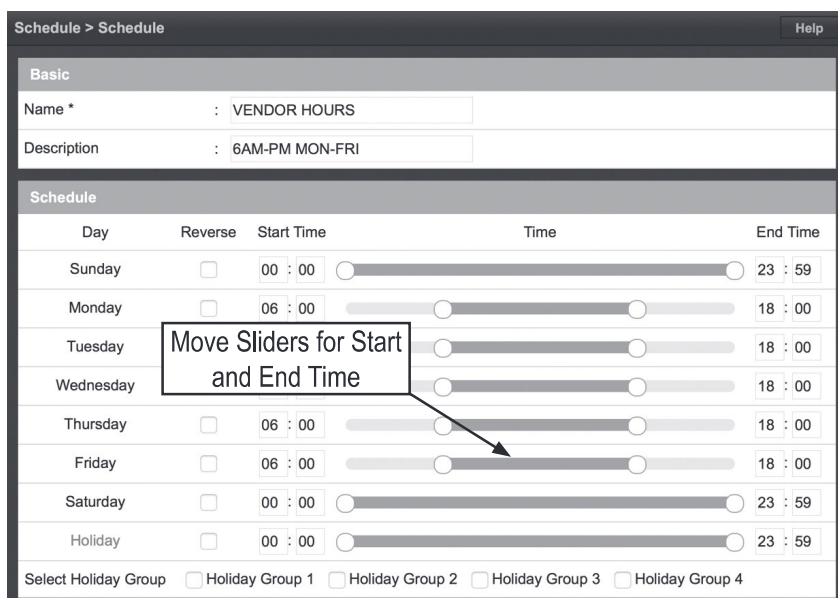
Schedules

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

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.



Doors

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

- ☒ Language
- ☒ License
- ☒ Card Format
- ☒ Holiday Group
- ☒ Schedule
- ☒ **Door**
- ☒ Access Level
- ☒ Resident
- ☒ Card
- ☒ Network
- ☐ Start Save

Device Setting > Door Help

No	Name	Client	Description	Door Lock Mode
12	Door 12	Client 4	Client Door 2	Normal
11	Door 11	Client 4	Client Door 1	Normal
10	Door 10	Client 3	Client Door 2	Normal
9	Door 9	Client 3	Client Door 1	Normal
8	Door 8	Client 2	Client Door 2	Normal
7	Door 7	Client 2	Client Door 1	Normal
6	Door 6	Client 1	Client Door 2	Normal
5	Door 5	Client 1	Client Door 1	Normal
4	Door 4	Server	Server Door	Normal
3	Door 3	Server	Server Door	Normal
2	Door 2	Server	Server Door	Normal
1	Door 1	Server	Server Door	Normal

Door 1 ⌵ ⌵ ⌵ ⌵

1

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

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

Reader

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

Door Contact

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

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.

Device Setting > Door Help

Basic

Name * :

Description :

Floor * :

Reader

Reader Function :

In Reader Name :

In Reader Type :

In Reader Region :

Out Reader Name :

Out Reader Type :

Out Reader Region :

Door Contact

☒ Enable

Door Contact Name :

Door Contact :

Held Open Time : (sec)

ADA Open Time : (sec)

Rex

Door Rex Name :

Rex :

Rex Activates Door Lock : ☒



Doors (Cont.)

Door Lock Mode

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:

Door Lock Mode	
Door Lock Name	: Lock 1
Door Lock Mode	: Normal
Default Status *	: De-Energized
Re-Lock on Open	: ☐
Door Unlock Time	: 3 (sec)

Normal
Door Lock Mode

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

Man-Trap
Door Lock Mode

Pair Door : Door 2

- 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 3 requires 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.



Doors (Cont.)

Door Status Alarm Output

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.

Door Status Alarm Output				
Enable	: ☒ Forced Door	☒ Held Door	Enable	: ☒ Alarm Shunt
Default State	: Energized		Default State	: Energized
Output	: AO 1		Output	: AO 1

Threat Level

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.

Threat Level	
Threat Level	: LOW
Ignore REX	: ☐

Anti-Passback

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.

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



Doors (Cont.)

First Man In Rule

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.

First Man In Rule	
☒ Enable	
Grace Period	0 Minutes (0 = no grace period)
Schedule 1	Always
Schedule 2	4-Day Weeks
Schedule 3	Weekly Employees
SelectType	Individual
Card Holder	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Monte Dezman

Manager In Rule

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.

Manager In Rule	
☒ Enable	
Schedule 1	Weekly Employees
Schedule 2	4-Day Weeks
Schedule 3	
SelectType	Individual
Door Manager	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Gerry Rumsfield

Two Man Rule

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.

Two Man Rule	
☒ Enable	Time : 6 (sec)
Card Holder 1	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Gerry Rumsfield
Card Holder 2	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Monte Dezman

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).

Wizard

- ☒ Language
- ☒ License
- ☒ Card Format
- ☒ Holiday Group
- ☒ Schedule
- ☒ Door
- ☐ Access Level
- ☒ Resident
- ☒ Card
- ☒ Network
- ☐ Start Save

Access Level

Administration > Access Level

Basic

Access Level Name * : Daily Workers

Description : 9-5 Guys

Schedule : Weekly Employee

Select Type : Individual

Door List

Door 8
Door 7
Door 6
Door 5

Door 6

Add Reset Cancel

Access Level Name	Description	Doors	ScheduleName
Main Door	Main Bldg Front	Door 8	Always
Server Room	Main Bldg SR	Door 5	Always

New Access Level Name Search List All

1

Prev Next

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.



Resident

Use **Resident** to enter card users in the database.

To Add a Card Holder

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

Creating a Card Holder

1. Click **New**.
2. Enter the name and contact information of the Card Holder.
3. A phone number is required for the resident to be listed on the display panel.

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



Card Holder (Cont.)

Card Holder Options

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. If desired, click **Vacation Mode** then set the Start and End Date. Enter a phone number.
6. If desired, click **Directory** Listed then enter the Directory Code.
7. Click **Save**.

Option	
Advanced Option	: ☐ Use ADA Timing ☐ Exempt
Web User Account	: None
Threat Level *	: LOW
Do Not Disturb	: ☐
Vacation Mode	: ☐
Start Date	:
End Date	:
Phone	:
Directory Listed	: ☐
Directory Code	:

Entry Code	
Entry Code	:

Access Level	
Select Type	: Individual
Select Level	:
→	
←	
Save Reset Cancel	

Assigning a Card to an Existing Card Holder

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

Card	Card Number	Card Format	Card Status
No			
Add Card			

Card Format

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

Card Enrollment	
Auto Scan *	: 37-bit card format
Card Format *	: 36-bit card format
Card Number *	: IEI 26 Bit Wiegand
Key Number	: Lenel 36bit
Card Status *	: Casi Rusco 40bit
Card Type *	: HID 35bit
	: Honeywell 40bit
	: HID 26bit
Card Status *	: Active
Card Type *	: Normal

Card Number

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



Card Holder (Cont.)

Card Status

1. Select the card's current status.

Card Type

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

Access Level

3. For Select Type select Individual or Group access level.
4. 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

5. Choose an optional activation and expiration date for the card.
6. 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.

DIRECTORY (Add)

Card Enrollment	
Auto Scan *	: Door 1 ▾
Card Format *	: IEI 26 Bit Wiegand ▾
Card Number *	: Card Scan
Key Number	:
Card Status *	: Active Lost Stolen Inactive ← Select the card status
Card Type *	:

Card Enrollment	
Auto Scan *	: Door 1 ▾
Card Format *	: IEI 26 Bit Wiegand ▾
Card Number *	: Card Scan
Key Number	:
Card Status *	: Active ▾
Card Type *	: Normal Guard tour Toggle Passage Relock One time Hazmat Unlock DeadMan Check Select the Card Type

Access Level	
Select Type	: Individual ▾
Select Level	: 🔍 Client 3 Client 2 Server All → All ← Use Arrows to Choose Levels

Activation Date *	
Never Expired	: ☐ Activation Date : 09-23-2015
Inactive Reason	: Expiration Date : 12-31-2015
Save Reset Cancel	

Card				
No	Card Number	Card Format	Card Status	Card Type
2	142(11)	IEI 26 Bit Wiegand	Active	Normal
Add Card				



Card

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

The screenshot shows the 'Wizard' interface for configuring a card. On the left is a sidebar with a list of steps: Language, License, Card Format, Holiday Group, Schedule, Door, Access Level, Resident, Card, Network, and Start Save. The 'Card' step is currently selected and highlighted. The main window is titled 'Administration > Card' and contains a 'Resident *' dropdown menu set to '2157 ADLER'. Below this is a table with the following data:

No	Card Number	Card Format	Card Status	Card Type
1	19286(11)	IEI 26 Bit Wiegand	Active	Normal

Below the table is an 'Add Card' button. At the bottom of the window are 'Prev' and 'Next' navigation buttons.

Assigning a Card to a Card Holder

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.

The screenshot shows the 'Administration > Card' configuration window. It includes a 'Card Holder *' dropdown menu. Below this is the 'Card Enrollment' section with fields for 'Auto Scan *' (set to 'Door 1'), 'Card Format *' (set to 'IEI 26 Bit Wiegand'), 'Card Number *' (set to '5'), 'Key Number' (set to '56'), 'Card Status *' (set to 'Active'), and 'Card Type *' (set to 'Normal'). There is a 'Card Scan' button next to the Card Number field. Below the enrollment section is the 'Access Level' section with a 'Select Type' dropdown (set to 'Individual') and a 'Select Level' list. The list contains 'Daily Workers', 'Main Door', and 'Server Room'. A search icon is next to the list. To the right of the list is a box with the text 'Use Arrows to Choose Levels' and two arrows pointing to the list and the right-hand field. At the bottom is the 'Activation Date *' section with 'Never Expired' and 'Activation Date' options.



Network

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

Basic	
IP Type *	: Static
IP Address *	: 172.16.120.66
Subnet Mask *	: 255.255.255.128
Gateway *	: 172.16.120.1
DNS Server 1	: 8.8.8.8
DNS Server 2	: 8.8.4.4
HTTP Port	: 80
HTTPS	: Off
HTTPS Port	: 443

Buttons: Edit, Prev, Next

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 (required for NTP, SMTP or FTP upgrade features).
6. Enter the IP address of the DNS Server 2 (recommended for NTP, SMTP or FTP upgrade features).
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**.



Start Save

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

Editing Startup Page

The screenshot shows a 'Wizard' window with a sidebar on the left and a main content area on the right. The sidebar contains a list of settings, each with a checked checkbox: Language, License, Card Format, Holiday Group, Schedule, Door, Access Level, Resident, Card, and Network. At the bottom of the sidebar is an unchecked checkbox for 'Start Save'. The main content area has a title bar with 'Start Save' and a close button. Below the title bar, it says 'Congratulation You are all set !! Click Save button.' There is a 'Default Page' dropdown menu set to 'Card Holder'. Below that is a checked checkbox for 'Save to SD Card'. At the bottom of the main area is a 'Save' button. Navigation buttons 'Prev' and 'Next' are at the bottom of the window.

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

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).

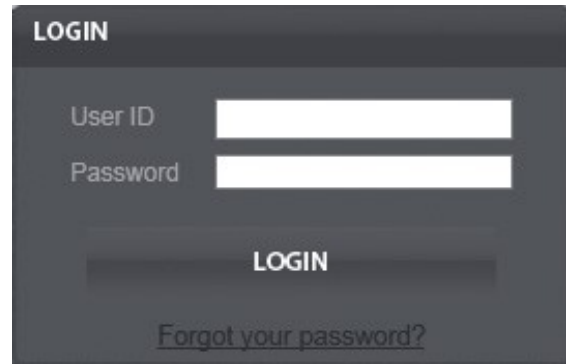
The browser presents the login page as shown.

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

Just in case, a link is displayed to send a message to the EP Series Super Administrator for a forgotten password.

NOTES:

- » *It is highly recommended to change the default password of the system.*
- » *The Super Administrator password is set in Device Settings > Controller.*





Card Holder

Card Holder



Card Holders are individuals who access the facility and are entered in the system. Access credentials are assigned to Card Holders. There are 3 main Card Holder functionalities that are required for the system to work properly.

Administration

1. Fill in your personal information.
2. Enter your First and Last name (required).
3. Enter your phone number (required).
4. Enter your email.

Administration > Resident Help

Personal

First Name * :

Middle Name :

Last Name * :

Phone Number :

Cell Phone :

E-mail :

User Def. Field

The Card

Card Enrollment must be completed for a card to be used on the system. To activate a card:

1. Input Card number on data entry line. Or scan card with reader.
2. Select Card Status as Active.
3. Select appropriate Card Type
4. Select Access Level type.
5. Click **Save**

Card

Card Enrollment

Auto Scan * :

Card Format * :

Card Number * : Card Scan

Key Number :

Card Status * :

Card Type * :

Access Level

Select Type :

Select Level : ➡

Directory Code

1. Check the Directory Listed check box
 2. Input a Directory Code into the data entry line.
- » **NOTE:** Phone number field must be populated for this feature to work.

Entry Code

3. Input an Entry Code in the data entry line.
 4. Click **Save**.
- » **NOTE:** A valid access level is required for the name to appear in the directory.

No	Card Number	Card Format	Card Status	Card Type
Add Card				
Option				
Advanced Option	☐ Use ADA Timing ☐ Exempt			
Web User Account	None			
Threat Level *	LOW			
Do Not Disturb	☐			
Vacation Mode	☐	Start Date		
		End Date		
		Phone		
Directory Listed	☐	Directory Code		
Entry Code				
Entry Code				



Card Holder (Cont.)

Card Holder



Certain features are available to address variable resident needs.

Do Not Disturb

The **Do Not Disturb** option can be used to temporarily prevent the resident's listing to appear on the panel directory.

1. Check the Do Not Disturb check box.
2. Click **Save**.

Unchecking the box will return the resident's phone number to the directory listing.

Vacation

When residents go on vacation, their profile can be set to Vacation Mode. Vacation Mode temporarily makes the resident's phone number unsearchable.

1. Check the Vacation Mode check box.
 2. Input a Start Date.
 3. Input an End Date.
 4. Input a secondary phone number. (Optional).
- » **NOTE:** *The Start Date and End Date must be filled out for Vacation Mode to work.*
5. Click **Save**.

Option	
Advanced Option	: ☐ Use ADA Timing ☐ Exempt
Web User Account	: None
Threat Level *	: LOW
Do Not Disturb	: ☐
Vacation Mode	: ☐
	Start Date :
	End Date :
	Phone :
Directory Listed	: ☐
	Directory Code :



Card Holder (Cont.)

Card Holder



Assigning a Card to an Existing Card Holder

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

Card Format

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

Card Number

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

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

Card Type

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

Card	Card Number	Card Format	Card Status
No			
Add Card			

Card Enrollment	
Auto Scan *	37-bit card format 36-bit card format IEI 26 Bit Wiegand Lenel 36bit
Card Format *	Casi Rusco 40bit HID 35bit Honeywell 40bit HID 26bit
Card Number *	
Key Number	
Card Status *	Active
Card Type *	Normal

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

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

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



Card Holder (Cont.)

Card Holder



Access Level

1. For Select Type select Individual or Group access level.
2. 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.

Access Level

Select Type : Individual ▼

Select Level :
Client 3
Client 2
Server
All

Use Arrows to Choose Levels

Activation Date

3. Choose an optional activation and expiration date for the card.
4. Click **Save** to assign the card to the Card Holder.

Activation Date *

Never Expired : ☐ Activation Date : 09-23-2015

Inactive Reason : Expiration Date : 12-31-2015

Save Reset Cancel

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				
No	Card Number	Card Format	Card Status	Card Type
2	142(11)	IEI 26 Bit Wiegand	Active	Normal
Add Card				



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

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**.
 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.

Administration > Card Format Help

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

New **Decoder** **Search** **List All**

[1]

Basic

Default Card Format :

Card Format Name * :

Description :

Total Bit Length * : Facility Code * :

Facility Code Start Bit * : Facility Code Length * :

Card Number Start Bit * : Card Number Length * :

Add **Reset** **Cancel**

Basic

Auto Scan :

Card Scan **Total 37 Bit :**

Default Card Format :

Card Format Name * : Description :

Facility Code Start Bit * : Facility Code Length * :

Card Number Start Bit * : Card Number Length * :

Facility Code * : Card Number :

Add **Reset** **Cancel**



Access Level

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

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.

Administration > Access Level Help

Access Level Name	Description	Doors	ScheduleName
Client 3	Access to Doors 9-12	Door 9,Door 11	Always
Client 2	Access to Doors 5-8	Door 5	Always
Server	Access to Doors 1-4	Door 3	Always
All	Access to All Doors	Door 3,Door 5,Door 9,Door 11	Always
Test		Door 11	Always

New Access Level Name Search List All

[1]

Administration > Access Level Help

Basic

Access Level Name * :

Description :

Schedule :

Select Type :

Door List

Add Reset Cancel

Adding Access Level

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.

Administration > Access Level Help

Basic

Access Level Name * :

Description :

Schedule :

Select Type :

Select Reader :

Edit Delete Cancel

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.

Administration > Access Level Help

Basic

Access Level Name * :

Description :

Schedule :

Select Type :

Door List

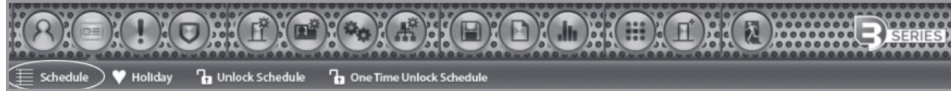
Save Reset Cancel

Editing Access Level



Schedule

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

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.

Schedule > Schedule Help

No		Mon	Tue	Wed	Thu	Fri	Sat
2	Weekly Employees	00:00~00:00	08:55~17:00	09:00~17:00	09:00~17:00	09:00~17:00	00:00~00:00
1	Always	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00

New **Search** **List All**

[1]

Schedule > Schedule Help

Basic

Name * : Weekly Employees

Description : 9-5 M-F

Schedule

Day	Reverse	Time
Sunday		
Monday		
Tuesday	☐	
Wednesday	☐	
Thursday	☐	
Friday	☐	
Saturday	☐	
Holiday		

Select Holiday Group ☐ Holiday Group 1 ☐ Holiday Group 2 ☐ Holiday Group 3 ☐ Holiday Group 4

Add **Reset** **Cancel**

No	Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	Always	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00	00:00~24:00

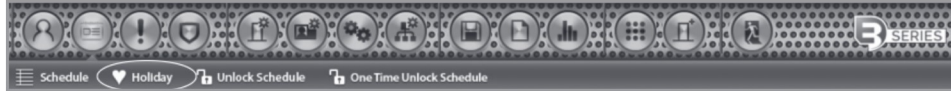
New **Search** **List All**

[1]



Holiday

♥ 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 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 setup.

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.
- » **NOTE:** Access will be restricted on any holiday assigned to a holiday group. See Schedules for information on how to allow access on holidays.

Year : 2015

No	Name	Start Date	End Date	Holiday Group
40	Christmas Day	12/25/2015	12/25/2015	
39	Thanksgiving Day	11/26/2015	11/26/2015	
38	Veterans Day	11/11/2015	11/11/2015	
37	Columbus Day	10/12/2015	10/12/2015	
36	Labor Day	09/07/2015	09/07/2015	
35	Independence Day observed	07/03/2015	07/03/2015	
34	Memorial Day	05/25/2015	05/25/2015	
33	Washington's Birthday	02/16/2015	02/16/2015	
32	Martin Luther King Day	01/19/2015	01/19/2015	
31	New Year's Day	01/01/2015	01/01/2015	

To Add a Holiday Click New

New name Search List All

Basic

Name * : Memorial Day

Start Date : 05/25/2015

End Date : 05/25/2015

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

Edit Delete Cancel

Select a Holiday then Click Edit

Schedule > Holiday Group Help

Basic

Name * : Groundhog Day

Start Date * : 02/02/2016

End : 02/02/2016

Group 1 ☐ Holiday Group 2 ☐ Holiday Group 3 ☐ Holiday Group 4 ☒

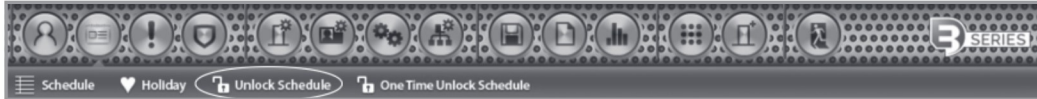
Click Add

Add Reset Cancel



Unlock Schedule

Unlock Schedule

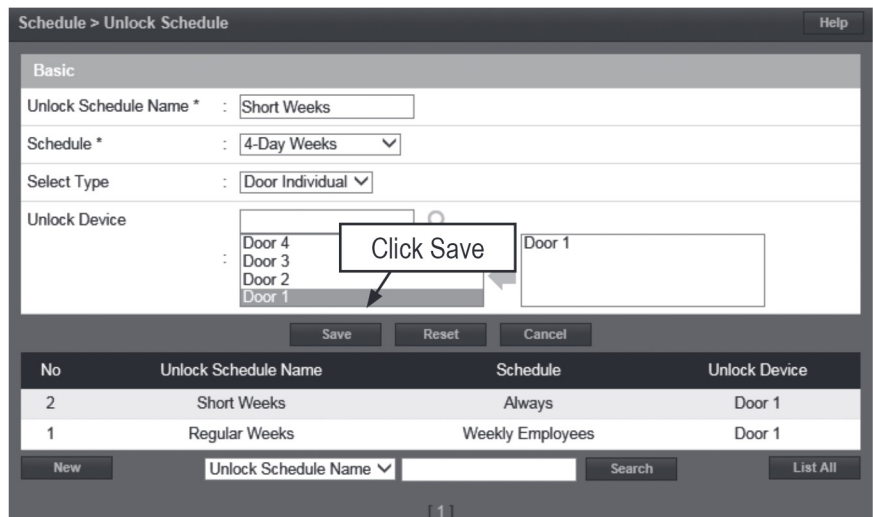
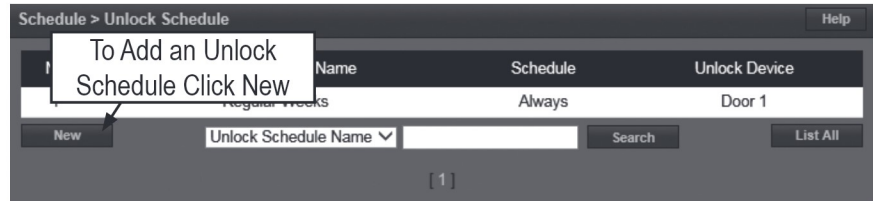


An Unlock Schedule defines which Schedule will be used with selected access devices to automatically unlock one or more doors.

Adding an Unlock Schedule

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.

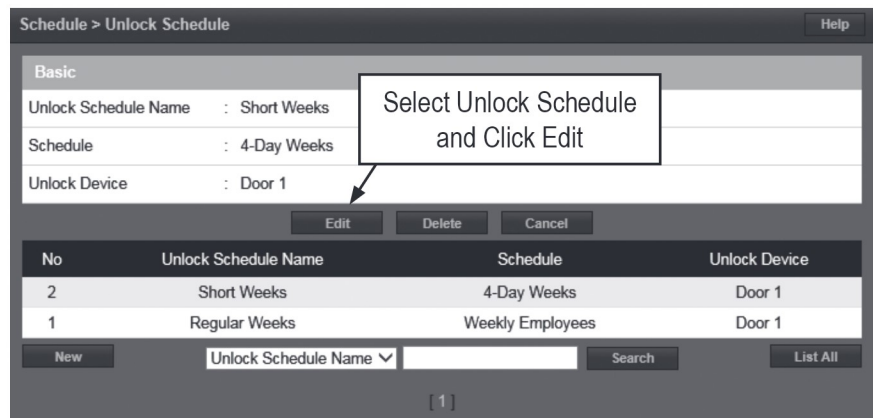


Editing an Unlock Schedule

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

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

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.

To Add a One Time Unlock Schedule Click New

Unlock Device	Date	Time
Door 1	09-26-2015	08:00~16:00

[1]

Editing a One Time Schedule

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

Click Save

Basic

Name * : Carpet Cleaning

Date * : 09-26-2015

Start Time * : 08:00

End Time * : 16:00

Unlock Device * : Door 1

Save Reset Cancel

No	Name	Unlock Device	Date	Time
1	Carpet Cleaning	Door 1	09-26-2015	08:00~16:00

[1]

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.

Select One Time Unlock Schedule and Click Edit

Basic

Name : Carpet Cleaning

Date : 09-26-2015

Time : 08:00~16:00

Unlock Device : Door 1

Edit Delete Cancel

No	Name	Unlock Device	Date	Time
1	Carpet Cleaning	Door 1	09-26-2015	08:00~16:00

[1]



Event Action

! 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.

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 Action > Event Action

No	Event Action Name	Description	Schedule
1		output w Reader	Weekly Employees

New [1] List All

To Add an Event Action Click New

Basic

Name * : Reader Used

Description : Aux output w Reader Schedule : Weekly Employees

Event

No Type Where

Event Source Type : Reader

Where

In Reader 2 In Reader 4

Out Reader 2

In Reader 3

Out Reader 3

Out Reader 4

Event

Access Denied, Zone Anti Pass

Access Denied, Hazmat Lockdo

Access Denied, Manager Absen

Access Denied, Threat Level Vir

Access Denied, Invalid Access I

Access Violation Two Man Rule

Access Granted

Save Cancel

Action

No Type Where Action

Action Source Type : Aux Output

Where

AO 2

AO 3

AO 4

AO 1

Action Triggers Aux Output

Delay Output by : 0 (sec)

ActionSave Cancel

Save Cancel

Action

No Type Where Action

1 System Backup to FTP Server Edit Delete

Action Source Type : System

Where

Pop Up Message to Dashboard

Message : Reader #4 was Used for Access

29 / 80 Bytes

Action Triggers System Event

Choose what the Action will do

Enter Text for E-Mail and Dashboard Messages

ActionSave Cancel

Save Cancel



Event Code

! 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

1. On the Event Code list, edit the checkboxes 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.

Event Action > Event Code Help

Event Code	Name	Dashboard Display ■ Select All	Ack ■ Select All
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 z	☒	☐
400	Granted	☒	☐
1170302	Scheduled Log Backup to SD Card Failed	☒	☒
1170303	Log Backup to SD Card was Successful	☒	☐
1170304	Log Backup to SD Card Failed	☒	☒
1170401	Scheduled Log Backup to FTP was Successful	☒	☐
1170402	Scheduled Log Backup to FTP Failed	☒	☒
1170403	Log Backup to FTP was Successful	☒	☐
1170404	Log Backup to FTP Failed	☒	☒

Save Reset

Name Search

Check to Display Event

Check to Require Event Acknowledgment



Threat Level

Threat Level

Optional
Feature

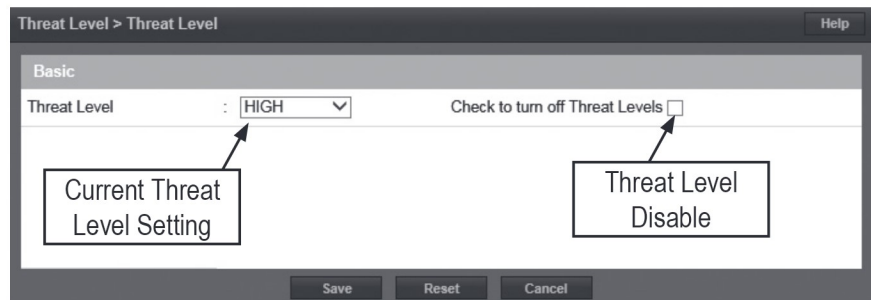
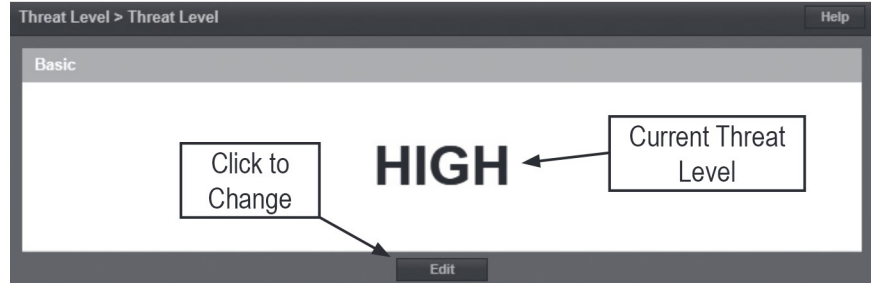


Threat Levels are used in systems to modify existing unlock schedules and Access Level privileges. The system has five predefined Threat Levels. The names of each can be changed to match installation requirements.

Current Threat Level Setting

1. Click **Edit** to change or disable the Threat Level.
2. Uncheck the Turn Off Threat Level checkbox to enable Threat Levels.
3. Use the Threat Level drop-down 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.





Threat Level Setting

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

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 drop-down. 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.

Threat Level > Threat Level Setting

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

Edit

Click to Edit Threat Levels

Threat Level > Threat Level Setting

Basic

Threat Level Count : Threat Level 5

Define Threat Level

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

Save Reset Cancel

Number of Threat Levels

Threat Levels Titles



Door

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

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

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

Reader

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

Door Contact

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

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.

Device Setting > Door Help

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

Name Search List All

[1]

Device Setting > Door Help

Basic

Name * :

Description :

Floor * :

Reader

Reader Function :

In Reader Name :

In Reader Type :

In Reader Region :

Out Reader Name :

Out Reader Type :

Out Reader Region :

Door Contact

☒ Enable

Door Contact Name :

Door Contact :

Held Open Time : (sec)

ADA Open Time : (sec)

Rex

Door Rex Name :

Rex :

Rex Activates Door Lock : ☒

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

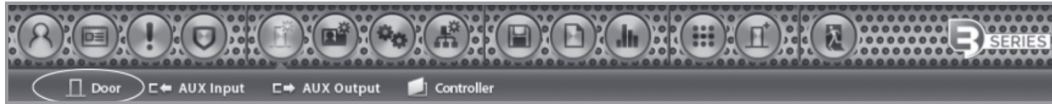
Postal Lock

Enable : No Schedule :



Door (Cont.)

Door



Door Lock Mode

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.

Door Lock Mode	
Door Lock Name	: Lock 1
Door Lock Mode	: Normal
Default Status *	: De-Energized
Re-Lock on Open	: ☐
Door Unlock Time	: 3 (sec)

Normal
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)

Man-Trap
Door Lock Mode

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 3 requires 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 (Cont.)

Door



Door Status Alarm Output

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.

Door Status Alarm Output			
Enable	:	☒ Forced Door	☒ Held Door
Default State	:	Energized ▼	
Output	:	AO 1 ▼	

Threat Level

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.

Threat Level	
Threat Level	: LOW ▼
Ignore REX	: ☐

Anti-Passback

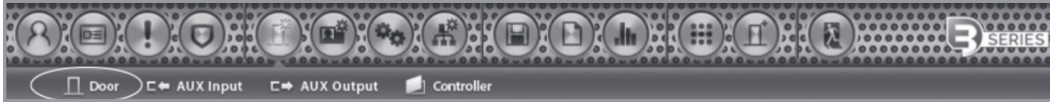
1. Check to enable Timed Anti Passback. Select a time in seconds to disable a credential after it has been used to grant access.
2. Check to enable Room Anti Passback. Select a time in seconds to disable access to a room after access has been granted to the room.

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



Door (Cont.)

Door



First Man In Rule

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.

First Man In Rule	
☒ Enable	
Grace Period	0 Minutes (0 = no grace period)
Schedule 1	Always
Schedule 2	4-Day Weeks
Schedule 3	Weekly Employees
SelectType	Individual
Card Holder	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Monte Dezman

Manager In Rule

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.

Manager In Rule	
☒ Enable	
Schedule 1	Weekly Employees
Schedule 2	4-Day Weeks
Schedule 3	
SelectType	Individual
Door Manager	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Gerry Rumsfield

Two Man Rule

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.

Two Man Rule	
☒ Enable	Time : 6 (sec)
Card Holder 1	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Gerry Rumsfield
Card Holder 2	Q Monte Dezman Gerry Rumsfield Ronnie Gaverty → ← Monte Dezman

Saving Changes

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



Aux Input

← 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

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**.

Device Setting > Aux Input Help

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 Unsupervised

Name Search List All

[1]

Device Setting > Aux Input Help

Basic

Input Name * :

Description : ×

Floor :

Input Type * :

Save Reset Cancel

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 Unsupervised

Name Search List All

[1]



Aux Output

➡ 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

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**.

Device Setting > Aux Output Help

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	Energized	Single Pulse	00:00:03	0	1

Name Search List All

[1]

Basic

Name * : Single Pulse Aux Output

Description :

Mode : On Time : (hrs) (min) (sec)

Floor :

Default State :

Save Reset Cancel

Basic

Name * : Repeating Aux Output

Description :

Mode : On Time : (hrs) (min) (sec)

Off Time : (sec)

Repeat : Number of cycles

Floor :

Default State :

Save Reset Cancel



Controller

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

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.
 - » **IMPORTANT:** The Super Administrator password can only be up to 12 alpha/numeric characters.
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.

Device Setting > Controller Help

No	Name	Controller Location	Tamper Type	Power Fault Type	Time Zone
5	Client 4		NC Unsupervised	NC Unsupervised	
1	Server		NC Unsupervised	NC Unsupervised	

Name Search List All

[1]

Device Setting > Controller Help

Basic

Name * :

Controller Location :

Tamper Input

Tamper Input :

Power Fault Input

Power Fault Input :

Super Administration Account

ID * :

Password * :

Change Password :

Confirm Password :

Email :

Language :

Save Reset Cancel

No	Name	Controller Location	Tamper Type	Power Fault Type	Time Zone
5	Client 4		NC Unsupervised	NC Unsupervised	
1	Server		NC Unsupervised	NC Unsupervised	

Name Search List All



User Defined Field

User Def. Field



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.

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 Setting > User Def. Field Help

Basic			
User Info 1	:	Employee ID #	User Info 2 : Parking Space #
User Info 3	:	License Plate	User Info 4 : Auto Model
User Info 5	:	Auto Make	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 :

Edit

User Setting > User Def. Field Help

Basic			
User Info 1	:	Employee ID #	User Info 2 : Parking Space #
User Info 3	:	License Plate	User Info 4 : Auto Model
User Info 5	:	Auto Make	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 :

Save Cancel



User Role

User Role



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

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

User Setting > User Role Help

:: LIST

No	Name
3	View Only
2	User
1	Super User

New Search List All

[1]

User Setting > User Role

Basic

Default User Role Name

Administration Select All

Card Holder	☐ View ☐ Add ☐ Modify Delete	Card Format	☐ View ☐ Add ☐ Modify Delete
Card List	☐ 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		

Event Action Select All

Event Action	☐ View ☐ Add ☐ Modify Delete	Elevator Action	☐ View
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		



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

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.

User Setting > Web User Account Help

No	User ID	Web User Name	User Role
1	john	john	Super User

New

[1]

User Setting > Web User Account Help

Basic

User ID * : john

Password * :

Web User Name * : john

User Role : Super User

Language : English

Default Page : Dashboard

Default Floor : Default Floor

Floor Show : Yes

Auto Disconnect Time : 01:00



Update



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

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.

System Setting > Update Help

Basic

Software Version : 0.32-07c

Update Type : ☐ User PC ☐ SD Card ☒ Update Server (Last Version : unknown)



Backup

Backup



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

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

System Setting > Backup Help

Schedule backup

Name : System Schedule Backup

Enable : Off

Backup Device : SD Card

Backup Time : 00:00 Backup Occurs Every Day at the Selected Time

Edit

Immediate backup

Backup Type : ☒ User PC ☐ SD Card ☐ FTP Server

Backup

Scheduled Backup

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**.

System Setting > Backup Help

Schedule backup

Name : System Schedule Backup

Enable : ☐

Backup Device : ☒ SD Card ☐ FTP

Backup Time : 00:00 Backup Occurs Every Day at the Selected Time

Save Reset Cancel

Immediate backup

Backup Type : ☒ User PC ☐ SD Card ☐ FTP Server

Backup

Immediate Backup

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



Restore

Restore



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

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.
3. Click **Restore**.

System Setting > Restore Help

Basic

Restore Type : ☒ User PC ☐ SD Card ☐ FTP Server

File : Browse...

Restore

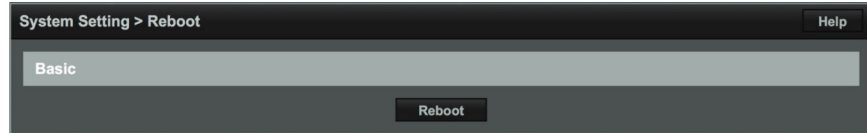


Save & Reboot

Save & Reboot



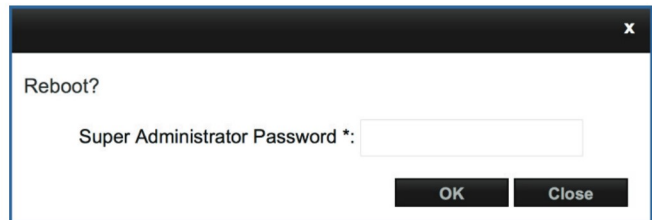
Save and Reboot the system.



Reboot

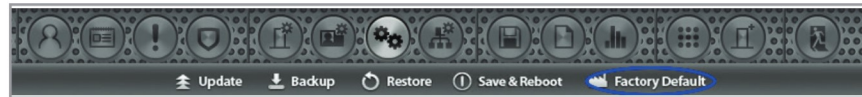
1. Click **Reboot** to force a data save on the Controller and restart the system.
2. Enter an super administrator password and click **OK**.

» **NOTE:** Without battery backup, if the system is powered down prior to saving data, data will be lost. The EP series performs an automatic backup every 1.5 hours and/or upon A/C loss when on battery to permanent memory. If programming prior to field installation, manual backup must be performed via the Save and Reboot tab (on user portal interface) to save data.



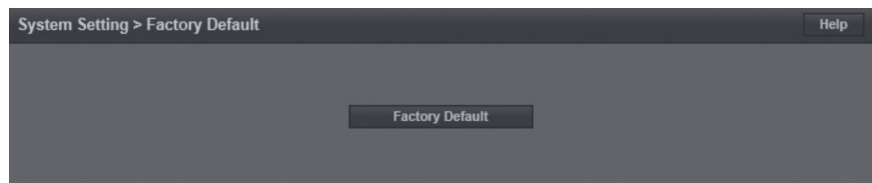
Factory Default

Factory Default



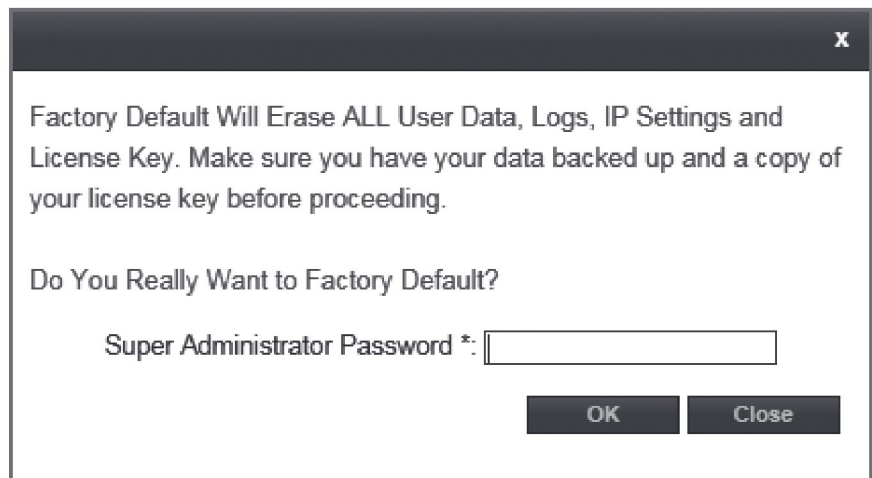
Factory Default will erase ALL Card Holder data, logs, IP settings and license key.

- » **!! 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.



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.
- » **Note:** If needed you can go to e3upgrade.com to recover a license key.





IP Address

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.

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 (required for NTP, SMTP or FTP upgrade features).
6. Enter the IP address of the DNS Server 2 (recommended for NTP, SMTP or FTP upgrade features).
7. Enter the HTTP Port number for remote Web browser connection (typically 80).
8. If using HTTPS, edit the HTTPS Port number if required (default is 443).
9. When finished entering the network settings, click **Save & Reboot**.

Network Setting > IP Address Help

Basic	
IP Type *	: ☐ DHCP ☒ Static
IP Address *	: 172.16.111.82
Subnet Mask *	: 255.255.255.0
Gateway *	: 172.16.111.1
DNS Server 1	: 172.16.111.84 (Optional)
DNS Server 2	: 172.16.111.88 (Optional)
HTTP Port	: 80 (Default 80)
HTTPS	: ☐
HTTPS Port	: 443 (Default 443)



FTP

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.

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.

Network Setting > FTP Help

Basic

Enable	:	
Server Address	:	
Server Port	:	
Server ID	:	
Server Passive Mode	:	
Upload DIR	:	

Edit

Network Setting > FTP Help

Basic

Enable	:	☒
Server Address	:	172.16.111.84
Server Port	:	21
Server ID	:	AKFBE6
Server Password	:	*****
Server Passive Mode	:	☒
Upload DIR	:	/e3Backup/apama/

Test Save Reset Cancel



SMTP

SMTP



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

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 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.*

Network Setting > SMTP

Basic

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

Edit

Network Setting > SMTP

Basic

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

Test

Save Reset Cancel



Time Server

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.

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 time server synchronization from the Sync Time dropdown. Skip to Step 7.
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**.

Network Setting > Time Server Help

Basic

NTP : Manual Time Setting

Sync Time Zone : Eastern

DST

DST :

Edit

Network Setting > Time Server Help

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

Save Reset Cancel

- » **NOTE:** If you do not set up the gateway then the system may not be able to sync time.



User Data Export

User Data Export



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

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.

Data Transfer > User Data Export Help

Basic

File Type : ☒ CSV

Export



User Data Import

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).

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**.



Log

Log



Log displays the most recent events for quick viewing.

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 > Log					Help
Time	Device Name	User Name	Event Code	Event Description	
09-29-2015 10:40:16	70.167.14.131	admin	12205	Data Export Complete	
09-29-2015 08:44:07	70.167.14.131	admin	15107	Web User Login	
09-29-2015 08:40:42	70.167.14.131	admin	15108	Web User Logout	
09-29-2015 07:54:40	Door 4		600	Door Locked	
09-29-2015 07:54:37	Door 4		601	Door Unlocked	
09-29-2015 07:54:37	Door 4	admin	11211	Dashboard M-Unlock	
09-29-2015 07:54:36	Door 3		600	Door Locked	
09-29-2015 07:54:33	Door 3		601	Door Unlocked	
09-29-2015 07:54:32	Door 3	admin	11211	Dashboard M-Unlock	
09-29-2015 07:53:56	70.167.14.131	admin	15107	Web User Login	
09-28-2015 16:24:45	70.167.14.131	admin	15108	Web User Logout	
09-28-2015 15:32:45	70.167.14.131	admin	14003	User Define Field Data Update	
09-28-2015 15:04:33	70.167.14.131	admin	16301	Region Data Added	
09-28-2015 14:24:27	Propped Door AO4		110328	Aux Output Off	
09-28-2015 14:24:26	70.167.14.131	admin	11403	Aux Output Data Update	
09-28-2015 14:18:49	Forced Door A01		110328	Aux Output Off	
09-28-2015 14:18:49	70.167.14.131	admin	11403	Aux Output Data Update	
09-28-2015 14:14:00	Forced Door AO4		110328	Aux Output Off	
09-28-2015 14:14:00	70.167.14.131	admin	11403	Aux Output Data Update	
09-28-2015 14:05:54	AO 4	admin	11414	Dashboard Aux Trigger	
09-28-2015 14:05:46	AO 1	admin	11414	Dashboard Aux Trigger	
09-28-2015 14:05:30	AO 1		110328	Aux Output Off	
09-28-2015 14:05:30	70.167.14.131	admin	11403	Aux Output Data Update	
09-28-2015 13:57:48	AO 1		110328	Aux Output Off	
09-28-2015 07:56:42	70.167.14.131	admin	12603	Threat Level Setting Data Update	
09-28-2015 07:55:29	70.167.14.131	admin	15107	Web User Login	
09-25-2015 16:18:19	70.167.14.131	admin	15108	Web User Logout	
09-25-2015 15:16:12	70.167.14.131	admin	12603	Threat Level Setting Data Update	
09-25-2015 15:15:49	70.167.14.131	admin	12603	Threat Level Setting Data Update	
09-25-2015 14:51:01	70.167.14.131	admin	12603	Threat Level Setting Data Update	
Print					
[1 2 3 >]					



1.Log Report



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

Customizing the Log Report

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.

Log > Log Report Help

DB

Select DB : ☒ Current DB ☐ User PC ☐ SD Card ☐ Current DB & SD Card

Search

Log Date : 09-27-2015 ~ 09-29-2015

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

Search

Date	Log Type	Device Name	Port	User Name	Event Description	Message
09-29-2015	Door Lock	Door 4	4		Door Locked	
09-29-2015	Door Lock	Door 4	4		Door Unlocked	
09-29-2015	Door Lock	Door 3	3		Door Locked	
09-29-2015	Door Lock	Door 3	3		Door Unlocked	
09-28-2015	Door Lock	Door 1	1		Door Unlocked	
09-28-2015	Door Lock	Door 2	2		Door Unlocked	by Man-Trap

Print **CSV**

[1]



Log Management

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

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

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.
2. Click **Backup**.

Log > Log Management Help

Automatic Backup

Automatic Backup or Message pop up when log is 90% full

Pop up message : Log data is full. Please data export!!!

Name :

Enable : Off

Backup Device : SD Card

Edit

Schedule backup

Name : Log Schedule Backup

Enable : Off

Backup Device : SD Card

Backup Time : 00:00 Backup Occurs Every Day at the Selected Time

Edit

Log Reset

Reset

Log Backup

File Type : ☒ CSV Export ☐ e3 DataBase

Backup

Log > Log Management Help

Automatic Backup

Automatic Backup or Message pop up when log is % full

Pop up message :

Name :

Enable : ☐

Backup Device : ☒ SD Card ☐ FTP

Save Reset Cancel

Schedule backup

Name :

Enable : ☐

Backup Device : ☒ SD Card ☐ FTP

Backup Time : Backup Occurs Every Day at the Selected Time

Save Reset Cancel



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

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.

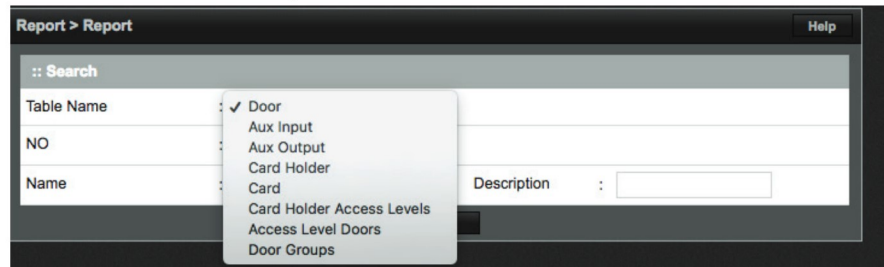
Access Level Number (NO), Access Level, Reader Number (NO), Reader Name, Door Number (NO), Door Name

Door Groups

- Select the filters for the report.

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

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



Report > Report Help

:: Search

Table Name : Door

NO : Floor : Default Floor

Name : Description :

Search

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

Print CSV

[1]



Access Report

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

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.

Report > Access Report Help

:: Search

Type : ☒ Door ☐ Elevator

Date : 09-27-2015 ~ 09-29-2015

Condition

Door : All

Card Holder :

Access Level : All

Search

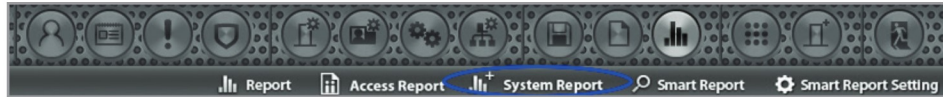
NO	DateTime	Device Name	Card Holder	Card Number
----	----------	-------------	-------------	-------------

Print CSV

[]

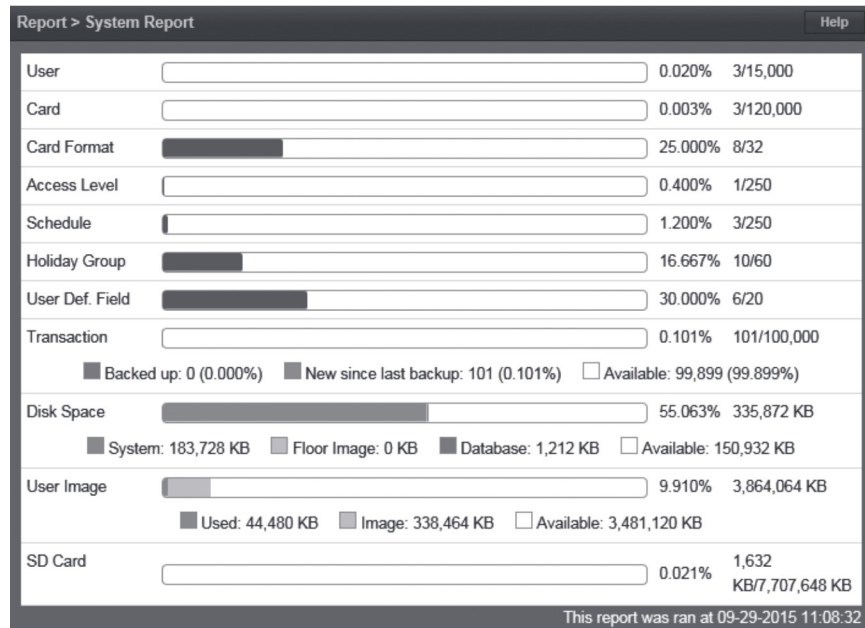


System Report



The System Report displays the current memory allocation of the database.

The report runs when System Report is selected.





Card Holder Group

Card Holder Group



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

Adding a Card Holder Group

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 card holder) 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.

Group Table > Card Holder Group Help

No	Card Holder Group Name	Card Holder List
New	Card Holder Group Name	Search List All

[]

Group Table > Card Holder Group Help

Basic

Group Name * : Core Group

Card Holder List

Monte Dezman
Gerry Rumsfield
Ronnie Gaverty

Monte Dezman
Gerry Rumsfield
Ronnie Gaverty

Adding a Card Holder Group

Add Reset Cancel

Group Table > Card Holder Group Help

No	Card Holder Group Name	Card Holder List
1	Core Group	Monte Dezman, Gerry Rumsfield, Ronnie Gaverty

New Card Holder Group Name Search List All

[1]

Editing a Card Holder Group

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**.

Group Table > Card Holder Group Help

Basic

Group Name * : Core Group

Card Holder List : Monte Dezman, Gerry Rumsfield, Ronnie Gaverty

Selecting a Card Holder Group to Edit

Edit Delete Cancel

No	Card Holder Group Name	Card Holder List
1	Core Group	Monte Dezman, Gerry Rumsfield, Ronnie Gaverty

New Card Holder Group Name Search List All

[1]

Deleting a Card Holder Group

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

Group Table > Card Holder Group Help

Basic

Group Name * : Core Group

Card Holder List

Monte Dezman
Gerry Rumsfield
Ronnie Gaverty

Monte Dezman
Gerry Rumsfield

Editing a Card Holder Group

Save Reset Cancel

No	Card Holder Group Name	Card Holder List
1	Core Group	Monte Dezman, Gerry Rumsfield, Ronnie Gaverty

New Card Holder Group Name Search List All

[1]



Door Group

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

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.

Group Table > Door Group Help

No	Door Group Name	Door List
New	Door Group Name	Search

[]

Group Table > Door Group Help

Basic

Group Name * : Building #2

Door List

Door 4
Door 3
Door 2
Door 1

Door 3
Door 4

Add Reset Cancel

Adding a Door Group

Editing a Door Group

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**.

Group Table > Door Group Help

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

New Door Group Name Search List All

[1]

Group Table > Door Group Help

Basic

Group Name * : Building #2

Door List : Door 3, Door 4

Edit Delete Cancel

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

New Door Group Name Search List All

[1]

Selecting a Door Group to Edit

Deleting a Door Group

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

Group Table > Door Group Help

Basic

Group Name * : Building #2

Door List

Door 4
Door 3
Door 2
Door 1

Door 3
Door 4
Door 2

Save Reset Cancel

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

New Door Group Name Search List All

[1]

Editing a Door Group



Access Level Group

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

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 a 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.

Group Table > Access Level Group

No	Access Level Group Name	Access Level List
New Access Level Group Name Search List All		

[]

Group Table > Access Level Group

Basic

Group Name * : Customer Service

Access Level List

Standard

Standard

Add Reset Cancel

Adding an Access Level Group

Editing a Access Level Group

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**.

Group Table > Access Level Group

No	Access Level Group Name	Access Level List
1	Customer Service	Standard

New Access Level Group Name Search List All

[1]

Group Table > Access Level Group

Basic

Group Name * : Customer Service

Access Level List : Standard

Edit Delete Cancel

1 Customer Service Standard

New Access Level Group Name Search List All

[1]

Selecting an Access Level Group to Edit

Deleting a Access Level Group

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

Group Table > Access Level Group

Basic

Group Name * : Customer Service

Access Level List

Standard

Standard

Save Reset Cancel

No	Access Level Group Name	Access Level List
1	Customer Service	Standard

New Access Level Group Name Search List All

[1]

Editing an Access Level Group



Client Management

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.

Client & Site Setting > Client Management Help

No	Name	Type	IP Address	MAC Address	Alive	Version	
1	Client 3	Elevator	172.16.108.45	F0:D1:4F:FF:FF:72	On	0.32-07e	   
2	Client 2	EV EXT	172.16.108.46	F0:D1:4F:FF:FF:73	On	0.32-07e	   
3	Client 1	Door 4	172.16.108.43	F0:D1:4F:FF:FF:71	On	0.32-07e	   

[1]

Client Management
Buttons

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

Client Replacement

Optional
Feature



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

Replace a Client

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 the **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.

Client > Client Replacement Help

No	Name	Type	IP Address	MAC Address
5	Client 4	Door 2	172.16.120.67	F0:D1:4F:FF:FF:9E

Name Search List All

[1]

Client > Client Replacement Help

Basic

Name : Client 4

Type : Door 2

IP Address : 172.16.120.67

MAC Address * : F0:D1:4F:FF:FF:9E

Edit Cancel

No	Name	Type	IP Address	MAC Address
5	Client 4	Door 2	172.16.120.67	F0:D1:4F:FF:FF:9E

Name Search List All

[1]



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



LOGIN

User ID

Password

LOGIN

[Forgot your password?](#)



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.

 **Site map**

**Administration**

- [Resident](#)
- [Card Format](#)
- [Access Level](#)

**Schedule**

- [Schedule](#)
- [Holiday Group](#)
- [Unlock Schedule](#)
- [One Time Unlock Schedule](#)

**Event Action**

- [Event Action](#)
- [Event Code](#)

**Threat Level**

- [Threat Level](#)
- [Threat Level Setting](#)

**Device Setting**

- [Door](#)
- [Aux Input](#)
- [Aux Output](#)
- [Controller](#)

**User Setting**

- [User Def. Field](#)
- [User Role](#)
- [Web User Account](#)

**System Setting**

- [Update](#)
- [Backup](#)
- [Restore](#)
- [Reboot](#)
- [Factory Default](#)

**Network Setting**

- [IP Address](#)
- [FTP](#)
- [SMTP](#)
- [Time Server](#)

**Data Transfer**

- [User Data Export](#)
- [User Data Import](#)

**Log**

- [Log](#)
- [Log Report](#)
- [Log Management](#)

**Report**

- [Report](#)
- [Access Report](#)
- [System Report](#)
- [Smart Report](#)
- [Smart Report Setting](#)

**Group Table**

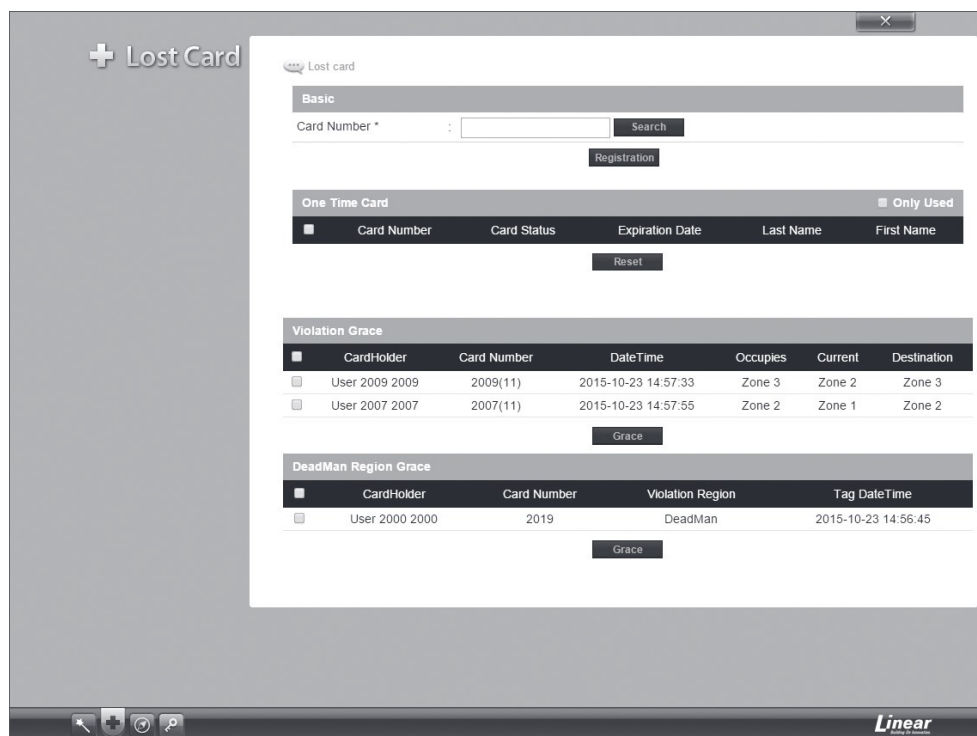
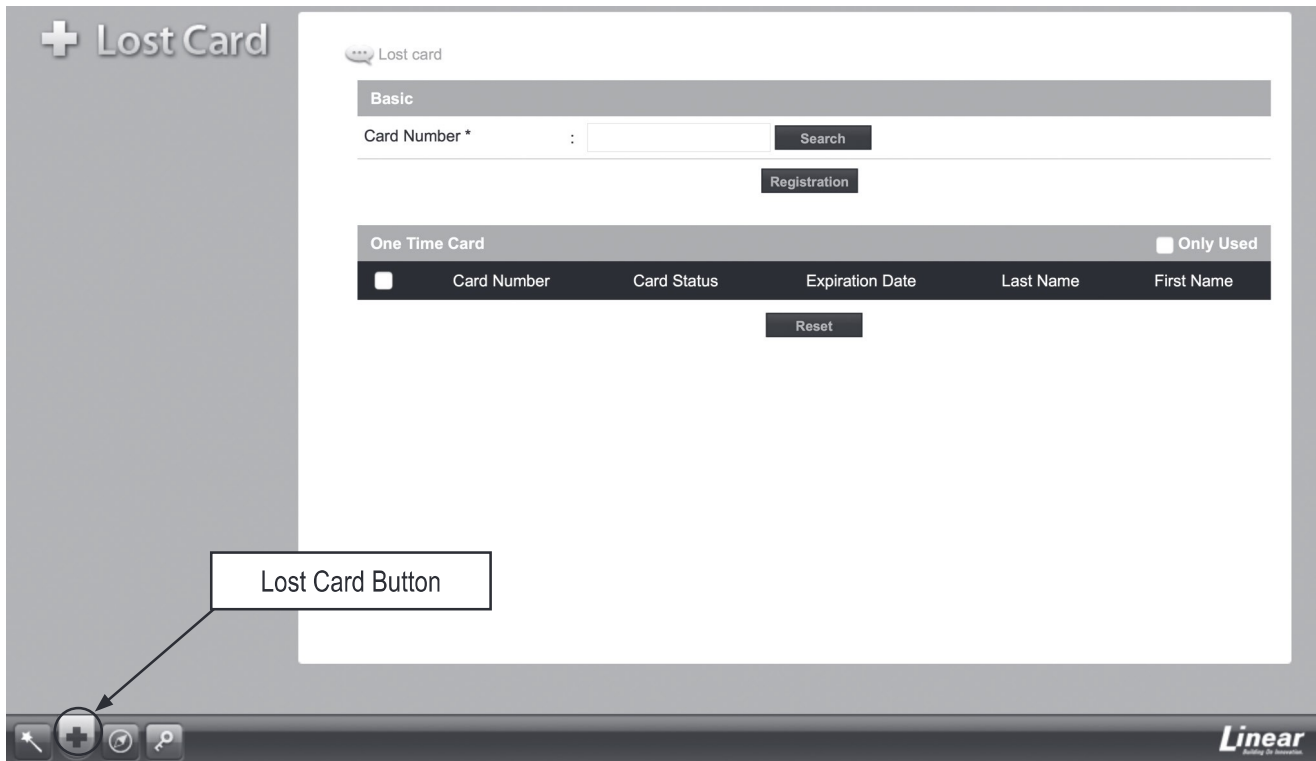
- [Card Holder Group](#)
- [Door Group](#)
- [Access Level Group](#)

**Client & Site**

- [Client Management](#)
- [Client Replacement](#)

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.

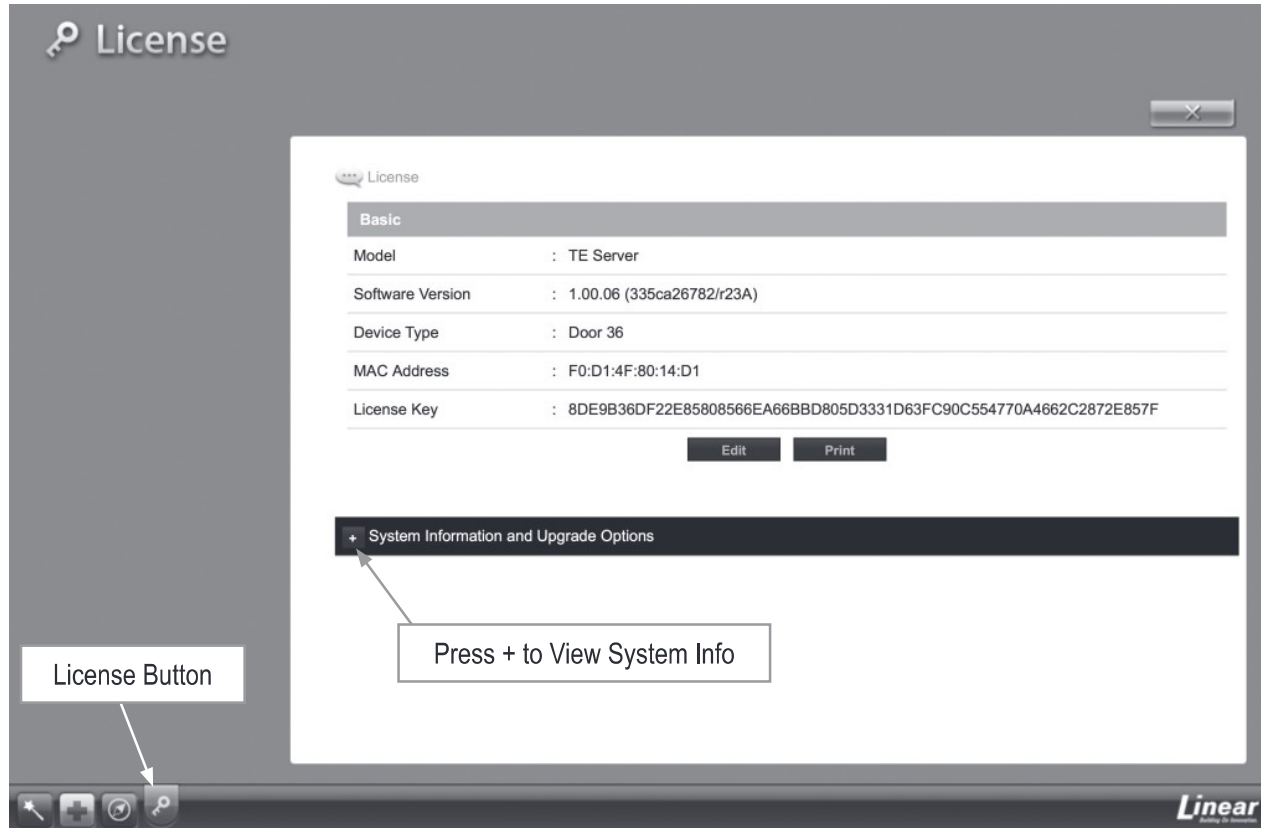




7. License

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

- » **NOTE:** You can use the MAC address to recover the license key for the system. Visit <http://www.e3upgrade.com> and enter the MAC address and follow the directions.



System Information

- 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.

CURRENT SYSTEM CONFIGURATION		DOOR & SYSTEM UPGRADE OPTIONS	
System	TE Server	System	TE Server
Readers per system	72	Readers per system	
Doors per system	36	Doors per system	36
Users per system	10,000	Users per system	
Access levels per person	32	Access levels per person	
Access cards	120,000	Access cards	
Cards per person	32	Cards per person	
Card formats	32	Card formats	
Expansion modules	8	Expansion modules	
Alarm Input Points	126	Alarm Input Points	
Output Points	72	Output Points	
Online Event history log	50,000 transaction	Online Event history log	transaction

Enter comments here

Request Upgrade

Cancel

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 NORTEK SECURITY & CONTROL 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. "Nortek Security & Control" means Nortek Security & Control LLC.
2. "Product" means only the Nortek Security & Control EP Series and other Nortek Security & Control products.
3. "Software" means only the Nortek Security & Control software program(s) and third party software programs, in each case, provided by Nortek Security & Control 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 EP Series product; provided, however, that, notwithstanding anything contrary contained herein, you may not use the Software on any non-Nortek Security & Control 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 Nortek Security & Control EP Series product following procedures authorized by Nortek Security & Control.
2. You agree that Nortek Security & Control 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 Nortek Security & Control 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.

3. License Restrictions

1. You may not make or distribute copies of the Software, or electronically transfer the Software from a Nortek Security & Control product to another Nortek Security & Control 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. You may not export the Software into any country prohibited by the United States Export Administration Act and the regulations thereunder.
6. In the event that you fail to comply with this EULA, Nortek Security & Control may terminate the license and you must stop using this Software and stop operating the Nortek Security & Control EP Series product (with all other rights of both parties and all other provisions of this EULA surviving any such termination).
7. 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 Nortek Security & Control EP Series Product or to determine if such software or other technology performs in a similar manner as the Software.
8. 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, Nortek Security & Control 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 Nortek Security & Control and its suppliers.

5. WARRANTY DISCLAIMER

1. THE SOFTWARE IS PROVIDED TO YOU ON AN "AS-IS" BASIS. NORTEK SECURITY & CONTROL PROVIDES NO TECHNICAL SUPPORT, WARRANTIES OR REMEDIES FOR THE SOFTWARE.
2. NORTEK SECURITY & CONTROL AND ITS LICENSORS AND SUPPLIERS DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS, IMPLIED, OR OTHERWISE, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OF NON-INFRINGEMENT AND TITLE OR QUIET ENJOYMENT. NORTEK SECURITY & CONTROL DOES NOT WARRANT THAT THE SOFTWARE IS ERROR-FREE OR WILL OPERATE WITHOUT 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 NOT FAULT TOLERANT, AND IS NOT DESIGNED, INTENDED OR LICENSED FOR SECURITY SYSTEMS USE OR ANY OTHER USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE CONTROLS, INCLUDING WITHOUT LIMITATION, THE DESIGN, CONSTRUCTION, MAINTENANCE OR OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, AND LIFE SUPPORT OR WEAPONS SYSTEMS. NORTEK SECURITY & CONTROL SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR SUCH PURPOSES.
3. IF APPLICABLE LAW REQUIRES ANY WARRANTIES WITH RESPECT TO THE SOFTWARE, ALL SUCH WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY.
4. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY NORTEK SECURITY & CONTROL, ITS DEALERS, DISTRIBUTORS, AGENTS OR EMPLOYEES SHALL CREATE A WARRANTY OR IN ANY WAY 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. NORTEK SECURITY & CONTROL SHALL HAVE NO RESPONSIBILITY IF THE SOFTWARE HAS BEEN ALTERED IN ANY WAY, OR FOR ANY FAILURE THAT ARISES OUT OF USE OF THE SOFTWARE WITH OTHER THAN A RECOMMENDED HARDWARE CONFIGURATION.

Restrictions. This warranty does not apply to any Nortek Security & Control Products that: (a) have been altered, except by Nortek Security & Control or with the written permission of Nortek Security & Control, (b) have not been installed, operated, repaired, or maintained in accordance with instructions supplied by Nortek Security & Control, (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 Nortek Security & Control has not received a payment of purchase price or license fee.

6. LIMITATION OF LIABILITY

1. NEITHER NORTEK SECURITY & CONTROL NOR ITS LICENSORS OR SUPPLIERS SHALL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, COVER OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR THE 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 NORTEK SECURITY & CONTROL OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.
2. NORTEK SECURITY & CONTROL'S AND ITS LICENSORS AND SUPPLIERS TOTAL LIABILITY TO YOU FOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER WILL BE LIMITED TO THE AMOUNT PAID BY 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 STATE TO STATE.
4. THE FOREGOING LIMITATIONS ON LIABILITY ARE INTENDED TO APPLY TO ALL ASPECTS OF THIS EULA.

The Warranty Disclaimer and Limited Liability set forth above inure to the benefit of Nortek Security & Control'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 Nortek Security & Control 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. U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND.

This Software and the documentation are provided with "RESTRICTED RIGHTS" applicable to private and public licenses alike. Without limiting the foregoing, use, duplication, or disclosure by the US Government is subject to restrictions as set forth in this EULA and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (c)(1)(ii)(OCT 1988), FAR 12.212(a)(1995), FAR 52.227-19, or FAR 52.227-14, as applicable. Manufacturer: Nortek Security & Control LLC, 5919 Sea Otter Place, Suite 100, Carlsbad, CA 92010.

9. (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.

10. 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.

11. This EULA shall be governed by the laws of the appropriate United States jurisdiction, without giving effect to principles of conflict of laws. In each case this EULA shall be construed and enforced without regard to the United

1. Nations Convention on the International Sale of Goods.

This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. You agree that any varying or additional terms contained in any purchase order or other written notification or document issued by you in relation to the Software licensed hereunder shall be of no effect. The failure or delay of Nortek Security & Control to exercise any of its rights under this EULA or upon any breach of this EULA shall not be deemed a waiver of those rights or of the breach.

No Nortek Security & Control dealer, agent or employee is authorized to make any amendment to this EULA. If any provision of this EULA shall be held by a court of competent jurisdiction to be contrary to law, that provision will be enforced to the maximum extent permissible, and the remaining provisions of this EULA will remain in full force and effect.

All questions concerning this EULA shall be directed to: Nortek Security & Control, 5919 Sea Otter Place, Suite 100, Carlsbad, CA 92010.

Nortek Security & Control and other trademarks contained in the Software are trademarks or registered trademarks of Nortek Security & Control LLC or its affiliates in the United States and/or other countries.

All rights strictly reserved. No part of this document may be reproduced, copied, adapted, or transmitted in any form or by any means without written permission from Nortek Security & Control LLC.

Corporate Office

Nortek Security & Control LLC
5919 Sea Otter Place, Suite 100
Carlsbad, CA 92010
Tel: (800) 421-1587 / 760-438-7000

Technical Support

Tel: (800) 421-1587
Hours: 5:00 AM to 4:30 PM Pacific Time, Monday - Friday



Appendix A:

Directory Segmentation

Objective:

- In case of multiple networked TE units with displays (say TE1, TE2 and TE3), residents can be assigned to be displayed on one or more TE units.
- This distribution or “segmentation” is done using the Access Level assigned to the Entry Code associated with each Resident. The reasons is that there can be only one Entry code assigned per Resident.

Steps to implement Directory Segmentation:

1. Create Access Level/s that will include “Door 1” for all TE units in the system. For example, if there are three 2-DR TE units (TE1, TE2 & TE3) networked together, the following Doors need to be given access:
 - 1.1. Door 1 for TE1 which is the server (Door 1 in the system) – being the server, the doors are automatically counted as 4.
 - 1.2. Door 1 for TE2 (Door 5 in the system)
 - 1.3. Door 1 for TE3 (Door 7 in the system)
 - 1.4. Note: The schedule associated with the Access Levels can be as little as 0 minutes. In other words, we can create dummy schedules just for Directory Segmentation, if installers do not want to give Entry Code access to residents.
2. Assign an Entry code to every resident.

Linear®
Building On Innovation.

Administration > Access Level

Basic

Access Level Name * : AL2

Description : Access Level for TE2

Schedule : Always

Select Type : Individual

Door List

Door 6
Door 5
Door 4
Door 3

Door 5

Save Reset Cancel

Access Level Name	Description	Doors	ScheduleName
AL2	Access Level for TE2	Door 5	Always
AL1	Access Level for TE1	Door 1	Always
All Door		Door 1,Door 2,Door 3,Door 4	Always

New Access Level Name Search List All

[1]

User Def. Field

Card

No	Card Number	Card Format	Card Status	Card Type
41	1234(11)	IEI 26 Bit Wiegand	Active	Normal

Option

Advanced Option : ☐ Use ADA Timing ☐ Exempt

Web User Account : None ▼

Threat Level * : LOW ▼

Do Not Disturb : ☐

Vacation Mode : ☐ Start Date :

End Date :

Phone :

Assign a Directory Code, and check (✓) the Directory Listed check box.

Directory Listed : ☒ Directory Code : 87654321

Entry Code

Entry Code : 12345678

Access Level

Select Type : Individual ▼

Select Level : 🔍

AL2
AL1
All Door

➡

AL1

Co Residents

Co-Resident Name	Directory Listed	Directory Code	Entry Code	Phone Number
------------------	------------------	----------------	------------	--------------

Save Reset Cancel

3. Select an appropriate Access Level, based on which TE unit the Resident should be displayed on, Typically, a Resident will only be listed on one TE unit's directory.
 - 3.1. Note: An Entry code with appropriate Access Level is a MUST for the residents to be listed on any directory. This means that even if there is only one TE unit in the system, an Entry code MUST be assigned to every Resident that needs to be listed on the Directory for that TE unit.
4. Ensure that Directory Code is assigned and Directory Listing.
5. Example:
 - 5.1. Resident1, Resident2 and Resident3 need to be listed on TE1, TE2 and TE3 respectively.
 - 5.2. Create Access Levels AL1, AL2 and AL3 that only give access to Door1 (Door 1 of TE1), Door5 (Door 1 of TE2) and Door7 (Door 1 of TE3) respectively.
 - 5.3. Create Entry codes for Resident1, Resident2 and Resident3 and assign Access Levels AL1, AL2 and AL3 respectively.
 - 5.4. Thus, Resident1 will only be listed on TE1, Resident2 will only be listed on TE2 and Resident3 will only be listed on TE3.

These pages in

tentionally left blank.



USA & Canada Toll Free (800) 421-1587
or dial (760) 438-7000
www.nortekcontrol.com