# Table of Contents

## Foreword

### Part I Introduction

1. Home Screen and Menus ................................................................. 7
2. Using List Views .............................................................................. 12
3. Using Property Views ...................................................................... 14
4. Logging In and Passwords ............................................................. 15
5. Product Registration and Licenses ................................................ 15
6. Notifications .................................................................................. 17
7. Emergency Features ................................................................------- 20

### Part II Monitoring

1. Events ............................................................................................. 22
2. Alarms ............................................................................................ 24
3. Door Status .................................................................................... 26
4. Maps .................................................................................................. 28
5. Muster ............................................................................................. 30
6. Audits ............................................................................................. 31
7. Event History .................................................................................. 33
8. Alarm History ................................................................................ 34
10. User Door Report .......................................................................... 36

### Part III Access Control

1. Users ............................................................................................... 38
   - User Properties ............................................................................. 40
   - Printing Cards ............................................................................ 45
   - Importing Users from a CSV File ............................................... 45
2. Shared Access Codes ...................................................................... 46
3. Emergency Codes ........................................................................... 48
4. Access Levels ................................................................................ 48
5. Schedules ....................................................................................... 49
6. Door Mode Schedules .................................................................... 50
7. Special Days .................................................................................. 51
8. Multi-User Access .......................................................................... 52

### Part IV Configuration

1. Understanding Controllers and Doors ........................................... 55
<table>
<thead>
<tr>
<th>Part V</th>
<th>Administration</th>
<th>92</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>User Roles</td>
<td>92</td>
</tr>
<tr>
<td>2</td>
<td>Backup and Restore</td>
<td>99</td>
</tr>
<tr>
<td>3</td>
<td>System Settings</td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>Network</td>
<td>103</td>
</tr>
<tr>
<td>5</td>
<td>Date and Time</td>
<td>105</td>
</tr>
<tr>
<td>6</td>
<td>Email Settings</td>
<td>106</td>
</tr>
<tr>
<td>7</td>
<td>Archive Downloads</td>
<td>107</td>
</tr>
<tr>
<td>8</td>
<td>Firmware Settings</td>
<td>107</td>
</tr>
<tr>
<td>9</td>
<td>Web Server Settings</td>
<td>108</td>
</tr>
<tr>
<td>10</td>
<td>Authorized Mobile Devices</td>
<td>108</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part VI</th>
<th>Features and Tasks</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lockdown</td>
<td>111</td>
</tr>
<tr>
<td>2</td>
<td>Emergency Unlock</td>
<td>113</td>
</tr>
<tr>
<td>3</td>
<td>Duress</td>
<td>114</td>
</tr>
<tr>
<td>4</td>
<td>Reports and Printing</td>
<td>115</td>
</tr>
<tr>
<td>5</td>
<td>Manual Commands</td>
<td>115</td>
</tr>
<tr>
<td>6</td>
<td>First Credential Unlock</td>
<td>116</td>
</tr>
<tr>
<td>7</td>
<td>Card Enrollment Points</td>
<td>117</td>
</tr>
<tr>
<td>8</td>
<td>Anti-Passback</td>
<td>118</td>
</tr>
<tr>
<td>9</td>
<td>Password Reset</td>
<td>120</td>
</tr>
<tr>
<td>10</td>
<td>Factory Reset</td>
<td>121</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11 Setup Wizard</td>
<td>122</td>
</tr>
<tr>
<td><strong>Part VII Reference</strong></td>
<td>128</td>
</tr>
<tr>
<td>1 Glossary</td>
<td>128</td>
</tr>
<tr>
<td>2 Event Categories and Types</td>
<td>134</td>
</tr>
<tr>
<td>3 Door Modes</td>
<td>142</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>145</td>
</tr>
</tbody>
</table>
1 Introduction

The Atlas Series by ZKTeco is a powerful, yet intuitive, electronic door access-control system supporting the latest innovations in physical security and biometric access. Atlas Series provides:

- Secure and convenient fingerprint access using ZKTeco’s industry-leading biometric technology (Biometric Atlas Series models only)
- Support for industry-standard Wiegand and OSDP card readers, with flexible card format definitions
- Powerful, intuitive, Web Management Application built in to the Controller — all you need is a web browser; no PC software to install or maintain.
- Scalability up to 84 Doors by adding Secondary Controllers, quickly and easily using network-based discovery
- Critical emergency functions: global lockdown, global emergency unlock, alarm management, duress PINs, emergency codes, and muster reporting
- Mobile app for iOS and Android

Using this Guide

The topics in this Introduction explain how to use the Web Management Application generally.

The four main sections correspond to the four main navigation menus: Monitoring, Access Control, Configuration, and Administration. These topics provide general guidance, and have a sub-topic for each menu item.

Features and Tasks describes special features that are not centralized, and explains tasks that are common to several screens.

Reference includes the Glossary and other reference material.
Getting Started

Your Primary Controller should already be installed and configured. (If the Setup Wizard appears when you log in, configuration is not complete. Complete the configuration before continuing.)

To get started:

1. Open a web browser and log in to the Web Management Application.
2. Register the product and add any additional licenses you purchased. Registration is required if you ever need to reset your system password, and optionally allows ZKTeco to contact you about software updates and other information. Additional licenses expand the capacity of your system.
3. Review the Home Screen and Menus.
4. Understand List Views and Property Views. Most screens use one of these views.
5. Take a look at the configuration of your Doors, particularly the Default Mode and the Door Mode Schedule.
6. Learn about the different ways you can assign door access to Users.
7. Consider setting up access for mobile devices.

You now have a fully functioning access control system. Read about Monitoring and Notifications so you can see what’s going on in your system.

Important: After getting started, learn to use the Atlas Series Emergency Features. Some of these require significant setup before you can use them to protect your Users.

1.1 Home Screen and Menus

The Home Screen displays a dashboard-style summary of your system, including recent Event activity. The Menu Bar is available on this screen, as it is on every screen in the application.
Potential security issues and problems are highlighted in red, including Lockdown and Emergency Unlock counts. You can click the links for more information. You can always return to this screen using the Home button towards the upper right on the Main Menu.

The dashboard summary squares include:

- Controllers status summary — link takes you to Hardware
- Doors status summary — link takes you to Door Status
- Backup status (next scheduled backup, most recent backup) — link takes you to Backup and Restore
- Web/Mobile connected client count, and whether the Admin password has been secured (Go to the Users module and change the Admin password to secure it.)
- Recent Events — + View More link takes you to Events

The exact summary squares visible depend on your User Role. Also note that when logging into a Secondary Controller, the summary squares are extremely limited due to the fact that the Secondary Controller gets its data from the Primary Controller.
The Main Menu bar is at the top right of all screens.

**Lockdown and Clear Lockdown**

Click **Lockdown** to quickly lock all Doors in an emergency situation. When a global lockdown is in effect, a message is displayed prominently in the Menu Bar. Note that initiating a lockdown will create an **Alarm** by default.

Click **Clear Lockdown** to re-enable access and return Doors to their default or Scheduled Door Mode.

See **Lockdown** for more information.

**Alarms**

When there are active Alarms, this icon will be red or yellow and show the number of current Alarms. Click to go to the **Alarms** screen.

**Notifications**

Click to view the **Notifications** you have subscribed to. The number of Notifications waiting for you is displayed under the icon.

**Home**

Return to the Home Screen.
Layouts allow you to view multiple features or screens at a time. For example, select a 3-panel layout to work on Access Levels and Schedules while viewing live Events. Each panel has its own navigation menu.

Select the single-pane layout to return to the standard view.

Menu

Opens a menu showing several miscellaneous options. See below.

The exact Main Menu items available depend on your User Role. Also note that when logging into a Secondary Controller, the menu items are extremely limited, because it is mostly managed by the Primary Controller.

Navigation Menu

The Navigation Menu contains items for all of the main screens in the application, organized under four subject buttons. The Navigation Menu is repeated in every panel of multiple-panel layouts. This help manual is organized like the menu—four main sections containing a subtopic for each menu item.

The subjects are Monitoring, Access Control, Configuration, and Administration.
Use the **Back** and **Forward** buttons to navigate through your own history of accessing the screens. (The browser's navigation buttons do not work inside the Web Management Application).

**Language**
Set's the language for the current User. Saved as the default for this User.

Available languages depend on your **software license**. Contact your authorized ZKTeco representative for license upgrades.

**Preferences**
Set's the preferences for the current User. Saved as the default for this User. The preferences are

- "Items per Page", the number of items shown in one page of a list, and
- "Card Enrollment Point"

**Save Logs...**
Creates a file containing program logs and other information for investigating problems. Use when asked to by technical support. If possible, save the logs right after you see a problem, and have it available when contacting technical support.

**Help**
Opens this Help.
About

Opens a window showing product information, including your current version and licenses. Register or add licenses on this screen.

Sign Out

Log out of the Web Management Application, returning to the Login Screen.

1.2 Using List Views

List Views show a list of items in columns. In many cases, the columns can be changed, moved around, and searched.

Note that Property Views also display a list on the left, which has the same controls.

Searching

To search in a column, enter the text in the box at the top of the list.

The default, gray text is the column that will be searched. Click the magnifying glass to change the column.

Column Selection
You can move the displayed columns by clicking and dragging on the column title.

Click the triple bar icon to select which columns to show.

Paging

Lists run to extra pages when the number of items exceed your personal **Items per Page** set in [Menu: Preferences](#).

This box appears at the bottom of the list when there are pages. You can go forward or back a page, go to the end or beginning, or enter a page number.
1.3 Using Property Views

Most configuration is viewed or changed in Property Views. These screens display a list of items you have created on the left, with their properties on the right.

The list can be searched using the same tools as in List Views.

Use the buttons above the properties to create new items, save changes, or delete items.

Many Property Views add additional action buttons to the menu bar. These are generally specific to the kind of screen they are displayed on, and their functions are described in
the documentation for the specific screens. These are shown in gray if they don't apply to the currently selected item.

1.4 Logging In and Passwords

To access the Web Management Application, open a web browser and enter the IP address of the Primary Controller provided by your Atlas Series administrator. (In some browsers, you must type "https://" before the address.) You should "bookmark" this link.

Your browser might display an insecure site warning. The means to bypass this varies among browser applications, but should be shown on the error page as a link labeled "Advanced", "Details", "More Information", or something similar. You can prevent this warning for all Users by installing a signed HTTPS certificate.

Enter the username and password provided by your administrator. If you have lost the password for the "admin" user, see Password Reset.

You cannot change your password unless you have access privileges to edit Users. Ask your administrator for password changes.

1.5 Product Registration and Licenses

Registration is required if you ever need to reset your system password, and optionally allows ZKTeco to contact you about software updates and other information.

Additional licenses let you increase the capacity of your Atlas Series system. You can

- increase the number of Doors or Secondary Controllers allowed,
- increase the number of mobile device connections, and
- add to the languages the system supports.

(Note that "Out" Doors are not counted towards your maximum authorized doors.)
Contact your authorized ZKTeco representative for license upgrades. Current license information can be viewed on the About screen.

How to Register

Follow these steps to register for the first time or to update your registration information.

1. Registration can be started in two ways:
   a. When you log in the first time, click Register Now in the Register Your Product pop-up window, or
   b. Select Menu: About, and click the Register button. (If you have previously registered, the link is Update Registration.)

2. Click the New Registration button in the next pop-up window. (If you have previously registered, the button is View/Update Registration.)

3. Fill in the registration information. Asterisks indicate required information. *The email address you enter must be able to receive your registration information.*

4. Submit your registration automatically or by email.
   a. For automatic registration, click the Submit Online button. You will see a progress window followed by a success message.
   b. For email registration:
      i. Click the Offline Registration button. Read the instructions in the following window.
      ii. Click the Download registration file link, and save the registration data file to your computer.
      iii. Create and send an email message by clicking the email link or entering it in your email program. Your email must contain the registration data file as an attachment, with its original name. The subject and text of the email do not matter.

You will receive a registration confirmation file by reply email. When you do,

1. Open the email and save the attachment to your computer.
2. Click the **Upload Confirmation** button. (If you have already exited from registration, then return to this option by selecting **Menu: About** and clicking the **Register** button.)

3. Find and open the registration confirmation file you saved. You should see a "Registration successful" message window.

### How to Add Licenses

When you acquire an additional license, you will receive a license file from ZKTeco. Save this file on your computer, then:

1. Select **Menu: About**.
2. Click the **Upload Additional Licenses** button.
3. Click on the **Browse** button, and **Open** the license file you received.
4. Click **OK**. Your new capabilities should be listed on the About screen.

### Related Topics

- [Home Screen and Menus](#)
- [Password Reset](#)

### 1.6 Notifications

Notifications allow each user to select certain **Events** they wish brought to their attention. When one of these Events occurs, it will appear in the Notification window of that User, and remain there until acknowledged.

Notifications can be copied to you by email.

Click the **Notifications** icon in the Menu Bar to open and close the Notifications Window at the bottom of the screen.
Configuring Notifications

Configure Notifications to select the Events that generate Notifications for the current User. No Notifications are created unless you select them.

1. Click **Notifications** on the Menu Bar.
2. Click the **Configure notifications** link in the Notifications Window.
3. If desired, check **Send a Copy of Notifications by Email**.
   - Otherwise, Notifications are displayed in the Web Management Application only.
   - You must have an email address configured in **Users** and an email server configured in **Email Settings**.
4. Check the Event categories and types you wish to receive Notifications for.
   - Select a category to receive Notifications for all Event Types in that category, or
   - Expand the category and select specific Event Types.
5. Click **Save**.

### Clearing Notifications

To clear Notifications in the list, click one of the buttons next to **Configure notifications**.

- Select one or more Notifications and click this to clear them.
- Click to clear all Notifications.

Note that since Notifications are on a per-User basis, if one User clears a Notification, other Users' Notifications are unaffected.

### Emailing Notifications

To receive copies of all Notifications by email, you must configure email for the system and for yourself.

1. Configure the Web Management Application **Email Settings**.
2. Enter an **Email Address** on your **User** page.
3. Select **Send a Copy of Notifications by Email** under **Configure notifications**, above.

### Maximum Number of Notifications

To define the maximum number of Notifications per User:

1. Go to **System Settings**.
2. Enter the **Maximum Notifications per User**.
3. Click **Save**.

The oldest Notifications are deleted when the maximum number is reached.

### Related Topics

- **Email Settings**
• **System Settings**

1.7 **Emergency Features**

Your Atlas Series system is designed with a number of important features used to aid in a variety of emergency situations.

- **Lockdown** can be configured and used to secure facilities against an active intruder or threat.
- **Emergency unlock** can be configured and used to aid access by emergency personnel in the event of an active emergency condition signaled from another system.
- **Duress PINs** can be used to allow users to signal a duress condition during their otherwise normal access.
- **Emergency Codes** can be configured and used to allow access to emergency or security personnel using a PIN-code only, regardless of Door Mode (including lockdown), or Multi-User Access Rules.
- **Muster** can be used to aid in the tracking of users during an evacuation, or evacuation drill.
- **Alarms** and **Notifications** can be configured and used to make sure the correct personnel are aware of potential emergency situations.

**Important:** All emergency functions intended to be used in your system should be tested ahead of time, to ensure that everything is configured and working correctly.

**Important:** These emergency functions are designed as a supplement to, but not a replacement for, life-safety infrastructure for your facility. Life-safety functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance.
2 Monitoring

Monitoring gives you live views of what's occurring in the system, and printable reports of configuration and history.

Live Monitoring

Events is a live view of everything that happens in the system.

Alarms shows Events that you have determined should be immediately reviewed and action taken. Each Alarm must be acknowledged and cleared by someone who has resolved the problem. Note that Events do not become Alarms until you set up Alarm Triggers.

Door Status shows the current state of every Door, whether it be on line, locked, alarmed, and so forth.

Maps show similar status as Door Status, with visual indicators displayed on a Map of your facilities. The Maps must first be created in Maps (Configuration).

Reports

Muster is a special report that can show you where Users are in an emergency or an evacuation drill. To use the Muster report, you should first designate Muster Areas. Users must check in at the Muster Areas to indicate that they are safely out of the facility.

The remaining menu items are simple reports.

Audits shows configuration changes and actions performed by Users logged into the Web Management Application.

Event History is a report view of Events, with the ability to display a larger number Events and export to CSV and PDF.

Alarm History shows all Alarms, including those that have been resolved (resolved Alarms are not shown on the live Alarms screen).

User Access Level Report shows which Users have a specific Access Level.
User Door Report shows which Users have access to a specific Door. This report includes Doors directly assigned to the Users as well as those assigned via an Access Level.

Related Topics

- Reports and Printing

2.1 Events

Events displays a real-time list of Events occurring within the system. Events that trigger Alarms are displayed in a configurable color.

To receive an email when important Events occur, see Notifications.

Up 1000 Events can be displayed. To view more Events, use Event History.

Menu Buttons

- **Filter**
  Opens a panel where you can restrict the Events you wish to see in the list view. Your filters remain in place each time you log in.

  Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

- **User and Device Filters**
  The display shows only the Events that match all the filters you specify. Note that the **Name** filters are case-insensitive, and will find partial matches. For instance, if you enter "john", the display will also show Events for "John", or "Johnny".

- **Event Type Filter**
  The display shows Events that match any of the Event Types you have checked. If nothing is checked, all Events are displayed.
Clear  Clear the current list of Events from the display, so only new Events appear. Events are hidden, but not deleted.

### Events Columns

Some columns will be empty for certain types of Events.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Category of Event</td>
</tr>
<tr>
<td>Occurred</td>
<td>When the Event actually occurred (determined by the Controller on which it occurred)</td>
</tr>
<tr>
<td>Description</td>
<td>Text of the Event</td>
</tr>
<tr>
<td>User</td>
<td>The User associated with the Event. This could also be a Shared Access Code, Emergency Code, or credential (card, PIN) that is not assigned to a single User.</td>
</tr>
<tr>
<td>Source</td>
<td>The device that recorded the Event. For door access Events, this is a Door. For other Events, this may be a Controller, input, output, or other device.</td>
</tr>
<tr>
<td>Recorded</td>
<td>(Hidden by default) The time the Event was received and recorded by the Primary Controller. This only differs from Occurred if the Secondary Controller where it occurred was offline with the Primary Controller at the time of the Event.</td>
</tr>
<tr>
<td>Controller</td>
<td>(Hidden by default) Controller where the Event occurred</td>
</tr>
<tr>
<td>Area</td>
<td>(Hidden by default) If the Event is associated with an Area (for example a Door entering an Area), the Area is indicated here.</td>
</tr>
</tbody>
</table>
Location (Hidden by default) If the source is associated with a Location, it is indicated here.

## Event Archiving

The oldest Events are automatically archived to CSV files on the Primary Controller when the maximum number is reached. To download the archived data, see Archive Downloads. To change the maximum number of Events in the system, go to System Settings and set the Maximum Events in Database.

## Related Topics

- Using List Views
- System Settings
- Event History

## 2.2 Alarms

Alarms are issues that may indicate a potential security threat or other problem. They cause a warning display on the Main Menu bar, and they remain in effect until they are resolved by a User.

Alarms are triggered by Events. Some Event Types are set to trigger Alarms by default. You can make more Events trigger Alarms, or change the defaults, in Alarm Triggers.

To receive an email when an Event causes an Alarm, see Notifications.

The color of an Alarm is determined by its state, which can be:

- New (Red) — this means the Alarm is active.
• Acknowledged (Yellow) — this means that some User has acknowledged the Alarm.

Resolved Alarms are removed from the list. They can be viewed in Alarm History.

Repeated Alarms are merged into a single Alarm. The Count column shows how many times it has occurred, and Last Recorded shows the most recent time it occurred. Alarms are merged when they are identical in all ways except for the date and time. Once resolved, any new occurrence will make a new Alarm.

Menu Buttons

Acknowledge

Indicates that a User is aware that the Alarm has occurred, changing its state to "Acknowledged." The User is indicating they have accepted an agreed level of responsibility for resolving the issue.

Resolve

Indicates that any problem has been dealt with, changing its status to "Resolved." The Alarm will be removed from this screen, but can be viewed in Alarm History. Alarms must be acknowledged before they can be resolved.

Acknowledge All

Acknowledges all Alarms that are in the "New" state

Resolve All

Resolves all Alarms that are in the "Acknowledged" state

Alarms Columns

Description

Description of the triggering Event

Source

The device that recorded the Event. For door access Events, this is a Door. For other Events, this may be a Controller, or other device.
Priority  The priority of this Alarm (as configured in Alarm Triggers [8])

Count  The number of times the triggering Event has occurred and merged into one Alarm

First Recorded  Time of the first triggering Event

Last Recorded  Time of the most recent duplicate triggering Event

State  "New" or "Acknowledged". The "Resolved" state is only visible in Alarm History [54]. The state determines the color (see above).

Location  Location [70] where the triggering Event occurred

Area  (hidden by default) Area [20] where the triggering Event occurred

Related Topics

- Using List Views [12]
- Alarm Triggers [8]
- Alarm History [54]
- Emergency Features [20]

2.3 Door Status

Door Status displays a real-time list of all Doors and their status. You can also use Manual Commands [11] to unlock a Door temporarily or change the Door Mode.

Menu Buttons
**Manual Commands**

Send a [Manual Command](#) to the selected Door, such as to temporarily unlock it or change its Door Mode.

<table>
<thead>
<tr>
<th><strong>Door Status Columns</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Door</strong></td>
</tr>
<tr>
<td><strong>Communications</strong></td>
</tr>
<tr>
<td><strong>Door Mode</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>Errors</strong></td>
</tr>
<tr>
<td><strong>Alarm</strong></td>
</tr>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>- In</td>
</tr>
<tr>
<td>- Out</td>
</tr>
<tr>
<td>- Muster Point</td>
</tr>
<tr>
<td>- Card Enrollment Point</td>
</tr>
<tr>
<td><strong>Location</strong></td>
</tr>
</tbody>
</table>
2.4 Maps

The Maps view is used to show the status of your Doors and Controllers on graphical backgrounds, for example, on Maps of your building or campus. It highlights all problems in red, and allows sending commands to Doors. Maps may also have links to other Maps for easy navigation.

In this example there are two Doors and two Controllers. The "Rear Door" is offline and should be checked on. They gray icons represent normal operation.

- **Using List Views**
- **Manual Commands**
Before they can be viewed, Maps must be created and configured in the Maps (Configuration) screen.

Menu Buttons

**Manual Commands**

Click on a Door to enable the Manual Commands button, allowing commands such as temporarily unlocking it, or changing its mode. See Manual Commands."
Zoom In / Zoom Out  Make the Map larger or smaller. When zoomed in, you can click and drag on the Map to see different areas.

- Related Topics

  - Using List Views
  - Maps (Configuration)
  - Manual Commands

2.5 Muster

The Muster report shows the last known location of Users who are not registered in a safe Area. Use this report when evacuating a building or buildings or performing an evacuation drill. This lets security personnel know who is still inside the building(s).

Users counted as "safe" are

- Users who have exited to Global Out or reported at a Muster Point and
- Users who have not used any Door within 24 hours.

Muster reports may or may not include Users who have used a Shared Access Code or Emergency Code.

- Creating a Muster Point

Muster points can be created when creating 1-door model Controllers.

1. Go to Hardware.
2. Select a 1-door model.
3. For Configuration, select a Muster option, such as In Only + Muster Point.

You can also modify 1-door or 2-door Controllers or enrollment points into Muster Points. For example:

1. Go to Hardware.
2. Select a 1-door or 2-door Controller.

3. Turn the spare readers into Muster Points.

--- Generating a Muster Report ---

1. Go to Muster. A list of existing muster points is displayed at the bottom.

2. Select List By — Last Name or Area.

3. Select Orientation — Landscape or Portrait.

4. Click Generate.

--- Related Topics ---

- Reports and Printing [115]
- Hardware [38]
- Emergency Features [20]

2.6 Audits

Audit reports list configuration changes and actions performed by Users of the Web Management Application. Use these reports to see who unlocked a Door, gave access to a User, configured Access Levels, and other system operations.

When generating the report, you are prompted for the following options. Options vary based on the Audit Type selected. Click Generate to create the report.

--- Report Options ---

Orientation  Displays the report in "Portrait" or "Landscape" view

Audit Type  
- Database Change — shows changes to items in the database (Users, Doors, Access Levels, etc.), and enables further filtering
options.

- **Manual Command** — shows Manual Commands executed on Doors, and enables further filtering options.
- **Any/All** — both of the above

**User**

If selected, the report will only show actions taken by a specific User.

**From / To**

Limits the report to a date range

**Change Type**

For **Database Change**, which types of changes to include:

- **Inserted**
- **Updated**
- **Deleted**
- **Any/All**

**Object Type**

For **Database Change**, which types of items to include (User, Door, etc.)

**Manual Command**

For **Manual Command**, limits the report to one command type

**Device**

For **Manual Command**, limits the report to a single Door

---

**Related Topics**

- **Reports and Printing**
- **Users**
2.7 Event History

Event History displays a list of Events according to a filter, and allows export to CSV and PDF. The maximum number of Events in this screen is limited only by the number of Events in the database. For a real-time view, see Events.

Menu Buttons

Export CSV  Export the displayed Events to a data file appropriate for importing into program like Excel. ("CSV" designates the "comma separated values" file format.)

Export PDF  Save the displayed Events as a printable report in PDF format.

Filter Pane

Settings take effect when you click the Search button, at the bottom of the panel. The Reset button clears all filters.

Date and Time Filter

Shows only Events from the specified time period.

User and Device Filters

The display shows only the Events that match all the filters you specify. Note that the Name filters are case-insensitive, and will find partial matches. For instance, if you enter "john", the display will also show Events for "John", or "Johnny".

Event Type Filter

The display shows Events that match any of the Event Types you have checked. If nothing is checked, all Events are displayed.

Events Columns
See [Events](#)

### Event Archiving

The oldest Events are automatically archived to CSV files on the Primary Controller when the maximum number is reached. To download the archived data, see [Archive Downloads](#).

To define the maximum number of Events in the system, go to [System Settings](#) and set the [Maximum Events in Database](#).

### Related Topics

- [Using List Views](#)
- [Reports and Printing](#)
- [System Settings](#)
- [Events](#)

### 2.8 Alarm History

Alarm History displays all Alarms, including resolved ones. Resolved Alarms are hidden in the [Alarms](#) screen. This view does not update in real-time or allow you to acknowledge or resolve Alarms.

### Menu Buttons

- **Filter**: Opens a panel where you can define the kind of Alarms you wish to see.
Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

**Date and Time Filter**

Display Alarms from a range of dates and times.

**User and Device Filters**

The display shows only the Events that match *all* the filters you specify. Note that the **Name** filters are case-sensitive. For instance, if you enter "john," the display will not show Events for "John."

**Event Type Filter**

The display shows Alarms that match *any* of the Event Types you have checked. If nothing is checked, all Alarms are displayed.

**Export PDF**  
Save the displayed Alarms as a printable report in PDF format.

**Alarms Columns**

See [Alarms](#).

**Related Topics**

- [Using List Views](#)
- [Reports and Printing](#)
- [Alarms](#)
- [Alarm Triggers](#)
- [Emergency Features](#)
2.9 User Access Level Report

User Access Level Report creates a report of all Users who have a selected Access Level. This report does not include Shared Access Codes or Emergency Codes.

Related Topics

- Reports and Printing
- Users
- Access Levels

2.10 User Door Report

User Door Report creates a report showing which Users have access to a specific Door. This report includes Doors directly assigned to the Users as well as those assigned via an Access Level.

This report does not include Shared Access Codes or Emergency Codes.

This report also excludes Users with no credentials (no cards, PIN, or biometrics).

Related Topics

- Reports and Printing
- Users
- Access Levels
3 Access Control

The Access Control menu is primarily for determining who can open Doors, when, and how (cards, PINs, and biometrics).

You can also perform related tasks such as creating Users for the Web Management Application and creating Door Mode Schedules.

### Access to Doors

Create Users to provide door access to individual Users who use a credential such as a card, a PIN, or a biometric fingerprint. This is the most common door access method and allows you to track who comes and goes. You can simply give each User unrestricted 24/7 access to Doors, or further restrict their access using the following features.

Set up Schedules to allow access only at certain times, such as during business hours.

Create Access Levels to predefine a set of Doors and Schedules that can be quickly assigned to multiple Users.

Specify Special Days to restrict access more than usual for holidays, corporate events, or other days when access rules should differ. Special Days are used in Schedules.

Create Shared Access Codes, which creates PIN codes that anyone can use to unlock designated Doors.

### Special Features

The following features are used in special situations:

Emergency Codes are PIN codes that unlock Doors in an emergency.

Multi-User Access requires more than one User to present credentials to unlock sensitive areas. For example, a rule could be created such that three Users must present their card to open a Door.

Door Mode Schedules function like normal Schedules but are used in the Doors configuration to schedule Door Mode changes.

### Access to the Web Management Application
Web Management Application Users are added in the same Users configuration screen. A User can have both Door access and web application access.

### 3.1 Users

Users can be created for the following purposes:

- Cardholders who can access Doors.
- Users who can log into the Web Management Application.

A single User can have both Door and application access.

#### Menu Buttons

- **Filter**: Displays a panel above the list where you can search for a User on several properties. Users are displayed if they match all filters.
  
  Settings take effect when you click the **Search** button, at the bottom of the panel. The **Reset** button clears all filters.

- **Import**: See Importing Users from a CSV File.

- **Forgive**: Resets the selected User's anti-passback status. Use this when anti-passback rules are preventing a User's access, and this needs to be overridden.

#### Key Properties

For the complete list and more details see User Properties.

- **First Name and Last Name**: The User’s first and last name. Both required, maximum 32 characters each.
Photo  A photo of the User. This is shown here, and can be printed on a card. To add or change the photo, click the photo image and select an image from your computer. Supported image formats are PNG, JPEG, and GIF.

Role  **Cardholder Only** for cardholder. The other Roles provide access to the Web Management Application. Each Role provides a different level of access; see User Roles. Users with the ability to log in also can have Door access.

Username and Password  If **Role** is not **Cardholder Only**, this is the username/password used to log in to the web application.

Cards  Add any number of cards that will be used for access. You can use a Card Enrollment Point to add a card number.

Adding a card does not provide access; the User will also need Access Levels or Doors assigned, below.

Fingerprints  Shows whether the User has any fingerprints enrolled, and allows them to be enrolled. (Fingerprints are only available if the Primary Controller supports biometrics.)

PIN  PIN (Personal Identification Number) for the User, numeric only. Click **Create New** to generate a random, unique PIN. The length must match the PIN length defined in System Settings. (The default is 4 characters).

Access Levels, Door Access  • Add **Access Levels** that have been defined, and/or

• Add **Door Access** entries to customize access for this User.

Card Design  Use to print cards.
3.1.1 User Properties

The following are the properties available on the Users screen:

**Identity**

- **Status**: Displays whether the current User's status is **Valid** or **Invalid**. The status will be **Invalid** if the current date is outside of the **Valid To** range, or if **Disable User** is checked.

- **First Name and Last Name**: The User's first and last name. Both required, maximum 32 characters each.

- **Photo**: A photo of the User. This is shown here, and can be printed on a card. To add or change the photo, click the photo image and select an image from your computer. Supported image formats are PNG, JPEG, and GIF.
Personnel ID  A unique identifier, such as an employee ID. Maximum 32 characters

Role  **Cardholder Only** for cardholder. For Users with the ability to log in, select another Role. See [User Roles](#). Users with the ability to log in also can have cards.

User Group  Select a [User Group](#) which will be used when applying Multi-User Access rules. This is used if multiple Users are required to present their credentials to open a Door.

Username  If **Role** is not **Cardholder Only**, this is the username used to log in to the web application.

Password  If **Role** is not **Cardholder Only**, this is the password used to log in to the web application.

Language  The User's preferred language, which will be

- displayed on card readers that support multiple languages (such as some OSDP readers), and

- the User's default language in the Web Management Application. Available languages depend on your [software license](#). Contact your authorized ZKTeco representative for license upgrades.

Valid From  The date when access should begin. The default is the current date. This applies to both Door access and Web Management Application access.

Until Further Notice, Valid To  If **Until Further Notice** is checked, then the User's access never expires. If it is unchecked, then the **Valid To** date must be provided, which determines when the User's access expires. This applies to both Door access and Web Management Application access.
Disable User  If checked, the User's access is disabled. This applies to both Door access and Web Management Application access.

Vacation From, Vacation To  If this date range is entered, it is a vacation date range during which the User's Door access is suspended. Web Management Application access is not affected by vacation dates.

Additional Information

Email  The User's email address. This is required for the User to receive system emails such as Notifications.

Mobile Phone  The User’s mobile phone number.

Custom 1-4  Custom fields corresponding to those configured in System Settings.

Access

Cards  Click Add to add card numbers for Door access. Click Enabled to enable or disable a card. To enter a card number by swiping the card, see Card Enrollment Points.

Fingerprints  Shows whether the User has any fingerprints enrolled, and allows them to be enrolled.

Fingerprint enrollment requires a ZKTeco USB enrollment reader and its Fingerprint Driver software (available on the Downloads page at ZKTecoUSA.com).
PIN

The PIN (Personal Identification Number) used for Door access. Numeric only. The length must match the PIN length defined in System Settings (default is 4 characters).

- PIN numbers must be unique, including Duress PIN codes, Shared Access Codes, and Emergency Access Codes.
- Click Create New to generate a random unique PIN number.
- Click Clear to clear the PIN.

Duress PIN

The duress PIN generates a duress access Event when used in place of the normal PIN. Access is still granted if all other normal access conditions are met. See Duress for more details. For Duress PIN Type:

- Select None if the Duress PIN is not used.
- Select Add 1 to Last Digit to add one to the last digit, only, of the normal PIN. For example, a normal PIN of 1111 would then have a duress PIN of 1112, and a normal PIN of 9999 would have a duress PIN of 9990.
- Select Explicit to enter an specific Duress PIN for this User. Numeric only. The length must match the PIN length defined in System Settings (default is 4 characters).

Use Extended Door Times

If checked, extended Door unlock and held times are used when this User is granted access. This is for Users requiring additional time to get through a Door, for example a person with a disability. The amount of extra time is set on each Door.

Anti-passback Exempt

If checked, the User is not subject to anti-passback rules.
Access Doors in No Access Mode

If checked, the User can access Doors in No Access mode. This is typically only for administrators and security personnel.

Access Doors in Lockdown Mode

If checked, the User can access Doors in Lockdown mode. This is typically only for administrators and security personnel.

Access Levels

Access Levels assigned to the User for Door access.

Door Access

Grants this User access to individual Doors during the selected Schedule. This is in addition to any Access Levels assigned.

Card Design

Card Design

Select a card design. If selected, a preview is displayed.

Click Print Card to print. When printing, if the card number is a part of the design, the card number must be selected.

Click Print Receipt if the card is printed to a remote location, and the recipient must go pick it up.

Related Topics

- User Roles
- User Groups
- Card Enrollment Points
- Access Levels
### 3.1.2 Printing Cards

You can print to a specialized printer that writes ID cards. You can also print a paper receipt for your use as a record or to authorize pickup at a remote printer.

To do either, you must first create Card Designs.

To print, select a User, and:

1. Select a card design. (Your choice will be saved for this User.)
2. Click Print Card or Print Receipt.
3. Select a card number from the list.
4. Click Print and follow the prompts.

To complete the prompts, see Reports and Printing.

### Related Topics

- Users
- Card Designs
- Reports and Printing

### 3.1.3 Importing Users from a CSV File

A CSV (comma-separated value) file can be add any number of Users using data from another software program. The other program must be able to export to CSV or a format you can convert to CSV. The CSV itself must be modified to exactly match the Atlas Series import format using software such as a spreadsheet editor.

On the Users screen:
1. Click **Import**.

2. Click the link to download a template file that includes a sample of the required data format.

   **In your own software:**

3. Open the file and read the included instructions.

4. Create a copy of the file.

5. Modify the file with data for the users you want to create.

6. Save the file in CSV format.

   a. Make sure the file is in plain text and does not include any additional characters or encoding.

   b. For example, if using any non-ASCII characters, the file must be encoded as UTF-8.

**On the Users screen:**

7. Click **Import**.

8. In the dialog, click **Import**.

9. Select the file from your computer. The file must have the ".csv" extension.

10. Click **Yes** to verify and import the file.

11. The number of imported Users is displayed. Click **OK**, and you will see the newly imported Users.

### Related Topics

- [Users](#)

- [User Properties](#)

### 3.2 Shared Access Codes

A Shared Access Code is a PIN that multiple people can use to access specified Doors.
These codes only work when the current Door Mode allows a PIN by itself to open the Door. For example, PIN-Only or any mode that says "or PIN", such as "Card or PIN".

Shared Access Codes do not work with:

- Doors that are in Card-only mode, Card and PIN, etc.
- Doors with Multi-User Access rules (because a user group cannot be assigned to a shared access code).

Shared Access Codes are always exempt from anti-passback.

Use of Shared Access Codes will impact the accuracy of a Muster report.

### Shared Access Code Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Required. Maximum 32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>The Shared Access Code itself. Numeric only. Click <strong>Create New</strong> to generate a random, unique code.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Checked to enable, unchecked to disable</td>
</tr>
<tr>
<td>Description</td>
<td>Description or comments</td>
</tr>
<tr>
<td>Access Rights</td>
<td>Add <strong>Access Levels</strong>, and/or add Door Access entries to directly assign Door/Schedule pairs for access.</td>
</tr>
</tbody>
</table>

### Related Topics

- **Using Property Views**
- **Emergency Codes**
- **Access Levels**
3.3 Emergency Codes

An Emergency Code is a PIN that allows access to Doors regardless of other settings, including the Door Mode. (Compare to Shared Access Codes.) It is intended to be used by emergency and security personnel to gain access in emergency situations.

This means that an Emergency Code can access a Door which is under Lockdown.


The Emergency Code Presented Event is configured as an Alarm Trigger by default, generating an Alarm. The Emergency Code Presented Event can also be used as a Linkage to trigger the activation of an auxiliary output on the Hardware screen.

Emergency Codes are exempt from anti-passback and Multi-User Access. (Compare to Shared Access Codes.)

Emergency Codes otherwise have the same properties as Shared Access Codes.

Use of Emergency Codes will impact the accuracy of a Muster report for the emergency personnel who use them.

Related Topics

- Using Property Views
- Shared Access Codes
- Access Levels
- Emergency Features

3.4 Access Levels

An Access Level is a predefined list of Doors paired with the Schedules during which access is allowed for each Door. When an Access Level is changed, the new definition immediately applies to each User or code assigned that Access Level.

Access Levels can be applied to Users, Shared Access Codes, and Emergency Codes. On each of those screens you can apply one or more Access Levels, and you can provide customized access to individual Door/Schedule pairs.
Using the Screen

Click the **Add** and **Remove** buttons to add and remove Doors from the list.

Use the **ellipsis buttons** (...) to change the selected Doors and Schedules.

You can include the same Door multiple times with different Schedules. Access will be allowed for a given Door during all the Schedules associated with it.

Related Topics

- **Using Property Views**
- **Schedules**
- **Users**
- **Shared Access Codes**
- **Emergency Codes**

### 3.5 Schedules

Schedules are used to limit access to certain days and times. They can be used in Access Levels and anywhere Door access is assigned.

By default, access is *not* allowed on **Special Days**.

The built-in "24/7" Schedule allows access at all times, *including* Special Days.

Using the Screen

Access will be allowed during all the time periods you create. Click the **Add** and **Remove** buttons to add and remove time periods from the list.

Times (Start-Stop)

The left-side bar shows the time period access is allowed in green. You can drag the ends of the green bar to change the time range. You can also enter the exact times you want in the boxes...
under the bar. Times are entered and shown using a 24-hour clock (as opposed to "a.m." and "p.m.") Each bar can only have one time range; to have two time ranges on the same days, add another entry. The **All day** button is a convenience to reset the bar.

**Days**

The middle bar shows the days that access is allowed in green. You can click each day to change access, or you can use the convenience buttons to change the current selection. The convenience buttons are **Weekdays, All days, and Weekend**.

**Special Days**

The right bar appears green if you have included any Special Days for that time period. Click the bar to select Special Days to include. In the Special Days selection screen, you may check one or multiple Special Day types.

Access is normally denied on Special Days. Access will be allowed if you include the Special Days in the Schedule. For more information, see **Special Days**.

---

**Related Topics**

- **Using Property Views**
- **Special Days**

---

### 3.6 Door Mode Schedules

Door Mode Schedules are used to change the mode of Doors at different times. For instance, they are commonly used to automatically unlock public Doors during business hours.

See **Door Modes** for a list of possible Door Modes.
Door Mode Schedules are assigned to Doors on the Doors screen.

A Door Mode Schedule can have multiple time intervals with different associated modes.

Note that emergency Door Modes cannot be scheduled.

### Using the Screen

Click the **Add** and **Remove** buttons to add and remove time periods from the list.

In the left column, select a single Door Mode. A Door will automatically change to this mode during the time period defined.

The time periods are defined the same way they are for Schedules. See Schedules.

### Related Topics

- Using Property Views
- Door Modes
- Special Days
- Schedules

### 3.7 Special Days

Special Days are single calendar days (such as May 5th) where access is denied by default, even if it would normally be allowed by a Schedule. They can be added to Schedules so that certain Users do have access on those days.

Special Days are used for holidays, corporate events, and other cases where you do not want your usual access to be granted. For instance, you might use Door Mode Schedules to automatically unlock Doors during business hours Monday-Friday, but you do not want to do that on holidays.

Note that the special Schedule, "24/7", allows access at all times and is not affected by Special Days.

### Special Day Types
Special Days are grouped into a number of Special Day Types. A type is essentially a calendar. For instance, one type might include all government holidays, while another might be teacher work days. You can then set different access rules for the different calendars.

Only Special Day Types can be added to a Schedule. So, you could add access on all government holidays, but not on a single one, unless you made a type with just that one day.

### Using the Screen

In the first section, **Special Day Types**, you can change the names of the types to something useful, such as "Government Holidays" or "Teacher Workdays". You may also change the color assigned to each type. The color has no effect except on this screen.

The second section, **Special Days**, shows a calendar highlighting all Special Days of all types in their color. To add or remove a day, click on it.

The two options above the calendar change what happens when you next click on a day. They cannot change the properties of current Special Days.

- **Select Special Day Type**: days added on the calendar will be this type. You cannot add days if no type is selected.

- **Set as Repeating**: when checked, days added on the calendar will be repeating. This means they will occur every year on the same calendar date. They are displayed with a small "R", and can be seen on every year.

Note that any single day can only be in one Special Day Type.

### Related Topics

- **Schedules**
- **Door Mode Schedules**

### 3.8 Multi-User Access

Multi-User Access is used to require multiple Users to present their credentials to open a Door. This is often used for high security areas. For example, an area might require two
managers and one security guard to present their credentials. The credentials they may submit are those required by the Door's current Door Mode.

Shared Access Codes cannot access Doors with Multi-User Access rules in effect. Emergency Codes are exempt from Multi-User Access rules.

Using the Screen

You must first create one or more User Groups whose members can cooperate to access a specific Door.

Click the Add and Remove buttons to add and remove User Groups from the Rules list. If multiple rules are created, they all must be satisfied in order for access to be granted. If there are no rules in a specific Multi-User Access definition, associated Doors will behave as if they have no Multi-User Access restriction.

Apply the Multi-User Access rule on the Doors screen.

Related Topics

- Using Property Views
- User Groups
- Doors
4 Configuration

Use the Configuration menu to:

- Connect and configure hardware and Doors.
- Organize your hardware into locations and Areas, and plot it on Maps.
- Configure general settings for the Monitor and Access Control features.

Users with the System Administration Role can add and configure Controllers and Doors. Access Control Management Users can only configure Doors. Other built-in User Roles can do neither.

See Administration for configuring system settings such as the time or network connection.

Configuring Hardware and Doors

Before doing any configuration, it's important to read the brief topic, Understanding Controllers and Doors. It is particularly useful for any Web Management Application User to understand the definition of "Door" in the Atlas Series software.

Hardware is where the physical equipment (Controllers and their readers, inputs, and outputs) is added and configured. Hardware configuration is usually done by an expert who installs the system.

Door configuration is the starting point for all access control. Most importantly, this is where you specify if and when Doors are locked and how they can be opened. All Access Control settings are affected by Door configuration.

Hardware Templates and Door Templates can be used to quickly set up multiple Sub-controllers (I/O) or Doors with the same settings.

Organizing Hardware

Locations are labels that can be applied to Doors, Controllers, Maps, and other items. Locations appear in Events and Alarms.
Areas are used with anti-passback and airlock. They define physical regions where you can restrict access using those features. The Muster Report also relies on Areas to determine whether each User is at a known, safe Area (Muster or Global Out).

You can also create Maps of your buildings and campus. Monitor these Maps to watch the live status of Doors and Controllers on an actual map of your facility.

### General Settings

**Card Designs** allows you to create the print layouts for Printing Cards.

**Card Formats** define what kind or brand of cards you use. Your Atlas Series system includes all of the card formats you will likely need. Use this screen to create a format for an unusual type of card, or to enter a "facility code" as instructed by your card vendor.

Create **User Groups** to use with Multi-User Access.

Set up **Alarm Triggers** to define which Events trigger Alarms.

### 4.1 Understanding Controllers and Doors

#### Controllers

Each system includes one Primary Controller. This is the one you log in to with your web browser to manage or monitor the entire system. It maintains all the data and configuration, and directs all Secondary Controllers.

Secondary Controllers are added to manage additional Doors. They receive their configuration from the Primary Controller. However, they keep a copy of the data, so they continue operate if the primary is not on line. You can log in directly to a Secondary Controller through a link on its Hardware page, but only to change a few local values, such as the Network settings.

**Important:** The Primary Controller must support biometrics if any biometric Controller will be used in the system.

#### Sub-controllers (I/O)
Every Controller has a built-in Sub-controller (I/O). It is displayed under the Controller in Hardware with the additional label, "I/O", meaning "input/output". The Sub-controller manages the advanced details of the readers, inputs, and outputs of the hardware.

### Doors

Every card, PIN, and biometric reader in the system is represented as a Door—though you might not think of some as doors at all! A Door in the Web Management Application might represent one of many things:

- A real, physical door that can be entered
- A second reader that allows exit through a physical door. Notice that this means an In/Out physical door is represented by two Doors, one for "In", and one for "Out".
- Something that functions like a physical door, such as a turnstile or garage gate
- A reader by itself, with no physical door, used as a Muster Point or Card Enrollment Point

Doors are created on the **Hardware** screen, either automatically when the Controller is created, or by customizing the Controller.

### Related Topics

- **Hardware**
- **Doors**

### 4.2 Hardware

Hardware represents the system's Controllers and all their physical connections to readers, locks, door contacts, and other inputs and outputs. This is where you configure electrical connections and Controller settings. Door behavior, such as Door Mode or opening times, are configured in **Doors**.

**Hardware Topics**
Models and Configurations

Modifying Controller Configuration

Hardware Properties

Adding Controllers

Firmware Updates

Resync Secondary Controllers

Related Topics

Doors

Hardware Templates

4.2.1 Models and Configurations

Atlas Series Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Type</th>
<th>Wiegand Ports</th>
<th>RS-485 Slots</th>
<th>Number of &quot;In&quot; Doors</th>
<th>Max &quot;Secondary&quot; Doors</th>
<th>Default Reader Type</th>
<th>Default Type for Secondary Readers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlas 100</td>
<td>1 Door</td>
<td>2</td>
<td>2 OSDP</td>
<td>1</td>
<td>1</td>
<td>Wiegand</td>
<td>Wiegand</td>
</tr>
<tr>
<td>Atlas 200</td>
<td>2 Door</td>
<td>4</td>
<td>4 OSDP</td>
<td>2</td>
<td>2</td>
<td>Wiegand</td>
<td>Wiegand</td>
</tr>
<tr>
<td>Atlas 400</td>
<td>4 Door</td>
<td>4</td>
<td>4 OSDP</td>
<td>4</td>
<td>4</td>
<td>Wiegand</td>
<td>OSDP</td>
</tr>
<tr>
<td>Atlas 160</td>
<td>1 Door Biometric</td>
<td>2</td>
<td>2 OSDP OR 2 ZKTeco RS-485</td>
<td>1</td>
<td>1</td>
<td>ZKTeco RS-485</td>
<td>ZKTeco RS-485</td>
</tr>
<tr>
<td>Atlas 260</td>
<td>2 Door Biometric</td>
<td>4</td>
<td>4 OSDP OR</td>
<td>2</td>
<td>2</td>
<td>ZKTeco RS-485</td>
<td>ZKTeco RS-485</td>
</tr>
</tbody>
</table>
**Important:** The Primary Controller must support biometrics if any biometric Controller will be used in the system.

"In" Doors are automatically created and are permanent, though they need not be used.

Secondary Doors are Out Doors, Card Enrollment Points, and Muster Points. The Readers of Secondary Doors are always paired with the Readers of In Doors in a defined way.

<table>
<thead>
<tr>
<th>Controller Type</th>
<th>&quot;In&quot; to &quot;Secondary&quot; Reader Pairings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 door</td>
<td>1 to 2</td>
</tr>
<tr>
<td>2 door</td>
<td>1 to 3</td>
</tr>
<tr>
<td></td>
<td>2 to 4</td>
</tr>
<tr>
<td>4 door</td>
<td>1 to 5</td>
</tr>
<tr>
<td></td>
<td>2 to 6</td>
</tr>
<tr>
<td></td>
<td>3 to 7</td>
</tr>
<tr>
<td></td>
<td>4 to 8</td>
</tr>
</tbody>
</table>

For example, on a 4 door Controller, Door 2 always uses reader #2 and is an "In" Door. If it has an "Out" Door, that Door will always use reader #6.

The reader number is not necessarily the same as its address. For Wiegand, the reader number is the same as the labels on the hardware, but any reader can be changed to use any available RS-485 address.
Notice that 4 door Controllers only have enough Wiegand reader ports for the "In" Doors. Any secondary Doors must use RS-485.

Configuration Property

The Configuration property of a Controller determines what the Controller's Doors will be used for: authorizing Door entry, perhaps Door exit, or as special purpose readers.

Configuration options available depend on the Controller model. Each option will involve one or more of the following possibilities. Each possibility determines the function of the card, PIN, or biometric readers connected to the Controller.

In Only

This the most common configuration, where a reader is used to gain entry, but no credentials are required to exit (although an exit button may be configured for opening the Door from the inside).

In/Out

The physical door will have a reader both inside and outside. Authorization is required to pass either direction.

+ Muster Point

The second reader will serve as a Muster Point, where Users can register that they have reached a safe location.

+ Card Enrollment Point

The second reader will be used to easily enter card numbers when adding Users. See Card Enrollment Points.

The available options do not cover all possibilities. For instance, 2 and 4 Door Controllers do not offer Muster Points or Enrollment Points as standard Configurations. To tailor the configuration to your needs, see Modifying Controller Configuration. Modifying might be easier if you start with "In Only" as a baseline.

Related Topics

- Adding Controllers
• **Modifying Controller Configuration**

4.2.2 **Modifying Controller Configuration**

The "Modify" button on the menu bar is used to customize the Configuration property of a Controller. You will need to understand Models and Configuration to effectively customize a configuration.

Clicking "Modify" brings up a list of options. Some options will be disabled when they cannot be applied to the Controller as its readers are currently configured.

All options present a dialog to enter specifics for your change. The options are:

- **Change to In/Out**
  Select the number of the "In" Door which will have an "Out" Door paired with it.

- **Add Muster Point**
  Enter a Name for the new Door, and select the "In" Door number to pair it with.

- **Add Card Enrollment Point**
  Enter a Name for the new Door, and select the "In" Door number to pair it with.

- **Remove Secondary, Muster, or Card Enrollment Point**
  Select the number of the "In" Door that will have its paired Door removed.

---

**Related Topics**
Models and Configuration

4.2.3 Hardware Properties

The body of the Hardware screen allows Controller configuration and displays data about the Controller. Each Controller is represented by two components: (1) the Controller itself for general configuration, and (2) a Sub-controller (I/O) for detailed settings of readers, locks, door contacts, and other inputs and outputs.

Sub-controllers can be configured to a saved group of settings using Hardware Templates.

Door behaviors, such as Door Modes and opening times, are configured in Doors.

Controller Properties

Name
The name of the Controller. Required, maximum 32 characters.

Model
The model of the Controller.

IP address
(Secondary Controllers only) IP address or hostname of the Controller.

Port
(Secondary Controllers only) Port number for the Controller.

Disconnected
If checked, the Secondary Controller is treated as if it does not exist, and communication is not allowed. This cannot be checked on the Primary Controller.

This can be useful during the installation of hardware.

Status
Displays the current status of the device, including Online/Offline. If any tamper, power, or battery problems are present, these will be
indicated here as well. **Lockdown** or **Emergency Unlock** will be indicated here, when active.

**Serial Number**
The serial number of the Controller. This is displayed only if the device is online.

**Firmware Version**
The firmware version of the Controller. This is displayed only if the device is online.

**Configuration**
See **Models and Configuration**.

**Location**
The **Location** of the Controller.

**Description**
Description or comments

**Language**
Set's the default language for
- the Web Management Application on the Primary Controller,
- the simplified management application on a Secondary Controller, and
- multi-language OSDP readers connected to this Controller, if they have displays.

Available languages depend on your **software license**. Contact your authorized ZKTeco representative for license upgrades.

**Time Zone**
(Secondary Controllers only) The time zone of the Secondary Controller. The time zone for the Primary Controller is set in **Date and Time**.
Managed Doors
A list of the Doors managed by the Controller, with links to their configuration screens.

Managed Sub-controllers
A list of Sub-controllers managed by this Controller, with links to their hardware configuration.

Firmware Download
(Secondary Controllers only) Select a previously uploaded firmware file and download it to the Controller. Primary Controller firmware is updated under Firmware Settings.

"Open admin web page in new window"
Click the link to log in directly to a Secondary Controller. You will enter a simplified web management application allowing limited Controller configuration options, such as Network settings.

Reboot Button
(Secondary Controllers only) Reboots the Controller

Resync Button
(Secondary Controllers only) Refreshes the configuration of this Secondary Controller.

Sub-controller (I/O) Properties

Name
(Read-only) The name of the Sub-controller.

Disconnected
(Read-only) Always unchecked and cannot be changed.

Status
(Read-only) Always Online for Atlas Series built-in Sub-controllers.

Model
(Read-only) The device model.
### Description
Description or comments

### Hardware Template
Select an existing template and click **Apply Template**. Deselect **Apply Template** to edit the settings.

Click **Create Hardware Template** to create a new template from the current settings. The template contains most of the Sub-controller configuration. See [Hardware Templates](#).

---

**Reader Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>If Wiegand, the address label printed on the Controller. Otherwise, <strong>Address</strong> is an arbitrary label.</td>
</tr>
<tr>
<td>Managed By</td>
<td>The Door that the device is associated with</td>
</tr>
<tr>
<td>Model</td>
<td>The device model:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Custom</strong> — for Wiegand or OSDP readers</td>
</tr>
<tr>
<td></td>
<td>• <strong>ZKTeco</strong> — for ZKTeco RS-485 readers</td>
</tr>
<tr>
<td>Reader Type</td>
<td>• <strong>Data0/Data1 (Wiegand)</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>OSDP</strong> — for model <strong>Custom</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>ZKTeco RS-485</strong> — for model <strong>ZKTeco</strong>. This is only available on biometric Controller models.</td>
</tr>
<tr>
<td>Keypad Type</td>
<td>For <strong>Data0/Data1 (Wiegand)</strong> readers only.</td>
</tr>
<tr>
<td></td>
<td>• If Auto, then PIN digits are accepted over Wiegand, automatically decoding the format.</td>
</tr>
</tbody>
</table>
• “None” is displayed for no PIN pad. (It generally makes sense to leave this on Auto, unless you want to specifically disable a PIN pad on a Wiegand reader.)

• OSDP and ZKTeco RS-485 readers send their PIN data differently, so this setting is not used for them.

Tamper  The type of tamper detection. Only **OSDP** is supported on OSDP readers.

LED Type  The LED control type:

- For Wiegand, this is either:
  - **None** — select this to disable LED control completely
  - **1-Wire (Green)** — one wire wired to the green LED (red LED generally lit when green is not)
  - **2-Wire (Red and Green)** — Biometric Atlas Controllers only

- For OSDP readers, this is **OSDP**.

OSDP/RS-485 Address  The "polling address" of the OSDP or ZKTeco RS-485 reader.

For most OSDP readers the default is 0. See **Reconfigure**, below, and installation instructions from the reader manufacturer, for how to change the address.

ZKTeco RS-485 readers have a DIP switch to configure the address. Please refer to the ZKTeco RS-485 reader installation instructions on how to set the address.

Reconfigure  Change the OSDP address that the reader itself is configured to use. This is **not** the **OSDP/RS-485 Address** the Sub-controller is set to use, though they must ultimately have the same value.

1. Set the **OSDP/RS-485 Address** to the reader's current address setting.
2. Click **Save**.

3. Click the **Reconfigure** button. Select a new address number for the reader.

4. Change the **OSDP/RS-485 Address** to the new number.

5. Click **Save**.

Some OSDP readers might not support **Reconfigure**.

### Input Properties

- **Address**
  - The printed address on the board.

- **Name**
  - The name of the input. Required, maximum 32 characters.

- **Enabled**
  - Check to enable, uncheck to disable.

- **Normally Open**
  - Whether the input is normally open (NO). Normally open inputs are active when the wires are normally not connected (open circuit). This is generally true for exit buttons. Most other inputs like tamper, power, and battery failure sensors are normally closed (NC).

- **Function**
  - What the input is used for. Not all options are available for all inputs, and some cannot be changed. The **Functions** are:
    - Exit Button
    - Door Sensor
    - Tamper
    - Power Monitor
    - Battery Monitor
- **Linkage**
- **Not Used**

**Managed By**
For exit buttons and door sensors, this is the Door that the input is a part of. For tamper, power monitor, and battery monitors, this is the Controller they are a part of. For Linkage inputs, this is the device affected by the policy. (See **Policy Type**.)

"Out" Doors cannot be used in linkages, nor to manage hardware.

**Policy Type**
For **Linkage** inputs, this is the policy to be executed when the input becomes active. The options depend on the **Managed By** setting:

- **Input-Triggered Alarm** (Managed By: empty) — This will cause an **Alarm** to be generated when the input becomes active. Do not confuse this with a relay activating an audible alarm, which can be configured for an output, below.

- **Input-Triggered Lockdown** (Managed By: a Controller) — When the input is activated, a **Global Lockdown** is initiated. The lockdown will only end when a User clicks **Clear Lockdown** on the **Main Menu** (with some exceptions*).

- **Input-Driven Emergency Unlock** (Managed By: a Controller) — Whenever the input is active, a **Global Emergency Unlock** condition will be active. The emergency unlock will only end when the input returns to inactive (with some exceptions*).

- **Input-Triggered Momentary Unlock** (Managed By: a Door) — This will cause a momentary unlock of the Door when the input becomes active.

*Important:* As with all emergency functions, you should thoroughly understand the relevant topics before relying on lockdown and emergency unlock.
Schedule  (Linkage only) If a Schedule is selected here, the Linkage will only be applied during this Schedule.

Output Properties

Address  The printed address on the board.

Name  The name of the output. Required, maximum 32 characters.

Function  What the output is used for: Not all options are available for all outputs, and not all can be changed. The options are:

- Reader Beeper
- Reader LED (Green)
- Reader LED (Red)
- Lock
- Linkage
- Not Used

Managed By  For Lock, Reader Beeper, and LEDs this is the Door they are used for.

For Linkage, this is the device whose Events can trigger this output.

"Out" Doors cannot be used in linkages, nor to manage hardware.

Event / Condition  (Linkage only) Defines the Event or condition that triggers an output.

Controller triggers:

- Tamper
Door triggers:

- Access Denied
- Access Granted
- Door Forced Open
- Door Held Open
- Duress
- Emergency Code Presented

Input triggers:

- Input Active

**Toggle / Pulse** 
(Linkage only) If **Pulse**, the Event activates this output briefly. If **Toggle**, this output is active until the Event is "ended" by its reverse Event. For example, "Door Held Open" is reversed by "Door Held Open Restored". **Toggle** is not an option when the Event has no reverse Event.

**Pulse Time** 
(Linkage only) The pulse time in seconds.

**Schedule** 
(Linkage only) If a Schedule is selected here, the Linkage will only be applied during this Schedule.

### Related Topics

- **Using Property Views**
- **Understanding Controllers and Doors**
- **Hardware Templates**
- **Models and Configuration**
4.2.4 Adding Controllers

Secondary Controllers can be automatically found and added by the Web Management Application. This is called “Discovery.” When Discovery cannot be used, you can add Controllers manually. You can also use manual installation to add Controllers that have not yet been installed.

Once a Secondary has been added, it cannot be reassigned to a new Primary, or a factory reset Primary, until it itself has had a Factory Reset.

The number of Secondary Controllers you can add and the number of Doors you can create are limited by your license. Contact your authorized ZKTeco representative for license upgrades.

Discovering Secondary Controllers

There are two important qualifications about Discovery.

- When using Discovery, you should connect and discover Controllers one at a time. This is the only way you can know which one is which.

- Discovery only works if all Controllers are networked on the same subnet. If you have a simple network, this will almost always be true. In a larger corporate environment, you might need to add Secondary Controllers manually.

To Discover Controllers:

1. Click Discover Controllers on the menu bar.
2. In a few moments, a form will display all Controllers discovered.
3. Click the link to add a Controller. The create controller screen will appear.
   a. Select a Configuration.
b. Enter a **Name**, and select **Custom Door Names** so you can name the doors in the box, below.

c. Leave all other settings as they are. These are the settings that were discovered.

4. Click **Save** on the menu bar.

### Manually Adding Secondary Controllers

To add a Controller manually:

1. Click **Create** on the menu bar. The create controller screen will appear.

2. Select a **Model**.

3. Select a **Configuration**.

4. Enter a **Name**, and select **Custom Door Names** so you can name the doors in the box, below.

5. Enter the Controller's **IP Address**.

6. Enter the default **Port** number, 443.

1. Click **Save** on the menu bar.

### Related Topics

- **Models and Configuration**
- **Modifying Controller Configuration**

### 4.2.5 Firmware Updates

"Firmware" means all the software running on a Controller, including both the Web Management Application and the software that operates the Doors. Updating the firmware installs upgrades received from ZKTeco.
You can update firmware in two ways: (1) log in to any Controller and update it directly, or (2) use the Web Management Application to update any Secondary Controller remotely. Note that only method 1 is used for the Primary Controller.

In either case, you must have an update file available on your own computer.

Both methods cause the updated Controller to reboot.

### Upgrading the Firmware On The Controller You Are Logged Into

1. Go to [Firmware Settings](#).
2. Click **Upgrade Firmware**.
3. Click **Browse** and select the firmware file from your computer.
4. Wait while the file transfers to the Controller.
5. When it completes, click **Okay**. There will be a delay while the update installs, then the Controller will go offline while it reboots.

### Upgrading the Firmware of a Secondary Controller from the Primary

This method involves two steps: (1) send the update file to the Web Management Application, then (2) download the file to Secondary Controllers.

1. Go to [Hardware](#).
2. Click **Upload Firmware** in the menu bar.
3. Click **Browse** and select the firmware file from your computer.
4. Follow the prompts and the firmware image will be uploaded, but *not applied to any Controller*.
5. Select a Secondary Controller.
6. Scroll down to **Firmware Download** and select the update file.
7. Click **Download**.
8. Follow the on-screen prompts to upgrade the firmware on the Secondary Controller you selected.
4.2.6 Resync Secondary Controllers

The Resync Secondary Controllers button on the menu bar causes a major reset of all Secondary Controllers. All configuration from the Web Management Application (on the Primary Controller) is freshly updated on all secondaries. This includes all hardware, Door, and access configuration, including Users data. It does not include Network or Firmware settings.

Individual Secondary Controllers can be resynced under Maintenance on their Hardware pages.

4.3 Doors

Every card, PIN, and biometric reader in the system is represented as a Door (see Understanding Controllers and Doors).

Doors are automatically created to match the Configuration property of Controllers in Hardware. The number of Doors you can create are limited by your license. Contact your authorized ZKTeco representative for license upgrades.

Menu Buttons

- **Manual Commands**: Allows direct control of the selected Door using Manual Commands to change Door Mode or unlock the Door.

Key Properties

For the complete list and details, see Door Properties.
Name  The name of the Door. Required, maximum 32 characters.

Type  Shows the Door's function: "In", "Out", "Card Enrollment Point", or "Muster Point". This is determined in Hardware[56].

Door Template  Used to configure this Door with a template[88], which overrides and disables some properties on this screen.

Default Mode  The Door Mode[142] for this Door whenever not altered by a Schedule, manual command, or Event. Door Mode determines whether a Door is locked, and what kinds of access can unlock it.

Door Mode Schedule  Pick a Door Mode Schedule[50] to change the Door Mode according to the day and time of day.

Multi-User Access  See Multi-User Access[52].

Areas and Anti-passback  See Areas[80].

Related Topics

- Using Property Views[14]
- Door Properties[75]
- Door Modes[142]
- Door Templates[88]
- Manual Commands[116]
- Door Status[26]
4.3.1 Door Properties

Door properties differ based on the door type. For example, Muster and Card Enrollment Points have far fewer properties since they do not control a door strike or have other door hardware.

Name  The name of the Door. Required, maximum 32 characters.

Status  The current status of the Door, including online/offline, Door Mode, locked/unlocked, open/closed, or errors such as forced, held, tamper, reader offline. Lockdown or Emergency Unlock will be indicated here, when active.

Alarm  If any Alarm is pending at the Door, it is shown here.

Type  How the Door is used:

- In — an entry Door. Either an entry-only Door, or an entry Door as a part of an entry/exit (in/out) Door pair.

- Out — an exit Door.

- Muster Point — used to check in during an emergency for the Muster report.

- Card Enrollment Point — used only to enroll cards.

Controller  The Controller that this Door is managed by.

Sub-Controller  The Sub-controller (I/O) which manages this Door’s hardware.

Door Template  A Door Template defines common parameters. Once a Door is linked to the template, the fields are read-only in the Door.
If the Door template is modified, the associated Doors are also updated.

**Location**

Location [70] of the Door.

**Description**

Description or comments

**Default Mode**

The [Door Mode][142] for this Door whenever not altered by a Schedule, Manual Command, or Event. Door Mode determines whether a Door is locked, and what kinds of access can unlock it.

**Door Mode Schedule**

Pick a [Door Mode Schedule][50] to change the Door Mode according to the day and time of day.

**Multi-User Access**

The [Multi-User Access][52] configuration, if multiple Users are required to open a Door.

**Unlock Time (s)**

The amount of time the lock is activated for an access (access granted, exit requested, etc).

**Held Open Alarm Time (s)**

The amount of time a Door can be held open before a held open Event is generated.

This Event can be configured in the [Sub-controller configuration][61] to drive an aux output, for example, to sound a beeper.

**Minimum Unlock Time (s)**

If [Re-lock On][44] allows for the Door to be re-locked before the strike time is up, then this is the minimum time the Door will stay unlocked. This is to avoid an unlock pulse that is too brief, which can be a problem for some hardware.
Extended Unlock Time (s)  
If a User has **Use Extended Door Times** checked, this time is used instead of **Unlock Time**.

Extended Held Time (s)  
If a User has **Use Extended Door Times** checked, this time is used instead of **Held Open Alarm Time**.

Held Open Pre-Alarm Warning Time (s)  
The amount of time before the **Held Open Alarm Time** is reached, when a held open pre-alarm warning Event is generated.  
This Event can be configured in the [Sub-controller configuration](#) to drive an aux output, for example, to sound a beeper.

Suppress Exit Button Events  
When selected, exit requested Events are not created for this Door.  
This can be used if the number of these **Events** is considered too numerous and unimportant.

Unlock on Exit Button  
If checked, the Door is unlocked when the exit button is pressed.  
This may not be required for systems where the exit button is wired directly to cut off power to the door lock, for example.

**Important:** Exit button functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance.

Re-lock On  
When the lock should be re-locked after access is granted:

- **End of Unlock Time**
- **Door Open**
- **Door Close**
- **Door Close or End of Unlock Time** (whichever is sooner)
Exempt From Global Lockdown
If checked, the Door will not be affected by a *global lockdown*.

Exempt From Global Emergency Unlock
If checked, the Door will not be affected by a *global emergency unlock*.

Entering Area
The Area the Door leads into for *anti-passback* (and airlock) configurations.

Exiting Area
The Area the Door leads out of for *anti-passback* (and airlock) configurations.

Anti-passback Method
- **None** — no anti-passback enforced
- **Door-Based** — cannot use same credential within certain amount of time at the same Door.
- **Area-Based** — checks that they are known to be in the correct Area before using a Door leading out of that Area, into another Area.

See *Anti-Passback*.

Anti-passback Mode
Available if **Anti-passback Method** is **Area-Based**: whether to deny or grant access on an anti-passback violation:
- **Hard (Deny Access)**
- **Soft (Grant Access)**
Minutes Denied

Available if Anti-passback Method is Door-Based. The number of minutes before the same credential can be used at the Door.

Related Topics

- Doors
- Door Templates
- Door Status
- Door Modes
- Anti-Passback
- Manual Commands
- Hardware Properties
- Locations
- Areas

4.4 Locations

Locations are labels you can apply to organize Doors and hardware on lists and reports, particularly on Events and Alarms. Locations can be assigned to Doors, Controllers, Areas, and Maps.

Location Properties

Name

The name of the Location. Required, maximum 32 characters.

Type

Category by Location size. From large to small, they are:
Region > Campus > Building > Floor > Room

Parent Location

Designates this Location as included in any larger Location. A Building’s parent could be a Campus or Region, but not a Floor or Room.

When you filter Events to a Location, all the smaller Locations that are included in it will also be displayed.

Related Topics

- Using Property Views
- Events
- Alarms

4.5 Areas

Areas are physical regions you define, and are used for Anti-Passback, Muster, and airlocks. A column to show the Area can be added on Events and Alarms.

Areas are actually nothing but a label. They serve no function until you define which Doors lead into and out of the Area. You do this by setting the Entering Area and Exiting Area of each relevant Door.

Predefined Areas

There are two Areas that are predefined by the system and cannot be edited or deleted:

- Global Out — Doors that enter from, or exit to, the “outside world” should use this as the Exit Area or Entry Area, respectively.

- Muster — An Area where all Muster Points “enter” to. Anyone who uses a Muster Point will have their last known Area set to the Muster Area and will be excluded from the Muster report.
Using the Screen

Name
The name of the Area. Required, maximum 32 characters.

Location
A Location to associate with the Area.

Type
- **Local** — Used only on a single Controller. Can be used for airlock.
- **Global** — Can be used on multiple Controllers, for global anti-passback enforcement.

Parent
(Local Areas only) The single Controller for this Area.

Airlock Mode
(Local Areas only)
- **No Exit During Entry** — A Door exiting the Area cannot be used while a Door entering the Area is open.
- **Strict Single Door** — No two Doors in the Area can be unlocked/opened at the same time.

Description
Description or comments

Related Topics
- **Using Property Views**
- **Anti-Passback**
- **Muster**
4.6 Maps

Maps configuration is used to create the screens for the Maps view.

The Maps view is used to show the status of your Doors and Controllers on graphical backgrounds, for example, on maps of your building or campus. It highlights all problems in red, and allows sending commands to Doors. Maps may also have links to other Maps for easy navigation.

Map Properties and Controls

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the Map (required, maximum 32 characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Optional Location of the Map.</td>
</tr>
<tr>
<td>Background</td>
<td>Click Upload to load an image from your computer. This will be the canvas on which you can place devices. Large images will shrink to fit the available space.</td>
</tr>
<tr>
<td>Elements</td>
<td>Elements, in three list boxes, can be clicked on and dragged to the Map. When on the Map, their blue wrench icon provides options to delete the element, or set the destination of a &quot;Link&quot; element from a list of other Maps.</td>
</tr>
</tbody>
</table>

Text entered in search filters all three element lists.

Related Topics

- Using Property Views
- Maps (Monitoring)
4.7 Card Designs

A Card Design is a print layout you create for use in Printing Cards. It can include User information such as the name and expiration date and images such as the User photo and logos.

**Properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the Card Design. Required, maximum 32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description or comments.</td>
</tr>
</tbody>
</table>

**The Design Area**

**Center Column**

The center area is your canvas to "draw" your card on. It shows a standard size access card, front and back sides.

**Important:** Review your card printer manual to understand its limitations, such as whether it can print both front and back and whether you are allowed to print to the edge of the card.

**Left Column**

Click and drag elements from the left panels onto the card area.

Click elements on the card area to select them. Shift-click to select multiple elements.

Drag selected elements to move them.

Images (only) can be sized by dragging on the corners.

**Right Column**

The first row of three icons performs standard delete, undo, and redo actions.
The second row has six options for aligning elements, followed by four options controlling which elements are on top of others. Hover over any icon to see its exact function. You must select more than one item to enable the alignment options.

The rest of this panel shows the properties of the currently selected item.

For **Images**, click **Select Image** to load an image file from your computer.

For **Text** and **User Fields**, enter the **Text**. Text between "{" and "}" will be replaced with the named property of the User. Additional text may be added outside the brackets, but the text inside must be a valid field name.

The remaining options for text set the font and color.

**X Origin** and **Y Origin** are properties of both images and text. They determine which direction the element will grow to fit the contents, *by choosing which corner will never move*. The default is top left, and the box will expand to the right and down when, for instance, the name field is long or its font size increases. If you change the origin to bottom right, the box will expand upwards and to the left, allowing you to place the box on the right or bottom edge of the card.

**Notes**

Supported image formats are PNG, JPEG, and GIF.

Text will print over of images (if on top), and transparency in images is supported.

**Related Topics**

- **Using Property Views**  
- **Users**  
- **Printing Cards**
4.8 Card Formats

Card Formats define what kinds or brands of cards you use. Your Atlas Series system includes all of the card formats you will likely need, although you might want to enter a "facility code" specified by your card vendor.

If you do use an uncommon type of card, you will have to create a custom card format. This is quite technical, and requires exact specifications from the card vendor.

Notes

You can use more than one card format in your system.

Card formats are neither associated with specific Doors nor specific Users—they all are used for all.

Two card formats with the same number of bits cannot be enabled at the same time, unless they both have facility codes and those codes are different.

Entering Your Facility Code

You must know which of the existing card formats matches your cards. Simply select that format, enter the Facility Code number, and save.

Card Format Properties

Note: Start and location fields are number of the bit, where the first bit on the card is number 0.

<table>
<thead>
<tr>
<th>Name</th>
<th>The format name. Required, maximum 32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits</td>
<td>The total number of bits on the card, including parity bits, etc.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Use or do not use the format.</td>
</tr>
<tr>
<td>Facility Code</td>
<td>(optional) If there is a facility code field (start/length specified), this is the value that the facility code must be equal to for the format to be matched.</td>
</tr>
<tr>
<td>Facility Code Start</td>
<td>The facility code start (bit number).</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>Facility Code Length</td>
<td>The facility code length (in bits).</td>
</tr>
<tr>
<td>Card Num Start</td>
<td>The card number start (bit number).</td>
</tr>
<tr>
<td>Card Num Length</td>
<td>The card number length (in bits).</td>
</tr>
</tbody>
</table>
| Parity (1-4)        | • **None/Even/Odd** — **None** to not use this parity field at all, **Even** or **Odd** for parity calculation method.  
|                     | • **Start** — The start bit of the parity source (the range of bits to be checked for parity). Does NOT include the location of the parity bit itself.  
|                     | • **Length** — The length in bits of the parity source.  
|                     | • **Location** — The bit number of the parity bit.  
|                     | • **Mask** — Normally, the entire source is used. If only some bits in a pattern are to be used in the source, this is entered here as the mask, as a string of 0s and 1s.  |

**Related Topics**

- Using Property Views  

4.9 User Groups

User Groups are used in Multi-User Access. A User Group is simply a name and a description. Members of the group are added in Users.

Related Topics

- Using Property Views
- Users
- Multi-User Access

4.10 Alarm Triggers

Alarms are triggered by Events, meaning that whenever an Event of a specified type occurs, an Alarm is also generated. The Alarm Triggers screen allows you to add to the Events that trigger Alarms and modify or remove the default triggers.

Alarm Trigger Properties

- Triggering Event: The Event Type which will trigger an Alarm.
- Priority: The importance of the Alarm created. The Priority can be used to sort the Alarms screen.
- Color Triggering Event: The triggering Event will be in this color on the Events screen. This does not affect the Alarm color. (Some Event Types also have a color, whether or not they are Alarm triggers.)
• Using Property Views

• Alarms

• Events

• Event Categories and Types

• Emergency Features

4.11 Door Templates

Door Templates can be created from existing Door configurations, then applied to other Doors that require the same settings. Subsequent changes to the template are applied to every Door using it. Only certain Door properties are controlled by the Template (see below).

When a Door Template is applied to a Door, the properties which come from the template are no longer editable on the Doors screen. To change them, you must either edit the template, or remove the template from the Door.

A Door Template cannot be applied to a Door that has a different Type in its Door properties.

Creating a Door Template from an Existing Door

1. Go to the Doors screen.

2. Select a Door.

3. Click the Create Door Template button in the Door's properties.

4. Enter a name (required, maximum 32 characters), and optionally, a description.

5. Click Save.

Applying a Door Template to a Door

1. Go to the Doors screen.
2. Select a Door.

3. Select a **Door Template** in the Door's properties.

4. Check **Apply Template**. The Door will use the settings from the template only when this is checked. If you remove the check, the Door will keep the template settings unless you change them.

5. Click **Save**.

### Door Template Properties

A Door Template overrides these Door Properties. Some Door types do not use all of these properties.

- Manual Commands Enabled
- Unlock Time
- Held Open Alarm Time
- Minimum Unlock Time
- Extended Unlock Time
- Extended Held Time
- Held Open Pre-Alarm Warning Time
- Suppress Exit Button Events
- Unlock on Exit Button
- Re-lock On

### Related Topics

- **Using Property Views**
- **Doors**
- **Hardware Templates**
4.12 Hardware Templates

Hardware Templates can be created from existing Sub-controller (I/O) properties, then applied to other Sub-controllers that require the same settings. Subsequent changes to the template are applied to every Sub-controller using it. Only certain Sub-controller properties are controlled by the Template.

When a Hardware Template is "applied" to a Sub-controller, the properties which come from the template are no longer editable on the Sub-controller screen. To change them, you must either edit the template, or remove the template from the Sub-controller.

Creating a Hardware Template from an Existing Sub-controller

1. Go to the Hardware screen.
2. Select a Sub-controller.
3. Click the Create Hardware Template button in the Sub-controller's properties.
4. Enter a name (required, maximum 32 characters), and optionally, a description.
5. Click Save.

Applying a Hardware Template to a Sub-controller

1. Go to the Hardware screen.
2. Select a Sub-controller.
3. Select a Hardware Template in the Sub-controller's properties.
4. Check Apply Template. The Sub-controller will use the settings from the template only when this is checked. If you remove the check, the Sub-controller will keep the template settings unless you change them.
5. Click Save.

Related Topics
• Using Property Views

• Hardware

• Door Templates
5 Administration

The Admin menu includes a variety of settings for the whole system.

User Roles lets you see the definition of the built-in User Roles for Users logging into the web application and define new, custom roles.

Backup and Restore lets you backup and restore the system database and manage the scheduled backups.

System Settings provides control over the archiving settings and the custom field labels.

Network allows configuration of the networking settings.

Date and Time allows configuration of the time zone and network time settings.

Email Settings allows an SMTP mail server to be configured for the emailing of Notifications.

Archive Downloads allows the download of archive files generated according to the System Settings.

Firmware Settings allows firmware upgrade, factory reset, and conversion between primary and Secondary Controller functionality.

Web Server Settings allows the upload of an HTTPS certificate.

Authorized Mobile Devices allows you to provide access to mobile devices that have the mobile app installed.

5.1 User Roles

User Roles define what different Users can do within the Web Management Application. The system comes with a number of built-in User Roles which may not be modified or deleted. Custom User Roles can be created.

Here is a summary of the built-in User Roles.

System Unlimited; able to access all screens and functions.
Administration

Access Control Management
Provide access to Users and define the Doors, times, and other access control rules that allow or deny access. Able to configure Doors, but not Hardware. Able to execute all manual commands.

Basic Monitoring
Most monitoring functions. Able to view Alarms but not acknowledge or resolve them. Able to view Users but not create or edit them.

User and Credential Management
Add and manage Users and their associated credentials. Also able to perform some limited monitoring tasks. No Alarm management, and no hardware or Door configuration.

Alarm Monitoring
Similar to Basic Monitoring, but also able to acknowledge and resolve Alarms.

User Role Options - Menu Items

<table>
<thead>
<tr>
<th>Option</th>
<th>System Administration</th>
<th>Access Control Management</th>
<th>Basic Monitoring</th>
<th>User and Credential Management</th>
<th>Alarm Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control: Access Levels</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control: Door Mode Schedules</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control: Emergency Codes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>System Administration</td>
<td>Access Control</td>
<td>Basic Monitoring</td>
<td>User and Credential Management</td>
<td>Alarm Monitoring</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>--------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Access Control: Multi-User Access</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Access Control: Schedules</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control: Shared Access Codes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Access Control: Special Days</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control: Users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>(Read-Only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Archive Downloads</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Backup and Restore</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Date and Time</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Email Settings</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Firmware Settings</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Network</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: System Settings</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>System Administration</td>
<td>Access Control Management</td>
<td>Basic Monitoring</td>
<td>User and Credential Management</td>
<td>Alarm Monitoring</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------</td>
<td>----------------------------</td>
<td>------------------</td>
<td>-------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Administration: User Roles</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration: Web Server Settings</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Alarm Triggers</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Areas</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Card Designs</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Card Formats</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Door Templates</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Doors</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Hardware</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Hardware Templates</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Locations</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: Maps</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration: User Groups</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring: Alarm History</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Option</td>
<td>System Administration</td>
<td>Access Control Management</td>
<td>Basic Monitoring</td>
<td>User and Credential Management</td>
<td>Alarm Monitoring</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
<td>---------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Monitoring: Alarms</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Alarms (Read-Only)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Audits</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Door Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Events</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Event History</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Maps</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: Muster</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: User Access Level Report</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring: User Door Report</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### User Role Options - Manual Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>System Administration</th>
<th>Access Control Management</th>
<th>Basic Monitoring</th>
<th>User and Credential Management</th>
<th>Alarm Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door: Momentary Access</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Door: Set Door Mode</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Option</td>
<td>System Administration</td>
<td>Access Control Management</td>
<td>Basic Monitoring</td>
<td>User and Credential Management</td>
<td>Alarm Monitoring</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------</td>
<td>----------------------------</td>
<td>-----------------</td>
<td>--------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Controller: Resync</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User: Forgive</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Controller: Reboot</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controller: Firmware Download</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### User Role Options - Door Modes

<table>
<thead>
<tr>
<th>Option</th>
<th>System Administration</th>
<th>Access Control Management</th>
<th>Basic Monitoring</th>
<th>User and Credential Management</th>
<th>Alarm Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel/Clear</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlocked</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Access</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Only</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card and PIN</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN Only</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card or PIN</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlocked (Emergency)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lockdown</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card Only (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>System Administration</td>
<td>Access Control</td>
<td>Basic Monitoring</td>
<td>User and Credential Management</td>
<td>Alarm Monitoring</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>-------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Card and Biometric</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card and Biometric and PIN</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric Only</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric and PIN</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric or PIN</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card or Biometric</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric or Card or PIN</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Access, No Exit Button</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card and PIN (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN Only (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card or PIN (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card and Biometric (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card and Biometric and PIN (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric Only (First Unlocks)</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Related Topics

- Using Property Views
- Users

### 5.2 Backup and Restore

Backup and Restore allows configuration of the scheduled backup settings and manual backup or restore of the database.

Backup files are saved in the `.dbbackup` format. Up to three backups can be saved on the Controller. Older backups are automatically deleted. You can also download backup files to your computer.

By default, the database is automatically backed up to the Primary Controller every night at midnight. You can also schedule a backup on a custom schedule. If a scheduled backup is not enabled, the automatic backups do not occur.
To schedule a backup to occur at a different time or frequency:

1. Under **Scheduled Backup**, leave the **Enabled** box checked (recommended).
2. Select **Daily**, **Weekly** or **Monthly**. **Daily** is recommended.
3. Select the time of day to perform scheduled backups.
4. Click **Save**.

---

### Manually Backing Up the Database

Click **Backup Now** to backup the database to a file on the Controller, and optionally download the newly created backup to your computer.

Click **Download Now** to download the file to your computer.

---

### Restoring a Backup

Backups can be restored from a file on the Controller or from an uploaded file.

**Caution**: Existing data will be erased if you choose to restore.

1. Under **Restore**, select the backup or select a `.dbbackup` file from your computer.
2. Click **Restore**, then click **Restore** again at the prompt to confirm.
3. Wait for the restore process to complete. You will be logged out automatically.
4. Log back in to the Web Management Application.

---

### 5.3 System Settings

System settings define assorted settings used by the system, for database maintenance, custom fields, and PIN length.

---

### Database Maintenance
These settings define the storage requirements for Notifications, Events, Audits and Alarms. The default settings are typically sufficient and do not need to be changed. Revise the following if necessary. The archive files generated according to these settings are available in Archive Downloads.

- **Maximum Notifications per User**: Older Notifications are automatically deleted, even if they have not been cleared by the User, to keep the total per User at or under this limit.

- **Maximum Events in Database**: Older Events are archived, to keep the total number of Events in the database at or under this limit.

- **Maximum Event Archive Files**: Events are archived to CSV files on the Controller. This is the maximum number of Event archive files to keep.

- **Maximum Event Archive File Size (Bytes)**: The maximum size of any individual Event archive file.

- **Maximum Audits in Database**: Older audits are archived, to keep the total number of audits in the database at or under this limit.

- **Maximum Audit Archive Files**: Audits are archived to CSV files on the Controller. This is the maximum number of audit archive files to keep.

- **Maximum Audit Archive File Size (Bytes)**: The maximum size of any individual audit archive file.
Maximum Alarms in Database

Older Alarms are archived, to keep the total number of Alarms in the database at or under this limit.

Maximum Alarms Archive Files

Alarms are archived to CSV files on the Controller. This is the maximum number of Alarm archive files to keep.

Maximum Alarm Archive File Size (Bytes)

The maximum size of any individual Alarm archive file.

Custom Fields

This section allows you to change the custom field labels which appear in the Users screen. Maximum 32 characters.

Shared Access/Emergency/PIN Codes

This section allows you to change the system-wide length of all Shared Access Codes, Emergency Codes, and PIN Codes. The same length is used for all of these.

Changing the length will alter all existing PINs.

- Increasing PIN length will prepend zeros to existing shared access codes, emergency codes, and User PIN codes.
- Decreasing PIN length will randomly regenerate all shared access codes and emergency codes, and will clear all User PIN codes.

This length must be between 4 and 8 characters. The default length is 4.

Related Topics

- Users
• **Notifications**

• **Events**

• **Audits**

• **Alarms**

• **Shared Access Codes**

• **Emergency Codes**

### 5.4 Network

Use the Network screen to view or change a Controller’s network settings. The settings apply only to the Controller you are logged into. To change networking for a Secondary Controller you must log in to that controller directly using the link on its **Hardware** page.

We recommend that your Primary Controller be assigned a static IP address. In most cases, Secondary Controllers should use DHCP unless you cannot use Discovery.

Select **Ethernet** to change your wired connection or **WiFi** to set up wireless networking (on supported models). When Network settings are saved, the Controller will reboot, and might be at a different network address when it does so.

#### Network Properties

These properties apply to both wired and wireless connections.

- **Configure IPv4**
  - **Manually** — The Controller will have a static IP address, and all settings must be entered in the remaining properties.
  - **Using DHCP** — The Controller will get all settings from the network. Its IP address will be essentially random, and can change from day to day. No other properties need to be entered.
IP Address  The static IP address to use for the Controller you are logged into

Subnet Mask  The mask for the network, usually "255.255.255.0"

Gateway  IP address of your internet gateway, usually the address of your network router

DNS Servers  The IP address of your DNS server, usually specified by your IT department or provided by your internet service provider. If you don't know, you may use a public DNS. (One such is "Google Public DNS" at "8.8.8.8" and "8.8.4.4".)

Search Domains  Only used as your network administrator directs

Setting Up WiFi

1. Select WiFi in the list.
2. Check Active to turn WiFi on.
3. Click the Scan for Networks button. In the results window, select a network to join.
4. Click the Change button to enter and confirm the network password.
5. Set the network properties.
6. Click Save.

Network Reset

If at any point you find you cannot connect to the Controller at the IP address you have defined, you can try a hard network reset.
Network reset changes the Controller to a "link local" IP address, which allows connecting directly to your computer. Using this connection you can enter the Web Management Application to fix the network settings.

1. Find the small opening on the Controller labeled “Reset.” Insert a paperclip to depress the button for 5-10 seconds. The wired address of the Controller will revert to the default, 169.254.202.242, until rebooted, reset, or the configuration is modified.

2. Connect an ethernet cable directly from your computer to the Controller.

3. If your computer is set to use a static IP address, you will need to temporarily change it to one in the range 169.254.202.xxx, or to DHCP. If you already use DHCP, skip this step. If you do not know, try assuming you use DHCP, which is common.

4. Open a web browser and enter the default controller address, 169.254.202.242. You should be directed to the Web Management Application login screen. Note that it might take a minute for the connection to become available.

Related Topics

- Using Property Views

5.5 Date and Time

Date and Time is used to set the Primary Controller's time zone and network time settings (NTP).

To set the Primary Controller's time zone, select the time zone where the Primary Controller is installed. By default, Controllers are set to the Eastern Time (US & Canada) time zone.

The Use Daylight Savings checkbox determines whether daylight savings is applied.

Date and Time shows the time on the Controller. Browser Time is the time on your computer.

The option Set Server Time to Current Browser Time may be used if NTP is not in use, for a one-time synchronization of the Controller's time to the browser time. Note that this does not synchronize the browser's time zone, only the absolute underlying time.
The **Update Date And Time Automatically From Network** checkbox determines whether NTP is used.

By default, Primary Controllers are configured to use NTP to get time from the network, and they are pre-configured with a default set of NTP servers. These defaults assume that your Controller has access to the Internet. If this is not the case, you may wish to use NTP servers within your network, or turn off NTP entirely if it is not available.

### 5.6 Email Settings

Email Settings are used to configure an SMTP server for sending copies of [Notifications](#) by email, if configured by any Users. The emails are sent to the email address associated with the specific User in the [Users](#) screen.

These settings are below. These settings usually come from an Internet provider, a mail service provider, or a company IT department. Be sure to test the settings with the **Send Test Mail** button.

- **Active**: Enable or disable the email settings.
- **Send Mail From**: Enter the “from” email address for email Notifications. The emails will be “from” this email address.
- **SMTP Mail Server**: The SMTP mail server hostname to send the mail messages through.
- **Port**: SMTP mail server port.
- **Username**: username for the SMTP mail server account.
- **Password**: password for the SMTP mail server account.
Use SSL/TLS  Check to use a secure encrypted connection when communicating with the mail server.

Under Test Mail, enter an email address to send to, and click Send Test Mail to test the settings.

Related Topics

- Users
- Notifications

5.7 Archive Downloads

Events, Audits and Alarms are archived after the system has been running long enough to exceed the limits defined in System Settings. This list will be empty until those limits have been reached.

Files are archived in CSV format. You may select any of them, and download them.

Related Topics

- System Settings
- Events
- Audits
- Alarms

5.8 Firmware Settings
This section shows the current firmware version, and allows it to be updated. See Firmware Update.

Factory Reset

This section allows a Factory Reset as well as a button to reboot the device.

5.9 Web Server Settings

Web Server Settings is used to upload a signed HTTPS certificate, for more secure connections.

**Note:** If a certificate is not uploaded, a self-signed certificate will be used, which results in a browser warning. Your IT department can optionally provide a signed certificate for HTTPS, which is not required for encrypted HTTPS communication but provides additional security and prevents the browser warnings.

1. Obtain a ".pem" or ".pfx" certificate file and copy it to your computer.

2. Click Upload Certificate.

3. Complete the online prompts to select and upload the certificate file.

Changing the certificate results in a reboot of the Controller.

5.10 Authorized Mobile Devices

A mobile device must be authorized before it can connect to the Atlas Series system.

To authorize a device, create an authorization here. Then take a picture of the Authorization Code (a QR code) when the mobile application requests it.

Each code can authorize only one mobile device. You may delete and add authorizations as needed to support several devices. The number of devices you can authorize is limited by your license. Contact your authorized ZKTeco representative for license upgrades.

Authorized Mobile Devices Properties
Name  The name of the authorization. Required, maximum 32 characters.

Enabled  Check to enable. Uncheck to disable.

Valid From  The date when authorization should begin. The default is the current date.

Until Further Notice, Valid To  If Until Further Notice is checked, then the device authorization never expires. If it is unchecked, then the Valid To date must be provided, which determines when the authorization expires.

Authorization Code  The authorization QR code is displayed here once the authorization is saved. You can right click this image to save it for emailing to a user.

Signing in from a Mobile Device

1. Install and run the “Atlas” mobile app, available in Apple’s “App Store” and in “Google Play.”

2. Press Scan QR Code.

3. You might have to confirm that Atlas may use the camera.

4. The photo viewfinder will appear. Point the square scanning box at any copy of the authorization QR code. A picture will be taken automatically when a QR code is within the box, showing the message, “Authorization code successfully located.”

5. The “Sign In” screen is next. Enter the “Server Address” of the primary Atlas Series controller. Enter your Atlas Series “Username” and “Password.” Press Sign In.

6. Once signed in you will see a list of everything you can do, including viewing alarms or status and initiating emergency lockdown.

Important: The mobile device must be connected by WiFi to the same local network as the Atlas Series controllers. To connect from a distance, your network administrator must
in some way open access from the Internet (such as by using a NAT) and provide the necessary “Server Address.”

Related Topics

- Using List Views
6 Features and Tasks

This section provides information on features which span multiple screens and information on common tasks.

**Lockdown**, **Emergency Unlock**, and **Duress** are used to handle emergency situations.

**Reports and Printing** explains how to print from the Web Management Application.

Operators use **Manual Commands** to directly unlock Doors or temporarily change their Door Mode.

**First Credential Unlock** allows the first arriving individual to completely unlock a Door.

Use **Card Enrollment Points** to enroll a User's cards by swiping the card.

**Anti-passback** discourages individuals from loaning or sharing their access card.

You can **reset your password** if you have registered the product.

**Factory Reset** returns your Controller to factory settings and removes all configuration and data.

The **Setup Wizard** must be completed one time during installation and after a Factory Reset.

### 6.1 Lockdown

Global lockdown is a feature to be used in emergency situations to lock all Doors in the system, such that no access is allowed. **Scheduled** and **manually commanded** Door Mode changes have no effect during lockdown.

There are exceptions:

- **Doors** with **Exempt From Global Lockdown** checked are not affected.

- **Emergency Codes** and **Users** with **Access Doors in Lockdown Mode** checked are able to access Doors in the lockdown state.

- Exit Buttons continue to work during lockdown.

- Lockdown versus **Emergency Unlock**.
An emergency unlock will override a lockdown if the emergency unlock occurs after the lockdown.

A lockdown will override an emergency unlock if the lockdown occurs after the emergency unlock.

An emergency unlock condition will return when a lockdown is cleared, if its triggering condition is still active.

Global lockdown can be initiated through the web application, with the button on the top toolbar. It can also be initiated through the mobile application. There is also a button to clear the lockdown, next to it.

In **Sub-controller (I/O) properties** an auxiliary input can be configured with a Linkage to initiate a lockdown if the input becomes active. This can be used to create a physical lockdown button. Note that if a lockdown is initiated by an input, it can only be cleared using the web or mobile application.

When lockdown is initiated, an **Event** is generated. There is a default **Alarm Trigger** which generates an **Alarm** based on this Event.

If active, the lockdown status of the system is clearly shown at the **top of the screen** (regardless of what is being viewed) - “SYSTEM UNDER LOCKDOWN!”, in red. Also, counts of locked down Controllers and Doors are shown in the dashboard statistics on the **home screen**. Note that when a Controller is in a lockdown state, that really just means all of the Doors on the Controller are in a lockdown state (apart from the exceptions above). Any screens which show Door or Controller status will show this state (**Door Status**, **Maps**, etc).

In a system with a Primary and Secondary Controllers, when the Primary Controller initiates lockdown, it also initiates lockdown for all Secondary Controllers, allowing for a total system lockdown.

Individual Doors may be manually put into lockdown mode using **Manual Commands**. Note that a Door cannot have a default or scheduled mode of lockdown.

**Important:** As with all emergency functions, lockdown should be tested ahead of time, to ensure that everything is configured and working correctly.

**Important:** Emergency exit functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance.
Related Topics

- Emergency Features
- Emergency Unlock

6.2 Emergency Unlock

Global emergency unlock is a feature to be used in emergency situations to unlock all Doors in the system. Scheduled and manual command Door Mode changes have no effect during the emergency unlock.

There are exceptions:

- Doors with Exempt From Global Emergency Unlock checked are not affected.
- Lockdown versus Emergency Unlock
  - An emergency unlock will override a lockdown if the emergency unlock occurs after the lockdown.
  - A lockdown will override an emergency unlock if the lockdown occurs after the emergency unlock.
  - An emergency unlock condition will return when a lockdown is cleared, if its triggering condition is still active.

In the Hardware screen, an auxiliary input must be configured to trigger an emergency unlock of all Doors. These Doors are kept unlocked as long as the input is active.

Global emergency unlock can only be triggered by an auxiliary input. Clearing the emergency is also governed by the input.

When a global emergency unlock is initiated, an Event is generated. There is a default Alarm Trigger which generates an Alarm based on this Event.

Counts of emergency unlocked Controllers and Doors are shown in the dashboard statistics on the Home Screen. Note that when a Controller is in an emergency unlock state, that really just means all of the Doors on the Controller are in an emergency unlock state (apart from the exceptions above). Any screens which show Door or Controller status will show this state (Door Status, Maps, etc).
In a system with a Primary and Secondary Controllers, when the Primary Controller initiates emergency unlock, it also initiates emergency unlock for all Secondary Controllers, allowing for a total system unlock.

Individual Doors may be manually put into emergency unlocked mode using Manual Commands. Note that a Door cannot have a default or scheduled mode of emergency unlocked.

**Important:** As with all emergency functions, emergency unlock should be tested ahead of time, to ensure that everything is configured and working correctly.

**Important:** Emergency exit functions are regulated by country- and region-specific fire codes. Please refer to these when designing and configuring your system to ensure compliance. Emergency unlock is intended as a supplement to, but not a replacement for, Doors correctly wired for emergency egress in compliance with fire codes.

### Related Topics

- [Emergency Features](#)
- [Lockdown](#)

## 6.3 Duress

A Duress PIN is an alternate PIN that a User can enter in place of their normal PIN to discreetly indicate duress during Door access (for example, being threatened by an intruder). Door access works as normal from the User’s point of view, without any indication that anything is different at the Door. The User is granted or denied access according to the same rules as usual. In the system, however, an additional Event, **Duress**, is recorded under these conditions.

The Duress Event is configured as an **Alarm Trigger** by default, generating an **Alarm**. Furthermore, the duress Event is one of the options that can be used as a Linkage to trigger the activation of an auxiliary output in the **Hardware** screen.

A **Duress PIN** is configured in the **Users** screen on a per-user basis.
The **Duress PIN** can be derived from the normal PIN automatically using the **Add 1 to Last Digit** method: For example, a normal PIN of 1111 would then correspond to a duress PIN of 1112, and a normal PIN of 9999 would then correspond to a duress PIN of 9990.

Alternatively, the **Duress PIN** can be explicitly specified.

Note that the **Duress PIN** value must be unique, also with respect to all normal PIN codes, **Shared Access Codes**, and **Emergency Access Codes**.

**Related Topics**

- [Emergency Features](#)

### 6.4 Reports and Printing

Printing from the Web Management Application is available in two situations.

- "Export PDF" Menu Buttons: Some list views include this button on the menu. Wherever this option appears, you can create a report of everything in the currently displayed list.

- Screen buttons with labels such as "Generate" or "Print Card." These buttons appear directly on screens that are devoted to printing special documents.

Printing of reports and other documents is performed via the web browser. In all cases, the application creates a formatted document called a PDF file. Depending on which brand of browser you use, you will have either or both of two options. Both are activated by controls in the browser, not in the Web Management Application.

- Save the file to your computer. You can then view or print the report using a PDF viewer program.

- Open the file immediately, where you can view and print it with the capabilities of the browser.

### 6.5 Manual Commands

Manual Commands is a menu button that directly commands Doors to unlock or change **Door Mode**. The button appears on any screen where Doors are listed. The command options are:
Momentary Access
Unlocks the Door momentarily for a single access

Set Door Mode
Changes the Door Mode.
- If Until canceled or next scheduled change is checked, the mode will be applied until canceled or until the next scheduled change.
- Otherwise, enter a Duration, specifying how long the mode change will last.

Cancel
Cancels a previous manual Door Mode change that was made on this screen

Related Topics
- Door Status
- Maps (Monitoring)
- Doors
- Door Modes

6.6 First Credential Unlock

Door Modes with “First Unlocks” stay locked only until the next valid access. The Door will then unlock and stay unlocked until the next scheduled mode change (or a mode change from a Manual Command).

First credential unlock is available anywhere where Door Modes are selected.

Once a valid Card and PIN is presented, the Door will change to Unlocked mode. This will be visible anywhere the Door status is shown. The mode can be changed later using Manual Commands.
6.7 Card Enrollment Points

You can designate readers to use for adding cards to a User without typing in a card number. You might not even know the card number. These are called Card Enrollment Points and are a type of Door. You can also use any card reader at all to create cards for new Users.

Set Up a Card Enrollment Point

You need a Controller with a Configuration that includes "+ Card Enrollment Point". You can do this when you add a Controller, or you can modify an existing Controller. When this is done, one of the Controller's Doors will be an Card Enrollment Point.

Each User may select one Card Enrollment Point to use. Select your choice under Menu: Preferences.

Using a Card Enrollment Point

While on the Users screen,

1. Click "Add" next to the "Cards" box.
2. Click in the "Card Number" field.
3. Swipe the card at the Card Enrollment Point.

Using Any Reader to Enroll
Any card reader in the system can be used to enroll a completely new User, or to find out the number of a card.

1. Swipe the card at any reader.

2. Go to the Events \[22\] screen.

3. Find the corresponding Access Denied (Unknown Card Number) Event. The card number is shown in the User column.

4. Click the card number to create a new User having this card.

If the card is currently assigned to another User, you will get some different Event.

Related Topics

Hardware [56]

Users [38]

6.8 Anti-Passback

Use anti-passback to prevent or detect Users going through the same Door twice in a row, without either exiting from the Area or waiting for the specified time period. For example, Users can enter through an Area with security screening, but must exit through a different Area.

Anti-passback is intended to prevent someone from "passing back" a credential for another person to use it at the same Door, or to another Door entering the same Area. This is commonly used with turnstiles and other special entry devices. Area-based anti-passback can also help prevent sharing of PINs. However, with a normal Door there is no way to prevent one User from simply holding it open for another.

If an access attempt is made which violates anti-passback rules, this will always create an Event [22]. The User may or may not be denied access depending on the configuration.

There are two methods of anti-passback enforcement.

- Door-based — A Door can be opened by the same credential only once during a set time period.
• Area-based — Area-based anti-passback tracks the location of a User and generates a violation if their credential is used somewhere else. For example, if Door 1 exits Area A and enters Area B, and Door 2 exits Area B and enters Area C, then presenting the same credential at Door 1, then Door 2, then Door 1 again is an anti-passback violation, because the User is known to be in Area C when attempting to use a Door which exits Area A.

**Note:** Anti-passback does not apply to Shared Access Codes, Emergency Codes or anti-passback exempt Users (see below).

## Defining Anti-passback Areas

In the Areas screen, you can define the Areas to use for anti-passback. You can also use the predefined Areas, such as Global Out.

## Configuring Anti-passback Doors

In the Doors screen, you can define the entering and exiting Areas and the anti-passback settings.

1. Go to Doors.
2. Under Areas and Anti-passback:
   a. Select the Entering Area. This is the Area that the Door enters into
   b. Select the Existing Area. This is the Area that the Door exits from.
3. Select the Anti-passback Method:
   a. **Area-Based** — Anti-passback is enforced at this Door using any entry to or exit from the Area. Select an anti-passback mode to grant or deny access.
   b. **Door-Based** — Anti-passback is enforced solely based on access to this Door. Enter the number of minutes the anti-passback status is reset after the User enters the Door.
4. Click Save.

## Anti-passback Exempt Users
To exclude Users from anti-passback rules, check the **Anti-passback Exempt** box on the **Users** screen.

### Forgiving Anti-passback Violations

The **Forgive** button on the **Users** screen resets the selected User's anti-passback status. Use this when anti-passback rules are preventing a User's access, and you determine to forgive the violation.

### Related Topics

- **Users**
- **Areas**
- **Doors**

### 6.9 Password Reset

If you lose the passwords for all Users with the Administrator Role, you can apply to ZKTeco for a password reset authorization over the internet. This is only available if you have previously **registered** with ZKTeco, so we can confirm your email address.

#### How to Reset the Admin Password

1. On the login screen, click **Reset Password**.

2. Click the **Request Password Reset** button.

3. If successful you will see the message, "A password reset authorization file has been emailed to...."

When you receive the reply email:

1. Open the mail and save the attachment ("password.reset") to your computer.
2. Return to **Reset Password**.

3. Click the **Upload Authorization File** button.

4. Find and open the emailed file you saved.

5. In the following window, enter and **Submit** a new password for the User, "admin".

### Related Topics

- **Product Registration**

### 6.10 Factory Reset

Factory Reset is used to reset a Controller to its initial configuration.

#### Warnings and Important Info:

- This operation will erase your database. All existing data and configurations will be erased.

- The admin password will reset to the default, "admin".

- **Product Registration** information will be lost, although you will still be registered with ZKTeco.

- The **Network** settings will **not** be reset. If the Controller has a static IP address, it will not change. If it is set for DHCP, it will probably reboot at the same address.

- If an **HTTPS certificate** has been installed, it will **not** be removed.

- The **Date and Time** settings will **not** be reset.

- Backups and Archives are **not** deleted.

1. Go to **Firmware Settings** and expand the **Factory Reset** section.
2. Click **Factory Reset**.

3. You will be logged out. Wait for the Controller to restart, and then log in.

4. You will be directed to the **Setup Wizard**, which must be completed.

### 6.11 Setup Wizard

The Setup Wizard appears when logging in for the first time and after a **Factory Reset**. It must be completed. However, you may exit at any time and complete it later.

**Page 1: Language**

Choose a language. Your choice will be used for this wizard. If this is a Primary Controller, it will also become the default language of the Web Management Application. If this is a Secondary Controller, it will become the default language of the simplified management application on this Controller.

Available languages depend on your **software license**. Contact your authorized ZKTeco representative for license upgrades.

This can be changed in the **Hardware Properties** of the Controller.

**Page 2: Function**
Choose whether this Controller will be a Primary or a Secondary, as discussed at Understanding Controllers and Doors.

Page 3: Primary Controller Name (primaries only)

The name of the Controller will be used for display in the Web Management Application and in reports.

Note: Secondary Controllers are named when they are connected to the system in the Web Management Application.

Page 4: Configuration (primaries only)
Note: Secondary Controllers are configured when they are connected to the system.

Select your time zone. In most cases you will never need to set the actual time; the Controller will get the time from the internet using a technology called NTP. In some cases NTP will not work due to firewalls or network policy. In that case, see [Date and Time](#) after completing the wizard.
Note: Secondary Controllers get their time and time zone from the Primary Controller.

Page 6: Password (primaries only)

Enter a strong password for the primary administrator account. The username for this account is “admin” and cannot be changed.

Page 7: Network Interface Settings
If you have just performed a Factory Reset, these settings should already be set to what they were before the reset.

The important choice here is “Configure IPv4.”

A Primary Controller must have a static IP address. This is because Secondary Controllers need to know how to find the primary on the network. Additionally, the Users need a consistent address to log in to the Web Management Application.

To assign a static IP address, choose “Manually” and enter the IP address and configuration specified by the network administrator.
“Using DHCP” is probably the right choice for Secondary Controllers, unless all Controllers cannot be located on one network subnet, or if Discovery is blocked by network restrictions. In that case:

? Assign these Controllers static IP addresses.

? Manually add these Secondary Controllers in the Web Management Application instead of using Discovery.

See Network[103] for more information or to make changes later.

Page 8: Review

All your entries are displayed for review. Click either “Back” or “Complete Setup.”
7 Reference

Reference material:

- Glossary
- Event Categories and Types
- Door Modes

7.1 Glossary

Access Level A set of Door/Schedule pairings defining access to those Doors during the associated Schedules.

Acknowledged When a User is aware of an Alarm, but nothing has necessarily been done about it

Airlock A rule applying to multiple Doors in an Area restricting which Doors can be opened at the same time

Alarm Trigger Triggers an Alarm from an Event

Alarm Triggered by an Event, an Alarm is like a copy of the Event which can change state from New to Acknowledged to Resolved, for the purposes of Users being made aware of the issue and keeping track of whether and which ones have been Resolved

Anti-passback A rule preventing or detecting the "passing-back" of a credential from one person to another, using the same credential twice in a row at the same Door or entering into the same Area

Audit A record of a change made in the system by a User, or of a manual command executed by a User

Battery Monitor An Input on a Controller configured to detect whether a battery is connected

Biometric A feature of a person which can be used as a credential for identification or verification purposes, like a fingerprint

Card A Card is a credential encoded with a number used for electronic access control. These can come in other form factors like a fob.
Also known as a "Badge"

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Design</td>
<td>A graphical design, including image and text elements, some of which come from a User's record, which can be used to print on the surface of a Card. Also known as a &quot;Badge Design&quot;</td>
</tr>
<tr>
<td>Card Enrollment Point</td>
<td>A Reader configured not for access control, but rather to obtain the card number for enrollment purposes</td>
</tr>
<tr>
<td>Card Format</td>
<td>A technical specification of the format of the data bits encoded onto a Card, including Card Number, Facility Code, Parity. Different vendors supply different Cards encoded using different Card Formats.</td>
</tr>
<tr>
<td>Card Number</td>
<td>The portion of the data bits encoded on a Card corresponding to a unique, identifying number.</td>
</tr>
<tr>
<td>Controller</td>
<td>A physical electronic device which controls input and output for access-control. Atlas Series Controllers can be either Primary Controllers or Secondary Controllers.</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma Separated Values. A text file format which is able to be imported into or exported from Microsoft Excel and other office spreadsheet programs</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol. A network option where a device obtains its IP Address and other networking settings automatically from a router, gateway, or other network device.</td>
</tr>
<tr>
<td>Door</td>
<td>A combination of Reader(s), Input(s), and Output(s) which electronically controls access to a physical door, or something functionally similar to a door, like a parking gate. Also known as an &quot;Access Point&quot;, or &quot;Portal&quot;</td>
</tr>
<tr>
<td>Door Mode Schedule</td>
<td>The mode of operation of a Door, specifying whether the Door is simply unlocked, whether it is locked and unavailable for access, or locked and requiring the presentation of credentials to unlock it. The mode also includes which types of credentials (Card, PIN, Biometric) are required.</td>
</tr>
<tr>
<td>Door Mode Schedule</td>
<td>A schedule with a set of time intervals (including days of the week and Special Day types), where each time interval can be associated</td>
</tr>
</tbody>
</table>
with a Door Mode. The Door Mode Schedule can be associated with a Door to change the Door Mode automatically, according to the schedule.

**Door Sensor**
An Input wired to detect whether a Door is opened or closed. Also known as a "Door Contact" or "Door Position Switch".

**Door Template**
A set of Door properties which can be associated with multiple Doors to re-use common combinations of properties without re-entering them. Also used to change the properties of multiple Doors at once, by simply changing the associated Door Template.

**Duress PIN**
An alternate PIN code which is used to signal a duress condition. Access is granted and denied normally as if the normal PIN was used. When access is granted using a Duress PIN, an Access Granted (Duress) Event is generated, which triggers an Alarm within the software, by default.

**Emergency Code**
A PIN code to be used by emergency or high-security personnel in an emergency situation to gain access to a Door, regardless of Door Mode (including Lockdown)

**Event**
A record of an occurrence within the system. Includes hardware and access activity. Also known as a "Transaction"

**Exit Button**
An Input wired to detect that the Door needs to be unlocked for exit purposes. Generally located on the insecure side of the Door (the side you face when exiting). May be a button, or may be another kind of device such as a motion sensor. Also known as a "Request to Exit (REX)"

**Facility Code**
A number encoded onto a Card in addition to Card Number, which is used to identify a facility, customer, or batch of cards. A single company will often order Cards with the same Facility Code. The exact length and location of the Facility Code within the data bits of the card can be specified in Card Formats, and the actual Facility Code value expected can be specified there as well.

**Fire Code**
Laws and rules in a given country or region which specify how buildings, fire alarm systems, and other electronic systems must be designed, built, configured, and operated for life-safety purposes.
| **Firmware** | Software which runs on an embedded device such as a Controller |
| **Forced Open** | A condition where a Door has been physically opened (according to the Door Sensor), but is also still locked. That is, it has been opened without any valid access, exit request, manual command, or Door Mode allowing it to be opened. |
| **Hardware Template** | A set of Controller properties which can be associated with multiple Controllers to re-use common combinations of properties without re-entering them. Also used to change the properties of multiple Controllers at once, by simply changing the associated Controller Template |
| **Held Open** | A condition where a Door was opened, but not closed within a set amount of time |
| **HTTPS** | A protocol for communicating between a web browser and a web server which is secured through encryption |
| **In (Door)** | A Door configured to enter (In). May be paired with an Out Door, in which case the In Door controls the shared Inputs and Outputs |
| **In/Out** | A configuration on a Controller with 2 Doors, one for entry (In), and one for exit (Out). These 2 Doors represent 2 sides of the physical door. |
| **Input** | An electronic input on a Controller which can detect a circuit being active or inactive. |
| **IP Address** | A numeric address for devices and computers on a network |
| **Location** | A label indicating a Location name, which can be arranged in a hierarchy, to organize Hardware, Doors, Areas, and Maps. |
| **Lock** | An Output on a Controller configured to connect to a physical electronic door lock. Also known as a "Door Strike" |
| **Lockdown** | An emergency state for a Door or Controller where the Door (or all Doors associated with the Controller) are locked and deny access to all credentials (with some exceptions). Lockdown is unaffected by scheduled Door Mode changes as well as normal Manual Commands. |
**Manual Command**
A command executed by a User in the web application or mobile app which affects a Door or Controller. Examples include momentarily allowing access to a Door, changing the Door Mode of a Door.

**Map**
A graphical layout of a facility, often with a floor plan, showing the location of Doors and Controllers, with their status.

**Multi-User Access**
Rules that require multiple Users from multiple User Groups to access a Door.

**Muster**
A report showing the last-known access of each User, if that access is not to the Global Out or Muster Areas.

**Muster Point**
A Door which is used simply to record that a User has reached the Muster Area, for Muster report purposes.

**Normally Closed (NC)**
A type of Input configuration where the normal, "Inactive" condition of the input is where the circuit is closed. Inputs which are typically Normally Closed are Door Sensor, Tamper, Power Monitor, Battery Monitor.

**Normally Open (NO)**
A type of Input configuration where the normal, "Inactive" condition of the input is where the circuit is closed. Inputs which are typically Normally Closed are Door Sensor, Tamper, Power Monitor, Battery Monitor.

**Notification**
An in-application copy of certain Events subscribed to by each User. A copy of Notifications can also be configured to be sent via email.

**NTP**
Network Time Protocol. A protocol for synchronizing time to computers and devices on a network or the Internet. NTP Servers provide reliable, accurate time to devices and computers which subscribe to their services.

**OSDP**

**Out (Door)**
A Door configured to exit (Out), which is always paired with a Door for entry (In). The In Door is the one controlling the shared Inputs and Outputs.
| **Output** | An electronic output on a Controller which functions as an electronic switch, and can control other devices, like a Lock |
| **Parity** | A type of data bit within a Card Format which is used to ensure the integrity of the data read. A parity bit acts as a check on a set of binary values, calculated in such a way that the number of 1s in the set plus the parity bit should always be even (or occasionally, should always be odd). |
| **PDF** | Portable Document Format. A format used for documents or reports which can be easily viewed or printed on a PC. |
| **PIN** | Personal Identification Number. A credential consisting of a numeric code to be entered on a reader’s keypad for identification or verification purposes. |
| **Policy** | A rule linking Events and conditions to actions or outputs. Also known as a "Linkage" |
| **Power Monitor** | An Input on a Controller configured to detect whether the main power is connected |
| **Primary Controller** | The Atlas Series Controller in the system which maintains the entire system configuration, and hosts the web application used to access, configure, and monitor it. A Primary Controller can manage multiple Secondary Controllers. |
| **Reader** | Reads cards or credentials, including possibly Card, PIN, or Biometrics. |
| **Resolved** | The state of an Alarm which means that it has been fully resolved, that is, it is no longer an issue that needs attention or needs to be visible. |
| **RS-485** | A serial communications protocol used for communications between devices, including between Controllers and Readers. OSDP uses the RS-485 protocol, for example. |
| **Schedule** | A set of time intervals (including days of the week and Special Day types), used to regulate Door access by time |
Secondary Controller
An Atlas Series Controller which obtains its configuration from a Primary Controller.

Shared Access Code
A PIN code shared by a group of people, used gain access to a Door.

SMTP Server
An email server for sending email.

Special Day
A day on the calendar (for example a holiday) where normal Door access is to be disallowed by default, unless the Schedule explicitly indicates that Special Days are allowed.

Special Day Type
A category or grouping of Special Days.

SSL
Another term for TLS, a networking encryption protocol.

Sub-controller
A type of Controller which manages inputs and outputs (I/O) but does not make access or other decisions by itself. In some systems, these Sub-controllers are separate physical devices. In Atlas Series, they are built-in to the Controllers.

Tamper
An Input on a Controller configured to detect physical tampering with a case, enclosure, etc.

TLS
A networking encryption protocol.

User Role
A set of permissions for what a User can and cannot do when logged into the web application or mobile app.

User Group
A classification or grouping of Users used for Multi-User Access.

Wiegand
A standard protocol for connecting Readers to Controllers.

### 7.2 Event Categories and Types

Event Colors:

- **Red**: Event is also an Alarm Trigger by default. If you create additional alarm triggers, those events will appear red in the Web Management Application. If you remove built-in triggers, those events will appear yellow.

- **Yellow**: Warnings

- **Green**: Normal access granted
- White: Informational

## System

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Sign In</td>
<td>A User signs in successfully to the application</td>
</tr>
<tr>
<td>Unsuccessful Sign In</td>
<td>A User unsuccessfully attempts to sign in to the application - generic</td>
</tr>
<tr>
<td>Signed Out</td>
<td>A User signs out of the application</td>
</tr>
<tr>
<td>Controller Startup</td>
<td>Controller starts up</td>
</tr>
<tr>
<td>Controller Resync</td>
<td>Data resynchronized to a Controller</td>
</tr>
<tr>
<td>Schedule Active</td>
<td>Schedule becomes active</td>
</tr>
<tr>
<td>Schedule Inactive</td>
<td>Schedule becomes inactive</td>
</tr>
<tr>
<td>Unsuccessful Sign In (Inactive)</td>
<td>A User unsuccessfully attempts to sign in to the application - inactive</td>
</tr>
<tr>
<td>Unsuccessful Sign In (Not Yet Effective)</td>
<td>A User unsuccessfully attempts to sign in to the application - not yet effective</td>
</tr>
<tr>
<td>Unsuccessful Sign In (Expired)</td>
<td>A User unsuccessfully attempts to sign in to the application - expired</td>
</tr>
<tr>
<td>Unsuccessful Sign In (No Privileges)</td>
<td>A User unsuccessfully attempts to sign in to the application - no User Roles</td>
</tr>
<tr>
<td>Unsuccessful Sign In (Outside Schedule)</td>
<td>A User unsuccessfully attempts to sign in to the application - outside schedule</td>
</tr>
<tr>
<td>Card Read (Enrollment)</td>
<td>A Card has been read on an Enrollment Point</td>
</tr>
<tr>
<td>Firmware Updated</td>
<td>Firmware updated</td>
</tr>
<tr>
<td>Firmware Update Failed</td>
<td>Firmware update failed</td>
</tr>
<tr>
<td>Database Backed Up</td>
<td>Database backed up</td>
</tr>
<tr>
<td>Access Granted</td>
<td>Access Denied</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Database Backup Failed</td>
<td>Access Denied</td>
</tr>
<tr>
<td>Access Granted</td>
<td>Generic</td>
</tr>
<tr>
<td>Access Granted (Door Already Open)</td>
<td>Door already open</td>
</tr>
<tr>
<td>Access Denied</td>
<td>Generic</td>
</tr>
<tr>
<td>Access Denied (Inactive)</td>
<td>Card Inactive</td>
</tr>
<tr>
<td>Access Denied (Not Yet Effective)</td>
<td>Before Valid From of User</td>
</tr>
<tr>
<td>Access Denied (Expired)</td>
<td>After Valid To of User</td>
</tr>
<tr>
<td>Access Denied (No Privileges)</td>
<td>No matching Access Level or Door/Schedule assignment</td>
</tr>
<tr>
<td>Access Denied (Outside Schedule)</td>
<td>Matching Access Level or Door assignment, but Schedule is inactive</td>
</tr>
<tr>
<td>Access Denied (Unknown Card Number)</td>
<td>Unknown card number</td>
</tr>
<tr>
<td>Access Denied (Unknown Format)</td>
<td>Bit pattern of data bits on card does not match any defined, enabled Card Format</td>
</tr>
<tr>
<td>Access Denied (Unknown Unique PIN)</td>
<td>Unknown PIN used for PIN-only or PIN-first access</td>
</tr>
<tr>
<td>Access Denied (Incorrect Facility Code)</td>
<td>Card Format recognized, but Facility Code does not match</td>
</tr>
<tr>
<td>Access Denied (No Access)</td>
<td>Door Mode is No Access</td>
</tr>
<tr>
<td>Access Denied (No Card Access)</td>
<td>Door Mode does not allow Card, but Card presented</td>
</tr>
<tr>
<td>Error Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access Denied (No PIN Access)</td>
<td>Door Mode does not allow PIN, but PIN presented</td>
</tr>
<tr>
<td>Access Denied (No Confirming PIN Defined)</td>
<td>Door Mode requires PIN, but User has no PIN defined</td>
</tr>
<tr>
<td>Access Denied (No Biometric Defined)</td>
<td>Door Mode requires biometric, but User has no biometric enrolled</td>
</tr>
<tr>
<td>Access Denied (Incorrect Confirming PIN)</td>
<td>Door Mode requires confirming PIN, but confirming PIN entered does not match</td>
</tr>
<tr>
<td>Access Denied (No Biometric Access)</td>
<td>Door Mode does not allow biometrics, but biometric presented</td>
</tr>
<tr>
<td>Access Denied (Unknown Biometric)</td>
<td>Unknown biometric presented in biometric-only mode, or biometric presented first (one to many biometric verification)</td>
</tr>
<tr>
<td>Access Denied (Incorrect Biometric)</td>
<td>Incorrect or invalid biometric presented (one to one biometric verification)</td>
</tr>
<tr>
<td>Access Denied (Bad Biometric Read)</td>
<td>A biometric was presented, but could not be read/processed</td>
</tr>
<tr>
<td>Access Denied (Anti-passback)</td>
<td>Anti-passback violation</td>
</tr>
<tr>
<td>Access Denied (Lockdown)</td>
<td>Door Mode is Lockdown</td>
</tr>
<tr>
<td>Access Denied (No PIN Presented)</td>
<td>Door Mode requires PIN, but no PIN presented</td>
</tr>
<tr>
<td>Access Denied (Incomplete)</td>
<td>Credentials incompletely presented (for example partial PIN digits)</td>
</tr>
<tr>
<td>Access Denied (No Biometric Presented)</td>
<td>Door Mode requires biometric, but no biometric presented.</td>
</tr>
<tr>
<td>Access Denied (No Card Presented)</td>
<td>Door Mode requires Card, but no Card presented.</td>
</tr>
<tr>
<td>Access Denied (Incorrect Card)</td>
<td>Door Mode requires/allows Card to be presented after PIN or biometric, but the Card does not match that PIN or biometric</td>
</tr>
<tr>
<td>Access Denied (Airlock Busy)</td>
<td>Airlock rules would be violated by the access (another Door in the Airlock-configured Area is unlocked/open)</td>
</tr>
<tr>
<td>Access Denied (No Multi-Credential Presented)</td>
<td>Multi-Credential rule in effect, but the additional credential(s) were not presented</td>
</tr>
</tbody>
</table>

### Communications

| Controller Online | Controller online (Secondary Controller, Sub-controller (I/O)) |
| Controller Offline | Controller online (Secondary Controller, Sub-controller (I/O)) |
| Reader Online | Reader online (OSDP, ZKTeco RS-485) |
| Reader Offline | Reader offline (OSDP, ZKTeco RS-485) |

### Door

<p>| Door Forced Open | Door opened while not unlocked |
| Door Forced Open Restored | Door Forced Open condition not present or no longer present |
| Door Held Open | Door held open too long after being opened |
| Door Held Open Restored | Door Held Open condition not present or no longer present |
| Door Opened | Door opened (according to Door Sensor) |
| Door Closed | Door closed (according to Door Sensor) |</p>
<table>
<thead>
<tr>
<th>Door Mode: Unlocked</th>
<th>Door Mode indication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door Mode: No Access</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card Only</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card and PIN</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: PIN Only</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card or PIN</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Unlocked (Emergency)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Lockdown</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card Only (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card and Biometric</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card and Biometric and PIN</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Biometric Only</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Biometric and PIN</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Biometric or PIN</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Card or Biometric</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Biometric or Card or PIN</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Exit Requested</td>
<td>Exit Button active, triggering exit access</td>
</tr>
<tr>
<td>Door Momentarily Unlocked</td>
<td>Momentary Access Manual Command sent from application</td>
</tr>
<tr>
<td>Door Held Open Warning</td>
<td>Warning prior to Door held open too long after being opened</td>
</tr>
<tr>
<td>Door Mode: No Access, No Exit Button</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Exit Requested (Door Already Open)</td>
<td>Exit Button active, triggering exit access - Door is already open</td>
</tr>
</tbody>
</table>

Copyright©2019 ZKTECO CO., LTD. All rights reserved.
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Door Momentarily Unlocked (Door Already Open)</td>
<td>Momentary Access Manual Command sent from application - Door is already open</td>
</tr>
<tr>
<td>Exit Request Denied</td>
<td>Exit Button active, but exit access not triggered - generic</td>
</tr>
<tr>
<td>Door Momentary Access Denied</td>
<td>Momentary Access Manual Command sent from application - not executed (denied) - generic</td>
</tr>
<tr>
<td>Exit Request Denied (Airlock Busy)</td>
<td>Exit Button active, but exit access not triggered, because it would violate Airlock rules (another Door in the Airlock-configured Area is unlocked/open)</td>
</tr>
<tr>
<td>Door Momentary Access Denied (Airlock Busy)</td>
<td>Momentary Access Manual Command sent from application - not executed (denied), because it would violate Airlock rules (another Door in the Airlock-configured Area is unlocked/open)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Door Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card and PIN (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>PIN Only (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Card or PIN (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Card and Biometric (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Card and Biometric and PIN (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Biometric Only (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Biometric and PIN (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Biometric or PIN (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Card or Biometric (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>Door Mode: Biometric or Card or PIN (First Unlocks)</td>
<td>Door Mode indication</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Controller Access Mode: Unlocked (Emergency)</td>
<td>Emergency Unlock at the Controller level</td>
</tr>
<tr>
<td>Controller Access Mode: Lockdown</td>
<td>Lockdown at the Controller level</td>
</tr>
<tr>
<td>Controller Access Mode: None</td>
<td>Emergency Unlock or Lockdown at the Controller level cleared</td>
</tr>
<tr>
<td>Duress</td>
<td>Duress (Duress PIN was entered)</td>
</tr>
<tr>
<td>Emergency Code Presented</td>
<td>Emergency Code Presented</td>
</tr>
<tr>
<td>Global Access Mode: Unlocked (Emergency)</td>
<td>Emergency Unlock at the Global level</td>
</tr>
<tr>
<td>Global Access Mode: Lockdown</td>
<td>Lockdown at the Global level</td>
</tr>
<tr>
<td>Global Access Mode: None</td>
<td>Emergency Unlock or Lockdown at the Global level cleared</td>
</tr>
</tbody>
</table>

### Input/Output

<table>
<thead>
<tr>
<th>Output Inactive</th>
<th>Output inactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Active</td>
<td>Output active</td>
</tr>
<tr>
<td>Input Inactive</td>
<td>Output inactive</td>
</tr>
<tr>
<td>Input Active</td>
<td>Input inactive</td>
</tr>
</tbody>
</table>

### Tamper/Power

<table>
<thead>
<tr>
<th>On Main Power</th>
<th>Power Monitor Input is inactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off Main Power</td>
<td>Power Monitor Input is active</td>
</tr>
<tr>
<td>Battery Restored</td>
<td>Battery Monitor Input is inactive</td>
</tr>
<tr>
<td>Battery Failure</td>
<td>Battery Monitor Input is active</td>
</tr>
</tbody>
</table>
7.3 **Door Modes**

The Door Mode determines whether or not the Door in an unchanging state (Unlocked, Unlocked (Emergency), No Access, Lockdown), or in an access-controlled state, requiring credential presentation for access. When credentials are required, the Door Mode also determines which types of credentials are required.

When the Door Mode is initially set for a Door, or it changes, a corresponding **Event** is generated (See: **Event Categories and Types**). For example, if the Door Mode becomes **Card Only**, an Event will be generated: **Door Mode: Card Only**.

The default Door Mode for a Door is set in the **Doors** screen.

**Door Mode Schedules** can be used to automatically change Door Modes according to a schedule.

**Manual Commands** can be used to set the Door Mode.

The Door Mode is also shown in **Door Status** and anywhere the status of a Door is shown (**Doors**, **Maps**).

Most access-controlled Door Modes have a **(First Unlocks)** variant. See **First Credential Unlock** for details.

The following is a list of all Door Modes for a Door:

- Unlocked
- Unlocked (Emergency)
- No Access
- Lockdown
- No Access, No Exit Button
- Card Only
Card Only (First Unlocks)
Card and PIN
Card and PIN (First Unlocks)
PIN Only
Pin Only (First Unlocks)
Card or PIN
Card or PIN (First Unlocks)
Card and Biometric
Card and Biometric (First Unlocks)
Card and Biometric and PIN
Card and Biometric and PIN (First Unlocks)
Biometric Only
Biometric Only (First Unlocks)
Biometric and PIN
Biometric and PIN (First Unlocks)
Biometric or PIN
Biometric or PIN (First Unlocks)
Card or Biometric
Card or Biometric (First Unlocks)
Biometric or Card or PIN
Biometric or Card or PIN (First Unlocks)

Note that a Controller can be placed in a special Door Mode during global [Lockdown][113] and [Emergency Unlock][112]. The Events generated for this at the global level are:

- **Global Access Mode: Unlocked (Emergency)**
• Global Access Mode: Lockdown

• Global Access Mode: None

The Events generated for this at the (secondary) Controller level are:

• Controller Access Mode: Unlocked (Emergency)

• Controller Access Mode: Lockdown

• Controller Access Mode: None

Related Topics

• Doors

• Door Mode Schedules

• Manual Commands

• First Credential Unlock

• Lockdown

• Emergency Unlock

• Events

• Event Categories and Types
Index

- F -

Firmware Update    107