VANDERBILT

Access Control
Aliro Software

User Manual

MP1.15

Edition date: 2015-09-17
Document No.: A-100007-3

Vanderbilt International (IRL) Ltd.

Document nr: A-100007-3

Content

1 About this document

This document is based on the dynamic Online help that is visible within in the Aliro Software application. Some guides are related to the Online navigation function.

Note that the electronic version of this manual (in PDF format) also includes navigating links to related topics.

Other related documents are:

Component	Document	Covers
Aliro Software	Installation Manual	Describes the installation of the software as well as important concepts
Aliro Software	Aliro Data sheet	Covers the capabilities and technical data of the software
AP AP01P	Installation Manual	How to install the Access Point controller hardware unit
AP AP01P	AP Data sheet	Technical data for AP
Card Reader ARxx-MF	Reader Illustration Guide	Illustration guide for mounting the card reader
Card Reader ARxx-MF	Reader Installation Manual	Installation manual for mounting and connecting the card reader, including connection to system
Card Reader ARxx-MF	Reader Data sheet	Technical data for card reader

2 Aliro Overview

Welcome to **Aliro Access Control** -- the innovative, next generation access control system, extending the modern art of security to you, through the following features:

- Simple and intuitive 'Point and Click' web based operator software
- Simplified portfolio of hardware enabling IP at door
- Automatic device discovery, and flexible hardware options
- Smart-phone compatible applications offering remote administration and real-time monitoring
- Single license setup, with flexible online update options
- Multi-language support, easily customized for each user
- Direct cardholder interaction on OLED reader displays
- Support for various types of doors
- Fully-customizable access control system, with preconfigured setup options available.

2.1 The Overview

The **Overview** is the Aliro home page, which gives you a general view of the entire access control system. From here, you can navigate to individual **Features** or **Guided Tasks** and view general **System Status** messages.

ACCESS Features	MONITORING Features	TEMPLATES Features
Users	Event log	Card Templates
Areas	Backup / Restore	Door Templates
Doors	System Settings	Hardware Templates
Access Groups	Monitor and Control	Reader Lighting Templates
Access Schedules	Roll Call	
Site Planner		
Roles		
Hardware		
Lightframe Effects		

System Status
The System Status provides detailed messages regarding the status of hardware, server and database. See "System Status" on page 13

2.2 The Aliro Workspace

You can use various flexible tools to effectively utilize the Aliro workspace. Most of these tools can be found on Aliro's main top toolbar. Details about these tools can be found below.

2.2.1 Notifications

The **Notifications** feature allows you to configure the Aliro client to alert or inform you about events as they arise in the system. As a new user, you will see the **Notifications** panel bar at the bottom of your user interface.

Note: The notifications displayed are specific to the user currently logged into the Aliro system.

Configuring Notifications

1. Click the **Configure Notifications** link, found at the bottom of the Aliro user interface.
2. Select the events that you want to be notified about from the tree of **Events** on the displayed window.

   Note: You can expand each event to view and select specific events. For example, click the **System** expander to view and select **The archiving and purging failed** event.

3. Click **Save**.

Displaying / Hiding Notifications Window

Display	Description	Required Action
Notifications window	Found at the bottom of the user interface.	Click the arrow to expand/hide this window.
Notifications button	Found on the top toolbar of the user interface, when there is at least one unacknowledged notification in the system.	Click to expand/hide the **Notifications** window. This button turns yellow on hiding the window.

Monitoring Notifications

The various columns displayed in the **Notifications** window provide detailed information about the event. You can also choose to acknowledge the notifications as they arise. See the table below for details.

Columns and Buttons	Description
Category	Displays the event type.
Occurred	Displays the date and time when the event occurred.
Message	Displays details of the occurred event.
User	Displays the user that caused the event.
Source	Displays the location from where event was initiated.
Acknowledge selected	This action allows you to select one or more notification rows, and acknowledge it.

Columns and Buttons	Description
notifications	In the Notifications window; 1. Select one notification row, or click Ctrl and multi-select more rows. 2. Click **Acknowledge the selected notifications**.
Acknowledge all current notifications	This action allows you to acknowledge all the notifications currently displayed. in the **Notifications** window; 1. Click **Acknowledge all current notifications**.

Changing Display Language of Notifications

1. Click **Menu** on the top toolbar of the user interface.
2. Select **Language**.
3. Tick the display **Language** required. The notifications will now display in the selected language as well as change the Aliro user interface for this user.

2.2.2 Layouts

The Aliro workspace can be customized to your viewing preference. Its features generally allow you to view panel windows of multiple features simultaneously.

Navigate to Layouts:

1. Click **Layouts** on the main toolbar of Aliro's user interface.

Multiviews

The dynamic **Multiview** tool allows you view window panels of related features, as you focus on configuring a particular feature. For example, if you use the **Users Multiview**, you can simultaneously view panels for **Users, Access Groups, Areas, Door** and **Access Schedules**. Choose from the following **Multiview** options:

Multiview	Description
Users	View window panels for **Users, Access Groups, Areas, Doors** and **Access Schedules** simultaneously.
Areas	View window panels for **Areas** and **Doors** simultaneously.
Site Planner	View window panels for **Site Planner, Doors** and **Areas** simultaneously.
Status	View window panels for **Monitor and Control** and **Event Logs** simultaneously.

You can drag and drop various panels to change their position in the current multiview layout.

Multiview Templates

Choose an option from the multiview templates to view either single or multiple panels simultaneously. When the template is displayed in your workspace, choose the feature you want for each panel.

Multiview Template	Description
	Displays a single panel for a selected feature. If a particular feature isn't selected, the **Overview** displays by default.
	Displays two separate vertical panels.
	Displays two separate horizontal panels.
	Displays three panels in total; One main vertical panel, and two horizontal panels adjacent to it.

2.2.3 Menu

The **Menu** contains various options to customize settings on the Aliro user interface. Click on a desired option below to view details.

Language
You can change the display language of the entire Aliro user interface.

1. Navigate to **Menu > Language**
2. Select a preferred language from the list of options.

The display language of the user interface changes to the selected language.

Preferences
You can use the options available here to set the display for lists, activate preferred enrollment readers or enable automatic log out of Aliro. The table below describes each feature and its configuration.

1. Navigate to **Menu > Preferences.**

Field	Description	Configuration
Items per page	This setting configures the number of items that appear in the Master List[1] of every feature. Additional items can then be viewed by using the paging controls at the bottom of the master list.	1. Set a value in the **Items per Page** field. 2. Click **Save**.
Enrollment Reader	This setting configures the enrollment reader to be activated for use by the user currently logged in. **Note**: An enrollment reader can be activated and used by a user, until it is chosen and activated as the preferred reader by a user who logs in later. For example, if a user currently uses a particular enrollment reader and the same reader is later selected by a second user, this second consecutive user can activate the reader to themselves for use. During this time, it will be unavailable for the first user unless re-activated by the first user.	1. Click the drop down list of the **Enrollment Reader** field to display all the enrollment readers configured in the system. 2. Select a reader and click **Activate**. 3. Click **Save**.
Enable automatic log	Tick this check box to set the time	1. Tick the **Enable automatic log**

[1]The Master List is displayed as the left panel of the the main view/window for almost every Aliro feature. This is generally a name list for entities like Doors, Users, Hardware, etc., depending on the feature displayed.

out period	(in minutes) after which the system will automatically log out, if no user action (click or type) is detected in the system. **Note**: Any pending changes in the system that have not been saved, will be discarded after the automatic log out period.	**out period** check box. 2. Set the time (in minutes) in the **Log Out Period** field. 3. Click **Save**.

Save Logs

You can save system log files which can aid technical support teams in case of trouble-shooting. The configuration below explains how to save a zipped log file.

1. Navigate to **Menu > Save Logs...**
2. Click **Download** in the displayed dialog box.
3. Proceed to **Save** or **Open** the downloaded zip file.

About

Registering a Product License

As an Aliro **System User**, you must register your Aliro system using a **Product License File**. This can be done in two ways:

1. **Online Product License Registration (automatic)**
2. **Offline Product License Registration (manual)**

Online Product License Registration (automatic)

1. The **About** dialog box displays all information relating to your Product License. Find this dialog box from Aliro's top toolbar in two ways:
    1. Click the **(... days left to register)** red link.
    2. Click **Menu** > **About**.
2. Click the **Register** button to display the next dialog box.
3. Click the **Request License** button.
4. Enter your details in the required fields.
5. Click **Register**.

If registration was successful:

1. Click **Register** to complete registration. Your system will be automatically registered at the Web Service Registration Service, with a license file.

If registration fails, proceed from your current position to manually register your system offline:

1. Follow the instructions of **Offline Product License Registration** provided below.

Offline Product License Registration (manual)

1. Ensure that you have completed step 1-5 of the previous section.
2. Click the **Download registration file** link. A registration file will be created.
3. Click **Download**.
4. Click **Save** to save a local copy of the registration file.
5. Click **Cancel** to close the dialog box.
6. Take the saved registration file to a device with internet access. In a web browser, open the **Registration Service url** which was displayed below the **Download registration file** link.
7. Click **Register a product key**.
8. Browse and select the registration file (also called a Product Key file).
9. Click **OK**.
10. **Save** the generated license file and take it back to the Aliro client.

11. In the **About** dialog box, click **Register**.
12. Click **Browse**.
13. Browse and select the saved local copy of the license file.
14. Click **Open**. A dialog box confirming the registration will be displayed.

Note: A registered license cannot be modified.

Viewing Current Product License

1. On the Aliro main tool bar, navigate to **Menu > About**.

   Your current product license details will be listed on the displayed dialog box.

Viewing the End User License Agreement (EULA)

1. On Aliro's main tool bar, navigate to **Menu > About**.
2. Click the **End User License Agreement (EULA)** link.

2 System Status

The **System Status** provides detailed messages regarding the status of **Hardware, Server** and **Database**.

Print a System Report
A **System Report** containing a system summary will be created. You can download this report to be saved or viewed.

1. Navigate to the **Overview** page.
2. Click the **Print system report** link, found next to **System Status**.
3. Click **Download**. The report is displayed in a new window.

Hardware

Status	Description
Online access points	Displays the count of **APs** that are online.
Access points currently initializing	Displays the count of **APs** that are currently being initialized.
Online readers	Displays the count of readers that are online.
Reader Mismatch	Displays the count of readers that fulfills any of the two criteria: 1. Belongs to a bus of a different type (for instance an OSDP reader to a Wiegand bus) 2. A reader is moved from an AP that is offline (which indeed cannot report this move) to another AP which is online.

Server

Status	Description
CPU usage	Displays the instantaneous **CPU usage** on the access control server. A warning will be displayed if this stays **above 50 %** for more than **10 seconds**, which may indicate the server processor is overloaded.
Memory usage	Displays the instantaneous **Memory usage** on the access control server. A warning will be displayed if this is above 90%, which may indicate the server machine is running out of memory.
Disk usage	Displays the instantaneous **Disk usage** on the drive on which the access control server is installed. A warning will be displayed if this is **above 90 %**, which may indicate the server machine is running out of disk space.
Active web clients	Displays the number of **web clients** that are currently logged in.
Active mobile clients	Displays the number of **mobile clients** (Android / iPhone) that are currently logged in.
Default admin account secured	Displays when the **default admin account** which was created during installation has not changed the password. Change the **Admin Password** to remove this warning.

Database

Status	Description
Last backup	Displays the time of last database backup, if a backup was done.
Last backup duration	Displays the time taken to perform the last database backup, if a backup was done.
Next backup	Displays the time when next database backup is scheduled. If no scheduled backup has been configured, a warning icon will be displayed. Use the **Backup / Restore** feature to configure a scheduled backup to resolve this warning.

3 Features

Aliro's extensive access control features are categorized into three main groups: **Access**, **Monitoring** and **Templates**.

Click on a particular feature to view description and configuration details.

ACCESS Features

- Users
- Areas
- Doors
- Access Groups
- Access Schedules
- Site Planner
- Roles
- Hardware
- Lightframe Effects

MONITORING Features

- Event log
- Backup / Restore
- System Settings
- Monitor and Control
- Roll Call

TEMPLATES Features

- Card Templates
- Door Templates
- Hardware Templates
- Reader Lighting Templates

3.1 Access

The **Access** features allow you to configure the main parameters required to build your access control system such as **Hardware, Doors, Users** and **Access Schedules**. Information for specific features can be found through the links below.

ACCESS Features

- Users
- Areas
- Doors
- Access Groups
- Access Schedules
- Site Planner
- Roles
- Hardware
- Lightframe Effects

3.1.1 Users

A **User** is a person registered in your access control system. The user must be assigned a **Role**[1], depending on their function in the Aliro system.

Panel Description and Toolbar description

Panels & Buttons	Description
Master List	Panel to the extreme left of this view, displaying a name list of saved users
Main Panel	Displays various user fields in a **Main Panel.**
Create	Creates a **new user**.
Delete	Deletes a selected item.
Save	Saves the current configuration.
Cancel	Cancels the changes since last save.
Filter	Show/Hide filter panel to reduce or search the list of users.
Import	A wizard for importing users from a file.
Forgive	Forgives all users from the **Antipassback** areas.

Related Topics

- Creating a User
- Assigning Cards or Codes
- Assigning Access Rights
- Printing a User Card

3.1.1.1 Creating a User

1. Click →Overview[2] then →Users[3]. The Users view is displayed.
2. Click the →Create[4] button.
3. The **Status** field displays as **Valid** by default.

Status	Description
Valid	Current date is between start and end dates inclusive, or current date is after start date and until further notice is checked, and user is not marked as inactive.

[1]These are functional designations. Roles can be assigned to various users of the security system who have different rights and responsibilities.
[2]Click to show in Aliro
[3]Click to show in Aliro
[4]Click to show in Aliro

Status	Description
Expired	Current date is after end date and user is not marked as inactive.
Pending	Current date is before start date and user is not marked as inactive.
User Inactive	A user can be manually marked as inactive. This means that none of the user's cards can be used for access. This setting will take precedence over all others.

4. Enter the user's →First Name[1] and →Last Name[2].
5. From the →Role[3] drop down list, select a role to assign to this user.
   For roles other than **Cardholder**, configure these following additional fields;

Field	Description
Username	This is the **Username** used to manually login to Aliro.
Password	This is the **Password** used to manually login to Aliro.
Domain Username	Entering a value in this field enables auto-login using Windows authentication. The value should be in the following format: **domainname\username** For example: **site340\Smith John**, where **site340** is the domain name, and **Smith John** is the username in that domain, who will be using Aliro logged in to Windows with that account. Contact your IT administrator to obtain your domain username. • To auto-login to Aliro, browse to **https://your.webserver.name/accesswin**, instead of **https://your.webserver.name/access**. Please note that the auto-login function is supported only when browsing within LAN networks.

6. Click →Save[4].

   A new user is created in the system.

Assigning Cards or Codes to a User

To assign cards manually

1. Ensure that the user **Name** fields are configured on the **Users** view.
2. Click →Add[5] button. A new row is added to the adjacent table.
3. Click **Card Number** field of new row.
4. Type in a card number.
5. Click →Save[6].

Note that the tick box in column **Inactive** can be used to manually disable a particular card. If the System settings is setup to block a user whenever a hard antipassback violation occurs, it will be automatically ticked by the system.

To assign cards using an enrollment reader

As a prerequisite to assigning cards to users using an enrollment reader, ensure that access mode of the reader is configured to **Enrollment Mode**. For further information, click here: Enrollment Reader.

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro
[4]Click to show in Aliro
[5]Click to show in Aliro
[6]Click to show in Aliro

1. Ensure user **Name** fields are configured on the **Users** view.
2. Click →Add[1]. A new row is added to the adjacent table.
3. Click **Card Number** field of new row.
4. Badge the card at the enrollment reader to populate the **Card Number** field.
5. Click →Save[2].

To assign codes to a User
There are two different types of codes: PIN and Personal Code.

- **PIN** is a 4-digit code used with a card in the security mode *Card and PIN*.
- **Personal Code** is an individual code that can be used instead of a card when the security mode at the doors are *Personal Code* or *Group Code*. The default length is 4 digits but can be changed to 4-8 digits in the System settings menu. Note that a **decrease** in code length will empty the Personal Code field and it must be manually generated again (for each user).

The **Reset** buttons empties the fields and the **Generate** button creates a new Personal Code.
The tick box **Personal Code Inactive** can be used to manually disable the use of Personal codes (for this user). If the System settings is setup to block a user whenever a hard antipassback violation occurs, it will be automatically ticked by the system.

Updating a User's Image
Click →Update Image[3] link. A new dialog box appears.

To capture a new photo:
1. Select whether the user is **Male** or **Female**.
2. Click **Start Webcam**. A live video of user is displayed.
3. Click **Take Photo**. The captured photo is displayed.
4. Click **OK**.

To update current user photo:
1. Click **Select File...** button. In the *Open* dialog box, specify location of new photo.
2. Click **OK**.

Access Rights
You can assign access rights to users for **Access Groups**, **Areas** and **Doors**.
1. Click **Access Rights**.

To assign access rights to access groups:
1. Click **Add** in the **Access Groups** tab.
2. Select an access group from the displayed dialog box. Click **OK**.
3. Click **Save**.

To assign access rights to areas:
1. Under **Area Access**, click the **Add**.
2. Select an **Area** from the displayed dialog box. Click **OK**.
3. Click **Save**.

To assign access rights to doors:
1. Under **Door Access**, click **Add**.
2. Select a **Door** from the displayed dialog box. Click **OK**.
3. Click **Save**.

---

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro

Details and Settings
Configure the fields of this section, to configure user details and other specific settings. Refer to the field descriptions below for detailed information.

Field	Description
Language	Choose a preferred language for this user. This will be the display language of the host web client when this user logs in to the system. This will also be the displayed language on the ARxxS-MF reader display when the user interacts with the reader.
Email	Enter user's email address.
Mobile Phone	Enter user's mobile phone number.
Custom Field 1, 2, 3 & 4	These custom fields are set by the operator. To set these fields: 1. navigate to **Overview page> Monitoring list > SystemSettings > Custom Fields**. 2. Configure the four **Custom Field Label** fields with labels of your choice. for example vehicle number, passport number.
User inactive	Ticking this check-box changes the user's status to **Inactive**.
Start Date	Select a date to begin user's **Valid** status in the system. **Note**: This field will not be displayed if the user's role is **System Administrator**.
Until further notice	Tick this check-box to give user a **Valid** status for an indefinite period. **Note**: This field will not be displayed if the user's role is **System Administrator.**
End Date	Select a date to define when the user's valid status ends. From the selected date onwards, the user will be made **Invalid**. **Note**: This field will not be displayed if the user's role is **System Administrator**.
Accessibility	Ticking this check-box means that when the user badges his/her card at a reader, the door will unlock for the **Accessibility Relock Timeout** period, rather than the normal **Relock Timeout** period, permitting easier access. Find the **Accessibility Relock Timeout** field using this navigation: 1. **Overview > Access list > Doors feature > Door Details** expander.
Antipassback exception	Ticking this check-box excludes the user from **Antipassback** areas in the system.

Card Printing
Configure the fields within this section to be able to print user's cards. Refer to the field descriptions below for detailed information.

Field	Description
Card Printing Template drop down	Select a **Card Template** for printing.
Front Side	Displays front side of selected card template.

Field	Description
Back Side	Displays back side of selected card template.
Print Card...	Clicking displays the **Print Preview** window. This window shows cards configured to this user, and a print preview of each. Click **Print...** to print a hard copy of the selected card. **Cancel** aborts printing.
Print Receipt...	This option prints a receipt for printed cards. Click to display a preview of the **Print Receipt**. Select the cards which require a receipt and click **Print**.

3.1.1.2 Assigning Cards

A User can have one or more cards assigned.
These can be registered manually, or by using an enrollment reader.

Assign Cards Manually

1. Ensure user **Name** fields are configured.
2. Click **Add** button. A new row is added to the adjacent table.
3. Click **Card Number** field of new row.
4. Type in a card number.
5. Click **Save** button.

Assign Cards using Enrollment Reader

As a prerequisite to assigning cards to users using a Enrollment Reader, ensure that the Access Mode of the reader is configured to Enrollment Mode. Please refer to the Hardware section.

1. Click **Overview** > **Features** list > **Access** section > **Users**.
2. Click **Users** item. The Users configuration page is displayed.
3. Select existing user from name list on the left, or click **Create** button to create a new user.
   The User configuration page is displayed.
4. Ensure user **Name** fields are configured.
5. Click **Add** button. A new row is added to the adjacent table.
6. Click **Card Number** field of new row.
7. Badge the card at the enrollment reader to populate the **Card Number** field.
8. Click **Save** button.

3.1.2 Areas

An **Area** is a space which access is controlled by at least one **Door** and one **Entry Reader**.

- A default area called **Global Out** exists in the system, which refers to the unsecured area outside your building. This area *must* be configured manually during system setup.
- All users in the system will automatically be given access rights to the global out area.
- Areas can be joined together, and have common doors.
- One or more **Sub Areas**[1] can exist within a **Parent Area**[2].
- When a user is given access rights to an area, they get access to all its entry readers.
- A user must be given access rights to parent areas, and sub-areas separately.

Note: Areas can be created in the **Site Planner** view *only*.
You can use the **Area** view for the following functions:

- To view details of existing areas.
- To execute manual commands on existing areas.

Panel Description

Panels & Buttons	Description
Master List	Panel to the extreme left of this view, displaying a name list of saved areas.
Forgive	Forgives all users from the **Antipassback** areas.
Manual Commands	Issues **Manual Commands** to selected areas.

Viewing details of existing areas:

1. Click to select the **Area** in the **Master Panel**.

   The area details are displayed in the adjacent panel, as given below:

Field	Description
Name	Name of the **Area**, as configured in the **Site Planner** view.
Description	Description of the **Area**, as configured in the **Site Planner** view.
Entry Readers	The **Doors** and **Readers** configured to this area, as configured in the **Site Planner** view.

Configuring the Global Out area
A default area called **Global Out** exists in the system and refers to the unsecured area outside your building. Entry readers of the **Global Out** area, will be automatically configured in the **Site Planner** view, during area configuration.

Related Topics

- Creating an Area

[1] An area contained within a Parent Area.
[2] An area which surrounds a so called sub-area. The sub-area is an area inside the parent area. See also Sub-Area.

3.1.3 Doors

A **Door** is a physically controlled entrance device that allows or denies access between areas.

In access control, a door can represent not only a standard door, but also a gate, gateway, barrier and so on. You can create a door from the **Hardware** view or the **Door** view. Refer to the sections below for more information.

Related Topics

- Create doors in **Door** view
- Create doors in **Hardware** View
- Altering **Door Configuration**
- Apply **Door Template on Door**

3.1.3.1 Creating Doors

1. Click →Overview[1] then →Doors[2]. The **Door** view is displayed.
2. Click →Create[3] to display the door configuration fields and expanders.
3. Proceed to configure the sections displayed.

   Details are provided below.

Panel and Toolbar description

Panels and Buttons	Description
Master List	The left panel of this view displaying a master list of door and Access Point names.
Main Panel	Displays various door configuration fields.
Create	Creates a new door.
Delete	Deletes a selected item.
Save	Saves the current door configuration.
Cancel	Cancels the changes since last save
Manual Commands	Issues manual command on selected door The following commands can be issued: • **Allow Access -** Unlocks the door for the user. This is equivalent to a valid card badge. • **Open** -Changes the current door mode to open. • **Block** - Changes the current door mode to block. • **Secure** - Changes the current door mode to secure. • **Unsecure** -Changes the current door mode to

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro

Panels and Buttons	Description
	unsecure. • **Cancel** - Cancels the previous manual command operation. The following parameters apply to **Open, Block, Secure** and **Unsecure** manual commands. • **Until next schedule change -** Issued manual command will remain in effect till the next access schedule change. • **Until further notice -** Issued manual command will remain in effect until the cancel manual command is issued. • **Duration (in minutes):** Duration for which the manual command is applied.
Modify	Modify brings up a wizard that allows you to make changes to a selected door.

Identification

1. Click the →Identification[1] expander.
2. Configure the fields of this section and click **Save**.

Field	Description
Name	Enter a relevant **Name** for the door.
Description	**Description** summary of the door providing relevant details.
Reader Lighting Template	Displays the currently active template for this door
Door Template	Select a **Door Template** with pre-defined configuration that will be applied to the selected door. When the door uses a template, door modifications need to go through **Door Alterations** or **Door Template.**
Create Door Template	Click to create a new **Door Template** from current door configuration.

Default Security Modes

[1] Click to show in Aliro

Default Door Modes	Description
Open	The door is physically wide open via a door opener.
Unsecured	The door is unlocked and can be opened.
Secured	The door is locked and can only be unlocked by a valid card.
Blocked	The door is locked and user access is disabled.

Default Reader Modes field description

Default Reader Modes and Options		Description
Reader		The logical name of the reader
Mode	**Card and PIN**	Door can be unlocked using **Card and PIN.**
	Card	Door can be unlocked using **Card only.**
	Personal Code	Doors can be unlocked with **Personal Code**.This mode also accepts Card.
	Group Code	Door can be unlocked with a **Group code**. This mode also accepts Card or Personal Code.
	Disabled	Reader is disabled.

Default Other Modes field description
The points in this table are a mixture of **Input** and **Output** points defined in logical door, like **Exit buttons, Door Locks, Door Contacts, Motor Locks** and so forth.

Default Modes and Options		Description
Point		Name of the input/output point.
Mode	**Enabled**	Point is enabled.
	Disabled	Point is disabled.

Security Modes

1. Click the **Security Modes** expander.
2. Configure the **Security Mode** time-range in this section, for specific days.
3. Select a **Scheduled Door Mode**.

Scheduled Door Mode	Description
Open	The door is physically wide open, via a door opener.
Unsecured	The door is unlocked and can be opened.
Secured	The door is locked, and can only be unlocked by a valid card.
Blocked	The door is locked and user access is disabled.

4. Configure the **Scheduled Reader Modes**, and **Scheduled Other Modes** section, as explained in the table below.

Scheduled Reader Modes field description

Field		Description
Reader		The logical name of the **Reader**.
Mode	**Card and PIN**	Door can be unlocked using **Card and PIN.**
	Card	Door can be unlocked using **Card only.**
	Personal Code	Doors can be unlocked with **Personal Code**.This mode also accepts Card.
	Group Code	Door can be unlocked with a **Group code**. This mode also accepts Card or Personal Code.
	Disabled	Reader is disabled.

Scheduled Other Modes field description
The points in this table are a mixture of **Input** and **Output** points defined in logical door such as **Exit buttons, Door Locks, Door Contacts, Motor Locks** and so forth.

Field		Description
Point		Name of the input/output point.
Mode	**Enabled**	Point is enabled.
	Disabled	Point is disabled.

Scheduled Exceptions

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Name</td><td>The Name of the exception.</td></tr>
<tr><td>Security Modes</td><td>
Security Modes
<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>No change to security mode</td><td>The security mode remains as defined by current default and door schedule, therefore no scheduled exception modification effects the security mode.</td></tr>
<tr><td>Standard exception mode</td><td>The security is automatically increased during the dates and times of the scheduled exception as defined in table below.</td></tr>
<tr><td>Custom security mode</td><td>The door or reader mode can be uniquely defined for the date and time exception periods.</td></tr>
</table>
The Standard Exception Mode is applied when:
• First applied to the door, and
• Any operator changes are made, and
• Any automatic changes are made for example via time schedule

The table below describes how the Standard Exception Mode is set in relation to the Door Mode when a scheduled exception is in use:
<table>
<tr><th>Current Door Mode</th><th>Standard Exception Mode</th></tr>
<tr><td colspan="2">Door Security Mode</td></tr>
<tr><td>Blocked</td><td>Blocked</td></tr>
<tr><td>Secured</td><td>Secured</td></tr>
<tr><td>Unsecured</td><td>Secured</td></tr>
<tr><td>Open</td><td>Secured</td></tr>
<tr><td colspan="2">Reader Mode</td></tr>
<tr><td>Card and PIN</td><td>Card and PIN</td></tr>
<tr><td>Card</td><td>Card</td></tr>
<tr><td>Personal Code</td><td>Card</td></tr>
</table>
</td></tr>
</table>

Field	Description
	<table><tr><th>Current Door Mode</th><th>Standard Exception Mode</th></tr><tr><td>Group Code</td><td>Card</td></tr><tr><td>Disabled</td><td>Disabled</td></tr><tr><td colspan="2">Other Modes (Enable/Disable)</td></tr><tr><td>Exit button</td><td>No change</td></tr><tr><td>Door lock</td><td>No change</td></tr><tr><td>Door contact</td><td>No change</td></tr></table>

Local Exceptions

1. Click the **Local Exceptions** expander.
2. Click to **Add** a local exception row.
3. Configure the fields as required. For more information, refer to the field description at the end of this section.
4. To remove a local exception, select it and click **Remove**.
5. Click **Save**.

Field	Description
Start Date	Start date of exception period.
End Date	End date of exception period.
Start Time	Start time of exception period.
End Time	End time of exception period.

NOTE: A **Local Exception** is active from the **Start Date/Time** to **End Date/Time** inclusively. This means that it the local exceptions begins at the start of the specified start minute, and ends at the end of the specified end minute. This allows local exception periods to be arranged sequentially without overlap. View an example below:

Start Date	Start Time	End Date	End Time	Comment
25/06/2014	11:00 am	25/06/2014	11:00 am	Starts at 11:00:00, ends at 11:00:59
25/06/2014	11:01 am	25/06/2014	11:59 am	Starts at 11:01:00, ends at 11:59:59

- Multiple exception periods can be defined but must not overlap.
- For each selected exception period, the user can define a set of security modes to be applied during this security period.

Details

1. Click the **Details** expander.
2. Configure the fields of this section and click **Save**.

Field	Description
Unlocking Time (s)	Specify the time duration (in seconds) that door should be kept unlocked,

Field	Description
	before re-locking after valid entry.
Opening Time (s)	This time duration (in seconds) is in addition to the **Unlocking Time (s)** , at the end of which the door frame should be closed. After this time duration, then the Aliro client flags that the door is held for too long in the **Event Log**.
Door Held Warning Time (s)	This time duration (in seconds) is in addition to the **Unlocking Time (s)** and the **Opening time (s)**. After this total time duration, a **Door Held** alarm is sent from the hardware device, and this event is reported in the **Event Log**.
Accessible Unlocking Time (s)	This time duration (in seconds) is similar to the **Unlocking Time (s)**, but is specifically for users with **Special Accessibility** needs.
Wait for first valid access to unlock	When configured with this option, the door will be unlocked within its **Access Schedule**, only after the first valid card badge.
Disable Manual Commands	This option provides the ability to enable/disable **Manual Command** execution for the door. By default, manual commands are disabled for the door.

Readers

1. Click the **Readers** expander.
2. Click to **Add** a new reader for this door to the table. If you wish to delete a reader row, click the **Remove** button.
3. Configure the fields of this section and click **Save**.

Field	Description
Door Template Reader Mapping	Select an appropriate reader. **Note**: This field lists all the available readers of the selected **Door Template**.
Name	Name of the reader configured to this row.

Field	Description
Activate Automatic Door Opener	This configures the reader to activate the **Automatic Door Opener**.
Reader Lighting Template	This defines any special lighting behavior for the reader

Door Contacts

1. Click the **Door Contacts** expander.
2. Click to **Add** a new door contact input to the table. If you wish to remove a door contact input, click **Remove**.
3. Configure the fields of this section and click **Save**.

Field	Description
Door Template Contact Mapping	Select an appropriate **Door Contact.** **Note**: This field lists all the available **Door Contacts** of the selected **Door Template**.
Name	Name of the door contact.

Exit Buttons

1. Click the **Exit Buttons** expander.
2. Click to **Add** an exit button input to the table. If you wish to remove an exit button input, click **Remove.**
3. Configure the fields of this section and click **Save**.

Field	Description
Door Template Exit Button Mapping	Select an appropriate **Exit Button**. **Note**: This field lists all the available exit buttons of the selected **Door Template**.
Name	**Name** of the exit button.
Activate Door Opener	Configures this button to activate the **Door Opener** and open the door when the exit button is pressed.
Use Accessibility Timeout	This time duration (in

Accessible Unlocking

Field	Description
	Time[1].
High Priority Unlocking	Configures this exit button to the input point defined for the High Priority Unlocking functionality[1].

Locks
This section configures both **Door Locks** and **Motor Locks**.

Door Locks
1. Click the **Locks** expander.
2. Click to **Add** a door lock output to the table. If you wish to remove a door lock output, click **Remove**.
3. Configure the **Door Locks** fields as required. For more information, refer to the field description below.
4. Click **Save**.

Door Locks field description

Fields and Options	Options and Description
Door Template Lock Mapping	Select an appropriate **Door Lock**. **Note**: This field lists all the available **Door Lock** of the selected **Door Template.**
Name	**Name** of the door lock.
Relock	**Options & Descriptions** **On door open**: After unlock, relocks when the door is opened. A delay can be configured on top of the door open. **On door close**: After unlock, relocks only when the door is closed **Pulse**: Pulses the relay to unlock. The external lock will lock automatically without involving the AP.
Relock After Open Time (ms)	For **On door open**, this is the delay to relock after the door open. For **Pulse**, this is the pulse time.

Motor Locks
1. Click **Locks** expander.
2. Click to **Add** a motor lock row to the table. If you wish to delete a row, click **Remove**.
3. Configure the **Motor Locks** fields as required. For more information, refer the field description below.

[1]This time duration (in seconds) is similar to the Unlocking Time (s), but is specifically for users with Special Accessibility needs.
[1]The configured input is defined as an Exit button with an automatic door opener and has a separate unlock time; this functionality configures the input as an emergency unlocking/locking input with no consideration for Time Schedules, Reader modes, etc.

4. Click **Save**.

Motor Locks field description

Field	Description
Door Template Motor Lock Mapping	Select an appropriate **Motor Lock**. **Note**: This field lists all the available **Motor Lock** of the selected **Door Template**.
Name	**Name** of the motor lock.

Door Opener

1. Click the **Door Opener** expander.
2. Configure the fields as required. For more information, refer to the field description below.
3. Click **Save**.

Field	Description
Configure door opener	Tick this check box to configure a door opener device.
Name	**Name** of the **Door Opener**.
Open Action	**Options & Descriptions** **None** — No action. **Turn on** — Turn the relay or output on to unlock the **Door Opener.** **Turn off** — Turn the relay or output off to unlock the **Door Opener**. **Pulse** — Pulse the relay or output (on and then off) to unlock the **Door Opener.** **Inverted pulse** — Pulse the relay or output in an inverted way (off and then on) to unlock the **Door Opener**
Open Pulse Time (ms)	For **Pulse** or **Inverted pulse**, this is the pulse time.
Open Delay Time (ms)	The time for the door opener to be unlocked.
Close Action	**Options & Descriptions**

Field	Description
	<table><tr><td>**None**</td><td>No action.</td></tr><tr><td>**Turn on**</td><td>Turn the relay or output on to lock the **Door Opener.**</td></tr><tr><td>**Turn off**</td><td>Turn the relay or output off to lock the **Door Opener**</td></tr><tr><td>**Pulse**</td><td>Pulse the relay or output (on and then off) to lock the **Door Opener.**</td></tr><tr><td>**Inverted pulse**</td><td>Pulse the relay or output in a inverted way (off and then on) to lock the **Door Opener.**</td></tr></table>
Close Pulse Time (ms)	For **Pulse** or **Inverted pulse**, this is the pulse time.
Close Delay Time (ms)	The expected time the door opener will take to close.

Antipassback

1. Click the **Antipassback** expander.
2. Configure the fields of this section as required. For more information, refer to the field descriptions below.
3. Click **Save**.

Fields and Options		Description
Antipassback Type	**Disabled**	Antipassback rules are not applied but user location still being tracked.
	Soft antipassback	Access is allowed despite the antipassback rules and only an alert is generated when the rules have been violated.
	Hard antipassback	Access is denied, and the all user's cards are immediately set as **Inactive**. Alert is generated when antipassback rules are violated. The only way to return the user's cards to **Active** state is to change their status from the Aliro client.
	Timed antipassback	Access is denied for the time-duration set in the **Access Denied For** field. Alert is generated with antipassback rules are violated.
Access Denied For		Time-duration (measured in hours and minutes) during which access will be denied.
Duration		Duration specifies a time period after which users inside the area are

Fields and Options	Description
	automatically forgiven from antipassback rules. This feature works with both **Soft** and **Hard antipassback**. Setting duration to zero disables this feature.
Entry Readers	Click to **Add** and configure an **Entry Reader** for this door. To remove this reader for this door, click **Remove**.
Exit Readers	Click to **Add** and configure an **Exit Reader** for this door. To remove this reader for this door, click **Remove**.

Intrusion[1]

1. Click **Intrusion** to expand the section.
2. Tick the **Configure intrusion system** check box to enable the fields of this section.
3. Configure the **Arming Schedule** time-range in this section, for specific days.
4. Click to **Add** a new **Arming Schedule Exception**.
5. Configure the fields of this section as described in the table below.
6. To remove an **Arming Schedule Exception**, select it and click **Remove**.

Field	Description
Start Date	Start date of exception period.
End Date	End date of exception period.
Start Time	Start time of exception period.
End Time	End time of exception period.

NOTE: An **Arming Schedule Exception** is active from the **Start Date/Time** to **End Date/Time** inclusively. This means that it the arming schedule exception begins at the start of the specified **Start** minute and ends at the end of the specified **End** minute. This allows arming schedule exception periods to be arranged sequentially without overlap. View an example below:

Start Date	Start Time	End Date	End Time	Comment
25/06/2014	11:00 am	25/06/2014	11:00 am	Starts at 11:00:00, ends at 11:01:00
25/06/2014	11:01 am	25/06/2014	11:59 am	Starts at 11:01:00, ends at 12:00:00

- Multiple exception periods can be defined, but must not overlap.
- For each selected exception period, the user can define a set of security modes to be applied during this security period.

7. Configure the **Intrusion** fields as required. For more information, refer to the intrusion field description below.
8. Click to **Save** the changes.

Field	Description
Exception Intrusion Mode	Please select **Arm** or **Disarm** event for the selected **Exception.**
Exception Automatic Re-arm Delay (m)	Same description as the **Automatic Re-arm Delay (m)** but applies to the selected **Exception.**

[1] The logical term which covers the actions used for controlling an intrusion system.

Field	Description
Automatic Re-arm Delay (m)	When a user disarms the intrusion system during a time specified by an automated **Arming Access Schedule**, the system will attempt to automatically rearm after this delay.
Manual Pre-Arm Delay (s)	Manual pre-arm delay is applied when arming is done by user at any reader or arming button or by remote operation action. **NOTE**: System will wait for the duration of pre-arm delay before initiating requested arming. During pre-arm delay users will be a given pre-warning. The user can abort the arming by presenting a valid card, or by pressing the exit button.
Automatic Pre-Arm Delay (s)	Automatic pre-arm delay is applied when arming is done by an access schedule. **NOTE**: System will wait for the duration of pre-arm delay before initiating requested arming. During pre-arm delay users will be given a pre-warning. The user can abort the arming by presenting a valid card or by pressing the exit button.
Unlock if disarm fails check box	If a disarming fails, for example if an alarm status feedback is still present after timeout, this setting specifies if the door shall unlock or if the door shall remain locked to prevent user entering armed area and causing intrusion alarm. When ticked, the door will unlock even if the area is still armed. In this case, the alarm will not be controlled by the settings in Aliro. Please contact your external intrusion system supplier for details regarding the alarm.
Wait for first valid access to disarm check box	When ticked, the door remains locked and armed until a valid access is made, even if the door/reader mode is set to unlock at an earlier time.
Arming Button	Name of input point which could be used to initiate arming. (optional)
Alarm Status Feedback	Name of input used to sense armed/disarmed state of external intrusion system. In the case when door intrusion system is configured, Alarm Status Feedback (ASF) input is mandatory.
Timeout	During arming sequence arming output is used to command external intrusion system to arm or disarm area and after that ASF input is used to sense change of intrusion state within specified timeout period to determine success or failure of attempted to arm / disarm. Timeout is specified in milliseconds since an external system may be able to react in less then one second.
Red LED Duration	Setting **Red LED Duration** to **0** will result in red LED staying on while ASF input indicates armed. Setting **Red LED Duration** to **1-99** seconds will result in LED turning on for specified duration and then turning off when ASF input indicates armed.
Arming Output	Name of output point used to command external intrusion system to arm or disarm area. In the case where the intrusion system is configured, **Arming Output** is mandatory.

Field		Description
Arm Action	None	No action
	TurnOn	Turns on the **Arming Output** to arm the external intrusion system.
	TurnOff	Turns off the **Arming Output** to arm the external intrusion system.
	Pulse	Pulses the **Arming Output** (on and then off) to arm the external intrusion system.
	PulseInverted	Pulse the **Arming Output** in an inverted manner (off and then of) to arm the external intrusion system.
Arm Pulse Time (ms)		Configured pulse time to turn arming action on or off. This is applicable only when the **Arm Action** is **Pulse** or **PulseInverted**.
Disarm Action	None	No action.
	TurnOn	Turns on the **Arming Output** to disarm the external intrusion system.
	TurnOff	Turns off the **Arming Output** to disarm the external intrusion system.
	Pulse	Pulses the **Arming Output** (on and then off) to disarm the external intrusion system.
	PulseInverted	Pulse the **Arming Output** in an inverted manner (off and then of) to disarm the external intrusion system.
Disarm Pulse Time (ms)		Configured pulse time to turn disarming action on or off. This is applicable only when the **Disarm Action** is **Pulse** or **PulseInverted**.

3.1.3.2 Modifying Door Configuration

There are two ways of modifying the door configuration:

- The **Doors** view
- The **Modify** wizard

Modification Restrictions

The ability to modify a door configuration depends on whether it is linked to **Hardware** and/or **Door Template.** The matrix below describes the **Door Dependency Scenario** to **Hardware**, as well as **Door Template**, and thereby the ability to modify door configurations.

	Linked to Hardware	Linked to Door Template	Ability to Add/Edit/Remove Door Functionality		
			Using Door view	Using Modify wizard	Using Door Template view
Door Scenario 1	×	×	✓	✓	×
Door Scenario 2	✓	×	✓*	✓	×
Door Scenario 3	✓	✓	×**	✓	✓

* In this particular scenario, you cannot add or remove door items in the **Door** view, as the **Add** and **Remove** buttons will be unavailable. Adding or removing door items must be done through the **Modify** wizard.
** In this particular scenario, all door settings on the **Door** view cannot be edited. The only fields that will be available are **Name**, **Door Template** and **Create Door Template**.

About the Door Modify Wizard
This wizard will allow you to make the following changes to a selected door:

- **Unlink from Hardware** - This section allows you to detach this door from the configured physical Access Point, without losing configured user access rights to the door. You can later link the door to a new Access Point.
- **Change Hardware** - This section allows you to alter the mapping of existing hardware or select a new hardware and alter its point mapping.
- **Change Door Configuration** - This section allows you to add, modify or remove door functionality. For example, you can add new **Exit buttons** or **Door Contacts** in this section.

Removing Doors

1. Navigate to **Overview** > **Doors**.
2. Select the door to be deleted from the **Master List**.
3. Click **Delete**.

Note: The system will not automatically unlink any dependent items of this door. You must manually remove all dependencies on the **Door**, like **Site Plan, User Access Rights** and **Access Groups**, before you can delete the **Door** from the system.

3.1.4 Access Groups

Access Groups are a way to specify access rights for doors and / or areas that may be applied to many users. Using access groups, you can update the access rights for multiple users in one step.

3.1.4.1 Creating Access Groups

1. Click →Overview[1], then →Access Groups[2]. The **Access Group** view displays.

Panel and Toolbar description

Panels and Buttons	Description
Master List	The left panel on this view displaying a master list with the names of all configured access groups.
Main Panel	Displays various access group configuration fields.
Create	Creates a new access group.
Delete	Deletes a selected item.
Save	Saves the current configuration.
Cancel	Cancels the changes since last save.

[1]Click to show in Aliro
[2]Click to show in Aliro

Configuring an Access Group

1. Click →Create[1]. The **Access Group** configuration fields appear.
2. Type in a →Name[2] for the **Access Group**. For example After Hours could define access to areas of a building outside normal working hours, or Employees could define access to common areas of a building during normal working hours.
3. Define the times for **Area Access** and/or **Door Access**:

- For access rights to **Areas**:
    1. In **Area Access**, click →Add[3]
    2. Select an **Area** from the displayed dialog box. Click **OK**.
    3. Select an **Access Schedule** to associate with the selected area.

- For access rights to **Doors**:
    1. In **Door Access**; click →Add[4].
    2. Select a **Door** from the displayed dialog box. Click **OK**
    3. Select an **Access Schedule** to associate with the selected door.
    4. Click →Save[5].

4. Click **Save**.

Configuring a Group Code

Every **Access group** can have a **Group code** enabled or disabled. The default code is four digits, however, the number of digits in the code (4-8) are specified in System settings and may be changed.Take care when changing the length since the:

- **Increase** will add zeroes in the beginning *and*
- **Decrease** will re-generate the codes

Remember that the same length also will apply to **Personal Code**. The code is always generated by the system - not manually entered. Note that if the security mode of a door is set to **Group Code**, any card or tags will also work for the users in the **Access Group**.

Field	Description
Use Group code	Check this if the code should be enabled for the **Access Group**. The security mode for the **Door** must be specified to allow for **Group code.**
Code	Actual **Group code** generated by the system. Click on **Generate new** to create a new one or replace an old one.

User actions at the door

1. Enter the correct and specified digits.
2. Press the **tick key** ✓ within 5 seconds.
3. The door unlocks.

- If the user presses the ✗ key - or the tick key is not pressed within 5 seconds the code is dismissed and the reader returns to normal state.
- The user has *three attempts* to enter the correct digits. After that, the reader is blocked and a message is shown. If a valid code then is entered *two times*, the system unlocks the door and the reader returns to normal state.

---

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro
[4]Click to show in Aliro
[5]Click to show in Aliro

3.1.5 Access Schedules

Access Schedules are a set of time intervals that are used to specify when access is granted. They are often connected to different days of a calendar, and different time-spans within a day.

3.1.5.1 Creating an Access Schedule

1. Click →Overview[1] then →Access Schedules[2]. The **Access Schedule** view displays.

Panel and Toolbar description

Panels and Buttons	Description
Master List	The left panel on this view displaying a master name list of all configured access schedules.
Main panel	Main area displaying various access schedule configuration fields.
Create	Creates a new access schedule.
Delete	Deletes a selected item.
Save	Saves the current configuration.
Cancel	Cancels the changes since last save.

1. Click →Create[3]. The **Access Schedule** configuration fields appear.
2. Type in a →Name[4] for the access schedule.

The topics listed below provide instructions for various access schedule configurations. Expand a topic to view the respective instructions.

Create Time-Span for and Access Schedule

1. Identify the **Day/s** for which an access schedule is required.
2. Click and drag on the **Time-Line** of that day/s, to mark access time in green. The selected duration is displayed in the **Selected Time span** field.
3. Click →Save[5].

Create an All-Day Access Schedule

1. Tick the **All Day** check box for the day that access is required. The time-line of the selected day turns green.
2. Click →Save[6].

---

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro
[4]Click to show in Aliro
[5]Click to show in Aliro
[6]Click to show in Aliro

Modify a Time-Span

1. Identify the **Time-Span** to be modified.
2. Drag the ends of the green highlight to increase or decrease the **Time-Span**.
3. Click →Save[1].

Remove a Time-Span

1. Click and select the **Time-Span**.
2. Click **Remove**.

Copy a Time Span between Days

1. Mark a **Time-Span** for a particular day.
2. Click **Copy** of the same day.
3. Click **Paste** of the days which required this time-span. The original **Time-Span** gets copied.
4. Click →Save[2].

Configure Start Date for Access Schedule

1. Open the **Advanced** expander.
2. In the **Start Date** field, enter the date on which the access schedule should start and be repeated from.
3. If you do not wish to configure an **End Date** for the access schedule, tick **Until further notice**.

Configure End Date for Access Schedule

1. Open the **Advanced** expander.
2. Ensure that a Start Date is entered.
3. Un-tick the **Until further notice** check box, to display the **End Date** field.
4. In the **End Date** field, enter the date on which the access schedule should end.
5. Click →Save[3] to save all configurations.

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro

3.1.6 Site Planner

The first step in creating a **Site Plan** is to graphically represent area/s of your site, along with existing doors. Aliro provides you with graphic tools to do this on the site planner view.

3.1.6.1 Creating Site Plans

1. Click →Overview[1] then →Site Planner[2]. The **Site Planner** view is displayed.
2. Click ⊕ **Create**.
3. Enter a **Name** for the site plan.
4. Use the commands described below to create and/or add areas and doors.
5. Click **Save**.

Alternatively, change to **Site Planner** multiview in **Layouts**, to view **Doors** and **Areas**.

Panel and Toolbar description

Panels and Buttons	Options	Description
Drawing Board		Central area displayed, onto which drawing tools can be applied.
Properties Panel		Right-panel which is displayed on applying or clicking on an item on the drawing board. It displays related properties of the selected item.
Master List		Panel to the extreme left of this view, displaying a name list of saved site plans.
⊕ **Create**		Displays a new site plan view.
Delete		Deletes a selected site plan. **Note**: The **Delete** button on individual **Door/Area Properties** panel deletes a selected item on the site plan.
Save		Saves the current configuration.
⊗ **Cancel**		Cancels the changes since last save.
Name		Name of the site plan.

[1] Click to show in Aliro
[2] Click to show in Aliro

Panels and Buttons	Options	Description
Set Background	**Browse**	An image file from a network location can be chosen to be set as the background image for the site plan.
	None	No background image will be set for the site plan. Select the canvas size, that is the white drawing panel on the screen and click OK.
Read only		Tick this check box to disable any editing of the existing site plan design or properties.
Move / Select		Click and click+drag any object on the drawing board. It allows you to select / move / re-size an object on the canvas board.
Polygonal Area		To draw and define a polygonal-shaped area.
Rectangular Area		To draw and define a rectangular-shaped area.
Door		To place a door that already exists in the system onto an area.
Slider tool		To zoom in or out of the drawing board view.
Center View		Resets the drawing board view to the center, so that entire board is displayed.

Areas

Create a Rectangular Area:

1. Click **Rectangular Area**.
2. Click and drag an area on the drawing board. The area will be shaded blue.
3. In the **Area Properties** panel, enter the area's **Name** and **Description**.
4. Next, add **Door/s** to the area.
   Read more on adding doors to site plan.
5. Click **Save**.

   It will be added to the **Area** view's master panel.

Create a Polygonal Area

1. Click **Polygonal Area**.
2. Click and mark out the various borders for the polygonal area, on the drawing board. The area will be shaded blue.
3. In the **Area Properties** panel, enter the area's **Name** and **Description**.
4. Add **Door/s** to the area.
   Read more on adding doors to site plan.
5. Click **Save**.

   It will be added to the **Area** view's master panel.

Re-size Areas:

1. Click **Move / Select**.
2. Click and drag a corner of the area to re-size it.
3. Click **Save**.

Add Points/Corners to Areas:

1. Click **Move / Select.**.
2. Ctrl+click on a desired position on an area edge. A new point will appear at the clicked position.
3. Modify the area shape by adding such points and resizing the area. Any point can be removed by using the keyboard delete key.

Delete Points/Corners from Areas

1. Click **Move / Select**.
2. Select point/corner to be deleted.
3. Click **Delete** on the **Area Properties** panel.

   The point/corner will be deleted from the area.

Delete Areas from Site plan

1. Click **Move / Select**.
2. Select the **Area** on the site plan.
3. Click **Delete** in the **Area Properties** panel.

   The area will be deleted form the site plan and from the area's view panel.

Doors

Add Doors to Areas

You can only add existing doors to areas. This can be done using the **Site Planner view**, or the **Site Planner multiview**.

Add Doors using Site Planner View	Add Doors Using Site Planner Multiview
1. Click **Place Existing Door** and drag over an area border, where the door should be placed. The Available Doors window displays. 2. Select an existing door from the displayed list. Click **OK**. 3. In the **Door Properties** panel of the Site Planner view, select an appropriate area from the adjacent drop down list for every **Entry Reader**. 4. Click **Save**.	1. From Aliro's main top toolbar, navigate to **Layouts** > **Site Planner** multiview. 2. Click and drag an existing door from the Door view's master panel, to an area border on the site plan. 3. In the **Door Properties** panel of the Site Planner view, select an appropriate area from the adjacent drop down list for every **Entry Reader**. 4. Click **Save**.

Note:

- It is not possible to edit **Door Name** and **Description** in the **Site Planner** view.
- A door can be used for *a maximum of two areas*:
  - A door can join *one* **Area** and the **Global Out area**
    or
  - A door can join *two* **Areas.**
- A saved area can be used in only *one* **Site Plan**.

Delete Doors on Site plan:

1. Click **Move / Select**.
2. Select a **Door** on site plan.
3. Click **Delete** on the **Door Properties** panel.

3.1.7 Roles

Roles are a set of permissions that grant or deny user-access to parts of the Aliro system. They can be assigned to various users of the security system, who have different rights and responsibilities.

System Permissions	Details	System Administrator	Site Administrator	Site Operator	Basic Cardholder
Login to Webclient	**Login** via host webpage	✓	✓	✓	
View and Operate	**Overview** feature	✓	✓	✓	
	Users feature	✓	✓	✓	
	Event log feature	✓	✓	✓	
	Notifications feature	✓	✓	✓	
	System Settings feature	✓	✓	✗	
	Areas feature	✓	✓	✗	
	Hardware Templates feature	✓	✗	✗	
	Access Groups feature	✓	✓	✗	
	Access Schedules feature	✓	✓	✗	
	Backup/Restore feature	✓	✓	✗	
	Hardware feature	✓	✗	✗	
	Doors feature	✓	✓	✗	
	Card Templates feature	✓	✓	✗	
	Roles feature	✓	✓	✗	
	Site Planner feature	✓	✓	✗	
Permissions	**Site Operators** Ability to create new, edit or delete existing users with **Site Operator** role assigned	✓	✓	✓	
	Site Administrators Ability to create new, edit or delete existing users with 'Site Administrator' role assigned	✓	✓	✗	
	System Administrators Ability to create new, edit or delete existing users with **System Administrator** role assigned	✓	✗	✗	
	Basic Cardholders Ability to create new, edit or delete existing users with **Basic Cardholder** role assigned	✓	✓	✓	

3.1.7.1 Assigning a Role to a User

1. From →Overview[1], select →Users[2]. The **Users** view is displayed.
2. Click →Create[3] to for a new user, or select an existing user from the →master list[4] on the left.
3. State the **First** and **Last Name**.
4. From the **Role** drop down list, select a role to assign to this user. For roles other than **Cardholder**, configure the additional fields for **Username**, **Password** and **Domain Username**.
5. Click →Save[5].

   The selected role is assigned to the user..

3.1.8 Hardware

An **Access Point (AP)** hardware is the basic unit of the Aliro access control system. You must first configure the AP in your system, before creating doors, or performing any other access control operations. For details on how to do this, refer the section Configuring Hardware.

Related Topics

- Configuring Hardware
- Altering Hardware Configuration

3.1.8.1 Configuring Hardware

1. Click →Overview[6], then →Hardware[7]. The **Hardware** view is displayed.

Panel and Toolbar description

Panels and Buttons	Description
Master List	Left panel on this view, displaying a **Master List** of hardware and door names.
Main Panel	Displays various hardware configuration fields in a **Main Panel.**
Delete	**Deletes** a selected item.
Save	**Saves** the current hardware configuration.
Cancel	**Cancels** the changes since last save.
Discover	**Discovers** all available hardware on the network.
Upload Firmware	**Uploads** a firmware **image** from the local machine to the selected hardware.
Create doors	Displays the door view to **Create Door** configurations.
Modify	A wizard to change configuration of selected hardware(s).

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro
[4]Click to show in Aliro
[5]Click to show in Aliro
[6]Click to show in Aliro
[7]Click to show in Aliro

Discovering Hardware

Note: If you have firewalls installed on your PC, you must open the UDP traffic for port 51526 (inbound) and port 20000 (outbound).
After discovery is complete, you can revert this change.

1. Click the →Discover[1] button, found on the top toolbar.

   The discovered hardware devices will appear in the master list of this view.The display color of each device depends on its status.

Hardware Display Color	Status	Description
Blue (italic)	Discovered	Hardware is available, but a host address is not set in the Aliro host to connect it to this hardware.
Red	Offline	Discovered hardware is connected, but not communicating to Aliro host.
Black	Online	Discovered hardware connected, and communicating to the Aliro host.
Grey	Unknown	Hardware is discovered, but its state is temporarily unknown because the system is trying to retrieve the AP hardware configuration.

Configuring a Discovered Hardware to Online State

1. Click on a discovered **Hardware** in the master list, displayed in *blue.* **Network** and **Host** parameter fields for this hardware displays in the adjacent panel.

   Multi-Select instructions:
   - Press **Shift + Click** to multi-select **APs.**
   - Configure the displayed fields. Refer to the table below.
   - Click **Update Selected Access Points**.
   - Select individual **APs** and modify default settings of **Inputs**/**Outputs**/ **Reader Interface** if required, before creating a door.
2. Configure as described below.

Field descriptions

Field	Description
Name	Modify the **Name** of the hardware device ,if required.
Serial Number	This is the unique **Serial Number** of the device, used for communication between the Aliro host server and hardware device. This field is auto-populated on discovery.
Firmware Version	**Firmware Version** of the hardware device. This field is auto-populated on discovery.
Hardware Version	**Hardware Version** of the hardware device. This field is auto-populated on discovery.
MAC Address	**MAC Address** of the hardware device. This field is auto-populated on discovery.

[1]Click to show in Aliro

Field	Description
Host Address	Enter the **IP address** of the **Aliro host**, to connect the Access Point to Aliro. **Note**: If this field is not configured correctly, the Access Point will not change to an online state.
Use DHCP to obtain addresses checkbox	If this checkbox is unticked, the fields given below need to be filled. If this checkbox is ticked, the **DHCP server** be used to auto-populate the fields below.
IP Address	**IP Address** of the hardware device.
Network Gateway	This is your **Network Gateway** address, and is mandatory, even if its not necessary for your network connection.
Netmask	**Netmask** used to access the remote network of the hardware device.
Preferred DNS Server	IP address of the first **DNS server.**
Alternate DNS Server	IP address of the second **DNS server.**

3. Click →Save[1] after configuring the fields on this page.

   The hardware device turns *black* in the master list, indicating that it is now online. More configuration options will be available after the hardware device has come online.

Configuring an Online Hardware Device

You can configure the sections within the following expanders for the hardware device:

Identification

1. Click the →Identification[2] expander. The field descriptions for this section are provided in the following table.

Field Descriptions

Field	Description
Name	By default, the serial number or **Name** of the hardware device displays.
Serial Number	**Serial Number** of the device. Auto-populated field. Cannot be edited by user.
MAC Address	**MAC Address** of the device. Auto-populated field. Cannot be edited by user.
Status	**Status** of the device. Auto-populated field. Cannot be edited by user.
Model	**Model** of the device. Auto-populated field. Cannot be edited by user.
Hardware Version	**Hardware Version** of the device. Auto-populated field. Cannot be edited by user.
Firmware Version	**Firmware Version** of the device. Auto-populated field. Cannot be edited by user. This field value changes on downloading new firmware version.

[1]Click to show in Aliro
[2]Click to show in Aliro

Template Properties
This configuration allows you to select and apply a pre-configured **Hardware Template** to this hardware device.

1. Click **Select and apply Hardware Template...**.Click →Save[1].

Firmware Download
This configuration allows you to download firmware images for readers and hardware devices. To do this, you will first specify a firmware image file to be copied from a local client location, to the Aliro web server. Next, you must find this firmware image through Aliro, and download it to the hardware device. The simple steps required to do this are explained below.

1. Click the **Firmware Download** expander button. The field descriptions for this section are provided in the table below .
2. Click Upload Firmware[2] found on the top toolbar of this page. Select the firmware image file to be downloaded to the web server.
3. Click the drop-down button in this section and select the same firmware image file from the displayed list.
4. Click **Download...**. A dialog box will display the download percentage until complete.

Field Descriptions

Fields	Description
Download File	Select from displayed firmware versions .
Download button	**Downloads** the selected firmware version from the web server to the selected hardware device.
Name	**Name** of the firmware image file.
Type	**Access Image** - Image is for a Access Point device. Full image includes OS and application. **Reader Image** -Selected firmware image is for a reader device. **Reader DB Image** **Full Image**
Version	Version number of the firmware image.
Download firmware to all readers	Select this field to **Download the selected firmware to all readers** connected to this hardware device. This option is displayed only when a reader firmware image has been selected.
Download firmware to individual readers	Select this field to **Download selected firmware to individual readers**. This option is displayed only when a reader firmware image is selected.

Details

1. Click the →Details[3] expander button. The field descriptions for this section are provided in the following table.

Field Descriptions

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro

Field	Description
System Language	Sets the **System Language** of the hardware device for system messages, those are messages not related to user or card.
Time Zone	Sets the **Time Zone** for the hardware device.
Use daylight saving time	Check this tick-box to configure this hardware device to **Use daylight saving time.**
Tamper Mode	**Options & Descriptions** **Auto reset** — **Auto reset** ensures hardware device to automatically reset itself after it has gone into tamper mode. **Disabled** — **Disabled** sets hardware device to be manually reset after it has gone into tamper mode

Communication Settings

1. Click the →Communication Settings[1] expander button. The field descriptions for this section are provided in the following table.

Field Descriptions

Field	Description
Use DHCP to obtain addresses	If this check box is unticked, the fields given below need to be filled. If this check box is ticked, the **DHCP server** be used to auto-populate the fields below.
IP Address	**IP address** number of the hardware device.
Network Gateway	**Network gateway address** ...
Netmask	**Netmask** used to access the remote network of the hardware device
Preferred DNS Server	IP address of the *first* **DNS server.**
Alternate DNS Server	IP address of the *second* **DNS server.**
Communication Enabled	Tick for **Communication Enabled** between the Access Point and Aliro host. Events from the Access Points will be communicated to the host.
Is multidrop	A read only field, that describes whether the selected Access Point has multi-drop RS485 communication with other Access Points. If ticked, this Access Point is considered the primary Access Point for the host to communicate with the other Access Points.
Can be discovered	If this check box is ticked, the hardware device will be displayed in the left master-list of the hardware view, on clicking **Discover**.
MAC Address	**MAC Address** of the hardware device. This field is auto-populated on discovery.

[1] Click to show in Aliro

Field	Description
Host Address	Enter the **IP address** of the Aliro host for connecting the hardware to Aliro.
Web Server Username	Login username for the Access Point web interface.
Web Server Password	Login password for the Access Point web interface.

Reader Interface 1 and 2

1. Click the →Reader Interface 1[1] or the →Reader Interface 2[2] expander. The field descriptions for both these sections are provided in the following table.

Field Descriptions

Field and Options	Options	Description
Reader Type dropdown	**Wiegand**	Specifies **Wiegand** protocol for this reader interface.
	OSDP	Specifies using **OSDP** protocol for this reader interface.
	Clock/Data	Specifies using **Clock/Data** protocol for this reader interface.
Name		**Name** of reader as defined in the hardware device. It is recommended that name not be changed.
Card Format		List of available **Card Formats** supported by the Access Points.
Access Mode	**Access**	The reader performs access functions in this mode, like door open, door lock. Events triggered by the reader in this mode are displayed in the event log.
	Card Enrollment	The reader performs only card enrollment functions in this mode. Events triggered by the reader in this mode are not displayed in the event log.
	Muster Point	The reader will be used as a muster point together with the roll call reporting function. The reader performs only muster point functions in this mode and antipassback is not available.
Tamper Mode	**Disabled**	Sets hardware device to automatically reset itself after it has gone into tamper mode.
	Auto reset	Sets hardware device to be manually reset after it has gone into tamper mode.
Hardware ID		This ID is specific to each hardware device. It is an auto-populated field and cannot be changed.
Serial Number		**Serial Numbe**r of the hardware device. This is an auto-populated field and cannot be changed.
Model		**Model** of the hardware device.
Firmware Version		Refers to the **Firmware Version** currently downloaded to this reader.

[1]Click to show in Aliro
[2]Click to show in Aliro

Inputs

1. Click the →Inputs[1] expander button.
   The field descriptions for this section are provided in the following table.

Field Descriptions

Fields and Options	Description
Name	**Name** of the input, which should ideally reflect its location and function in the overall system.
Inverted	The logic of the input signal is **Inverted.**
Enabled	The input is **Enabled.**
Functionality	**Options and Descriptions**

Options and Descriptions	
Not used	No functionality is configured
Door contact	Defines this input point as a **Door Contact** sensor, monitoring the open or closed state of the door.
Lock contact	Defines this input point as a **Lock Contact** sensor, monitoring that the lock action is performed.
Exit button	Defines this input as an **Exit button**.
Alarm status feedback	Configures this input to signal **Alarm status feedback** from an intrusion panel that defines if an area is armed or disarmed.
Elbow switch	Defines this input as an exit button with the accessibility right **Elbow switch**.
High priority unlocking	If this input is defined as an exit button with an automatic door opener and has a separate unlock time, the **High priority unlocking** configures the input as an emergency unlocking/locking input with no consideration for access schedules, reader modes and so on.
Tamper detection	Configures this input to any **Tamper detection** to the hardware device.
Arming button	Defines this input as a an **Arming button** that arms an area.
Power failure	Configures this input to indicate **Power failure**. Event logs are generated when such an event is triggered.

Enable Notifications	When **Enable Notifications** is ticked, the input will trigger an event when its state changes.

Outputs

[1] Click to show in Aliro

1. Click the →Outputs[1] expander button. The field descriptions for this section are provided in the following table.

Field Descriptions

Field	Options and Description	
Name	**Name** of the output, which should ideally reflect its location and function in the overall system.	
Functionality	**Drop down options and descriptions**	
	Alarm bypass	Configures the output point to bypass an armed area.
	Door lock	Configures this output point to lock/unlock a door.
	Door opener	Configures this output point to open a door.
	Event notification	Configures this output to be triggered by the event notification type selected.
	Intrusion arm/disarm	Configures this output point to signal arm/disarm to the intrusion panel., which returns its status via the Alarm Status Feedback functionality[2].
	Intrusion arming pre-warning	This is a pre-alarming output, that is connected to a device which warns before arming an intrusion area.
	Motor lock	Defines this point as a combined output-input device that signals when locking has occurred. The point is configured as an output point for motor lock, and as an input point for lock contact.
	Not used	Output is not defined for any functionality.
	Wiegand - buzzer	Output is defined for Wiegand reader buzzer.
	Wiegand - green	Output is defined for Wiegand reader green LED control.
	Wiegand - red	Output is defined for Wiegand reader red LED control.
	Wiegand - yellow	Output is defined for Wiegand reader yellow LED control.
Event Notification	**Drop down options and description**	

[1] Click to show in Aliro
[2] An Input Point functionality of the hardware device that the input to signal from an Intrusion Panel that defines if an area is armed or disarmed.

Field	Options and Description	
	Undefined Event Type	No event is indicated by this output.
	Card expired	Notifies that users' card has expired.
	No access rights for door	Notifies that user has no access right for the door.
	Card unknown	Notifies of an unknown card.
	Schedule violation	Notifies of a schedule violation.
	Antipassback violation	Notifies of an antipassback violation.
	Pending activation	Notifies of a pending activation.
	Card inactive	Notifies that the card is inactive.
	Valid access - duress	Notifies that the user is under duress.
	Valid card access	Notifies of valid access using card.
	Valid card and PIN access	Notifies of valid access using card and PIN.
	Valid REX access	Notifies of valid access using an exit button.
	Door forced	Notifies that door has been forced.
	Door held	Notifies that door is being held.
	Door never opened	Notifies that door was never opened.
	Door unsecured with manual command	Notifies that the door was unsecured when its manual command was issued.
	Motor lock failed to lock	Notifies that the motor lock failed to lock.
	Motor lock failed to unlock	Notifies that the motor lock failed to unlock.
	Door unlocked exit request PC	Notifies that exit request is sent from the PC.
	Door reset by operator	Notifies that the door was reset by an operator.
	Arming initiated by access schedule	Notifies that arming was initiated by a configured access schedule.
	Arming acknowledged	Notifies that arming was acknowledged.
	Arming failed	Notifies that arming failed.
	Arming initiated from intrusion panel	Notifies that arming was initiated from intrusion panel.
	Disarming initiated from intrusion panel	Notifies that disarming initiated .
	Disarming acknowledged	Notifies that disarming was acknowledged.

Field	Options and Description
	Disarming failed — Notifies that disarming failed. **Arming aborted** — Notifies that arming was aborted. **Arming Pre-warning** — Notifies, through a warning, that that an area is going to be armed. **AP lid tamper** — Notifies of tamper to the AP lid. **AP wall tamper** — Notifies of tamper to the AP wall. **AP tamper** — Notifies of tamper to the AP. **Reader tamper** — Notifies of tamper to the reader.
Hardware ID	This ID is specific to each hardware device. This is an auto-populated field, cannot be changed by an Alrio user.

Maintenance

1. Click the →Maintenance[1] expander. The command descriptions for this section are provided in the following table.

Command	Description
Initialize	This will initialize the Hardware Device
Cancel Initialize	Stops the initialization
Request description	The AP is forced to described itself
Activate Buzzer	Activates the Hardware buzzer for 10 seconds
Deactivate Buzzer	Deactivate the Hardware buzzer

Creating a Door from the Hardware View

This operation will create a new door, and link it to the selected Access Point. **Note**: You can simultaneously create multiple doors for different APs using the multi-select option. To do this, press **Shift + Click** and required **AP**s in the master list.

1. Click →Create Doors[2].
2. In the displayed dialog box, specify the **Door Name**. If you have configured **Door Templates**, you can optionally select one. The created door will display side-by-side this Access Point in the master list.

When the required configurations have been made, click →Save[3].

3.1.8.2 Modifying Hardware Configuration

This wizard will allow you to make the following changes to a selected hardware:

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro

- **Replace Hardware** - To replace the existing hardware.
- **Unlink from Door** - To detach this hardware from the door, without losing configured user access rights to the door. You can later link this hardware to another door.
- **Change Door Configuration** - To add/modify/remove door functionality, for example to add new exit buttons, or door contacts.

3.1.9 About Lightframe Effects

This function enables for a customized colour scheme for the **Lightframe**. Those can be used in any specific **Reader Lighting Templates**.

Related Topics

- Creating Lightframe Effects
- About Reader Lighting Templates
- Creating Reader Lighting Template

3.1.10 Creating Lightframe Effects

This function enables for a customized colour scheme for the **Lightframe** used in any specific **Reader Lighting Templates.**

1. Click →Overview[1] then →Lightframe Effects[2]. The **Lightframe Effects** view is displayed.
2. Click ⊕ **Create**. A new **Lightframe** page displays.
3. Enter a **Name** and **Description** for this lightframe effect.
4. Select **Colour 1** and **Colour 2**.
5. Select the **On Period** in seconds. The **On Period** determines how many seconds each colour will be displayed on the lightframe.
6. Select the **Off Period** in seconds. The **Off Period** determines how many seconds the lightframe will, optionally, be turned off after each colour has been displayed, before it starts over and the lightframe goes back to colour 1 again. Set to 0 in order to skip turning the lightframe off at all.
7. Click →Save[3].

[1]Click to show in Aliro
[2]Click to show in Aliro
[3]Click to show in Aliro

3.2 Monitoring

The **Monitoring** features of Aliro allow you to observe and monitor your system, by receiving detailed information about both user and system events. It also allows you to configure certain system related settings. For more information, click on a feature below.

MONITORING Features


Event log


Backup / Restore


System Settings


Monitor and Control


Roll Call

3.2.1 Event Logs

An important part of Aliro is to have an overview of what is happening in the system. This is compiled in **Event Logs**. Aliro enables event monitoring in real-time, and/or search for events in a log. The settings for both ways are done in a similar way by initially selecting **Live** or **Report.**

Navigate to the **Event Log** feature:

1. Click →Overview[1] then →Event Log[2]. A live **Event Log** window displays event log lists using a default fields.
2. To add or remove fields to the event log, right-click the field-bar and make your selection from fields described in the table that follows.

Live Event Log Field	Description
Category	The event type category that the live event log message belongs to.
Occurred	The date and time that the event occurred.
Message	A short description of the occurred event.
User	Displays the user that caused the event.
Source	Displays the client location from where event was generated.
Recorded	Displays the date and time of the reported event, when it is recorded into the server database. Most often, this value will match the **Occurred** field. In the event that it doesn't, it could signal that the server has faced a delay in receiving information regarding an occurred event, or that the AP is in a different time-zone to the server.

[1]Click to show in Aliro
[2]Click to show in Aliro

Live event log related functions and controls, that are available on the menu bar of this window, are detailed below.

Button function details

Button	Description
Filter	Displays a left panel, where you can choose the event log **View Mode**. And also filter events by **Event Text** or **Event Type**.
Pause **Resume**	Click **Pause** to temporarily freeze the display of new events in the live event log window. The button itself changes to a **Resume** button when clicked. Click **Resume**, to continue displaying all live event log generated since pause. Note that this button is disabled for the **Report** view mode.
Clear	Clears the live event log window of any event log messages. However, messages will be saved in the database. Note that this button is disabled for the **Report** view mode.
Export CSV	Generates a **.CSV file** of the displayed events.
Export PDF	Generates a **.PDF** file file of the displayed events.

3.2.1.1 Live Event Logs

Live Event Logs display a real-time list of occurred events on the screen. This list can be customized based on various filter criteria. It is also possible export CSV or PDF reports of displayed live event logs.

3.2.1.2 Configuring Live Event Logs

1. Click →Overview[1] then →Event Log[2]. The **Live Event Log** view appears. Event log lists are displayed with default fields.
2. To add or remove fields to the live event log, right-click the field-bar, and make your selection from fields described below.

Filtering Event Log

A. **Filtering by Event Text**
   1. Click **Filter** to display a left-panel.
   2. Five **Event Text Filters** are now displayed: **AP**, **User**, **Door**, **Area**, and **General**. All of these except the general filter have a selection button where a relevant item may be selected from the list. As well as the selection buttons, you may also enter free text to filter the events. Multiple items in the same box should be separated by a semi-colon.
   3. The **AP** filter will always show all events matching any of the search items without any effect from the other four filters.
   4. The **User**, **Door**, and **Area** filters will also show all matching events for any search item, unless the **User @ Door/Area** is ticked. Ticking User @ Door/Area ensures that only the events that match the combination of **User** and **Door**, or **User** and **Area** as selected will be displayed.
   5. The **General** filter may be used to show events that match the complete combination of its selected terms by using the **AND** button, or to displayed events that match any of its selected terms by using the **OR** button.

[1]Click to show in Aliro
[2]Click to show in Aliro

B. **Filtering by Event Type**

1. Click **Filter** to display a left-panel.
2. Under **Event Type Filter**; expand the **Events** menu.
3. All categories under **Events** are selected, by default. To customize this filter, select/deselect any of the displayed categories. The adjacent **Live Event Log** window will display filtered results.

Highlighting Event Logs in Color

You can apply specific colors to an event types. Once applied, these events will appear color-highlighted in the displayed **Event Log**, making it easier to visually categorize them.

1. Click and expand a specific event, for example **System**.
2. Tick a check box for a specific event type to select it for **Event Log** display.
3. Click the circle next to the tick-box.
4. Select a color from the displayed drop down list to be applied to the specific event type. Refer the screen shot to the left.

Important Note about Valid access - duress Event

A **Duress** is a covert signal a cardholder can send during a card badge operation to notify the operator that he/she is in a state of distress.

Requirements to configure a duress:

- In the **Door** feature:

  The **Reader** must be set to the **Card and PIN** mode.
- In the **Event Log** feature:

  Select the **Valid access - duress event**, in the **Event Type Filter** and set a highlight color for this event.

Cardholder action to send a duress signal

A cardholder can send a duress signal to an operator by entering their **Duress PIN** at the reader. Their unique duress PIN is the cardholder's standard PIN with its last digit incremented by 1.
For example: If the cardholder's PIN is 2356, the duress PIN becomes 2357.
Note: If a cardholder's PIN is 9999, the duress PIN will be 9990 and not 10000.

If your system is configured for duress correctly, entering a valid duress PIN at a reader should display a highlighted **Valid access - duress** event log in the system, specific to the cardholder.

Create and Export Live Event Log

1. Click **Pause** to temporarily freeze display of new events in the **Live Event Log** list.

2. Ensure that displayed **Live Event Log** list contains all details for the report.
3. Click **Export CSV** to create a report that will be exported and saved as a CSV file.

   Or, click **Export PDF** to create a report to be exported and saved as a PDF file.
4. To continue displaying **Live Event Log** messages, click **Resume**.

3.2.1.3 Event Log Reports

When a choice of **Report** is done, the events can be searched in an **Event Log** database.

3.2.1.4 Configuring Event Log Reports

1. Click →Overview[1] then →Event Log[2]. By default, the live **Event Log** view is displayed.
2. Click **Filter** to display a left-panel.
3. Select **Report** under the **View Mode** section.
4. In the **From** and **To** fields, enter the start date and time, and end date and time respectively. This sets the date and time interval for which generated event log messages should be retrieved.
5. Click **Run**.

   The retrieved event log messages will display on the adjacent right window.

   Note: There is a limit of 5000 messages that can be displayed on the screen. A message ***There are more event log entries matching filter criteria. Refine it to reduce the result size.*** will appear at the bottom of the report should the selected date and time interval contain more than 5000 log messages. Both narrowing date and time interval and applying filter can help to reduce the number of messages included in the report.

Filtering Event Log Reports

1. Five **Event Text Filters** are now displayed: **AP**, **User**, **Door**, **Area**, and **General**. All of these except the general filter have a selection button where a relevant item may be selected from the list. As well as the selection buttons, you may also enter free text to filter the events. Multiple items in the same box should be separated by a semi-colon.
2. The **AP** filter will always show all events matching any of the search items without any effect from the other four filters.
3. The **User**, **Door**, and **Area** filters will also show all matching events for any search item, unless the **User @ Door/Area** is ticked. Ticking User @ Door/Area ensures that only the events that match the combination of **User** and **Door**, or **User** and **Area** as selected will be displayed.
4. The **General** filter may be used to show events that match the complete combination of its selected terms by using the **AND** button, or to displayed events that match any of its selected terms by using the **OR** button.

1. Under **Event Type Filter**; expand the **Events** menu.
2. All categories under **Events** are selected by default. To customize this filter, select/deselect any of the displayed categories. The adjacent **Event Log Report** window will display filtered results.

1. Configure the **From** and **To** fields in the left panel. Click **Run**.
2. Click **Export CSV** to create a report that will be exported and saved as a CSV file. Or, click **Export PDF** to create a report of the displayed window, to be exported and saved as a PDF file.
3. To continue displaying live **Event Log** messages, click **Resume**.

[1] Click to show in Aliro
[2] Click to show in Aliro

3.2.2 Backup and Restore

The **Backup / Restore** functionality allows you to manage the system database.

Backing up the Database
A database backup can performed to save a copy of the system configuration and/or event logs. It is recommended that scheduled database backups are configured to be stored on a **network location** where possible. Instructions for configuring this are detailed in **Scheduled Backup** below.

1. Click →Overview[1] then select →Backup / Restore[2]. The **Backup / Restore** view is displayed.

To configure a Scheduled Backup

1. Click **Scheduled Backup**.
2. Tick **Enable**.
3. Configure the fields now displayed, as explained below:

Field	Options	Description
Frequency	**Daily**	Scheduled backup will be performed everyday.
	Weekly	Scheduled backup will be performed once a week. Exact day of the week is specified in the **Day** field.
	Monthly	Scheduled backup will be performed once a month. Exact date is specified in the **Day** field.
Day	**Sunday to Saturday / 1-28**	If **Weekly** or **Monthly** is selected, specify which **Day** and date the backup should be performed.
Time	**-**	Specify the exact **Time** (hh:mm) when backup should be performed.
Store In	-	Displays the location (relative to the server) where database backups will be saved. Note that this path must be accessible from your access control server. In order to store backup files on a network location for example a UNC path, follow these steps: 1. Create a folder on a network computer where you intend to store the backups. 2. Share this folder and give permission to change the contents. 3. On the security tab of the folder, click **Edit**, then click **Add**. 4. Click **Object Types** and check **Computers**, then **Ok**. 5. Type the **computer name** of your **Aliro Server** machine and click **Ok**. 6. Check **Modify** to ensure this account has permission to write. The computer account will be displayed with a $ symbol. 7. Enter the **UNC path** to the share you created in the **Store In** field, for example \\remotecomputer\backups

4. Click **Save**.

To perform a Manual Backup

1. Click **Manual Backup**.
2. Select an option from **Include** drop down. Details found below.

[1] Click to show in Aliro
[2] Click to show in Aliro

Option	Description
Everything	All **Event Log** and **System Configuration** data will be backed up.
Event Logs Only	All **Event Logs** currently in the database will be backed up.
System Configuration Only	All **System Configuration** will be backed up.

3. Click the **Backup Now** button.

Restoring the Database
Restoring the database overwrites current system records, with a backed-up database from a server location. This feature can be used restore a previously backed up database to the system.
Note: All existing data will be deleted if you choose to restore.

1. Click **Restore**.
2. Choose to restore database from a **Stored Backup** or **From a File**. Refer details below.

Option	Description
Stored Backup	Select a file stored on the server. These files are stored in the location specified in the Store In field of the **Scheduled Backup** section.
From a File	Browse to select a backup **File** to be restored.

3. Click **Restore**.

   Note: You will be logged off from the Aliro client until restoration is complete. You will be required to log in to the client after restoration.

3.2.3 Monitor and Control

The **Monitor and Control** feature allows your to monitor the doors of your site. It is also possible to control them by executing specific **Door** and **Intrusion** commands.

Using Monitor and Control

1. Click →Overview[1] then →Monitor and Control[2]. The **Monitor and Control** view is displayed.

Panel and Toolbar description

Buttons and Fields	Description
Door Name	Displays the **Name** of door.
Door Mode	Displays the **Mode** configured to door.
Door Status	Displays the **Status** of the door.
Reader Status	Displays the **Reader Status**.

[1]Click to show in Aliro
[2]Click to show in Aliro

Buttons and Fields	Description
Door Errors	Displays the **Door Errors** reported from doors.
Alarm Status Feedback	Provides the **Alarm Status Feedback**, See "Alarm status feedback" on page 51
Door Commands	1. Select a **Door.** 2. Click **Alarm Status Feedback** to execute a selected **Door** or **Intrusion** command. **Note**: You can send the same **Door Command** to multiple doors by multi-selecting multiple doors: 1. Press **Shift+Click** multiple doors in the **Door Name** column.

3.2.4 System Settings

This feature allows viewing and editing of various **System Settings** that apply to the entire access control system.

General Settings

Setting Name	Description
System Language	Defines the **Language** field for a new user under the **Details** expander in the **User** view. Also defines the **System Language** field for a newly created Access Point under the **Details** expander on the **Hardware** view.
Deactivate cards and personal codes	This tick box enables that a person's card and personal code is deactivated if a hard antipassback violation occurs. To activate a user's card or personal code again, please go to the User view.

Event log Settings

Setting Name	Description
Enable Nightly Purging	This check box is ticked by default. When ticked, each night, at midnight, the stored **Event Log** data that is older than the specified number of days (as defined in **Days to keep Event Log data**) is purged.
Save purged data to disk	This check box is ticked by default. When nightly purging is enabled, this option allows saving of the deleted data to disk before it is removed from the database.
Default archive path	This is the path to which purged event log is saved, if that option is enabled (non-editable).
Days to keep event log data	Defines how long to keep event logs in the database, before they are purged. For example, if set to 90 days, event log messages will be kept for 90 days after which they will be deleted, and optionally saved to disk.
Days to keep unacknowledged event notification data	Defines how long the **unacknowledged** notifications are kept in the system, before they are purged. **Note!** There are internal system limit of 11000 unacknowledged events per user. If the number of events exceeds this limit, the system will purge the events irrespective of date.

Hardware Settings

Setting Name	Description
Device Poll Time (ms) Purging	Controls the rate at which Access Point polls the access control server for events. A larger value means the Access Point will react slower but network traffic and server load will be reduced. Conversely, a smaller value means the Access Point will react faster, at the cost of increased network traffic and server load. You should only modify this value on the advice of a Vanderbilt technician.

Custom Field Settings

Setting Name	Description
Custom Field N Label	Allows editing of the label text for each of the four **Custom Fields** that are shown on the user details screen.

Group Code/Personal Code length setting

Setting Name	Description
Length	Allows for setting the number of digits to be used in the **Group Code** and the **Personal Code**. Four to eight digits can be specified. The actual codes are generated and enabled/disabled in the access group menu. All group codes will have the same length. Kindly note that the following applies for increased and decreased codes: • **Increase code** - should the code length be increased, zeroes will be added in the beginning of all existing codes. • **Decrease code** - should the code length be decreased, all group codes will be re-generated and personal codes will be cleared. Those must be manually generated for each user.
Modify Length	Click to activate the wizard for altering the length of the codes.

Reader Lighting Templates

Setting Name	Description
System default template	This displays the current template used in the system.

Applying a Reader Lighting Template

1. Click **Apply Template** to start the wizard. The window **Select the reader lighting template you want to apply** opens.
2. Click the button to the right of the field **System default template**. The window **Select one reader lighting template** opens.
3. The templates are listed in the window below the header **Name**. Select the template and click **OK**.
4. Ensure to note that:
   - The option **Apply and override on all levels** will apply the new template to every area, door and reader regardless of their previous settings.
   - Should the option **Apply and override on all levels** *not* be selected, only the areas, doors and readers which are using the previous system default template will be updated to the new template.
   - It is always possible to apply the default settings by selecting the **Default Lighting Template**.
5. Click **Next** and then **Finish**.The new template is applied.

Exception Scheduler

The Exception Scheduler allows for days that require a change in security mode to be applied, such as public holidays or early closing. For example, a door to be programmed to behave according to a specific mode during

selected hours. A lightframe can be programmed be lit according to exceptions as well, thus indicating the exception by colour.

Creating an Exception Day

1. Give the exception a **Name** which describes what **Type** the exception is.
2. Set a **Start Time** and an **End time**.
3. Select a **Colour** for the exception.
4. Click to **Save** the exception day.

The new name is now listed in the drop down **Select Exception Type.**

Adding an Exception Day to the calendar

1. Pick the day from **Select Exception Type.**
2. Click on the **Day** to add the exception.
3. Click **Save.**

The scheduled exception is now applied system wide.

Removing an Exception day

1. In the calendar, click on the **Day** on which the exception day is to be removed.
2. Click **Save**.

The exception day is removed from the calendar and the system.

Changing an Exception day

1. Select the new **Exception Type** in the drop down.
2. In the calendar, click on the **Day** you want to apply the exception day to. On the first click, the previous exception type is removed.
3. Click again on the same **Day**.
4. Click **Save**.

The exception day is changed to the new exception type.

Name	Description
Name	The **Name** of the exception.
Types	There are eight different **Types,** only one per day can be applied. Each of the day types have the same options: name, start time, end time and colour. The types are listed in the drop down menu below.
Colour	Click the arrow to select a **Colour** for the type of exception. The colour will appear in the day which the exception is connected to.
Start Time **End Time**	The **Start Time** and **End Time** of the exception. *Kindly note that exceptions do not span across days.*

Name	Description
Year	Click the arrows to see the current, previous or coming **Years**. Exceptions can be scheduled for the current date and coming years. All days which are passed are greyed out and no exception days can be added.
Months	The **Months** of the year are displayed to the left.
Day	Select the **Day** for the exception by clicking on it. The day will be highlighted with the colour as set in **Exception Types**.

3.2.5 Roll Call

The **Roll Call** enables the listing of the presence and last known point of card activity of cardholders in specified areas. The main use for a roll call is for checking that cardholders are outside an area in the case of evacuation. Those listings can be compiled in a **Roll Call Report**. A **Muster Point** is used to eliminate cardholders from the report, as they will be deleted from the roll call once the card is badged at the **Muster Reader**.

Roll Call Report
A report which shows the current locations of cardholders at the time the report was run.

Creating roll call reports
1. Select how the roll call report should be listed, **List by** the **Last name** or **Area name**.
2. Select the **Orientation**, **Landscape** or **Portrait**.
3. Click **Generate**. The window System summary report created confirms that the report is compiled.
4. Click **Download** to save or open the report.

Muster Points
A **Muster Point** is a defined safe area with a **Muster Reader**. This is where cardholders can assemble in the case of evacuation.The muster reader acknowledges that a cardholder is at this point once the card has been badged. When a roll call report is created, these cardholders will not be included in that report.

A reader is designated to be a muster reader in **Hardware > Reader Interface > Access Mode**. The configured readers are displayed in the list **Access Point** and **Muster Readers**.

3.3 Templates

These features provide **Templates** with pre-defined values and configurations for **Hardware, Doors** and **Cards**. You can easily apply any of these templates to a hardware, door or card, and later customize them to your requirements. For more information, click on a feature below.

TEMPLATES Features


Card Templates


Door Templates


Hardware Templates


Reader LightingTemplates

3.3.1 Card Templates

A **Card Template** is a way to visually design the information that is printed on cards, such as a user's name, photo and company logo.

- Data fields, such as a user's name, are added to the card template, which are then filled in with the actual data for each user when the card is printed.
- Plain text and images, such as a company name and logo, can be added to the card template, which are common to all cards to be printed.

3.3.1.1 Creating Card Templates

Creating Card Templates

1. Click →Overview[1] then →Card Templates[2]. The **Card Template** view is displayed.
2. Click ⊕ **Create**. A new card template design page displays.
3. Enter a **Name** for the card template.
4. Drag fields from the toolbox on the left, and drop them on the design surface in the middle of the page.

The toolbox controls **Stack panel** and **Grid** can be used to easier align the fields. When dragging a field onto a stack panel or grid, the area where the field can be dropped will be highlighted in blue.
Expand a topic to view its instructions.

Field details of Controls

Control	Fields	Description
Text Enter label text for fields using this control	**Text**	Enter the label **Text** for this field.
	Font Size	Enter **Font Size** of displayed text for this field on card template.
	Font Family	Select **Font Family** of displayed text for this field on card template.
	Font Weight	Select **Font Weight** of displayed text for this field on card template.

[1]Click to show in Aliro
[2]Click to show in Aliro

Control	Fields	Description
	Text Color	Select **Text Color** of displayed text for this field on card template.
	Height	Enter the display **Height** of this field on card template.
	Width	Enter the display **Width** of this field on card template.
Image	**Height**	Enter the display **Height** of this field on card template.
	Width	Enter the display **Width** of this field on card template.
	Select Image...	**Select Image** to be displayed in this field of the card template.
Date	**Date Format**	The default date format is **dd/MM/yyyy:** **dd** is the day of the month, from 01 through 31 **MM** is the month, from 01 through 12 **yyyy** is the year as a four-digit number **Note**: Any other date formats entered, other than the standard formats, will be displayed as entered.
	Font Size	Enter **Font Size** of displayed text for this field on card template.
	Font Family	Select **Font Family** of displayed text for this field on card template.
	Font Weight	Select **Font Weight** of displayed text for this field on card template.
	Text Color	Select **Text Color** of displayed text for this field on card template.
	Height	Enter the display **Height** of this field on card template.
	Width	Enter the display **Width** of this field on card template.
Stack panel	**Stack Orientation**	**Vertical**: Drag a field into the stack panel, to snap it into position. with a stacked vertical orientation.
		Horizontal: Drag a field into the stack panel, to snap it into position with a stacked horizontal orientation.
Grid The fields of this grid appear when at least one grid is placed within a parent grid	**Auto-fit grid row height**	Automatically fits the height of the grid row
	Auto-fit grid row width	Automatically fits the width of the grid row
	Horizontal Alignment	**Left** Moves a selected grid to the left horizontally within its cell of the parent grid **Center** Moves a selected grid to the center horizontally within its cell of the parent grid **Right** Moves a selected grid to the right horizontally within its cell of the parent grid

Control	Fields	Description	
		Stretch	Re-sizes a selected grid to fit horizontally within its cell of the parent grid
	Vertical Alignment	**Top**	Moves a selected grid to the top vertically within its cell of the parent grid
		Center	Moves a selected grid to the center vertically within its cell of the parent grid
		Bottom	Moves a selected grid to the bottom vertically within its cell of the parent grid
		Stretch	Re-sizes a selected grid to fit vertically within its cell of the parent grid
	Margin	Expand this field to enter the values for the Left, Right, Top and Bottom margins of the grid.	

User Fields

The following fields can be dragged and dropped onto the **Front View** or **Back View** of a card template. When a card template is selected for printing a user's card, their details will be displayed in the format, as specified in the table below.

Field	Field Type	Description
First Name	Text field	Displays the user's **First Name** on the card, as entered in the system.
Last Name	Text field	Displays the user's **Last Name** on the card, as entered in the system.
E-mail	Text field	Displays the user's **Email** address on the card, as entered in the system.
Mobile Phone	Text field	Displays the user's **Mobile Phone** number on the card, as entered in the system.
Language	Text field	Displays the user's preferred language on the card, as entered in the system. This will also be the display language of the host web client, when the user logs into the Aliro system. It will also be the displayed language on the ARxxS-MF reader display, when the user interacts with the reader.
Until further notice	Text field	Displays **Yes** on card, if the **Until further notice** tick-box is checked for the user and the user's **End Date** is not specified. Or else, this field displays as **No**.
Accessibility	Text field	Displays **Yes** on card, if **Accessibility** is checked for the user. Or else, this field displays as **No**.
User inactive	Text field	Displays **Yes** on card, if **User inactive** is checked for the user. Or else, this field displays as **No**.
Antipassback exception	Text field	Displays **Yes** on card, if **Antipassback exception** is checked for the user. Or else, this field displays as **No**.
Photo	Image field	Displays the saved **Photo** on the card for the user.

Field	Field Type	Description
Custom Field 1	Text field	The label of these **Custom Fields** will be displayed, as set in the **System Settings** feature.
Custom Field 2		
Custom Field 3		
Custom Field 4		
Start Date	Date field	Displays the user's **Start Date** on the card, as saved for the user.
End Date	Date field	If an **End Date** is specified for the user, this field displays this date on the card. If no end date is specified and **Until further notice** is checked, this field displays as **No Expiry**.
Card Number	Text field	Displays the user's **Card Number** on the card.

Add User's Name to Card Template

1. Drag a **Stack Panel** from the toolbox on the left onto the **Front View** section in the middle.
2. Change the value of **Stack Orientation**, seen in the properties on the right of the **Front View** to **Horizontal**.
3. Re-size the **Stack Panel** to fit the fields it will hold.
4. Drag the **First Name** field from the toolbox on the left onto the **Stack Panel** in the **Front View.**
5. Drag the **Last Name** field from the toolbox on the left onto the **Stack Panel**, just below the **First Name**. Iit will highlight in blue when you can drop it.

Add Image to Card Template

1. Drag an **Image** from the toolbox on the left onto the **Front View** section in the middle.
2. Change the **Height** and **Width** (in the right-hand properties) - or drag the corners - until the image reaches the size you want it to be.
3. Click on **Select Image…** to choose the image to be printed.

Add User's End date to Card Template:

1. Drag the **End Date** from the toolbox on the left onto the **Front View** section in the middle.
2. Change the **Date Format** to whichever date format you wish to use.

Change Text Font in Card Template

1. Click on any text item in the **Front View** or **Back View**, either a **User Field** or **Text Control.**
2. Change the **Font Size** to make the text bigger or smaller.
3. Change the **Font Family** to use a different font.
4. Change the **Font Weight** to make the text bold.

Remove a field from the Card Template:

1. Click on any item in the **Front View** or **Back View.**
2. When you have the item you want to remove selected, drag the item to the **recycle bin** icon on the right hand side of the view. Or just select and then click on the **recycle bin** icon.

Un- or redo changes

1. Click on the **undo** arrow on the right hand side of the view to undo changes.
2. Click on the **redo** arrow on the right hand side of the view to redo changes.

3.3.2 Door Templates

A **Door Template** allows the user to prepare a door setup, with defined configuration for **Door Details, Readers, Door Contact, Exit Buttons, Locks, Door Openers, Security Modes** and **Security Exceptions**. Once saved, you can apply a template to any newly created door. This unique feature makes it easy for a user to setup a standard door, and also ensures consistency in setup.

3.3.2.1 Creating Door Templates

1. Click →Overview[1] then →Door Templates[2]. The **Door Template** view is displayed.
2. Click **Create**. A new **Door Template** page displays.
3. Enter a **Name** and **Usage** for this template.
4. Proceed to configure the other door settings of this template. Click the expander for each section to view its fields.
5. Click **Save** when complete.

Details

1. Click the **Details** expander.
2. Configure the fields of this section and click **Save**.

Field	Description
Unlocking Time (s)	Specify the time duration (in seconds) that door should be kept unlocked, before re-locking after valid entry.
Accessible Unlocking Time (s)	This time duration (in seconds) is similar to the Unlocking Time (s), but is specifically for users with **Special Accessibility** needs.
Opening Time (s)	This time duration (in seconds) is in addition to the **Unlocking Time (s)** , at the end of which the door frame should be closed. After this time duration, the Aliro client flags Event Logs that the door is held for too long.
Waiting for first valid access to unlock	When configured with this option, the door will be unlocked within its access schedule, only after the first valid card badge.
Door Held Warning Time (s)	This time duration (in seconds) is in addition to the Unlocking Time (s) and the Opening time (s). After this total time duration, a Door Held alarm is sent from the hardware device, and reported in Event Logs.

Readers

[1]Click to show in Aliro
[2]Click to show in Aliro

1. Click the **Readers** expander.
2. Click to **Add** a reader row to the table. If you wish to delete a reader row, click **Remove**.
3. Configure the fields of this section and click **Save**.

Field	Description
Name	**Name** of the reader configured to this row.
Activate Automatic Door Opener	This configures the reader to **Activate Automatic Door Opener.**

Door Contacts

1. Click the **Door Contacts** expander.
2. Click to **Add** a **Door Contact** row to the table. If you wish to delete a row, click **Remove**.
3. Configure the fields of this section and click **Save**.

Field	Description
Name	**Name** of the **Door Contact.**

Exit Buttons

1. Click the **Exit Buttons** expander.
2. Click to **Add** an **Exit Button** row to the table. If you wish to delete a row, click **Remove**.
3. Configure the fields of this section and click **Save**.

Field	Description
Name	**Name** of the **Exit Button.**
Activate Door Opener	Configures this button to **Activate Door Opener** and open the door when the exit button is pressed.
Use Accessibility Timeout	The time duration (in seconds) **Use Accessibility Timeout** allows the door to be unlocked for the Accessible Unlocking Time[1].
High Priority Unlocking	Configures this exit button to the input point defined for the High Priority Unlocking functionality[1].

Locks

This section configures both **Door Locks** and **Motor Locks**.

Door Locks

1. Click the **Locks** expander.
2. Click to **Add** a **Door Lock** row to the table. If you wish to delete a row, click **Remove**.

---

[1]This time duration (in seconds) is similar to the Unlocking Time (s), but is specifically for users with Special Accessibility needs.

[1]The configured input is defined as an Exit button with an automatic door opener and has a separate unlock time; this functionality configures the input as an emergency unlocking/locking input with no consideration for Time Schedules, Reader modes, etc.

3. Configure the **Door Locks** fields as required. For more information, refer the field description below.
4. Click **Save**.

Field	Description
Name	**Name** of the **Door Lock**
Relock	**Options and Descriptions** **On door open**: After unlock, relocks when the door is opened. A delay can be configured on top of the door open. **On door close**: After unlock, relocks only when the door is closed. **Pulse**: Pulses the relay to unlock. The external lock will lock automatically without involving the AP.
Relock after Open Time (ms)	For **On door open**, this is the delay to relock after the door open. For **Pulse**, this is the pulse time.

Motor Locks

1. Click the **Locks** button expander button.
2. Click **Add** to add a Motor Lock row to the table. If you wish to delete a row, click the **Remove** button.
3. Configure the Motor Locks fields as required. For more information, refer the field description below.
4. Click **Save**.

Field	Options and Description
Name	Name of the Motor Lock
Unlock Action	**Options and Descriptions** **None**: No action **Turn on**: **Turn on** the relay or output to unlock the motor lock. **Turn off**: **Turn off** the relay of output to unlock the motor lock. **Pulse**: **Pulse** the relay or output (on and then off) to unlock the motor lock. **Inverted pulse**: Use **Inverted pulse** for the relay or output (off and then on) to unlock the motor lock.

<table>
<tr><th>Field</th><th>Options and Description</th></tr>
<tr><td>Unlock Pulse Time (ms)</td><td>For Pulse or Inverted pulse, this is the pulse time.</td></tr>
<tr><td>Unlock Delay Time (ms)</td><td>The time to expect the motor lock gets unlocked.</td></tr>
<tr><td>Lock Action</td><td>Options and Descriptions<table><tr><td>None</td><td>No action</td></tr><tr><td>Turn on</td><td>Turn on the relay or output to lock the motor lock.</td></tr><tr><td>Turn off</td><td>Turn off the relay of output to lock the motor lock.</td></tr><tr><td>Pulse</td><td>Pulse the relay or output (on and then off) to lock the motor lock</td></tr><tr><td>Inverted pulse</td><td>Use Inverted pulse for the relay or output (off and then on) to lock the motor lock.</td></tr></table></td></tr>
<tr><td>Lock Pulse Time (ms)</td><td>For Pulse or Inverted pulse, this is the pulse time.</td></tr>
<tr><td>Lock Delay Time (ms)</td><td>The time to expect the motor lock gets locked.</td></tr>
</table>

Door Opener

1. Click the **Door Opener** expander.
2. Configure the fields as required. For more information, refer the field description below.
3. Click **Save**.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Name</td><td>Name of the Door Opener.</td></tr>
<tr><td>Open Action</td><td>Options and Descriptions<table><tr><td>None</td><td>No action</td></tr><tr><td>Turn on</td><td>Turn on the relay or output to unlock the Door Opener.</td></tr><tr><td>Turn off</td><td>Turn off the relay of output to unlock</td></tr></table></td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>the Door Opener.</td></tr>
<tr><td>Pulse</td><td>Pulse the relay or output (on and then off) to unlock the Door Opener.</td></tr>
<tr><td>Inverted pulse</td><td>Use Inverted pulse for the relay or output (off and then on) to unlock the Door Opener.</td></tr>
</table>
</td></tr>
<tr><td>Close Action</td><td>Options and Descriptions
<table>
<tr><td>None</td><td>No action</td></tr>
<tr><td>Turn on</td><td>Turn on the relay or output to lock the Door Opener.</td></tr>
<tr><td>Turn off</td><td>Turn off the relay of output to lock the Door Opener.</td></tr>
<tr><td>Pulse</td><td>Pulse the relay or output (on and then off) to lock the Door Opener.</td></tr>
<tr><td>Inverted pulse</td><td>Use Inverted pulse for the relay or output (off and then on) to lock the Door Opener.</td></tr>
</table>
</td></tr>
<tr><td>Open Pulse Time (ms)</td><td>For Pulse or Inverted pulse, this is the pulse time.</td></tr>
<tr><td>Close Pulse Time (ms)</td><td>For Pulse or Inverted pulse, this is the pulse time.</td></tr>
<tr><td>Open Delay Time (ms)</td><td>The time to expect the door opener gets unlocked.</td></tr>
<tr><td>Close Delay Time (ms)</td><td>The expected time the door opener will take to close.</td></tr>
</table>

Security Modes

1. Click the **Security Modes** expander.
2. Configure the **Access Schedule** time-lines in this section, for specific days.

3. Configure the **Default Door Mode**, **Default Reader Mode** and **Default Other Modes** section, as explained in the table below.
4. Click **Save**.

Section	Fields	Options & Description
Default Door Mode	**Open**	The door is physically wide open, via a door opener.
	Unsecured	The door is unlocked, and can be opened.
	Secured	The door is locked, and can only be unlocked by a valid card.
	Blocked	The door is locked and user access is disabled.
Default Reader Modes	**Reader**	The logical name of the reader.
	Mode	The mode is Card, Card+PIN or disabled.
Default Other Modes	**Point**	Name of the input/output point.
	Mode	The mode of the point, which is enabled or disabled.

Schedule Exceptions

Scheduled Exceptions

Field	Description
Name	The **Name** of the exception.
Security Modes	**Security Modes** **Field** / **Description** **No change to security mode** — The security mode remains as defined by current default and door schedule, therefore no scheduled exception modification effects the security mode. **Standard exception mode** — The security is automatically increased during the dates and times of the scheduled exception as defined in table below.

Field	Description
	<table><tr><th>Field</th><th>Description</th></tr><tr><td>**Custom security mode**</td><td>The door or reader mode can be uniquely defined for the date and time exception periods.</td></tr></table> The **Standard Exception Mode** is applied when: • First applied to the door, *and* • Any operator changes are made, *and* • Any automatic changes are made for example via time schedule The table below describes how the **Standard Exception Mode** is set in relation to the **Door Mode** when a scheduled exception is in use: <table><tr><th>Current Door Mode</th><th>Standard Exception Mode</th></tr><tr><td colspan="2">**Door Security Mode**</td></tr><tr><td>**Blocked**</td><td>Blocked</td></tr><tr><td>**Secured**</td><td>Secured</td></tr><tr><td>**Unsecured**</td><td>Secured</td></tr><tr><td>**Open**</td><td>Secured</td></tr><tr><td colspan="2">**Reader Mode**</td></tr><tr><td>**Card and PIN**</td><td>Card and PIN</td></tr><tr><td>**Card**</td><td>Card</td></tr><tr><td>**Personal Code**</td><td>Card</td></tr><tr><td>**Group Code**</td><td>Card</td></tr><tr><td>**Disabled**</td><td>Disabled</td></tr><tr><td colspan="2">**Other Modes (Enable/Disable)**</td></tr><tr><td>**Exit button**</td><td>No change</td></tr><tr><td>**Door lock**</td><td>No change</td></tr><tr><td>**Door contact**</td><td>No change</td></tr></table>

Security Exceptions

Field	Description
Start Date	**Start Date** of exception period.
End Date	**End Date** of exception period.

Field	Description
Start Time	**Start Time** of exception period.
End Time	**End Time** of exception period.

3.3.2.2 Altering Door Template Configuration

This wizard will allow you to make the following changes to a selected door template:

- **Add New Setting** - This section allows you to add a new door functionality.
- **Remove Existing Setting** - To select and remove items from the list of door functionality.

Note: Any modifications made to existing **Door Templates,** will be automatically inherited by all doors using the modified ones.

3.3.3 Hardware Templates

A **Hardware Template** allows you to prepare a hardware setup, with defined configuration for the **Access Point**, its **inputs, outputs** and **relays**. Once saved, you can apply a template to a newly created hardware device, and even customize it as required. This unique feature makes it easy for a user to setup a standard hardware device, and also ensures consistency in setup.

3.3.3.1 Creating Hardware Templates

1. Click →Overview[1] then →Hardware Templates[2]. The **Hardware Template** view is displayed.
2. Click ⊕ **Create**. A new **Hardware Template** page displays.
3. Enter a **Name** and **Description** for this template.
4. Proceed to configure the **Access Point, Input/s, Relay/s** and **Output/s** sections. Click the expander for each section to view its fields. Details of these sections can be found below.

Access Point

Field	Description
System Language	Sets the **System Language** of the hardware device for system messages. Those are messages not related to user or card.
Time Zone	Sets the **Time Zone** for the hardware device.
Use daylight saving time	Check this tick-box to configure this hardware device to **Use daylight saving time.**
Use DHCP to obtain addresses	If this checkbox is unticked, the fields given below need to be filled. If this checkbox is ticked, the **DHCP** server be used to auto-populate the fields below.
Network Gateway	**Network Gateway** address.
Netmask	**Netmask** used to access the remote network of the hardware device
Preferred DNS Server	IP address of the first **DNS server.**
Alternate DNS Server	IP address of the second **DNS server.**
Host Address	Enter the **IP address** of the **Aliro host**, to connect the hardware to Aliro.
Can be discovered	If this check box is ticked, the hardware device will be displayed in the left master-list of the **Hardware** view, on clicking **Discover**.

Input

[1] Click to show in Aliro
[2] Click to show in Aliro

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enabled</td><td></td></tr>
<tr><td>Functionality</td><td>Options and Descriptions
<table>
<tr><td>Not used</td><td></td></tr>
<tr><td>Door contact</td><td>Defines this input point as a Door contact sensor, monitoring the open or closed state of the door.</td></tr>
<tr><td>Lock contact</td><td>Defines this input point as a Lock contact sensor, monitoring that the lock action is performed.</td></tr>
<tr><td>Exit button</td><td>Defines this input as an Exit button.</td></tr>
<tr><td>Alarm status feedback</td><td>Configures this input to signal Alarm status feedback from an Intrusion Panel that defines if an area is armed or disarmed.</td></tr>
<tr><td>Elbow switch</td><td>Defines this input as an Exit button with accessibility rights, known as Elbow switch.</td></tr>
<tr><td>High priority unlocking</td><td>If this input is defined as an Exit button with an automatic door opener and has a separate unlock time, High priority unlocking configures the input as an emergency unlocking/locking input with no consideration for access schedules, reader modes and so on.</td></tr>
<tr><td>Tamper detection</td><td>Configures this input to Tamper detection made to any hardware device.</td></tr>
<tr><td>Arming button</td><td>Defines this input as a an Arming button that arms an area.</td></tr>
<tr><td>Power failure</td><td>Configures this input to indicate Power failure. Event Lolgs are generated when such an event is triggered.</td></tr>
</table></td></tr>
<tr><td>Enable Notifications</td><td>Enable Notifications ensures that the linked hardware device triggers an input if an event occurs.</td></tr>
</table>

Relay

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Enabled</td><td></td></tr>
<tr><td>Functionality</td><td>Drop down options and description
<table>
<tr><td>Alarm bypass</td><td>Alarm bypass configures the output point to bypass an armed area.</td></tr>
<tr><td>Door lock</td><td>Configures this output point to lock/unlock a door, if it is configured as a Door lock.</td></tr>
</table></td></tr>
</table>

Field	Description	
	Door opener	Configures this output point to open a door, if it is configured with a **Door opener.**
	Event notification	
	Intrusion arm/disarm	Configures this output point to signal **arm/disarm** to the **Intrusion Panel**, which returns its status via the Alarm Status Feedback functionality[1].
	Intrusion arming pre-warning	This is an **Intrusion arming pre-warning** output which is generally connect to a device, which warns before arming an area.
	Motor lock	Defines this point as a combined output-input device, that signals when locking as occurred. The point is configured as an output point for **Motor lock**, and as an input point for lock contact.
	Not used	Output is not defined for any functionality.
	Wiegand - buzzer	Output is defined for **Wiegand reader buzzer**.
	Wiegand - green	Output is defined for **Wiegand reader green** LED control.
	Wiegand - red	Output is defined for **Wiegand reader red** LED control.
	Wiegand - yellow	Output is defined for **Wiegand reader yellow** LED control.
Enable Notifications	**Enable Notifications** ensures that the linked hardware device triggers a relay if an event occurs.	
Event Notification		

Output

Field	Description	
Enabled		
Functionality	**Drop down options and description**	
	Alarm bypass	**Alarm bypass** configures the output point to bypass an armed area.
	Door lock	Configures this output point to lock/unlock a door, if it is configured as a **Door lock.**

[1] An Input Point functionality of the hardware device that the input to signal from an Intrusion Panel that defines if an area is armed or disarmed.

Field	Description
	Door opener — Configures this output point to open a door, if it is configured with a **Door opener.** **Event notification** **Intrusion arm/disarm** — Configures this output point to signal **arm/disarm** to the **Intrusion Panel**, which returns its statuss via the Alarm Status Feedback functionality[1]. **Intrusion arming pre-warning** — This is an **Intrusion arming pre-warning** output which is generally connect to a device, which warns before arming an area. **Motor lock** — Defines this point as a combined output-input device, that signals when locking as occurred. The point is configured as an output point for **Motor lock**, and as an input point for lock contact. **Not used** — Output is not defined for any functionality. **Wiegand - buzzer** — Output is defined for **Wiegand reader buzzer**. **Wiegand - green** — Output is defined for **Wiegand reader green** LED control. **Wiegand - red** — Output is defined for **Wiegand reader red** LED control. **Wiegand - yellow** — Output is defined for **Wiegand reader yellow** LED control.
Enable Notifications	
Event Notification	

3.3.4 Reader Lighting Templates

When Aliro is installed, a **Default Lighting Template** which cannot be edited, is applied. This template includes **Lightframe, LED** control and **Keypad backlight.** It is currently valid for the ARxxS-MF readers.

- **Lightframe** - customizes how the lightframe is used in the readers, both in idle mode and when different events occur. There are three options available:
  - **Follow LED -** The default setting, during which the lightframe prioritises this above any configured events. The default colour is set to **No colour**, as is reflected in the default lighting template.
  - **Event** - The lightframe is lit up according to various door modes, events or access schedules.
  - **Scheduled Exceptions colour** -If other than **Off**. Should off be selected, no colour is activated.
  - **Default Colour -** Defines the colour when other than **Off**.
- **LED** - can be controlled separately, with or without an access schedule. The default is **OFF**.

[1] An Input Point functionality of the hardware device that the input to signal from an Intrusion Panel that defines if an area is armed or disarmed.

- **Keypad Backlight** - turns on the backlight of the keys, with or without an access schedule. The default is **OFF** and it applies to keypad readers only.

Example of a Lightframe setting
A customized lightframe can be as follows:
1. Set the **Default color** to blue.
2. Add an event from an **Access schedule**,for example **Office Hours,** and select purple.
3. Tick **Follow LED**.

The result is:
- During the night, the lightframe is blue unless an event occurs.
- During the office hours, the lightframe is purple.
- Whenever someone badges a card, or any LED-altering event occurs, the lightframe changes colour accordingly.

Template selection
There are three ways to apply **Reader Lighting Templates** to features like areas, doors or readers:

Apply a template by using the wizard
1. Select the template in the list and click **Apply a Template.** A wizard starts and a list of objects with the current settings for the features are displayed.
2. If needed, change the **Template** by pressing the button to the right of the field.
3. Select the **Level** in the drop down: **Door, Area** or **DoorReader**.
4. Define which **Item(s)** are to be included. Those are listed in the pop up window which is displayed when the button to the right of the field is clicked and vary depending on the level selected in the previous step.
5. In the list below, tick the items which the template should be applied to. Note that the previous template is displayed in the square brackets. When:
   - **Grey** - the template will be *replaced*.
   - **Black** - the template will *not be replaced.*
6. Click **Next** and then **Finish.**

Please note that **Areas, Doors** and **Readers** will start using the new template when this is applied.

Apply a template in the Doors feature
Individual reader lighting templates can be applied to **Readers:**
1. Click to expand **Readers**.
2. Select the **Reader Lighting Template** to be applied. The templates are listed in the drop down.
3. Click **Save**.

Apply a template using the wizard in System Settings
1. Use the wizard in System settings to administrate how the templates are applied.
2. For instructions, open the help files.

The **Reader Lighting Templates** which are applied for **Areas, Doors** and **Readers** are displayed in the respective fields for those functions. The templates displayed for readers can be edited. The templates for areas and doors are read only, but can be edited according to the instructions above.

3.3.4.1 Creating Reader Lighting Templates

1. Click →Overview[1] then →Reader Lighting Templates[2]. The **Reader Lighting Template** view is displayed.
2. Click ⊕ **Create**. A new **Reader Lighting Template** page is displayed.
3. Enter a **Name** and **Description** for this template.

[1]Click to show in Aliro
[2]Click to show in Aliro

4. Proceed to configure the **Lightframe, LED Control** and **Keypad Backlight** sections. Click the expander for each section to view its fields. Details of these sections can be found below. Note that the lightframe functions are prioritized:
    1. **Follow LED**.
    2. **Events** - ranking from top to low, use the arrows to move up or down. Please note that the events are sorted by priority, where the one on the top has the highest priority and the one furthest down has the lowest priority.
    3. **Scheduled Exceptions colour**, if other than **Off**. Should off be selected, no colour is activated.
    4. **Default Colour**, if other than **Off**.
5. Click →Save[1].
6. Optionally, click →Apply a template[2] to customize specific areas, doors or readers. Also, the wizard in **System settings** can be used to select a general setting for the system.

Panel and Toolbar description

Panels and Buttons	Description
Name	Displays the different templates, including the default.
Create	Creates a new reader lighting template.
Delete	Deletes a selected item.
Save	Saves the current configuration.
Cancel	Cancels the changes since last save.
Apply a template	Activated when a reader lighting template has been selected in the list. Used for applying a lighting template to one or more areas, doors or readers.

Lightframe

[1]Click to show in Aliro
[2]Click to show in Aliro

<table>
<tr><th>Field</th><th>Options and description</th></tr>
<tr><td>Follow LED</td><td>Tick if the lightframe should Follow LED. This choice has higher priority than any event setup.
Description of LEDs
In Aliro, the LEDs of the reader are lit in a standardized manner. There are some system specific events which generates different colours:
Access granted or Exit button request - normally green.
Access denied, for reasons such as no rights, time schedule violation, card expired, inactive user, card void - normally red.
New PIN entry - normally flashing yellow.
For other kind of events, such as Door forced and Door held, which are listed in the the Reader Lighting Template setup, the lightframe can be customized.

Options for Follow LED
This option is selected by default. The lightframe follows the LED behavior.<table><tr><th>Follow LED option</th><th>Description</th></tr><tr><td>OFF</td><td>The specified events only will take effect in a prioritized order. Should no events be created and no default colour be selected, the lightframe will never lit, only the LEDs.</td></tr><tr><td>ON - no event added</td><td>Any event will activate the lightframe same as the LED.This is the initial state when creating a new reader lighting template.</td></tr><tr><td>ON - events added</td><td>The specified events only will take effect in a prioritized order. System specific events such as Access granted and Access denied will override.</td></tr><tr><td>ON - and event Follow LED Only</td><td>Events with Follow LED Only in the Start Action will still be overridden by events such as Access granted and Access denied.</td></tr></table></td></tr>
<tr><td>Default colour</td><td>Defines the Colour if other than Off. This choice has lowest priority. When off is selected, no colour is activated.</td></tr>
<tr><td>Scheduled Exception Colour</td><td>The Scheduled Exception Colour overrides the default color during a Scheduled Exception time, providing that no higher priority colour is being displayed.</td></tr>
<tr><td>Event (max 10)</td><td>Options for Door Mode<table><tr><td colspan="2">Kindly note that these modes are related to the selected door only and will not apply to every door in the system.</td></tr><tr><td>Open</td><td rowspan="4">When Door Mode is selected, those modes are listed in the drop down to the right. When any of these modes are selected and active,the Lightframe will act according to the settings configured in Start Action and continue until the time set in the End Condition.</td></tr><tr><td>Unsecured</td></tr><tr><td>Secured</td></tr><tr><td>Blocked</td></tr></table></td></tr>
</table>

<table>
<tr><th>Field</th><th>Options and description</th></tr>
<tr><td></td><td>
Options for Event
<table>
<tr><td colspan="2">Kindly note that these modes are related to the selected door only and will not apply to every door in the system.</td></tr>
<tr><td>Door blocked</td><td rowspan="9">When Event is selected, those events are listed in the drop down to the right. When any of these events are selected and active,the Lightframe will act according to the settings configured in Start Action and continue until the time set in the End Condition.</td></tr>
<tr><td>Door forced</td></tr>
<tr><td>Door held</td></tr>
<tr><td>Door held too long</td></tr>
<tr><td>Input active</td></tr>
<tr><td>Arming in progress</td></tr>
<tr><td>Antipassback violation</td></tr>
<tr><td>Access granted by operator</td></tr>
<tr><td>Door blocked with manual command</td></tr>
</table>
Options and description for Access Schedule
<table>
<tr><td>Access Schedule</td><td>Every created Access Schedule is listed in the drop down. The Lightframe will act according to the settings configured in the selected access schedule.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Field</th><th>Options and description</th></tr>
<tr><td>Start action</td><td>Options and description<table>
<tr><td>Lightframe Effect</td><td>Every created Lightframe Effect is listed in the the drop down to the right. At Start Action, the settings in this Lightframe are applicable until the End Condition is met.</td></tr>
<tr><td>Follow LED only</td><td>The Lightframe follows the Follow LED only settings.</td></tr>
<tr><td>Static Colour</td><td>At Start Action, the Lightframe has a Static Colour until the End Condition is met.</td></tr>
<tr><td>Off</td><td>When the lightframe is Off, no colour is displayed.</td></tr>
</table></td></tr>
<tr><td>End Condition</td><td>Options and description<table>
<tr><td colspan="2">Kindly note that should any Access Schedule be selected, these options are unavailable.</td></tr>
<tr><td>Event ends</td><td>The lightframe effect is active until the Event ends.</td></tr>
<tr><td>Duration</td><td>The lightframe effect is active for the set Duration. The duration is set in the field to the right and is active for the stated seconds.</td></tr>
</table></td></tr>
</table>

LED Control

Field	Description
Red	Tick to select **Red** .
Orange	Tick to select **Orange**.
LED turned on	Tick for **LED turned on**.
Only during the following access schedule	Tick to make the LED control be active **Only during the following access schedule**. Every created Access Schedule is listed in and selected from the drop down menu.
Led turned off	Tick for **LED turned off**. This is the default setting.

Keypad Backlight

Field	Description
Keypad back light turned on	Tick to activate **Keypad back light turned on**.
Only during the following access schedule	Tick to activate the keypad back light **Only during the following access schedule**. Every created Access Schedule is listed in and selected from the drop down menu.

Field	Description
Keypad back light turned off	Tick to activate the setting **Keypad back light turned off**. This is the default setting.

4 Glossary

A

Access
The principle of being granted or denied entrance to an area which is controlled by Aliro.

Access Control
The selective restriction of access to an area or other resource. Access can be granted by the use of a credential, conditions or different access modes which are controlled by the security system.

Access Control System
A security system that selectively restricts access to an area or other resource. Access can be granted by the use of a credential, conditions or different access modes which are controlled by the security system.

Access Group
A grouping of door access and/or area access with access schedules that defines what time of day, and through which doors users are granted access.

Access Point (AP)
The hardware point which controls a door environment, which a user can use to gain access to an area.

Access Rights
The various rights a user has related to access groups, area access and door access.

Access Schedule
A set of time intervals during which access is configured, often connected to the different days of a calendar.

Accessibility
The ability to program individual cards so that those open a door as well as unlocks it and holds it open for a longer time, this to ensure for the user to enter safely.

Administrator
A user with rights to change the settings of a system and handle access rights, as well as designating the rights to control the system to other users. Those rights can be defined to include functions such as monitoring and control, settings and access rights.

Alarm
A device which gives a signal should there be a deviating condition in Aliro.

Alarm Status
The status of the alarm regarding how it should act in case of any deviation from the normal settings in Aliro.

Antipassback
A pre-defined logic which prevents an access card from being used to enter an area a second time without first leaving the same area. The access card can thereby not be used by second person who is outside the area.

Archiving
The act of saving event log data as a CVS file before it is purged from the database.

Area
A space in your building, whose access is controlled by at least 1 Door and 1 Entry Reader.

Area Access
The permission to enter an area.

Arm
The function which arms an area, as in activates the alarm.

Arming Readers
The readers connected to an AP which are used to arm or disarm and intrusion area.

B

Backup
The process of copying and archiving system data. By saving the system data, it can be restored, should it be lost.

C

Card
A card programmed for interaction with Aliro, typically used to unlock doors in order to gain entry.

Card Number
The individual number of a card.

Card Printing
The creation of cards where the front- and back side is designed and printed.

Card Template
The pre-set design of a card, used for card printing.

Communication Settings
The parameters which enable communication between an AP and Aliro.

CPU
The Central Processing Unit (CPU) which is the hardware within a computer and ensures that the instructions as entered in the software of a system are executed.

CPU Usage
The value, displayed in the overview system status panel, which gives an idea how busy the client is.

Custom Field
The fields in the user interface which can be renamed to personal preferences in the users feature. The custom fields can be edited in system settings.

D

Database
An organized collection of stored data. In Aliro, MS SQL is supported.

Day-light Savings Time
The practice of adjusting the clocks so that the evenings gain more daylight.

DHCP
The Dynamic Host Configuration Protocol (DHCP) which is a standardized networking protocol used for parameters for interfaces and services on the Internet.

Disarm
The function which disarms an area and deactivates the alarm.

Disk usage
The estimated use of space for data saved in a directory or on a file. It is displayed in the overview system status panel.

DNS Server
The Domain Name System (DNS) which is a naming system for computers and devices connected to the Internet or a private network.

Door
A physically controlled entrance device for allowing or denying access between areas. In access control, this can also be a gate, gateway, in- or front door and so forth.

Door Access
The doors to which a user has access according to an access schedule.

Door Contact
The monitoring of whether a door is open or closed. It is connected to an input of an AP.

Door Lock
The number of milliseconds and in which manner the door should remain unlocked before being locked again. See also Lock.

Door Mode
The various ways a door can be programmed to grant a user access to an area.

Door Opener
A motorized device which is used to hold a door open. In Aliro, a separate AP output can be used.

Door Template
The pre-developed settings for doors which can be applied to individual or many doors in Aliro.

Duress
A Duress is a covert signal a cardholder can send during a card badge operation, to notify the operator that he/she is in a state of distress.

E

Enrollment Reader
A reader which can read user information from a card. It is typically connected to a computer.

Entry Readers
The readers which are placed at a position so that a user would enter an area.

Event
The various occurrences which are registered in the security system. This refers to: Administrative events, such as when an administrator edits the settings or executes a manual command. User events, such as when a registered user unlocks a door.

Event log
The log which registers various occurrences in the security system. This refers to: Administrative events, such as when an administrator edits the settings or executes a manual command. User events, such as when a registered user unlocks a door.

F

Firmware
The fixed programs and data structures which control various electronic devices in use in Aliro.

Firmware Download
The receiving of firmware from one source to the Aliro.

H

Hardware
The electronic and mechanical components of a product.

Hardware Mapping
The act of creating a link between the hardware and logical functions. For instance, an AP must be linked to a door name.

Hardware Template
The pre-developed settings for the hardware which can be applied to different hardware devices in Aliro.

Host Address
The address used to identify hosts on a network.

I

Image
A picture of the registered user.

Initialize
To commence a process in Aliro.

Input
The connectors where signals from external equipment is received.

Intrusion
The logical term which covers the actions used for controlling an intrusion system.

Intrusion System
A system which monitors areas and networks for unauthorized access and reports any actions which would be considered to deviate from normal.

IP Address
Internet Protocol (IP) address, the numerical label designated devices which are connected to a network using IP for communication.

L

Linked Hardware
The result when a hardware mapping is created. For example, a logical door contact function can be mapped to an AP input called Input 3.

Local Time
The time which is adjusted to the local time zone, based on UTC.

Lock
A mechanical or electrical fastening device which is controlled by the access control system.

Logged faults
The deviations from what would be considered as normal which are compiled in the event log.

M

Manual Command
A command which allows the user to take control over the automated settings in Aliro.

Memory usage
The amount of space used up by memory/data in the storage. It is displayed in the overview system status panel.

Mobile Client
The application for iOS and Android which allows access to Aliro remotely using a smartphone.

Monitoring
The surveillance of the access control system, areas, users and commodities which collects, stores, compiles and presents data.

Motor Lock
A lock with a motorized hook bolt, where the door and frame are interconnected.

N

Netmask
The 32-bit mask which is used to divide an IP address into subnets and specify the networks available hosts.

Network
A communication system which allows computers which are connected to each other to exchange data and information.

Network Gateway
A mechanical device which routes between networks.

Notification
The message which relays to a receiver that something has occurred in the security system.

O

Offline access point
An AP which is offline and therefore out of contact with Aliro.

Online access point
An AP which is online and therefore in contact with Aliro.

Output
The connector which sends signals to external equipment.

P

Parent Area
An area which surrounds a so called sub-area. The sub-area is an area inside the parent area. See also Sub-Area.

Permissions
The different rights a user has to access areas, edit settings and control Aliro.

Personal Access
The for each user personal permissions to enter different areas and/or edit settings and control Aliro.

Personal Identification Number (PIN)
A personal identification number.

Purging
The act of automatically erasing event log data compiled in the data base. The data can be archived.

R

Reader
A device which interprets physical credentials.

Reader Interface
The interface on a reader which enables a user to send information to Aliro.

Reader Mode
The definition should a reader be used for access or as a registration reader.

Reader Type
The different kind of reader which is connected to Aliro. Readers which operate OSDP, Wiegand and Clock/Data are supported.

Relay
An electrically operated switch which when activated controls for example door locks, motor locks, antipassback and alarms in Aliro.

Restore
The act of put or bring something back into use or a former state.

Role
These are functional designations. Roles can be assigned to various users of the security system who have different rights and responsibilities.

S

Scheduled Backup
The backup of system data which occurs at a set time.

Security Exception
The ability to temporarily override an access schedule without changing its general settings.

Security Mode
The different security modes are: open, unsecured, secured or blocked. Those are connected to the door environment.Those control whether a door is locked or not, as well as if a user can open the door by badging a card to the respective reader.

Server
The computer on which the software is installed and ensures that Aliro can be reached from any computer connected to the same network.

Site Administrator
A role with the ability to view and modify all but the hardware components of Aliro.

Site Operator
A role which gives the user the ability to manage user access and system events.

Site Planner
A graphic overview of an area and doors.

Sub Area
An area contained within a Parent Area.

System Administrator
A role which gives the user complete and unrestricted access to view and modify Aliro.

System Language
The language which is selected for the user interface and help files. Aliro offers eleven different languages.

System Settings
The feature which allows viewing and editing of various settings for Aliro.

System Status
The status of hardware, server and database included in Aliro, displayed on the overview page.

T

Tamper
A switch which when altered from the original position activates a warning or alarm.

Tamper Mode
The tamper is activated.

Time Zone
The different zones which as a standard time for legal, commercial and social purposes.

U

User
A person in contact with the security system. This can be a Cardholder, or a System User.

User Field
The fields in Aliro which holds information about users.

W

Web Client
A client which accesses Aliro system through a web browser.

Web Server
The server a web client connects to, which in turn communicates with the Aliro backend server(s).

V

Visitor
A person who is temporarily in contact with the security system.

Issued by
Vanderbilt International (IRL) Ltd.
Clonshaugh Business and Technology Park
Clonshaugh
Dublin 17
Ireland

www.vanderbiltindustries.com

Document No. A-100007-3
Edition Date 2015-09-17