impro technologies®

Access Portal LITE

SOFTWARE MANUAL

Scope of Document

This document guides the user through the various functions available in the APLITE Web user interface.

Document Conventions

We use the following conventions in this document:

	*Note – points out extra information*
	*Tip – points out alternative methods to perform a task*
	*Important – points out important information*
	***Warning – points out potential danger to you or the product***

Before You Begin

Have the following available:

- An active Ethernet connection to the Cluster Controller Module (using a standard Ethernet cable).
- Access to Any HTML 5 compliant browser.

1 System Settings

Starting the Access Portal LITE over a LAN

Ensure that the CCM DIP Switches are set for AP LITE (Switch 2 ON, all others OFF)

Do NOT open more than 1 instance of the Web Interface per Controller.

*If the Web Server resides on a Port other than Port 80, the URL becomes: **http://aplite:XX/**. The **XX** highlighted in the URL refers to the new Port number.*

If your Controller connects direct to the PC, refer to page 36 for information on accessing the Web Interface.

1. In the case of a new installation, using your browser, go to **http://aplite/**
2. Enter the default **Admin Code (12345)**. For information on changing this code, refer to page 35.
3. Click the Logon button.
4. Access Portal LITE should start up, presenting you with the main Ribbon:

Figure 1 – The Main Menu Ribbon

5. Clicking on **Settings>** **About** will bring up a copyright message with the Firmware and Website Version Numbers.

Date or Time Setup

1. From the Main Ribbon select **Settings>Configuration>Date/Time**.
2. Synchronise the Cluster Controller Module's Date and Time to your PC by clicking the Sync button, and close the dialogue if done.
3. If necessary, set the **Start** and **End Date** for Daylight Savings using the buttons.
4. Set the time that Daylight Savings takes effect using the **Switch Time** textbox.
5. Set the duration of the Daylight Savings time shift using the **Shift Duration** textbox.
6. Click the Save button.

Auto-ID

1. From the Main Ribbon select **Settings>Setup >Auto ID**.

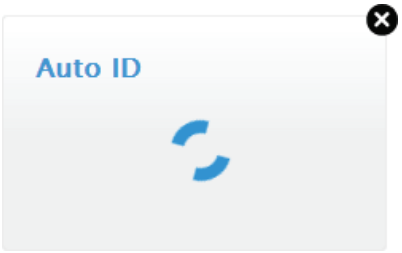

Figure 2 – Auto ID in progress…

2. When the process is complete, a pop-up dialogue will appear:

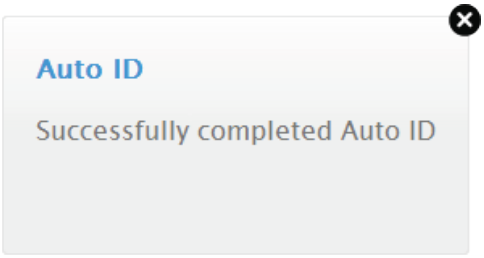

Figure 3 – Successfully completed Auto ID

3. Close the Pop-up dialogue.

Door Configuration

Before adding any doors it is a good idea to first configure the **Door Template** settings. The Door Template settings become the default settings when you add a new door, so this can save you some time when adding a number of similar doors.

Setting the Door Template

From the Main Ribbon, select **Settings**>**Setup**>**Doors**, and then click on **Door Template**.

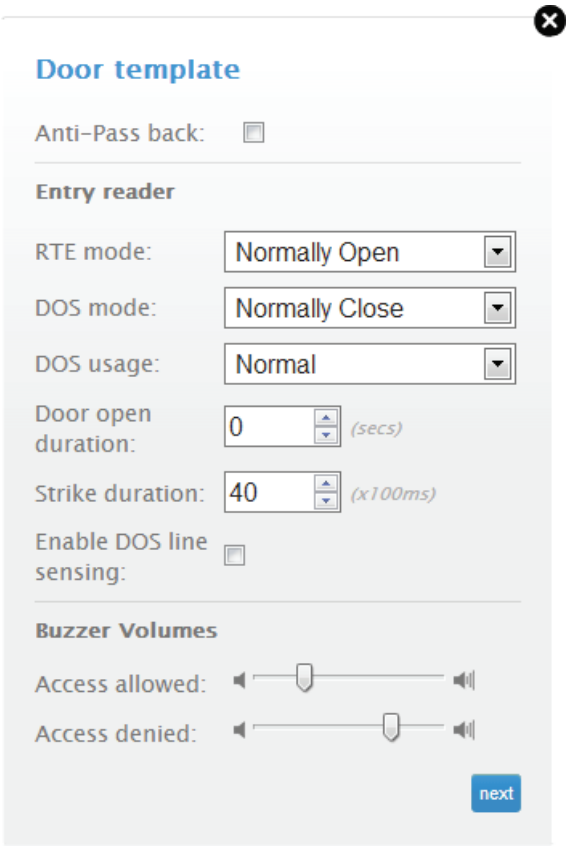

Figure 4 – Door Template

Add a Door

The Access Portal LITE System supports a maximum of **8** Doors and **1** Anti-passback (APB) Zone. Each Door has a Door Mode Pattern, which is made up of a maximum of four time periods per any day. Patterns may NOT overlap each other. The user interface allows for configuration of each Door individually.

General Settings

1. From the Main Ribbon select **Settings>Setup>Doors**.

Figure 5 – Doors Screen

2. Click on **add** to open the **New Door** dialog.

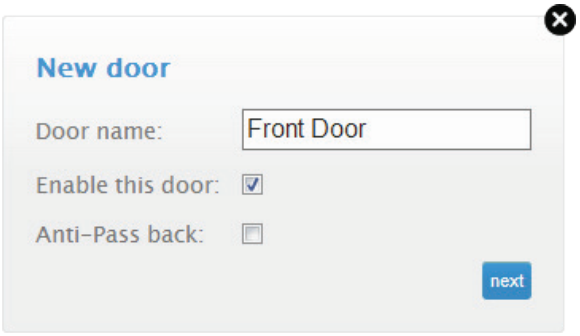

Figure 6 – New Door Dialog

3. Assign a suitable name (maximum **32** characters) in the **Door Name** textbox.
4. If required, add the Door to the Anti-passback (APB) Zone, by selecting the **Anti-Pass back** checkbox.
5. If necessary, de-select the **Enable Door** checkbox.

6. Click the next button

You should have a "site map" of your installation, showing you where the various readers (identified by their fixed addresses) are installed in relation to the doors in your building. Use this information for allocating entry and exit readers to the correct doors, in the following way:

7. Select the **Entry Reader** using the drop-down list. Make your selection from the list of displayed list of Readers. This list will include ALL readers that were detected (during Auto ID, pg 3), and are not yet allocated to doors.

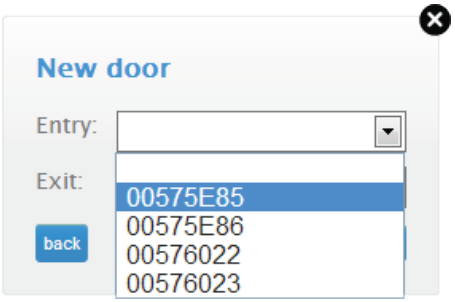

Figure 7 – Reader Entry drop-down slection

8. Do likewise for the **Exit Reader** for this door, using the **Exit** drop-down list

9. Click the next button.

The Door Mode Pattern Configuration screen will appear – see Figure 8 on the next page.

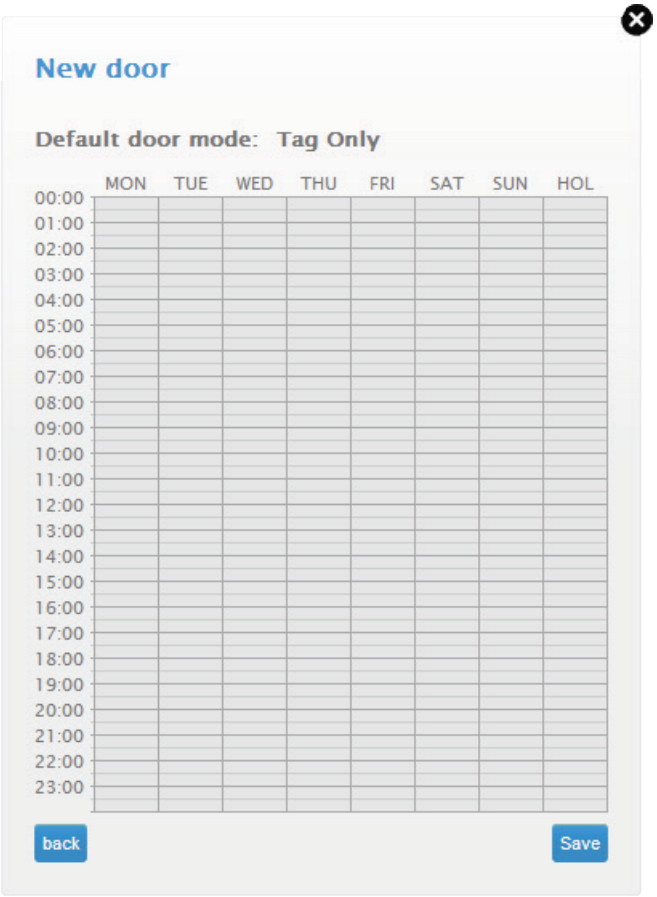

Figure 8 – Selecting the Default Door Mode

The default Door Mode is fixed on Tag only. This is the door mode that is assumed where nothing otherwise is indicated in the graphic area**.**

10. Clicking and dragging within the **Door Mode Pattern** configuration chart will mark out rectangular areas that determine the **Mode** of the **Door** at different times. The following rules apply:

    – There may only be four different areas per day.
    – Marked up areas cannot overlap.

11. Edit the rectangular patterns by clicking on them and then moving the outlines by dragging on the four round handles. Use the drop-down list to select what **Door Mode** (explained above) is in effect during the times covered by the rectangle.
12. A drop-down menu within the rectangular patterns will allow you to set the Door Mode during the enclosed periods.

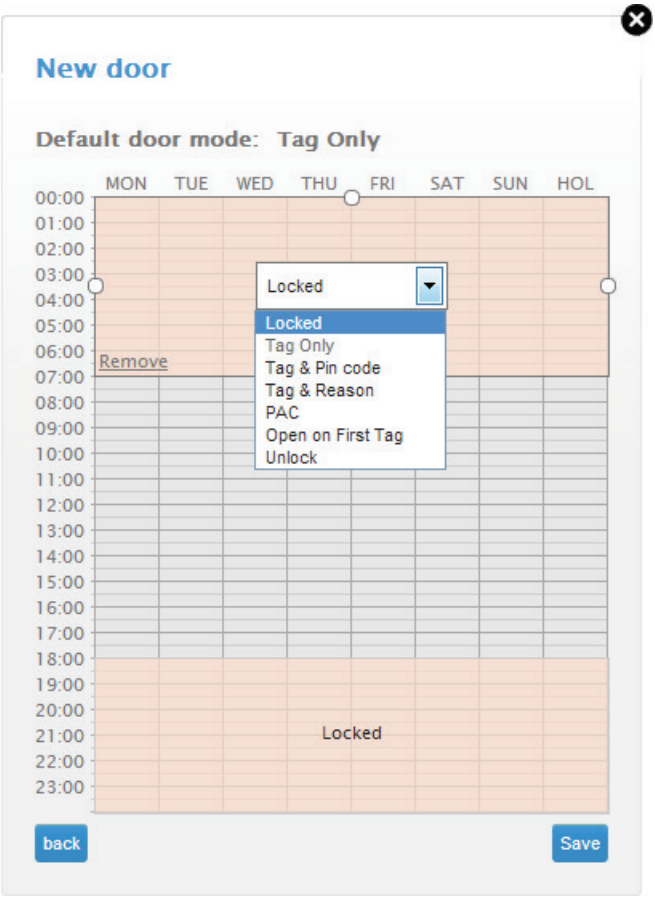

Figure 9 – Selecting the Door Mode for the time period

13. **Door Modes** explained:
    - **Locked**—the Door is locked and cannot be overridden with any Tag. In this Mode the Reader's LED flashes Red.
    - **Tag Only**—requires presentation of a Tag to open the Door. In this Mode the Reader's LED is steady Red.
    - **Tag + PIN-code**—requires presentation of a Tag followed by entry of a PIN-code to open the Door. PIN-codes range from **00000 to 65534**. After entering the PIN-code, complete the entry by pressing the **#** key). In this Mode the Reader's LED blinks Red then Green. Selecting this mode without connecting a keypad reader, applies **Tag** rules.
    - **Tag + Reason**—requires presentation of a Tag followed by entry of a Reason Code to open the Door. In this Mode, the Reader's Red LED follows a continuous cycle of brief OFF blinks (Long ON, Short off…). Selecting this mode without connecting a keypad reader, applies **Tag** rules.
    - **Open on First Tag**—the Door is opened when the first valid Tag Holder presents their Tag and remains open. In this Mode the Reader's LED flashes Green.
    - **Unlock**—The door is unlocked. A Tag is not required to open the Door. In this Mode the Reader's LED is steady Green.
14.

In the example in Figure 9*, access through this door will be via only tag, and only between 07:00 and 18:00 every day.*

15. Click Save when done.

    (The new door will now be displayed on the **Doors** screen)

Entry Reader Settings

1. If not already on the **Doors Screen,** navigate there by going: Settings>Setup>Doors

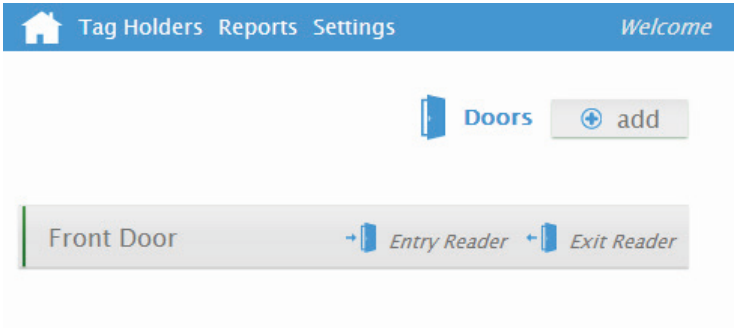

Figure 10 – Door Screen after adding one door

2. Click on ***Entry Reader,*** *the Entry Reader Settings dialogue will appear as shown in* Figure 11 *on the next page.*

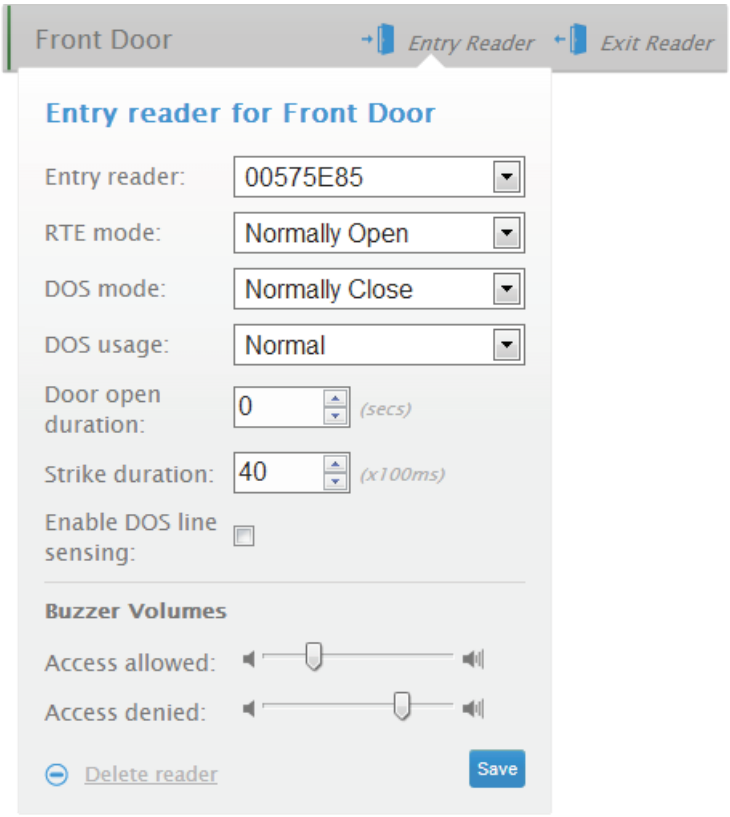

Figure 11 – Editing the Entry Reader settings

3. Using the **RTE Mode** drop-down list (Figure 11, page 11), make your selection:
   - **Normally Closed**—sensor remains closed until opened by an operator.
   - **Normally Open**—sensor remains open until closed by an operator.

4. Edit the **DOS Mode** using the drop-down list, your options include:
   - **Normally Closed**—sensor remains closed until the door is opened.
   - **Normally Open**—sensor remains open until the door is opened.

*Do not configure the **DOS Usage** while the System is in **Emergency** mode. To deactivate Emergency mode, click on*  *Revert to normal State, just under the Main Ribbon*

5. Edit the **DOS Usage** using the drop-down list, your options include:
   - **DOS** (Normal)—alarm sounds if the Door remains open too long or if the Door is forced. Use this feature for monitoring real Door open states.
   - **Inhibit Reader**—deactivates the Reader as long as the Door is open. Used to disable the reader while the Door remains open.
   - **Terminate Strike**—deactivates the relay if Door is opened and closed or forced. Use this feature where the lock must re-engage once the Door is closed.
   - **Emergency Open Mode**—opens all Doors immediately.
   - **Lock down mode** – Sets all mag locks and strike locks to the locked state.

6. Set the Door Open Duration—The period of time (in seconds) the door stays open before an alarm triggers. By default, the Open Duration is set to 0, disabling the Door Open Sensor (DOS).
7. Set the Strike Duration—The period of time (in hundreds of milliseconds) for which the Door remains unlocked. The default Strike Duration is 40 x 100 ms = 4 seconds. The maximum Strike Duration is 999 999 ms (27 Hours, 46 minutes and 40 seconds)
8. Set the **DOS Line Sensing**—By default end-of-line sensing is disabled, to enable end-of-line sensing on the Door Open Sensor (DOS), select the checkbox.

9. Set the **Buzzer Volume (Allowed)** using the drop-down list, select from the options (Off, Soft, Medium and Loud) given.

Standard Wiegand Readers only have two Buzzer volumes: Off and Loud.

10. Set the **Buzzer Volume (Denied)** using the drop-down list, select from the options (Off, Soft, Medium and Loud) given.
11. You can remove this reader from the system by clicking on **Delete Reader** at the bottom of the Reader Setting Screen
12. Click the Save button when done.

Exit Reader Settings

1. Click on ***Exit Reader*** and then follow the same procedure as described for the Entry Reader, beginning on page 11.

Delete a Door

1. From the Doors Screen, select the Door you wish to delete.
2. Click on **Delete Door** (bottom left of the opened Door Setting Screen)
3. You will be asked if you are sure, click on Yes, and the door (together with its Entry and Exit Reader details) will be deleted.

Access Group Setup

The Access Portal LITE System allows you to create a **maximum of 8 Access Groups**.

*The **Default Access Group** allows ALL Tagholders access to ALL Doors at ALL times. Therefore, create Access Groups to restrict or allow access as required. (Access groups are assigned to **Tags** – see page 23 for how to set **Tag Information.***

Add an Access Group

1. From the Main Ribbon select **Settings**>**Setup**>**Access Groups**.

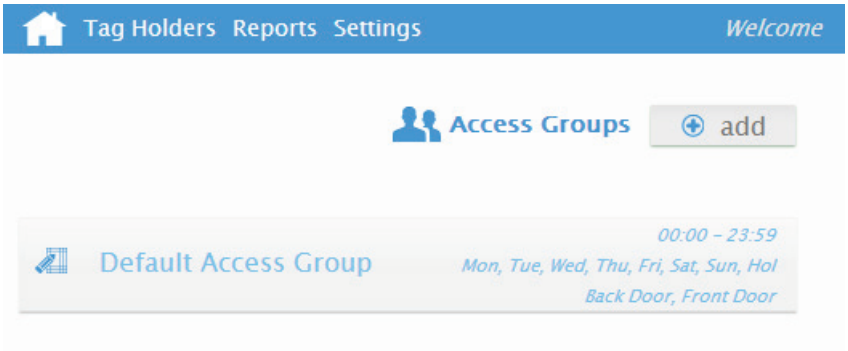

Figure 12 – Access Groups Screen before adding a new Access Group

2. Click on **add**.
3. Enter a suitable name in the **Group Name** textbox.
4. Set the **Start** and **Stop Time**.
5. Make your selection from the list of available **Days**.
6. Make your selection from the displayed **Doors**.

Tip – The next page shows sample input

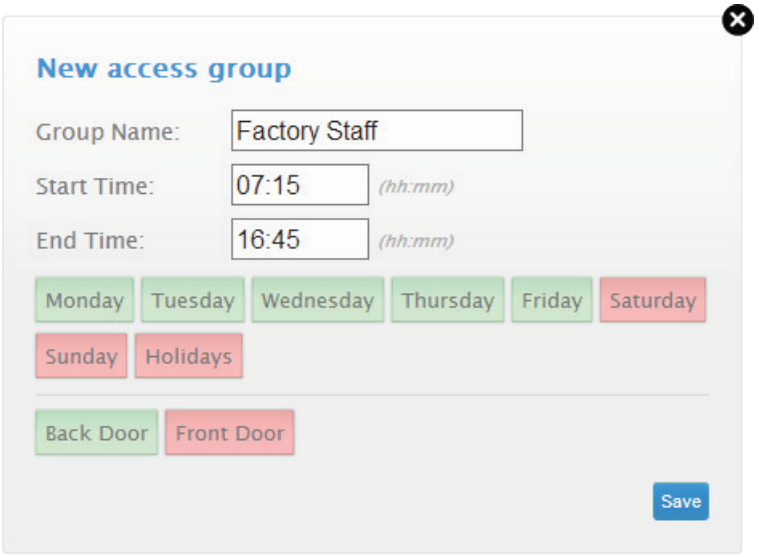

Figure 13 – New Access group being entered

1. Click the Save button when done.

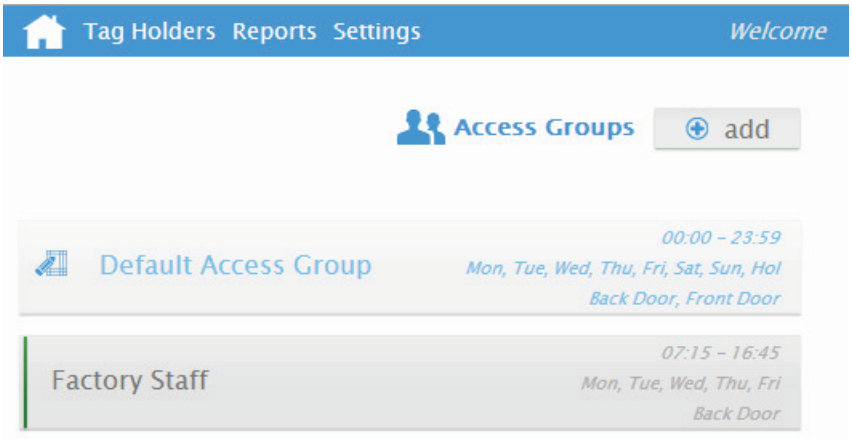

Figure 14 – Access Groups Screen with the new entry "Factory Staff" listed

Delete an Access Group

1. From the Main Ribbon select **Settings**>**Setup**>**Access Groups**.
1. Select the **Group Name** for deletion.
2. Click on **Delete access group**.
3. You will be asked if you are sure that you would like to do this.
4. Click the Yes button.

Edit an Access Group

1. From the Main Ribbon select **Settings**>**Setup**>**Access Groups**.
2. Select the Access Group for editing.
3. Edit the settings in the same manner as for adding a new group (page 14).

Holidays Setup

The Access Portal LITE System allows you to configure a **maximum of 18 Holidays**.

Add a Holiday

1. From the Main Ribbon select **Setting**s>**Setup**>**Holidays**.
2. Click the add button.
3. Enter a suitable Holiday name in the **Name** textbox.
4. Set the **Start Date** by clicking the button.
5. Set the **End Date** by clicking the button.
6. Click the Save button.

Edit a Holiday

1. From the Main Ribbon select **Setting**s>**Setup**>**Holidays**.
2. Select the **Holiday Name** tag for editing.
3. Edit the settings in the same manner as they were entered (refer to page 17

Delete a Holiday

1. From the Main Ribbon select **Setting**s>**Setup**>**Holidays**.
2. Select the **Holiday Name** for deletion.
3. Click on Delete holiday
4. When prompted with a “Delete item?” dialogue, click on the Yes button to go ahead with the deletion.

Reason Code Setup

The Access Portal LITE System allows for storage of **up to 10 Reason Codes**. You may assign any number between **1** and **99** as a Reason Code.

1. From the Main Ribbon select **Setting**s>**Setup**> **Reasons**.

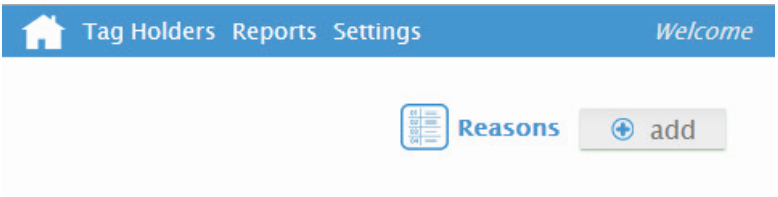

Figure 15 – Reasons screen

2. To add a new **Reason,** click on the add button.
3. The **Reason** entry dialogue will appear (next page).

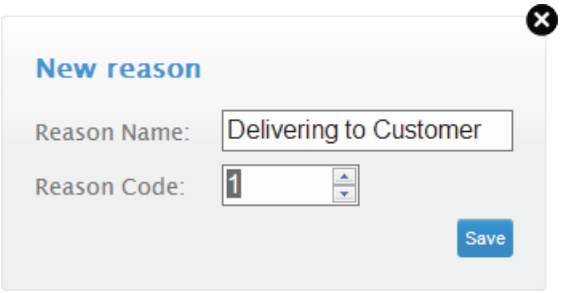

Figure 16 – Reason entry dialogue

4. Type a **Reason Name** into the **Reason Name** textbox.
5. Enter a number in the **Reason Code** box.
6. Click the Save button.
7. The **Reason Number** and **Reason Name** now appear as a tag on the Reasons screen .

2 Tagholder Configuration

Setting up a Template before batch enrolling Tagholders, streamlines the Tagholder addition process.

Because of the way standard Wiegand Readers handle HID Tag codes, Access Portal LITE Sites using standard Wiegand Readers connected to a Wiegand Reader Module can only support one of two options:

- *HID Tags only (set the DIP-switch to Wiegand Open Format and the Wiegand Reader to HID Raw Mode) or*
- *other 125 kHz Tag types (such as Slim Tags, Omega Tags, Philips HITAG™ 1 and Philips HITAG™ 2 depending on the Reader). Set the DIP-switch to Wiegand 26-bit/44-bit.*

For more information refer to the Wiegand Reader Module Installation Manual. If you need a combination of HID Tags and other Tag types, make use of the Impro Multi-discipline Readers.

The Access Portal LITE System supports a maximum of **1 000** Tagholders, each with a maximum of **3** Tags.

Tagholder Template Setup

Note – The Tag holder template determines the default settings for new Tag holders that are added. This feature can save you from having to manually enter the same information repeatedly for similar Tag Holders.

1. From the Main Ribbon select **Tag holders**.
2. Click the Tag Holder Template button.

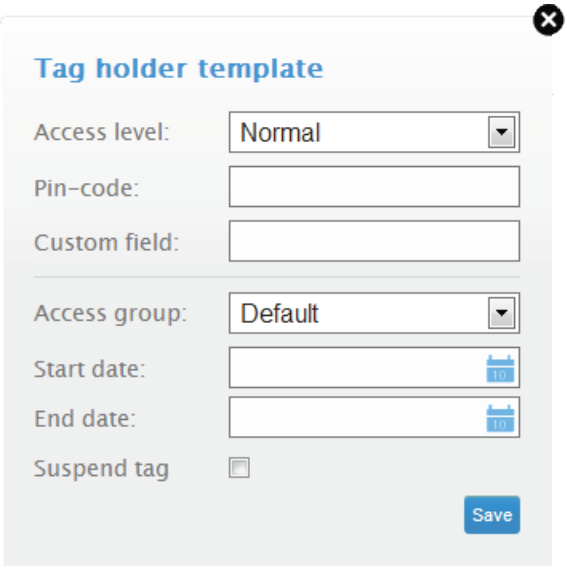

Figure 17 – Tag Template Dialog

3. From the **Access Level** drop-down list, select from the following:
   - **Visitor**—restricted access, valid for day of issue only.
   - **Normal**—employee Tagholder, access restricted by Door Mode.
   - **Administrator**—overrides Anti-passback (APB) Rules.
4. Enter that Tag Holder's **PIN Code**, if applicable

5. Populate the **Custom Field** if necessary
6. Select an **Access Group**, using the drop-down list.
7. Complete the **Start** and **End Date** requirements using the associated buttons.
8. Click the Save button when done.

Add Tagholder

Tag Holders screen

1. From the Main Ribbon, select **Tag Holders**.

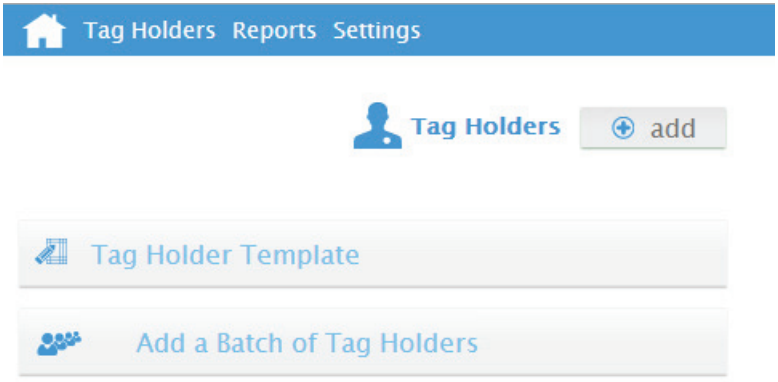

Figure 18 – Tagholder Screen

2. To add an individual Tag Holder Click the add button.

A New Tag Holder dialog will appear as per Figure 19 on page 22.

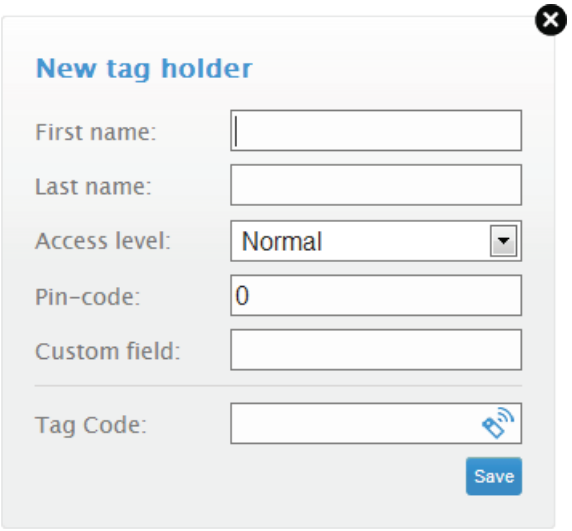

Figure 19 – New Tagholder Dialog

3. Complete the **First** and **Last Name** textboxes.
4. Using the **Access Level** drop-down list, select from the following:
   - **Visitor**—restricted access, valid for day of issue only.
   - **Normal**—employee Tagholder, access restricted by Door Mode.
   - **Administrator**—overrides Anti-passback (APB) rules.
5. If necessary, complete the **PIN-code** textbox.
6. Edit the **Custom Field** textbox.
7. Enter the **Tag Code**, if known.
8. Click the Save button.

Tip: if you are adding more than one Tag Holder – or a batch of similar Tag Holders, consider first setting the Tag Holder Template to save on typing (see page 20).

Tag Information

9. After saving the first **Tag Holder**, you will see that Tag Holder displayed on the **Tag Holders** screen.

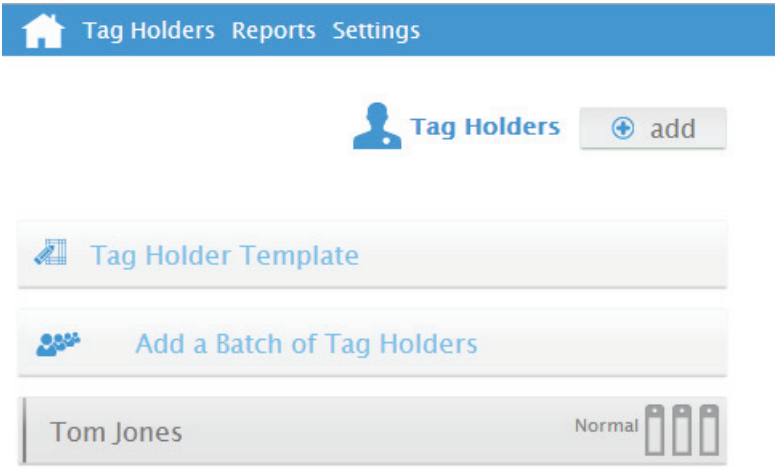

Figure 20 – First new Tag Holder displayed on Tag Holder screen

10. You will see three tag icons on the right of each of the **Tag Holders** listed.

Note – The colour of the tag icons indicates the status of the tags stored under these icons:

A GREY tag means there is no tag information stored

A BLACK tag will become active in the FUTURE

A GREEN tag is ACTIVE

A RED tag is SUSPENDED (manually disabled)

A PINK tag has EXPIRED

11. Click on the Tag Icon whose data you wish to edit.

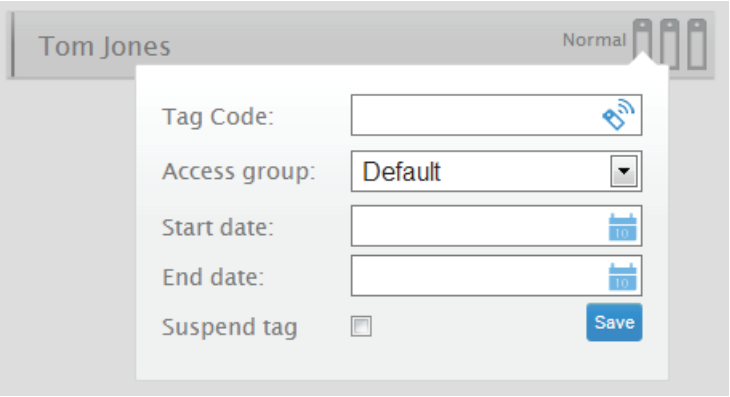

Figure 21 – Editing a Tag Holder's Tag

12. The Tag Edit Dialog will pop up (Figure 20, on page 23)
13. To capture the Tag Code by scanning the Tag, click on the icon.
14. Choose the desired Entry or Exit Reader from the list that appears.

Note – Make sure that the Reader is set up for Tag Only Mode

15. While the Tag is is presented to the Reader, click on the Scan now button to scan the Tag. The scan is completed within 1.5 seconds, and displayed in the Tag Code entry box.

*Alternatively, enter a Personal Access Code (PAC) in the **Tag Code** textbox. Your Personal Access Code may range from between **1 to 999999999**.*

16. Complete the **Start** and **End Date** requirements using the associated buttons. (If left blank, the tag will not expire)
17. If necessary, select the **Suspend Tag** checkbox, which will render this tag unusable - until the **Suspend Tag** checkbox is unchecked.
18. Click the Save button.

Add a Batch of two or more Tag Holders

Tip: Set the Tag Holder Template (pg 20) first.

1. Click on Tag Holders on the Main Ribbon
2. Select **Add a Batch of Tag Holders**.

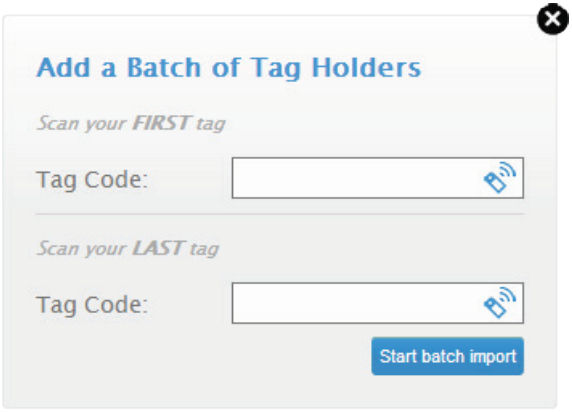

Figure 22 – Enter the first and last tag numbers

*A **Tag Code** is a minimum of 1 digit, and a maximum of 16 digits. The **First Tag Code** must be smaller in value than the **Last Tag Code**. The difference between the **First** and **Last Tag Code** values cannot be more than 1 000.*

3. Enter the first and last Tag Codes by either typing the Tag Codes into the two spaces available, **OR** by clicking on the Get Tag icons and then scanning the relevant tags at the desired scanner
4. Click on Start batch import.

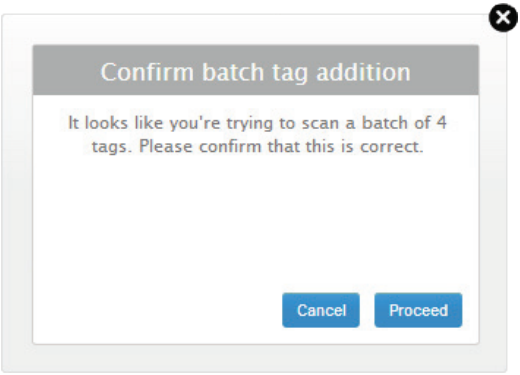

Figure 23 – Confirmation of the batch tag count.

1. Click on Proceed if the batch tag count is correct.

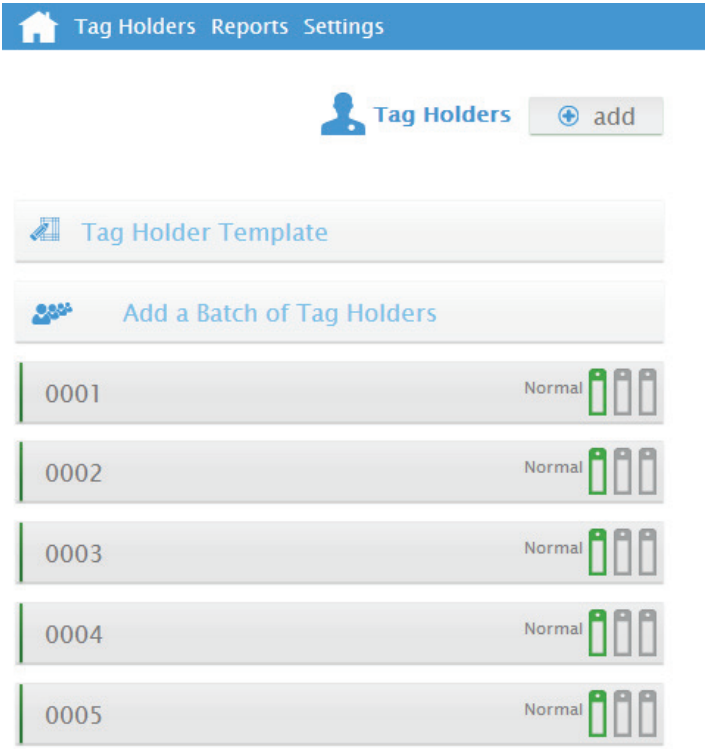

Figure 24 – The new Batch of Tag Holders appears on the Tag Holders Screen

The System generates a numerical sequence of new Tag Holders in accordance with the existing Tag Holders Template, each with the first Tag Icon shown as active (Figure 24).

Edit a Tagholder

1. From the Main Ribbon, select **Tag Holders**.
2. Select the **Tagholder** you wish to edit.
3. Follow the same procedure as Adding a Tag holder (page 21).

Delete a Tagholder

4. From the Main Ribbon select **Tag Holders**.
5. Select the **Tagholder** you wish to delete.
6. Click on Delete tag holder at the bottom of the Tag Holder Settings Dialogue.
7. At the confirmation message, click on Yes.

Edit or delete individual Tags

Note – This does not alter or delete Tag Holders

1. From the Main Ribbon select **Tag Holders**.
2. Scroll to the Tag Holder of the Tag in question
3. Click the Tag Icon representing the tag that you wish to Edit or Delete
4. Edit the information for that Tag and click on the Save button when done
5. Alternatively, if you wish to delete the Tag, click on Delete tag at the bottom left of the tag data dialogue.
6. You will then be prompted “Are you sure…?”
7. Click on Yes to go ahead and delete the Tag Data.
8. When the Tag Data for a Tag is cleared, that Tag Icon becomes grey, indicating that it holds no data.

3 System Overides

Emergency Unlock

Note – In case of an emergency evacuation, or similar event, this will UNLOCK every door that is controlled by the system

1. **Click on Settings> Emergency Unlock**
2. The orange ***EMERGENCY OPEN*** Banner will be displayed just beneath the Main Ribbon.

Figure 25 – Emergency Open Banner below Main Ribbon

1. ALL Doors will unlock - and will remain unlocked until you click on Revert to normal State - at which point normal operation will immediately return.

Lock Down

Note – This locks all doors on the system, no tags or codes will be able to open any door

1. **Click on Settings> Lock Down**
2. The red ***LOCKDOWN*** Banner will be displayed just beneath the Main Ribbon.

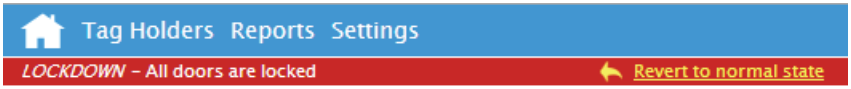

Figure 26 – Lock Down Banner below Main Ribbon

3. ALL Doors will lock - and will remain locked until you click on Revert to normal State - at which point normal operation will immediately return.

4 Reports

Report Generation

1. From the Main Ribbon select **Reports**

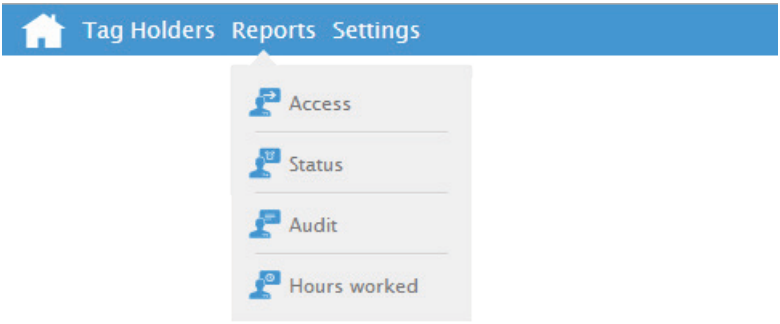

Figure 27 – Report options

2. Choose the category of report you require:

- ***Access*** *— this Report provides access data for the selected Tagholder over a specified date range.*
- ***Status*** *—this Report displays all the status transactions from Controllers and Terminals on a selected date.*
- ***Audit*** *—this Report provides a list of Tags added, edited or deleted over a specified date range.*
- ***Hours Worked****—this Report calculates hours worked from the IN and OUT Transactions of the Anti-passback (APB) Zone.*

3. Select the **Tagholder** using the drop-down list, when this is present.
4. Set the Report's **Start** and **End Date** using the buttons.
5. Click the Run report button to generate the report.

6. The report will be displayed on screen (Figure 28)

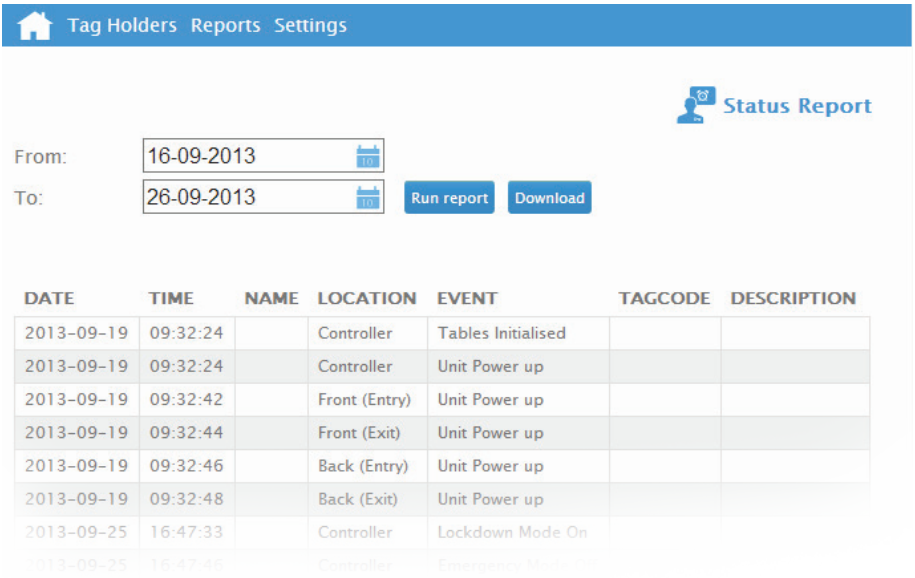

Figure 28 – Report displays onscreen

7. Click the Download button to save the report as a CSV (Comma Separated Value) file. This can be opened and edited in a spread sheet application, such as Microsoft's Excel:

	A	B	C	D	E	F	G
1	DATE	TIME	NAME	LOCATION	EVENT	TAGCODE	DESCRIPTION
2	2013/09/19	09:32:24		Controller	Tables Initialised		
3	2013/09/19	09:32:24		Controller	Unit Power up		
4	2013/09/19	09:32:42		Front (Entry)	Unit Power up		
5	2013/09/19	09:32:44		Front (Exit)	Unit Power up		
6	2013/09/19	09:32:46		Back (Entry)	Unit Power up		
7	2013/09/19	09:32:48		Back (Exit)	Unit Power up		

Figure 29 – Report as it appears in a spread sheet application

5 Advanced Setup

Controller Setup

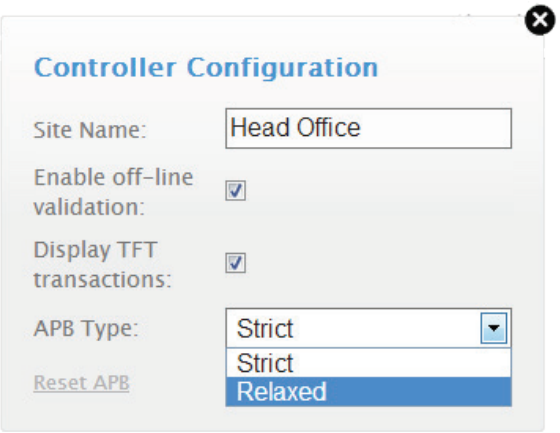

Figure 30 – Controller Configuration Dialog

1. From the Main Ribbon select **Settings**>**Controller**.
2. Complete the **Site Name** textbox.
3. The **Off-line Validation** checkbox is selected by default, allowing Terminals connected to the Controller to make certain access control decisions even when unable to communicate with the Controller. De-select the checkbox if necessary.

Note – Ignore "Display TFT Transactions" checkbox – this is reserved for use in a future release of AP Lite.

4. Using the **APB Type** drop-down list, select from the following:
   - **Strict**—enforced Anti-passback Zone rules for **in** and **out** directions. A Tagholder cannot enter or exit a Zone consecutively.
   - **Relaxed**—after entering a Zone, the Tagholder must exit the Zone using their Tag *before* they can re-enter. However, Tagholders can use their Tags for multiple, consecutive exits in this Mode.
5. Click on **Reset APB** to reset the Anti-Pass-Back status of all tags.

Note – Resetting the APB will cause the system to "forget" whether Tag Holders are inside or outside of APB zones, which means that they will all be able to enter or exit, whether they were already in or out, or not.

6. Click the Save button when done.

Ethernet

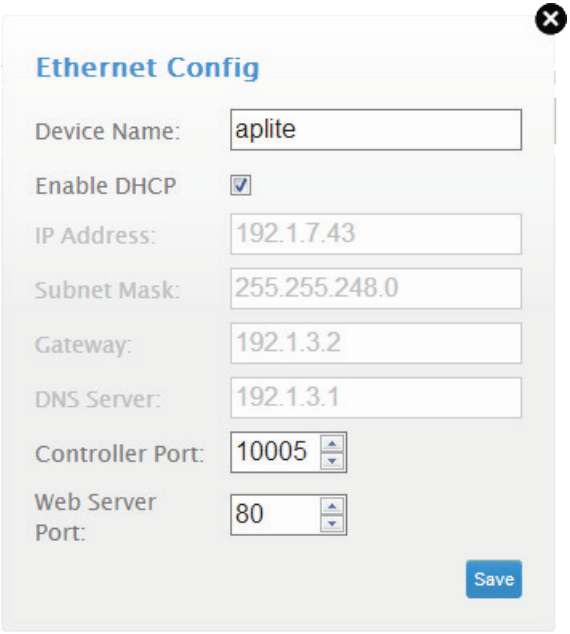

Figure 31 – Ethernet Settings Dialog

1. From the Main Ribbon select **Settings**>**Ethernet**.
2. Edit the **Device Name** textbox. This is the URL used to connect to the Web Interface.
3. The **Enable DHCP** checkbox is selected by default, de-select the checkbox to set a static IP Address for the Controller.

*The default Web Browser Port Number is **80** and the default Application Port Number is **10005**. Only change these Port Numbers, if they clash with other devices or services on your network.*

4. Complete the **Web Browser Port** textbox.
5. Complete the **Application Port** textbox.
6. Click the Save button.

UDP Output

The UDP Output feature sends events generated in the Access Portal LITE System to a third-party application.

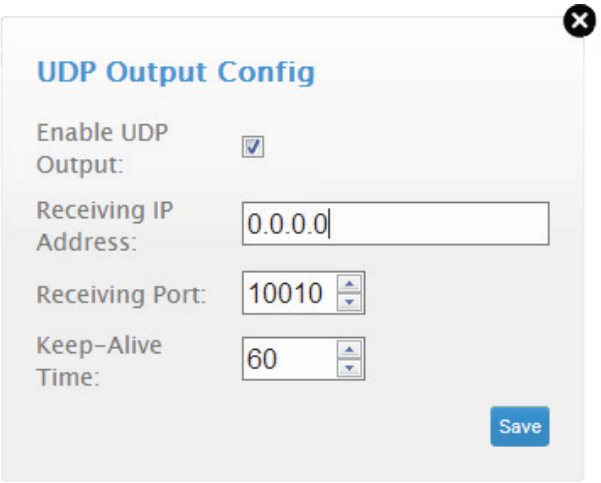

Figure 32 – UDP Output Config Dialog

Configure this feature as follows:

1. From the Main Ribbon, select **Settings**>**UDP Output**.
2. Select the **Enable Output** checkbox.
3. Complete the **Receiving IP Address** textbox.
4. Complete the **Receiving Port Number** textbox.

*The default Receiving Port Number is **10010**. Only change this Port Number if it clashes with other devices or services on your network.*

5. Set the time (in seconds) between notifications using the **Keep Alive Time** textbox. The default Keep Alive Time is **60 seconds**.
6. Click the Save button.

Replacing the Cluster Controller Module

In the event that the Cluster Controller Module is replaced with a new unit, all settings are lost. All Tag Holder data, etc, will have to be re-entered/enrolled again.

In the event that the replacement Cluster Controller Module is not new, it is important to reset it to factory default condition (Page 36) before setting it up, this will ensure that the settings are correct for your installation.

Security

Set or change the administrator password as follows:

1. From the Main Ribbon select **Settings**>**Security**.
1. Complete the **Current Password** textbox.
2. Complete the **New Password** textbox.
3. Complete the **Confirm Password** textbox.
4. Click the Save button.

6 Troubleshooting

Restoring Factory Defaults

Restoring factory defaults will reset the Cluster Controller Module's device name to aplite.

1. Set the DIP-switch Switch 1 to the **ON** position.

Refer to your Cluster Controller Module's Hardware Installation Manual for location of the DIP-switch.

2. Reset the Controller by removing and then reapplying the power source.
3. With the Controller running, set the DIP-switch Switch 1 back to the **OFF** position.
4. The Cluster Controller Module will take approximately a minute to complete the restarting and defaulting process.

Connecting the Cluster Controller Module directly to a PC

When using more than one Cluster Controller Module, ensure each Controller has a unique Device Name (see page 33).

Setting a static IP Address for your Controller may result in difficulties when connecting direct to a PC. If the **Enable DHCP** checkbox has previously been de-selected in the Web Interface, ensure that you reselect the **Enable DHCP** checkbox before continuing (see page 33 for more information).

When connecting the Controller direct to a PC or Switch, if DHCP is enabled (the default) the following applies:

If a server is found. The unit is given an IP by the server.

If no server is found, the unit uses the last remembered IP. This is either the default 192.168.100.1 or the value previously assigned by a DHCP server. Defaulting the unit will clear any cached IP previously assigned by a DHCP server.

If there is no DHCP server:

On the PC:

1. Select **Start>Control Panel**.
2. Click the **Network and Sharing Centre** icon.
3. Select **Local Area Connection**.
4. Click the **Properties** button.
5. Select the **Internet Protocol Version 4 (TCP/IPv4)** option.
6. Click the **Properties** button.
7. Set the **IP Address** to 192.168.100.X (X being any available number between 2 and 254. Ensure that your chosen number is unique between all Cluster Controller Modules and the PC.).
8. Set the **Subnet Mask** to 255.255.255.0.
9. Click the **OK** button.

Extra Information

Further information is available at the following resources:

- **Impro Cluster Controller Module Product Specification Catalogue** (HCM370-0-0-GB-XX).
- **Impro Cluster Controller Module Installation Manual** (HCM320-0-0-GB-XX).

*Download the Impro Access Portal LITE Firmware Upgrade Utility from the following URL: **www.impro.net**.*

The referenced documents are available for download at www.impro.net. Alternatively, contact your Impro dealer for a copy.

This manual is applicable to: Access Portal LITE Version 4.35, Website Version 1.0.938			
HCM321-0-0-GB-00	Issue 01	October 2013	APLITE\Software\English Manuals\LATEST ISSUE\APLite-swmb-en-01.docx