EN Series
User Programming Guide
Document Number: 10017453 X2
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.
## Contents

1. Introduction .............................................. 2  
   General Features ................................... 2  
   System Information ................................... 2  

2. Software Layout ....................................... 3  
   System Server Software .............................. 3  
   Toolbar Menu ......................................... 4  

3. System Programming ................................. 5  
   Connect to the Controller ......................... 5  
   Card Holder .......................................... 6  
   Card Holder (Cont.) .................................. 7  
   Card Format .......................................... 10  
   Access Level ........................................ 11  
   Schedule ............................................. 12  
   Holiday .............................................. 13  
   Unlock Schedule ..................................... 14  
   One Time Unlock Schedule ......................... 15  
   Event Action ........................................ 16  
   Event Code .......................................... 17  
   Threat Level ........................................ 18  
   Threat Level Setting ................................. 19  
   Door .................................................. 20  
   Aux Input ............................................ 24  
   Aux Output .......................................... 25  
   Controller .......................................... 26  
   User Defined Field .................................. 27  
   User Role ........................................... 28  
   Web User Account ................................... 29  
   Update ............................................... 30  
   Backup ............................................... 31  
   Restore .............................................. 32  
   Save & Reboot ....................................... 33  
   Factory Default .................................... 34  
   IP Address .......................................... 35  
   FTP ................................................. 36  
   SMTP ................................................. 37  
   Time Server ......................................... 38  
   RMC ................................................. 39  
   User Data Export .................................... 40  
   User Data Import .................................... 41  

4. Using the Wizard ...................................... 54  
   Language ............................................. 55  
   License ............................................... 55  
   Card Format ......................................... 56  
   Using the Decoder ................................... 56  
   Holiday Group ........................................ 57  
   Schedules ............................................ 58  
   Doors .................................................. 59  
   Access Levels ....................................... 63  
   Card Holder ......................................... 64  
   Card ................................................... 67  
   Network .............................................. 68  
   Dealer Registration .................................. 69  
   Start Save .......................................... 70  

5. Site Map .................................................. 71  

6. Lost Card ............................................... 72  

7. License .................................................. 73  

8. End User License Agreement ....................... 74  

Log ......................................................... 42  
Log Management ....................................... 44  
Report ................................................... 45  
Access Report ......................................... 46  
System Report ......................................... 47  
Card Holder Group .................................... 48  
Door Group ............................................ 49  
Access Level Group .................................... 50  
Client Management .................................... 51  
Client Replacement ................................... 52  
Logout .................................................... 53  

Log Management ....................................... 44  
Report ................................................... 45  
Access Report ......................................... 46  
System Report ......................................... 47  
Card Holder Group .................................... 48  
Door Group ............................................ 49  
Access Level Group .................................... 50  
Client Management .................................... 51  
Client Replacement ................................... 52  
Logout .................................................... 53  

Factory Default ....................................... 34  
IP Address ............................................ 35  
FTP ..................................................... 36  
SMTP .................................................. 37  
Time Server .......................................... 38  
RMC .................................................... 39  
User Data Export .................................... 40  
User Data Import .................................... 41  

5. Site Map .................................................. 71  

6. Lost Card ............................................... 72  

7. License .................................................. 73  

8. End User License Agreement ....................... 74  

---

EN Series User Programming Guide
1. Introduction

This manual contains information regarding the programming and configuration of the EN 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 iPhone, iPad and Android devices.
- Intuitive Wizard allows for ultra-fast setup.
- Configure the system to perform automatic functions on specific days and times. For example, schedule when a door is unlocked or when an employee can gain access to the facility.
- Create, view and print customized reports using the reporting tool.
- Create a set of instructions that the system will follow when an event occurs. For example, when a door is forced open the system can be instructed to turn on a camera and display a graphic.
- Configure the system to store custom information 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

<table>
<thead>
<tr>
<th>Feature</th>
<th>System Capacities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EC</td>
</tr>
<tr>
<td>Model Readers per</td>
<td>2</td>
</tr>
<tr>
<td>System Doors</td>
<td>4</td>
</tr>
<tr>
<td>System users per</td>
<td>2</td>
</tr>
<tr>
<td>System Access Levels</td>
<td>1000</td>
</tr>
<tr>
<td>Per person access</td>
<td>32</td>
</tr>
<tr>
<td>Card</td>
<td>5000</td>
</tr>
<tr>
<td>Person Card</td>
<td>32</td>
</tr>
<tr>
<td>Formats Expansion</td>
<td>32</td>
</tr>
<tr>
<td>Modules Alarm Input</td>
<td>0</td>
</tr>
<tr>
<td>Points output</td>
<td>8</td>
</tr>
<tr>
<td>Points ONline event</td>
<td>4</td>
</tr>
<tr>
<td>History log access level</td>
<td>10000</td>
</tr>
<tr>
<td>per system schedule</td>
<td>250</td>
</tr>
<tr>
<td>per system web user role</td>
<td>250</td>
</tr>
<tr>
<td>per system one time unlock</td>
<td>32</td>
</tr>
<tr>
<td>schedule per system concurrent</td>
<td>150</td>
</tr>
<tr>
<td>user per system phone number</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>3000</td>
</tr>
</tbody>
</table>
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
- Card Holder Setup
- Card Setup
- Network Setup
- Dealer Registration
- System Startup Screen Selection

Refer to the Section in the rear of this manual “Using the Wizard” for details on each Wizard screen.
Toolbar Menu

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

- **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.
- **Site Management:** View and edit client, site, and device information, option to add a custom logo.
- **Logout:** Logs the operator out of the system.
3. System Programming

Connect to the Controller

Open a web browser on a local computer and enter the IP address of the Controller (Default = 192.168.0.250).

The browser presents the login page as shown.

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

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

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

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

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.
Card Holder (Cont.)

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.
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 Holder (Cont.)

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.

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

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

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

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

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

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

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.

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

Deleting a One Time Schedule
1. Select the desired One Time Unlock Schedule to be deleted.
2. Click Delete. A confirmation box will appear.
3. Click OK to confirm.
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 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.
Threat Levels are used in systems to modify existing unlock schedules and Access Level privileges. The system has five pre-defined Threat Levels. The names of each can be changed to match installation requirements.

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

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

There is a three-tier hierarchy of Threat Levels to consider when configuring a 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 dropdown. Up to 25 Threat Levels can be defined.
3. The titles of each Threat Level can be customized to suit the installation.
4. Click Save when finished.
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.
Door (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:
     • 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 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.
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.
7. Select an Output to use for the Alarm Shunt Output.

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.

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.
Door (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.

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.

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.

Saving Changes
After making any edits, be sure to click Save at the bottom of the page.
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.
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.
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.
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.
User Defined 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 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.
Web User Account

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

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.

Immediate Backup
1. Select User PC, SD Card or FTP Server for the backup device.
2. To run an immediate backup, click Backup.
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 from.
3. Click Restore.
Save & Reboot

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

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

Saving Data and Rebooting
1. Click Save Data & Reboot to force a data save on the Controller and restart the system.
2. Enter an super administrator password and click OK.
3. 

NOTE: Without battery backup, if the system is powered down prior to saving data, data will be lost. The EN 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 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.
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 (optional, use for NTP time server access or SMTP e-mail connection).
6. Enter the IP address of the DNS Server 2 (optional, use for NTP time server access or SMTP e-mail connection).
7. Enter the HTTP Port number for remote Web browser connection (typically 80).
8. Check the HTTPS checkbox if RMC is being used.
9. If using HTTPS, edit the HTTPS Port number if required (default is 443).
10. When finished entering the network settings, click Save & Reboot.

Upload cer-key
For installations using HyperText Transport Protocol Secure (HTTPS) communications, the EN Series system uses a default security key and certificate. If the installations network requires a different specific security key and certificate, edit the two items.

1. Click Upload cer-key.
2. Enter the Private Key into the SSL Toolbox.
3. Enter the Certificate into the SSL Toolbox.
4. Click Save & Reboot.
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.
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”) in the SMTP Server field.
3. Enter the incoming port number of the SMTP mail server in the Port field.
4. Enable TLS if your mail server uses secure server communication (this is common). Check the TLS Used checkbox to enable TLS.
5. Enter your SMTP mail server user ID (your email address) in the ID field.
6. Enter your SMTP mail server Password in the Password field.
7. Test the system by entering an email address in the Send to (E-mail Address) field and click Test.
8. Click Save to save the changes.

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

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

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

**Editing Time Server Settings**

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.

**NOTE:** If you do not set up the gateway then the system may not be able to sync time.
The Remote Management Console (RMC) server is used to manage multiple Controllers, usually from a remote location.

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

Editing RMC Settings
1. Click the Connect to RMC checkbox if an RMC server will be used.
2. Enter the RMC Server URL.
3. Enter the RMC Domain UUID.
4. Enter the Device ID.
5. Click Save to keep the changes.

Refer to the RMC User Guide P/N 620-100701 for details on RMC setup and operation.
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.
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 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.
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 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.
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.
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.
The System Report displays the current memory allocation of the database. The report runs when System Report is selected.
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.

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.

Deleting a Card Holder Group
1. Click on the Card Holder Group name to delete.
2. Click Delete.
Door Group

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

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

   **NOTE:** Ctrl-click or shift-click will select multiple doors.
4. Click Add to save the changes.

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

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

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.

Deleting a Access Level Group
1. Click on the Access Level Group name to delete.
2. Click Delete.
Client Management

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.

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 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 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.
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.
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.

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.
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.

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.
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.

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.
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.

**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.
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:
     - 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.
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.
7. Select an Output to use for the Alarm Shunt Output.

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-Unlocks and E-Unlocks may be used to unlock a door that has been locked due to elevated system Threat Level.

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

Anti-Passback
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.
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.

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.

Two Man Rule
With Two Man Rule enabled, two Card Holders must present credentials at the same time in order to unlock the door.

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

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

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

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

Use Card Holder to enter card users in the database. An image may be assigned to the Card Holder for identification purposes.

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. Under File Upload, click Snapshot to take a picture from an attached USB camera or click Browse to select a file to assign an image to the Card Holder for identification purposes.

**NOTE:** Picture files can be 20 Kb maximum. JPG, BMP, or PNG formats.
Card Holder (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. Click Save.

Card Holder Badge
1. Select the Template for the badge.

NOTE: See Section Badge Printing for details on setting up badge design templates.
2. Click Print Badge to launch the badge printing window.
3. Click Print Badge to select the printer and print out the badge.

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 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)
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.
Network

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

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

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

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

Upload cer-key

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

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

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

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

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

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

Editing Startup Page

- Default Page: Use the dropdown selector to choose the page that the system will display upon logon.
- Save to SD Card: Leave this box selected to save the startup information to the SD card. Un-check to save the startup information to the Controller’s memory.
5. Site Map

The Site Map is an overview of the pages within the Controller interface. Each page listed in the site map is linked to the page it represents. This allows the user to quickly jump to any section listed in the site map.
6. Lost Card
Lost Card is a utility to quickly identify the Card Holder associated with a lost card. The operator may enter any card number to view the Card Holder that is associated with the card, reset a One Time Card, or override a Violation Grace.
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.
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.
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 EN 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 EN 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, adopt 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.

4. Event of Termination

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 EN Series product (with all other rights of both parties and all other provisions of this EULA surviving any such termination).

5. Restrictions

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 procedures that seeks to develop like software or other technology, to determine communications protocols used by the Nortek Security & Control EN Series product or to determine if such software or other technology performs in a similar manner as the Software.

6. 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 USE IN CRITICAL ENVIRONMENTS OR FOR USE WITH LIFE-SUPPORTING OR OTHER FUNCTIONALLY CRITICAL APPLICATIONS, INCLUDING ATOMIC, ASTRONOMICAL, METEOROLOGICAL, 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.

7. 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 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 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 OR 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 Forgoing Limitations on Liability are Intended to Apply to All Aspects of This EULA.

The Warranty Disclaimer and Limited Liability set forth above are intended to benefit the 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 licensees alike. Without limiting the foregoing, use, duplication, or disclosure by the United States 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), FAR 227.7202-3(c)(1)(ii)(OCT 1988), FAR 12.212(a) (1995), FAR 52.227-11, or FAR 52.227-14, as applicable. Manufacturer: Nortek Security & Control LLC, 1950 Camino Vida Roble, Suite 150, Carlsbad, CA 92008-6517.

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.

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. General

This EULA shall be governed by the laws of the appropriate United States jurisdiction, without giving effect to principles of conflict of laws.

EN Series User Programming Guide 74

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 1950 Camino Vida Roble, Suite 150, Carlsbad, CA 92008-6517.

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
1950 Camino Vida Roble, Suite 150
Carlsbad, CA 92008-6517
Tel: (800) 421-1587 / 760-438-7000
Fax: (800) 468-1340 / 760-931-1340

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